Secorvo Security News
Juli 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 1, 1. Jhrg. 2002
Stand 25. April 2003

Inhalt

Editorial: Eine Schneise in die Informationsflut

1 Security News

1.1 „Gummi Fingers“

1.2 Bugs in Open Source

1.3 Überwachung am Arbeitsplatz

1.4 Telekommunikations-überwachung

2 Secorvo News

2.1 IT-Outsourcing? Aber sicher!

2.2 IT Risk Management

2.3 Secorvo College

2.4 PKI-Symposium

3 Veranstaltungstermine

Impressum

Editorial: Eine Schneise in die Informationsflut

Der Berg an Nachrichten und Informationen wächst auch im Gebiet IT-Sicherheit täglich – und damit auch der Zeitbedarf, den Sie aufwenden müssen, um „auf dem Laufenden“ zu bleiben, wesentliche Entwicklungen nicht zu verpassen und die wichtigsten Informationen zu bewerten: Was bedeutet diese Erkenntnis oder jenes Ereignis für mich und meine IT-Systeme?

Mit den in dieser Ausgabe erstmals vorliegenden Secorvo Security News möchten wir Sie dabei unterstützen.

Auch auf uns prasseln täglich unzählige Informationen ein, die wir in unserem Expertenteam filtern, diskutieren, abwägen und bewerten. Daraus entstand die Idee, auch Sie davon profitieren zu lassen.

Die Secorvo Security News sollen

- Sie auf **wichtige aktuelle Ereignisse und Entwicklungen** in der IT-Sicherheit aufmerksam machen,
- Ihnen durch die **Angabe der wesentlichen Quellen** die Informationsrecherche erleichtern und
- Ihnen durch eine **unabhängige Expertenmeinung** bei der Bewertung dieser Nachrichten helfen.

Zugleich möchten wir die Informationsflut nicht unnötig vermehren. Daher erscheinen die Secorvo Security News nicht mehr als **12 mal im Jahr** – genug, um der Schnelllebigkeit heutiger Entwicklungen ein besonnenes Urteil entgegen zu stellen.

Außerdem beschränken wir uns auf Wesentliches: Sie erfahren nicht alles, aber das, was Sie unserer Ansicht nach wissen sollten – weniger erscheint uns hier mehr.

Schließlich schicken wir Ihnen nicht das gesamte Dokument, sondern nur das Inhaltsverzeichnis der aktuellen Ausgabe und den Web-Link: Sie entscheiden, ob Sie das etwa 100 kB große PDF-Dokument laden möchten.

1 Security News

1.1 „Gummi Fingers“

Mit seinem Beitrag auf der „Rump Session“ der diesjährigen Kryptokonferenz „Eurocrypt“ ließ der japanische Forscher T. Matsumoto eine „Bombe“ hochgehen: Er stellte die Ergebnisse von Experimenten seiner Forschungsgruppe vor, die sich vorgenommen hatte, mit „Hausmitteln“ wie Silikon und Gelatine und einfachsten Hilfsmitteln Fingerprint-Scanner zu überlisten.

Die Ergebnisse sind ernüchternd: Alle 11 getesteten kapazitiven und optischen Fingerprint-Systeme unterschiedlicher Hersteller ließen sich in mindestens 67% der Testfälle von den falschen Fingern täuschen. Ein herber Schlag für den Hoffnungsträger der Biometrie.

Original: http://cryptome.org/gummy.htm

Präsentation: http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf

1.2 Bugs in Open Source

Gerne werden in der Diskussion um Open Source Software Sicherheitsargumente bemüht: Ist der Quellcode offengelegt, so die Open-Source-Verfechter, könne er von einer weit größeren Zahl von Experten überprüft werden als bei herkömmlicher kommerzieller Software.

Das Argument verkennt, dass im wirklichen Leben häufig Welten zwischen „Können“ und „Tun“ liegen. Das hat nicht zuletzt der schwere Spezifikationsfehler im OpenPGP-Standard bewiesen, der von Klíma und Rosa im April 2001 entdeckt wurde – 2,5 Jahre nach Veröffentlichung des Standards als RFC.

Die Security Alerts des Juni 2002 haben dem Glauben an fehlerarme Open Source Software weiter zugesetzt: In drei wichtigen Softwarepaketen wurden schwer wiegende Bugs entdeckt – die dort jahrelang unbemerkt schlummerten.

1.2.1 Löcher in Apache

Oft als die „sichere Alternative“ gelobt und nicht zuletzt deswegen mit einem erheblichen Marktanteil unter installierten HTTP-Servern, traf es Apache im Juni gleich zweimal hart: Am 17.06.2002 wurde ein Heap Buffer Overflow gemeldet, der einen DoS-Angriff und das Ausführen beliebigen Codes auf dem Server erlaubt. Betroffen sind die Versionen 1.2 bis 2.0 sowie OpenBSD und eine große Zahl verbreiteter Linux-Derivate von Caldera bis SuSE.

http://www.iss.net/security_center/static/9249.php

Nur acht Tage später wurde ein zweiter Buffer Overflow gemeldet, über den ein Angreifer beliebige Kommandos auf dem System ausführen kann. Diesmal sind alle Versionen des Apache HTTP Server, alle Linux- und Unix-Versionen, OpenBSD 3.1 sowie alle Versionen des mod_ssl Moduls bis Version 2.8.9 betroffen.

http://www.iss.net/security_center/static/9415.php

1.2.2 Fehler in OpenSSH

Am 26.06.2002 wurde von ISS und CERT ein schwerer Fehler in OpenSSH publiziert: Mit geeignet formatierten Response-Paketen kann ein Angreifer einen Integer Überlauf im Code der Challenge Response Authentication (SKEY oder BSD_AUTH) verursachen und beliebigen Code mit den Privilegien des sshd Prozesses ausführen – wenn Privilege Separation nicht aktiviert ist, entspricht das der Root-Berechtigung.

Betroffen sind alle OpenSSH-Versionen von 2.9.9 bis einschließlich 3.3.

http://www.kb.cert.org/vuls/id/369347

Die fehlerfreie Version 3.4 findet sich unter

ftp.openbsd.org:/pub/OpenBSD/OpenSSH

1.2.3 BIND Bugs

Das CERT-Advisory vom 05.06.2002 warnt vor einem Fehler in der aktuellen Version 9

des Berkeley Internet Name Daemon (BIND). Angreifer können den Fehler nutzen, um den Dienst zum Absturz zu bringen. Ausnahmsweise sind Sie diesmal mit älteren Versionen besser bedient.

http://www.kb.cert.org/vuls/id/739123

Alle BIND-Versionen sowie OpenBSD 2.9 bis 3.1 ermöglichen einem Angreifer, einen Buffer Overflow in der DNS Resolver Library zu verursachen, der die Ausführung beliebigen Codes erlaubt (27.06.2002):

http://www.iss.net/security_center/static/9432.php

1.3 Überwachung am Arbeitsplatz

Die Datenschutz-Arbeitsgruppe der EU-Kommission („Art. 29 Gruppe“) hat am 29.05.2002 ein Arbeitspapier zur "Überwachung der elektronischen Kommunikation von Beschäftigten" veröffentlicht. Dort werden die (EU-) rechtlichen Grenzen der Kommunikationsüberwachung am Arbeitsplatz zusammengefasst und eine Unterscheidung von privat nutzbarer und geschäftlicher E-Mail-Adresse empfohlen:

http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp55_en.pdf

1.4 Telekommunikations-überwachung

Telekommunikationsüberwachung hat seit dem 11.09.2001 Konjunktur. Fast monatlich erweitern neue Bestimmungen die Eingriffsbefugnisse des Staates. Lesenswert dazu der Bundesratsantrag des Landes Thüringen vom 12.06.2002:

http://www.dud.de/dud/documents/brdrs513-02-020612.pdf

Beunruhigend auch die Tischvorlage zum Europol Expert Meeting on Cyber Crime zwischen Law Enforcement Experten vom 11.04.2002, die nun bekannt wurde:

http://www.dud.de/dud/documents/europol-expmeeting-020411.pdf

Auch die deutschen Behörden waren nicht untätig. Auf der Grundlage des § 11 TKÜV wurde von der Regulierungsbehörde für Telekommunikation und Post (RegTP) am 07.05.2002 eine ETSI-konforme Richtlinie (Version 3.1) der Anforderungen an technische Einrichtungen zur Überwachung der Telekommunikation veröffentlicht (pdf, 1,58 MB).

http://www.dud.de/dud/documents/trtkue31.pdf

Liste aller wichtigen Abhörbestimmungen:

http://www.datenschutz-und-datensicherheit.de/dudserver/abhoeren.htm

2 Secorvo News

2.1 IT-Outsourcing? Aber sicher!

Spätestens seit der spektakulären Ankündigung der Deutschen Bank AG, über ein Outsourcing ihrer gesamten IT-Infrastruktur nach zu denken, steht das Thema „IT-Outsourcing“ – gewollt oder ungewollt – oben auf der Tagesordnung vieler CIOs und IT-Verantwortlicher.

Welche Argumente auch immer für oder gegen ein IT-Outsourcing sprechen mögen: Ohne Zweifel kommt der IT-Sicherheit bei Planung und Umsetzung eine zentrale Rolle zu.

Welche Fragen sich dabei stellen und von Ihnen gelöst werden sollten, skizzieren Ingmar Camphausen, Dr. Volker Hammer, Stefan Kelm, Dr. Dörte Neundorf und Dr. Holger Petersen im neuen, noch „druckfrischen“ **Secorvo White Paper „IT-Outsourcing? Aber sicher!“**.

Nicht das „ob“ oder „ob nicht“ ist Gegenstand dieses vierten Secorvo White Papers: In Gestalt einer Checkliste will es Ihnen Hilfestellung bei der Bewältigung sein.

http://www.secorvo.de/whitepapers

2.2 IT Risk Management

KontraG und Basel II haben mit der Forderung einer unternehmensweiten Risikovorsorge auch IT Risiken in das Blickfeld des Managements gerückt. Mit den brutalen Anschlägen des 11. September 2001 haben diese Risiken eine neue Dimension gewonnen; „Best Practices" erfreuen sich seither großer Nachfrage.

Zusammen mit der Computas GmbH, mit der uns viele Jahre enger Zusammenarbeit verbinden und die als Veranstalter besonders hochwertiger Fachkonferenzen bekannt ist, haben wir die Konferenz „**IT Risk Management 2002**" (**23.-24.09.2002**) inhaltlich konzipiert. „Best Practices" wurde dabei breiter Raum gewährt.

http://www.computas.de/itrisk2002-fly.html

2.3 Secorvo College

Im Oktober 2002 beginnt die „Herbst-Saison" von Secorvo College.

http://www.secorvo.de/college

Erstmalig bieten wir am **10.10.2002** ein PKI-Vertiefungsseminar „**PKI für Fortgeschrittene**" an.

2.4 PKI-Symposium

In den beiden vergangenen Jahren war es bis auf den letzten Platz ausgebucht – das von Secorvo im Jahr 2000 erstmals durchgeführte „PKI-Symposium" für den Erfahrungsaustausch und die Diskussion aktueller Fragestellungen im Bereich PKI.

Der Hype ist vorüber: Welche Anwendungen bergen nun den erwarteten Return of Invest? Was lässt sich aus den Erfahrungen der Innovationsträger lernen? Was sind die Herausforderungen von morgen?

Auf der Agenda des diesjährigen **PKI-Symposiums 2002** (**08.-09.10.2002**) werden wieder spannende Fragestellungen und aktuelle Praxisberichte rund um das Thema PKI stehen (in Kürze online).

http://www.pki-symposium.de

3 Veranstaltungstermine

August 2002	
24.08.	Kieler Datenschutz Sommerakademie 2002 (ULD SH)
September 2002	
23.-24.09.	IT Risk Management 2002 (Computas)
24.-25.09.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
Oktober 2002	
07.-08.10.	Public Key Infrastrukturen (Secorvo College)
08.-09.10.	PKI-Symposium 2002 (Secorvo)
10.10.	PKI für Fortgeschrittene (Secorvo College)

Web-Tipp: Veranstaltungsübersicht zu Datenschutz und Datensicherheit:

http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Ein Archiv aller Ausgaben finden Sie unter

http://www.secorvo.de/security-news

Eine automatische Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News") an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feed-Back an
redaktion-security-news@secorvo.de

Secorvo Security News
August 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 2, 1. Jhrg. 2002
Stand 09. August 2002

http://www.secorvo.de/security-news

Inhalt

Editorial: Lang ist lang genug

1 Security News

1.1 SPHINX-Einsatzempfehlungen des BSI

1.2 ISIS-MTT Version 1.0.2

1.3 Bugs in OpenSSL, Trojaner in OpenSSH

1.4 Win2000 Security Patch

1.5 AES im SSL-Standard

1.6 PKI-Umfrage

1.7 IT-Sicherheitskongress

1.8 „Liberty Alliance“ strikes back

2 Secorvo News

2.1 ISIS-MTT-Testbed

2.2 IT-Grundschutz-Audit

2.3 Anwendungsintegration statt „One Size Fits All“

2.4 „PKI-Woche 2002“

3 Veranstaltungshinweise

Impressum

Editorial: Lang ist lang genug

Seit 25 Jahren tobt die Diskussion über angemessene Mindestschlüssellängen für kryptografische Verfahren. Sie begann mit dem Data Encryption Standard (DES): Erst nachdem die National Security Agency (NSA) die Schlüssellänge des ursprünglichen IBM-Entwurfs von 128 auf 56 bit verkürzt hatte, wurde der DES 1977 zum amerikanischen NBS-Standard. Im selben Jahr skizzierten die Kryptologen Diffie und Hellman die Konstruktion eines Chips, der in etwa 12 Stunden einen DES-Schlüssel finden sollte.

Tatsächlich wurde erst 22 Jahre später eine funktionierende DES-Entschlüsselungsmaschine konstruiert: Die von der Electronic Frontier Foundation (EFF) finanzierte Entwicklung benötigte mit 1.800 parallelen Spezialchips ("Deep Crack") immer noch knapp 56 Stunden, um einen DES-Schlüssel heraus zu finden.

Das Beispiel zeigt, dass aus theoretischen Betrachtungen abgeleitete Befürchtungen und reale Möglichkeiten weit auseinander klaffen können. Das gilt gelegentlich auch für Empfehlungen einer Mindestlänge für kryptografische Schlüssel. Insbesondere bei asymmetrischen Kryptoverfahren ist für die Bestimmung der Mindestschlüssellänge nicht nur die zukünftige Entwicklung der Rechenleistung zu prognostizieren, sondern es müssen auch mögliche neue mathematische Erkenntnisse berücksichtigt werden. Groß ist die Versuchung, auf „Nummer Sicher“ zu gehen, wie im Entwurf der Algorithmenempfehlung 2002 des BSI zum Signaturgesetz, deren Endfassung von der RegTP für Herbst 2002 angekündigt wurde:

http://www.bsi.bund.de/esig/basics/techbas/krypto/bund02v5.pdf (43 kB)

In einer Stellungnahme hat Secorvo die Entwicklung der Faktorisierungserfolge der vergangenen 25 Jahre ausgewertet – und hält deutlich kürzere RSA-Schlüssellängen für ausreichend sicher:

http://www.secorvo.de/whitepaper

1 Security News

1.1 SPHINX-Einsatzempfehlungen des BSI

Das BSI hat jüngst die Ergebnisse der im ersten Quartal 2001 durchgeführten Interoperabilitätstests mit einer Empfehlung für Sphinx-konforme E-Mail-Verschlüsselungslösungen publiziert. Darin erhielten nur drei Produkte (zwei Plugins für Outlook 98 und eine Lösung für Groupwise 5.5) eine uneingeschränkte Empfehlung:

http://www.bsi.de/aufgaben/projekte/sphinx/interop/empf102.htm

1.2 ISIS-MTT Version 1.0.2

Mit Unterstützung des BMWi wurde im vergangenen Jahr unter der Federführung von TeleTrusT Deutschland der Standard ISIS (Industrial Signature Interoperability Specification) der Trustcenter-Gruppe „T7“ mit dem von Secorvo für TeleTrusT entwickelten PKI- und E-Mail-Sicherheitsstandard MailTrusT zu einem gemeinsamen Standard ISIS-MTT verschmolzen. Die erste Version dieser auf X.509, PKIX und S/MIME aufbauenden Spezifikation wurde am 01.10.2001 veröffentlicht. Inzwischen ist ISIS-MTT obligatorischer Teil von SAGA (Standards und Architekturen für eGovernment Anwendungen). Auf der Grundlage zahlreicher Kommentare wurde am 19.07.2002 die Version 1.0.2 publiziert:

http://www.teletrust.de/teletrust.asp?id=61040

1.3 Bugs in OpenSSL, Trojaner in OpenSSH

Am 30.07.2002 informierten DFN- und RUS-CERT über fatale Fehler in OpenSSL: In allen Versionen bis einschließlich 0.9.6d kann auf unterschiedliche Weise ein Buffer Overflow verursacht werden, der die Ausführung beliebigen Codes auf dem SSL-Server im privilegierten (Root-)Mode ermöglicht. Gegenmaßnahme: Update auf OpenSSL Version 0.9.6e oder Lösungen der Hersteller abwarten:

http://cert.uni-stuttgart.de/ticker/article.php?prev=905

Ende Juli 2002 wurden die Domainen ftp.openbsd.org und ftp.openssh.org Hackeropfer: Am 01.08. wurden mehrere SSH-Versionen mit integriertem trojanischen Pferd entdeckt (und entfernt):

http://cert.uni-stuttgart.de/ticker/article.php?mid=911

1.4 Win2000 Security Patch

Am 01.08.2002 wurde von Microsoft das lange angekündigte Service Pack 3 (SP3) für Windows 2000 publiziert, das überwiegend Sicherheitslücken behebt:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/w2ksp3.asp

1.5 AES im SSL-Standard

Ende November 2001 wurde nach einem vierjährigen fachöffentlichen Bewertungsprozess der in Belgien entwickelte Verschlüsselungsalgorithmus Rijndael vom amerikanischen National Institute of Standards and Technology (NIST) als Advanced Encryption Standard (AES) ausgewählt und als FIPS 197 veröffentlicht:

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (243 kB)

Nun wird diesem Nachfolger des in die Jahre gekommenen DES der Weg in die Anwendungen geebnet: Mit RFC 3268 hat die Internet Engineering Task Force (IETF) im Juni 2002 die Liste der von SSL (Transport Layer Security Protocol – TLS) unterstützten Verschlüsselungsverfahren um den AES ergänzt:

http://www.ietf.org/rfc/rfc3268.txt

Bisher unterstützte der SSL-Standard (RFC 2246 vom Januar 1999) nur die Algorithmen RC2, RC4, IDEA, DES und 3DES.

1.6 PKI-Umfrage

Die TeleTrusT-Arbeitsgruppe „Public Key Infrastrukturen“ (AG 7) hat eine Web-Umfrage zum Stand von Public Key Infrastrukturen in Deutschland gestartet:

http://www.teletrust.de/glossar.asp?ID=60880,3&HomePG=0&sw=1&Sprache=D_

Die Arbeitsgruppe erhofft sich eine repräsentative Erfassung aktueller PKI-Trends. Einen Zwischenstand der Umfrage wird der Leiter der AG 7, Fritz Bauspieß, auf dem diesjährigen PKI-Symposium 2002 in Karlsruhe vorstellen.

1.7 IT-Sicherheitskongress

Der 8. Deutsche IT-Sicherheitskongress des BSI wird vom **13.-15.05.2003** in Bonn stattfinden. Das Programmkomitee des alle zwei Jahre organisierten Kongresses hat am 18.07.2002 den "Call for Papers“ veröffentlicht. Damit werden interessierte Autoren zur Einreichung fachkundiger Beiträge bis 10.10.2002 aufgefordert:

http://www.bsi.bund.de/veranst/bsikongr/cfp.pdf (91 kB)

1.8 EU-Datenschutzrichtline

Die am 12.07.2002 verabschiedete EU-Datenschutzrichtlinie für elektronische Kommunikation ist nun online verfügbar. Sie muss bis 31.10.2003 in nationales Recht umgesetzt werden:

http://europa.eu.int/eur-lex/de/dat/2002/l_201/l_20120020731de00370047.pdf (167 kB)

1.9 „Liberty Alliance“ strikes back

Nachdem die Akzeptanz von Microsofts .NET-Konzept, eines Web-basierten Authentifikationsdienstes, bisher bescheiden ausfällt, haben nun die unter Führung von Sun in der „Liberty Alliance“ zusammengeschlossenen Mitbewerber am 15.07.2002 ihre Architektur-Spezifikation publiziert:

http://www.project-liberty.org/specs/main.html

2 Secorvo News

2.1 ISIS-MTT-Testbed

Im Auftrag von TeleTrusT Deutschland e.V. hat Secorvo auf Basis der Testspezifikation für ISIS-MTT-konforme Produkte einen Testbed Prototyp entwickelt, der am 01.08.2002 fertiggestellt wurde.

Diese weit gehend automatisierte, auf angepasster Open-Source-Software und eigenen Tools basierende Testumgebung wird im Herbst verfügbar sein. Den Prototyp wird Projektleiter Hans-Joachim Knobloch auf dem diesjährigen PKI-Symposium 2002 in Karlsruhe präsentieren.

2.2 IT-Grundschutz-Audit

Mit dem IT-Grundschutz-Zertifikat hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Februar 2002 ein amtliches Prüfsiegel geschaffen, mit dem die wirkungsvolle Umsetzung von IT-Grundschutzmaßnahmen in einem Unternehmen bzw. einer Behörde dokumentiert werden kann. Voraussetzung für die Erteilung eines solchen Zertifikats durch das BSI ist die Durchführung eines Grundschutz-Audits nach einem festgelegten Prüfschema durch einen vom BSI lizenzierten Auditor:

http://www.bsi.bund.de/gshb/zert/pruef.pdf (105 kB)

Seit dem 10.07.2002 zählt Claus Stark, Security Consultant bei Secorvo, zu den bisher vierzig vom BSI lizenzierten IT-Grundschutz-Auditoren. Damit kann Secorvo zukünftig Grundschutz-Audits durchführen und, bei Erfüllung der Anforderungen des Prüfschemas, dem BSI die Ausstellung eines IT-Grundschutz-Zertifikats empfehlen.

2.3 Anwendungsintegration statt „One Size Fits All“

Das Image der sicherheitstechnischen „Eier legenden Wollmilchsau“, das Public Key Infrastrukturen lange anhaftete, hat Risse bekommen – und gibt den Blick frei auf den wahren Kern einer PKI: Sie ist eine notwendige Infrastruktur für ausgewählte Mechanismen der IT-Sicherheit. Der Hype ist der ernsthaften Hinwendung zu sinnvollen Anwendungen gewichen.

Diese Entwicklung spiegelt das Programm des diesjährigen PKI-Symposiums 2002 (**08.-09.10.2002**): Mit PKI-Praxisberichten wie den „Lessons Learned“ der UBS AG, der Vorstellung spezieller PKI-basierter Anwendungen wie dem digitalen Fahrtenschreiber und einem Microsoft-Blick in die Zukunft der Webservices wird die Diskussion aktueller Entwicklungen und realistischer Perspektiven von PKIs eröffnet. Workshops und das Begleitprogramm werden auch in diesem Jahr reichlich Gelegenheit zu Erfahrungsaustausch und Diskussion geben:

http://www.pki-symposium.de

Kostenbeitrag: 390 € zzgl. MwSt.
(Aus der Erfahrung der Vorjahre empfehlen wir eine möglichst frühzeitige Anmeldung.)

2.4 „PKI-Woche 2002“

Die 41. Kalenderwoche haben wir in Karlsruhe dem Thema Public Key Infrastrukturen gewidmet: Um Ihren Reiseaufwand zu minimieren, haben wir unser PKI-Seminar, das PKI-Symposium 2002 und ein PKI-Vertiefungsseminar in derselben Woche konzentriert. So können Sie an vier aufeinanderfolgenden Tagen, vom **07.-10.10.2002**, in das Thema PKI eintauchen:

http://www.secorvo.de/college/pki-woche

Teilnehmern des PKI-Symposiums bieten wir die Seminarteilnahme zu einem Sonderpreis an (siehe Anmeldung). Natürlich können die Seminare und das PKI-Symposium auch unabhängig von einander gebucht werden.

3 Veranstaltungshinweise

September 2002	
23.-24.09.	IT Risk Management 2002 (Computas)
24.-25.09.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
Oktober 2002	
02.-04.10.	Information Security Solutions Europe – ISSE 2002 (EEMA)
	„PKI-Woche“
07.-08.10.	Public Key Infrastrukturen (Secorvo College)
08.-09.10.	PKI-Symposium 2002 (Secorvo)
10.10.	PKI für Fortgeschrittene (Secorvo College)
14.-16.10.	7th European Symposium on Research in Computer Security – ESORICS 2002 (ETH/IBM Zürich)
22.-23.10.	Virtual Private Networks im praktischen Einsatz (Secorvo College)
29.-30.10.	SAP-Sicherheit im Betrieb (Secorvo College)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:

http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine automatische Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
September 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 3, 1. Jhrg. 2002
Stand 09. September 2002

http://www.secorvo.de/security-news

Inhalt

Editorial: Freiwild WLAN

1 Security News

1.1 Neuer SHA-Standard

1.2 PGP auferstanden

1.3 Grundschutzhandbuch des BSI aktualisiert

1.4 CrypTool (v1.3.03)

1.5 TKÜV 2002

1.6 Bug in Macromedia Flash

2 Secorvo News

2.1 VPN-Interoperabilität

2.2 Bluetooth Security

2.3 „KA-IT-Si“ am 24.10.2002

2.4 Video „Safer Surfen“

3 Veranstaltungshinweise

Impressum

Editorial: Freiwild WLAN

Wireless LANs verbreiten sich schier unaufhaltsam – eingefrorenen IT-Budgets zum Trotz. Dabei wird die kabellose Freiheit mit Risiken erkauft: Häufig werden WLANs gänzlich ohne Sicherheitsmechanismen betrieben, oft beschränken sich die Betreiber auf einen reinen Passwortschutz, und selten nur wird das Wired Equivalent Privacy (WEP) Protokoll verwendet. Selbst WEP bietet – anders als der Name verspricht – nur ungenügenden Schutz: Im Februar, April und Juli 2001 wurden mehrere kryptoanalytische Angriffe veröffentlicht; kurz darauf waren zahlreiche Angriffsprogramme im Internet verfügbar.

Daher ist seit einer Weile Hacking „by driving around“ in Mode – ein Laptop mit WLAN-Karte und ein Auto genügen auch Laien, um sich in fremden Netzen zu tummeln. Erleichtert wird die Suche nach WLANs in jüngster Zeit durch Kreidezeichen an Hauswänden und auf Trottoirs: Matt Jones, ein Web-Designer aus London, entwickelte im Juni einen Kennzeichnungscode, mit dessen Hilfe „WLAN-Surfer“ gefundene Einwahlpunkte markieren. Die Zeichen wurden kürzlich in Paris, New York und Los Angeles entdeckt – und bald werden vielleicht auch aus deutschen Administratoren Spurenleser:



Die IEEE WG 802.11 arbeitet an einer „Reparatur“ des Standards, dem Temporal Key Integrity Protokoll (TKIP). So lange ist Vorsicht die beste Empfehlung.

Resultate von Borisov, Goldberg, Wagner; Umsetzung des Fluhrer-Mantin-Shamir-Angriffs von Rubin, Joannidis, Stubblefield:

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

http://www.cs.rice.edu/~astubble/wep

1 Security News

1.1 Neuer SHA-Standard

Am 28.08.2002 gab das amerikanische National Institute of Standards and Technology (NIST) einen neuen Secure Hash Standard (SHS) bekannt, der den SHS (FIPS PUB 180) aus dem Jahr 1993 (aktualisiert im Mai 1995) ab 01.02.2003 ersetzt:

http://csrc.nist.gov/encryption/tkhash.html

FIPS PUB 180-2 umfasst neben SHA-1, dem Secure Hash Algorithmus mit Hashwertlänge 160 bit, drei weitere Algorithmen, die jeweils einen 256 bit (SHA-256), 384 bit (SHA-384) und 512 bit (SHA-512) langen Ausgabewert erzeugen. Die neuen Hashfunktionen ermöglichen ein höheres Sicherheitsniveau für digitale Signaturen: Ab einer Schlüssellänge von 1.500 bit (RSA) bzw. 168 bit (DSS) ist bislang der Hashwert das kryptografisch schwächste Glied.

1.2 PGP auferstanden

Tot Geglaubte leben länger: Seit der unerwarteten Ankündigung von Network Associates (NAI) im Oktober 2001, dass die Produktsparte Pretty Good Privacy (PGP) verkauft werden solle, sowie der Einstellung des Vertriebs am 26.02.2002 galt PGP als „klinisch tot“. Abgesehen von der vom BMWi geförderten Open-Source-Entwicklung GnuPG bot einzig die Anfang 2002 aus der insolventen Biodata AG neu gegründete Glück & Kanja GmbH noch eine kommerziell verfügbare, PGP-kompatible Produktlösung an.

Überraschend kam daher am 19.08.2002 die Nachricht von der Ausgründung der PGP Corporation – mit Venture Capital (14 Mio. US$) und dem „Vater“ Phil Zimmermann an Bord:

http://www.pgp.com

Schon für November 2002 ist eine neue PGP-Version 8.0 für MacOS und Windows XP angekündigt.

1.3 Grundschutzhandbuch des BSI aktualisiert

Seit Mitte August 2002 ist die aktualisierte und erweiterte Version des IT-Grundschutzhandbuchs des BSI (Stand Mai, letzte Änderung 7/2002) online verfügbar:

http://www.bsi.de/gshb/deutsch/menue.htm

In der Neufassung wurde das Methodik-Kapitel (Kapitel 2) überarbeitet. Weiter enthält sie die folgenden zusätzlichen Bausteine:

- Windows 2000 Client und Server
- Internet PC
- Novell eDirectory

Das IT-Grundschutzhandbuch kann beim BSI auf CD-ROM bezogen (frankierter Rückumschlag) oder als Loseblattsammlung beim Bundesanzeiger Verlag bestellt werden (Grundwerk: € 111,50):

http://www.bsi.bund.de/gshb/deutsch/aktuell/bezug.htm

1.4 CrypTool (v1.3.03)

Mit Hilfe des Freeware-Programms CrypTool können kryptografische Verfahren angewendet, demonstriert und analysiert werden. Es ermöglicht damit einen „spielerischen" Einstieg in die klassische und die moderne Kryptografie. CrypTool wurde vor vier Jahren von der Deutschen Bank initiiert und zusammen mit der Secude GmbH, dem FZI Karlsruhe und den Universitäten Darmstadt, Siegen und Karlsruhe zu einem didaktischen Hilfsmittel für die Sensibilisierung der Mitarbeiter für IT-Sicherheit sowie für Ausbildung und Lehre weiterentwickelt. Das Programm wurde für MS-Windows-Betriebssysteme implementiert:

http://www.cryptool.de

Mit der in Kürze verfügbaren Version 1.3.03 gibt die Deutsche Bank die Projektleitung der Weiterentwicklung an die Fraunhofer Gesellschaft ab. Eine Umsetzung in Open Source unter GNU-ähnlichen Lizenzbedingungen ist geplant.

1.5 TKÜV 2002

Seit 24.08.2002 ist die geänderte Fassung der Telekommunikations-Überwachungs-Verordnung (TKÜV) vom 16.08.2002 in Kraft. Sie verpflichtet alle Betreiber von Telekommunikationsanlagen, die Telekommunikationsdienste für die Öffentlichkeit anbieten, zur Aufzeichnung der Kommunikationsdaten und Weiterleitung an die Strafverfolgungsbehörden. Die dafür erforderlichen technischen Einrichtungen müssen die Betreiber auf eigene Kosten einrichten und vorhalten:

http://217.160.60.235/BGBL/bgbl1f/bgbl102s3317.pdf

1.6 Bug in Macromedia Flash

Jetzt hat es auch die beliebten Flash-Programme erwischt: Am 13.08.2002 wurde ein Fehler in Macromedias Shockwave Flash-Plugin bekannt, der einem Angreifer über einen Buffer Overflow die Ausführung beliebigen Codes ermöglicht – und zwar unabhängig von verwendetem Browser und Betriebssystem. Dringende Empfehlung: Download und Installation der korrigierten Flash-Version des Herstellers:

http://www.macromedia.com/shockwave/download/frameset.fhtml?P1_Prod_Version=ShockwaveFlash

2 Secorvo News

2.1 VPN-Interoperabilität

Nicht nur bei Firmenzusammenschlüssen, sondern auch bei heterogenen, gewachsenen IT-Infrastrukturen ist ungenügende Interoperabilität der Produkte unterschiedlicher Hersteller oft Ärgernis und Kostentreiber. Bei IT-Sicherheitslösungen gilt dies besonders für Virtual Private Network (VPN) Gateways: Verschlüsselte Verbindungen zwischen unterschiedlichen Standorten lassen sich am elegantesten über VPN-Tunnel realisieren – und stellen dabei erhöhte Anforderungen an die Interoperabilität der unterschiedlichen Komponenten.

Im Evaluationslabor von Secorvo wurden daher in einer internen Untersuchung acht VPN-Geräte führender Hersteller auf ihre Interoperabilität in einem Standardszenario untersucht. Die (ermutigenden) Ergebnisse wurden in einem Beitrag für die Zeitschrift iX zusammengefasst, der in Ausgabe 10/2002 am 12.09.2002 erscheint.

Hintergründe, Testerfahrungen und Konfigurationsempfehlungen werden außerdem im Rahmen des Seminars von Secorvo College VPNs im praktischen Einsatz vermittelt. Das zweitägige Seminar findet am **22.-23.10.2002** in Karlsruhe statt.

2.2 Bluetooth Security

Der Kommunikationsstandard Bluetooth erfreut sich zunehmender Herstellerunterstützung: Neben Handy-Zubehör werden nun auch Produkte angeboten, die die „letzte Meile“ lokaler Netzwerke kabellos realisieren. Damit wird Bluetooth zur ernsthaften Konkurrenz zu Wireless LAN (WLAN) Lösungen. Der rapide Preisverfall durch den Masseneinsatz von Bluetooth-Chips könnte diese Entwicklung in den kommenden Jahren noch verstärken. Um so größer wird die Bedeutung der Sicherheitsarchitektur von Bluetooth.

Die Darstellung der Sicherheitsmechanismen im Bluetooth-Standard wenig geeignet, einen schnellen Überblick zu vermitteln. Das erschwert eine Bewertung der spezifizierten Verfahren. Das noch „druckfrische“ **Secorvo White Paper** „Bluetooth Security“ von Dirk Fox will Abhilfe schaffen:

http://www.secorvo.de/whitepapers

2.3 „KA-IT-Si“ am 24.10.2002

Ende des Jahres 2000 wurde von Secorvo gemeinsam mit den Karlsruher Versicherungen die „Karlsruher IT-Sicherheitsinitiative“ (kurz: KA-IT-Si) aus der Taufe gehoben. Sie will für das Thema IT-Sicherheit sensibilisieren, Grundwissen vermitteln und

versteht sich als Plattform für den Erfahrungsaustausch von Führungskräften und IT-Sicherheitsverantwortlichen.

Zahlreiche Unternehmen aus der TechnologieRegion Karlsruhe, darunter die Deutsche Bausparkasse Badenia, die L-Bank, SAP und die Sparkassen Informatik, schlossen sich inzwischen der Initiative als Partner an. Der Oberbürgermeister der Stadt Karlsruhe übernahm die Schirmherrschaft, und IHK und der Technologiepark Karlsruhe unterstützen die Aktivitäten.

Gut besucht sind die von der KA-IT-Si angebotenen abendlichen Vortragsveranstaltungen – mit intensiven Kontaktmöglichkeiten und anschließendem Buffet. Die nächste Veranstaltung der KA-IT-Si findet am **24.10.2002 (18 Uhr)** statt. Unter dem Titel „**Wie gut schwimmt Ihr Server?**“ wird Wolfgang Mühlböck von den Karlsruher Versicherungen über die Frage des Transfers von Restrisiken vortragen:

http://www.ka-it-si.de

2.4 Video „Safer Surfen“

Ermutigt durch die große Nachfrage, der sich das Video „Trojanisches Pferd“ erfreut, hat Secorvo ein weiteres Lehrvideo entwickelt. Thema diesmal: „Browsen ohne Reue“ mit Microsofts Internet Explorer.

Das Video besteht aus zwei Teilen: Einer frappierenden Demonstration dessen, was bösartige aktive Komponenten auf einer Webseite (ActiveX, VisualBasic Script etc.) bei einem schlecht konfigurierten Internet Explorer anrichten können, sowie einer Kurzeinführung in die wichtigsten Aspekte einer sicheren Konfiguration des Browsers.

Das auf CD ausgelieferte Video wird ab Mitte Oktober verfügbar sein und kann bis zum 30.09.2002 zu einem Vorzugspreis von 59 €[1] reserviert werden (Preis ab 01.10.2002: 64 €[1]):

http://www.secorvo.de/video

[1] Alle Preisangaben zzgl. MwSt.

3 Veranstaltungshinweise

September 2002	
23.-24.09.	IT Risk Management 2002 (Computas)
Oktober 2002	
02.-04.10.	Information Security Solutions Europe – ISSE 2002 (EEMA)
	„PKI-Woche“ (Secorvo und Secorvo College)
07.-08.10.	Public Key Infrastrukturen (Secorvo College)
08.-09.10.	**PKI-Symposium 2002** (Secorvo)
10.10.	PKI für Fortgeschrittene (Secorvo College)
22.-23.10.	Virtual Private Networks im praktischen Einsatz (Secorvo College)
24.10.	„Wie gut schwimmt Ihr Server?“ (KA-IT-Si, Karlsruhe)
28.-29.10.	IT-Sicherheit für kleine und mittelständische Unternehmen (VDI/IHK Köln)
29.-30.10.	SAP-Sicherheit im Betrieb (Secorvo College)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:

http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine automatische Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feed-Back an
redaktion-security-news@secorvo.de

Secorvo Security News
Oktober 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 4, 1. Jhrg. 2002
Stand 13. Oktober 2002

http://www.secorvo.de/security-news

Inhalt

Editorial: Was die 40 Räuber dem Präsidenten voraus hatten

1 Security News

1.1 Cyber Security – strategisch

1.2 Zeit der Security Surveys

1.3 CERT-Verbund

1.4 RC5-64 Contest gelöst

1.5 Würmerplage

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Browser-Konfiguration

3 Veranstaltungshinweise

Impressum

Editorial: Was die 40 Räuber dem Präsidenten voraus hatten

Die Diskussion über Mindestanforderungen an Passworte ist mindestens so alt wie die 270ste Geschichte der 1001 märchenhaften Nächte des Kalifen von Bagdad aus dem 9. Jahrhundert. Darin knackt Ali Baba den Zugang zur Räuberhöhle durch Abhören des Passworts „Sesam, öffne dich!“. Immerhin ein Passwort mit 18 Zeichen, darunter zwei Sonderzeichen – zumindest in der deutschen Übersetzung.

Damit waren die Räuber weit fortschrittlicher als 1.100 Jahre später Bill Clinton, der als Präsident der Vereinigten Staaten Ende Juni 2000 das Bundesgesetz zur digitalen Signatur elektronisch unterzeichnete – und dabei den Namen seines Hundes Buddy als Passwort wählte. Offenbar hatte ihn niemand darauf hingewiesen, dass nicht nur ein Passwort mit lediglich fünf Stellen ohne Sonderzeichen viel zu leicht erratbar ist, sondern dass Namen von Familienangehörigen auch keinen Schutz vor Social Engineering bieten und daher grundsätzlich tabu sein sollten. Mit dem Ausplaudern des verwendeten Passworts vor laufenden Kameras outete er sich gänzlich als Negativbeispiel – Ali Baba musste sich immerhin in einem Baum verstecken, um das Passwort belauschen zu können.

Trotz der gestiegenen Sensibilität in Fragen der IT-Sicherheit sind Passworte bis heute nicht nur zentrales, sondern häufig auch wohlfeiles Objekt der Begierde. Dabei gibt es zahlreiche öffentlich verfügbare Empfehlungen zur Wahl guter Passworte, wie z. B. – pars pro toto – die des Datenschutzbeauftragten des Kantons Zürich:

http://www.cnlab.ch/pwcheck/empfehlungen.html

Einen Vorzug zumindest haben moderne Passwortsysteme gegenüber dem Schutzmechanismus der Räuberhöhle: Ein Passwort kann (und sollte regelmäßig) geändert werden – damit lässt sich der mögliche Schaden immerhin begrenzen.

1 Security News

1.1 Cyber Security – strategisch

Die amerikanische Regierung hat am 17.09.2002 den Entwurf eines Strategie-Papiers zur Verbesserung der Sicherheit des Internet („National Strategy To Secure Cyberspace“) veröffentlicht:

http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf (2,4 MB)

Die Veröffentlichung erfolgte nicht ganz freiwillig: Durch eine Indiskretion war eine Vorversion des Konzepts an die Öffentlichkeit geraten – und hatte einen Aufschrei der Internet-Zugangs-Provider ausgelöst: Sie sollten zur kostenlosen Verteilung von Schutzsoftware an private Kunden verpflichtet werden. Aus der nun für zwei Monate zur öffentlichen Kommentierung freigegebenen Fassung wurden alle „Kanten“ herausgefeilt. Sie hat daher eher den Charakter einer Empfehlungssammlung denn den eines wirksamen Maßnahmenpapiers.

1.2 Zeit der Security Surveys

In unübersichtlichen Zeiten schlägt die Stunde der Studien. Zahlreiche Security Surveys bieten derzeit Einschätzungen der Bedrohungslage, des Verbreitungsgrads von Sicherheitslösungen und Abschätzungen der Budgets für IT-Sicherheit.

Die Repräsentativität der einzelnen Erhebungen ist allerdings sehr unterschiedlich. Und auch die Ergebnisse klaffen zum Teil stark auseinander. Die konkreten Zahlen erscheinen daher wenig verlässlich. Aussagekraft haben eher Studien übergreifende Trends. Davon sind einige wenig überraschend, wie z. B. die nach wie vor hohe Bedeutung der Bedrohung durch Viren.

Eine Entwicklung ist jedoch bemerkenswert: Der Anteil externer Attacken hat erheblich zugenommen – und übertrifft in einigen Befragungen erstmals den der Insiderangriffe. Offen bleibt, ob dies tatsächlich auf eine geänderte Bedrohungslage hinweist – oder eher Resultat einer verbesserten Protokollierung ist.

Hier eine Auswahl aktueller Studien:

Global Information Security Survey (März 2002), Ernst & Young, 459 Teilnehmer (weltweit):
http://www.ey.com.pl/gcrdownload/GISS_2002.pdf (2 MB)

KES/KPMG-Studie (Frühjahr 2002), 260 Teilnehmer (D):
http://www.kes.info/studie2002/ (mehrteilig)

CSI/FBI Computer Crime and Security Survey (April 2002); 503 Teilnehmer (US):
http://www.gocsi.com/pdfs/fbi/FBI2002.pdf (2,2 MB)

Information Security Breaches Survey 2002 (April 2002) von PWC und dem britischen dti; 1000 Teilnehmer (UK):
https://www.security-survey.gov.uk/isbs2002_detailedreport.pdf (1 MB)

Australian Computer Crime and Security Survey (Mai 2002) von AusCert und Deloitte Touche Tohmatsu; 95 Teilnehmer:
http://www.auscert.org.au/Information/Auscert_info/2002cs.pdf (347 kB)

Umfrage „IT-Sicherheit 2002“ (Juni 2002) von silicon.de; 483 Teilnehmer (D):
http://www.sicherheit-im-internet.de/download/IT-Sicherheit.pdf (428 kB)

BSA Cyber Security Survey (Juli 2002), BSA, 395 Teilnehmer (US):
http://www.bsa.org/security/resources/2002-07-22.131.pdf (315 kB)

Information Security Magazine Survey (September 2002), 215 Teilnehmer (US):
http://www.infosecuritymag.com/2002/sep/2002survey.pdf (267 kB)

IT-Security Studie (September 2002) von InformationWeek, 8.188 Teilnehmer weltweit (828 aus D):
http://www.informationweek.de/studien/stud_it_security2002.ppt (8,5 MB)

1.3 CERT-Verbund

Mit der Gründung eines CERT Verbunds durch sechs deutsche Computer Emergency Response Teams – CERT-Bund (BSI), DFN-CERT, S-CERT (Sparkassenorganisation), Siemens-CERT, BCRS (IBM) und Telekom-CERT – gibt es seit dem 01.09.2002 ein Koordinationsgremium für übergreifende CERT-Aktivitäten in Deutschland. Durch eine Intensivierung der Zusammenarbeit sollen u. a. die Reaktionszeiten bei sicherheitsrelevanten Ereignissen verkürzt werden:

http://www.bmi.bund.de/dokumente/Pressemitteilung/ix_90395.htm

1.4 RC5-64 Contest gelöst

Am 28.01.1997 startete RSA Security Inc. einen groß angelegten „Crypto Contest“: 13 „Krypto-Rätsel“, mit unterschiedlich langen (40 bis 128 bit) Schlüsseln verschlüsselte Texte (einmal DES, zwölf mal RC5), wurden zur Kryptoanalyse freigegeben:

http://www.rsasecurity.com/rsalabs/challenges/secretkey/secret-key.html

Die ersten vier Rätsel (RC5-40/-48/-56 und DES-56) wurden noch im Jahr 1997 gelöst. Seitdem war es ruhig um den Contest geworden – bis nun die mit einem Preis von 10.000 US$ dotierte RC5-64-Verschlüsselung gebrochen wurde: von 331.252 über das Internet verbundenen Rechnern, die in vier Jahren 15.769.938.165.961.326.592 verschiedene Schlüssel – 47% des Schlüsselraums – systematisch ausprobiert hatten („Brute Force“):

http://www.distributed.net/rc5

Zuletzt erreichten die vernetzten Rechner einen Durchsatz von über 127 Milliarden Schlüsseln pro Sekunde. Die richtige Lösung wurde schon am 14.07.2002 entdeckt; durch einen Softwarefehler wurde die Entschlüsselung – und damit der Beleg für die faktische Unsicherheit von 64 bit langen symmetrischen Schlüsseln – aber erst am 27.09. 2002 bekannt.

1.5 Würmerplage

Zwei Würmer mit dramatischen Auswirkungen halten derzeit Administratoren in Atem:

Der Wurm „Slapper“ bzw. „bugtraq.c“ nutzt einen bekannten Fehler im SSLv2-Handshake des OpenSSL-Moduls (siehe Secorvo Security News 2/2002), um auf einem Linux-Server einen Buffer Overflow zu erzeugen. Dann kopiert er das Programm „bugtraq.c“ auf den kompromittierten Server und übersetzt es mit gcc. Dieses schaltet einen Port zur Nutzung des Servers für verteilte DoS-Angriffe frei und sucht dann nach weiteren Linux-Servern. Betroffen sind Linux-Systeme mit Apache und mod_ssl. Schutz bietet die Installation der OpenSSL-Versionen ab 0.9.6e:

http://www.openssl.org

Derweil leidet die Windows-Welt unter dem Wurm „Bugbear“, der sich über E-Mail-Anhänge mit zufälligem Dateinamen und wechselndem Betreff sowie Netzlaufwerke verteilt. Er nutzt eine Schwachstelle im IE 5.01 und 5.5, durch die Attachments von HTML-E-Mails beim Öffnen ausgeführt werden. Anschließend versucht er, installierte Virenscanner und Sicherheitsprogramme zu deaktivieren. Er öffnet eine Hintertür auf Port 36794, über die ein entferntes System beliebige Kommandos und Programme ausführen kann, protokolliert alle Tastatureingaben und versendet sie per E-Mail an ein externes System:

http://cert.uni-stuttgart.de/ticker/article.php?mid=974

2 Secorvo News

2.1 Secorvo College aktuell

„Security Awareness“ wird zunehmend zum zentralen Thema in Unternehmen und Behörden. Mit dem Seminar „Defense Lab“ bietet Secorvo College am 03.-04.12.2002 in Zusammenarbeit mit der Schweizer Firma Compass Security Network Computing erstmals ein „Online-Hacking“-Seminar, in

dem die Vorgehensweise von Angreifern erläutert und zahlreiche typische Angriffe life vorgeführt werden:

http://www.secorvo.de/college

2.2 Browser-Konfiguration

Dass von aktiven Komponenten auf Webseiten erhebliche Bedrohungen ausgehen können, ist keine Neuigkeit. Viele Unternehmen haben inzwischen zentrale Filtersysteme eingerichtet, die das Eindringen bösartigen Codes über Webseiten verhindern. Aber nicht jeder PC nimmt hinter einer gut konfigurierten Firewall Deckung: Mobile Systeme mit Internet-Zugang, die sich nicht nur bei Außendienstmitarbeitern großer Beliebtheit erfreuen, sind oft unzureichend geschützt. Denn hier hängt alles an der Konfiguration des Browsers (oder der „Personal Firewall“).

Eine anschauliche Darstellung von Bedrohungen durch aktive Komponenten und Konfigurationshinweise für Microsofts Internet Explorer bietet das von Secorvo in Zusammenarbeit mit Microsoft Deutschland entwickelte Video „Safer Surfen“, das Mitte Oktober fertiggestellt wird. Vorbestellung:

http://www.secorvo.de/video

Für Surfer, die sich ihrer Sache nicht sicher sind, hat der Datenschutzbeauftragte des Kantons Zürich zusammen mit der Hochschule für Technik in Rapperswil (CH) einen Online-Sicherheitscheck für Browser entwickelt, den seit Ende März 2001 schon mehr als 400.000 Besucher genutzt haben:

http://152.96.120.35/

Nach Abschluss des vierstufigen Tests gelangen Sie zur statistischen Auswertung, die Erschreckendes offenbart: 69-85% aller getesteten Systeme haben Scriptsprachen (VBScript, JScript, JavaScript) freigeschaltet, und 25,5% erlauben die Ausführung von signierten ActiveX-Komponenten. Obwohl die Test-Teilnehmer sicher für Datensicherheit sensibilisiert waren: ca. 3.600 Systeme (1,5%) waren für ActiveX ein offenes Scheunentor, und auf etwa 4.800 Rechnern (1,6%) waren freigegebene Laufwerke sichtbar.

3 Veranstaltungshinweise

Oktober 2002	
24.10.	„Wie gut schwimmt Ihr Server?“ (KA-IT-Si, Karlsruhe)
28.-29.10.	IT-Sicherheit für KMU (VDI/IHK Köln)
November 2002	
05.-07.11.	IT-Sicherheit heute (Secorvo College)
07.-08.11.	Praxis des betrieblichen DSB (Euroforum, Berlin)
12.-13.11.	Inside Windows Security (Secorvo College)
19.-20.11.	Lotus Notes Security (Secorvo College)
20.-22.11.	IT-Security- und Riskmanagement (ZfU, Zürich)
26.-27.11.	Sichere E-Mail-Kommunikation (Secorvo College)
Dezember 2002	
02.-03.12.	IsSec 2002 (Computas, Berlin)
03.-04.12.	Defense Lab (Live Hacking) (Secorvo College)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine automatische Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail an security-news@secorvo.de (Subject: „Subscribe Security News“) anfordern.

Secorvo Security News

November/Dezember 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 5, 1. Jhrg. 2002
Stand 29. November 2002

http://www.secorvo.de/security-news

Inhalt

Editorial: Das Dorf, die Sau und die Kryptologie

1 Security News

1.1 Big Brother Awards

1.2 TCPA

1.3 Windows 2000 zertifiziert

1.4 „Backdoor“ im EFS

1.5 Sammelpatch IE 5.x-6.0

1.6 Mcert gegründet

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Förderpreis Baden-Württemberg für Secorvo

2.3 In neuem Gewand

2.4 IT-Grundschutz-Auditor

3 Veranstaltungshinweise

Impressum

Editorial: Das Dorf, die Sau und die Kryptologie

Nachdem die Veröffentlichung einer neuen, vermeintlich wesentlich effizienteren Methode zur Kryptoanalyse von RSA-Schlüsseln durch Daniel Bernstein im vergangenen Jahr große Verunsicherung ausgelöst hatte, wird derzeit eine neue „Krypto-Sau“ durch‘s Dorf gejagt. Diesmal hat es die symmetrischen Verfahren erwischt.

Schon 2001 war es Ferguson, Schroeppel und Whiting gelungen, den AES als überraschend einfache geschlossene Formel auszudrücken. Dies ist eine beunruhigende Erkenntnis, wenn daraus auch nicht unmittelbar ein Angriff abgeleitet werden konnte. Auf der diesjährigen Welt-Kryptologie-Konferenz „Crypto“ versetzte jedoch ein neuartiger Angriff auf den AES, die „eXtended Sparse Linearization“ (XSL), die Kryptologen-Elite in Aufregung. Als elektronische Vorab-Veröffentlichung kursierte eine diesbezügliche Arbeit von Courtois und Pieprzyk, die die Autoren auf der Konferenz „AsiaCrypt 2002“ Anfang Dezember präsentieren werden.

http://eprint.iacr.org/2002/044

Nachdenklich stimmt weniger der Angriff selbst: Er ist bislang „nur“ ein theoretisches Konzept, und der tatsächliche Aufwand ist mit 2^{200} Operationen so groß, dass er sich zumindest zu Lebzeiten der Autoren nicht testen lassen wird. Der AES könnte gut damit leben – ein Sicherheitsniveau von 2^{200} liegt jenseits des heute Angreifbaren, und das gilt nach Kryptografenschätzungen sicher noch bis weit in das 22. Jahrhundert. Der Ansatz des Angriffs ist jedoch bedenklicher, denn er wirkt auch beim AES-Kandidaten „Serpent“, den alle Experten für den sichersten Algorihmus im Auswahlverfahren hielten.

Wieder ein Beleg, dass die Kryptografie immer für Überraschungen gut ist. Und dass sich die Krypto-Forschung daher nicht auf ihren Erfolgen ausruhen darf. Und – dass auch bei den besten Kryptologen Irren eine menschliche Eigenschaft ist.

1 Security News

1.1 Big Brother Awards

Die 1990 gegründete internationale Menschenrechtsgruppe „Privacy International“ (PI) initiierte im Jahr 1988 die „Big Brother Awards“ als „Oskar für Datenkraken“. Inzwischen wird diese Auszeichnung für besondere Leistungen beim Missbrauch personenbezogener Daten jährlich in 12 Ländern vergeben.

http://www.privacyinternational.org/bigbrother/

In Deutschland organisiert der Bielefelder „Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs“ (FoeBuD e.V.) seit dem Jahr 2000 die Auswahl der Preisträger und die Preisverleihung. Die diesjährigen deutschen Awards wurden am 25.10.2002 in acht Kategorien verliehen. Die Preisträger finden sich unter

http://www.bigbrotherawards.de/

1.2 TCPA

Ziel der im Frühjahr 1999 von Intel initiierten Trusted Computing Platform Alliance (TCPA) ist die Schaffung einer Betriebssystemumgebung, in der durch einheitliche Mechanismen Integrität und Identität überprüfbar sichergestellt werden. Zu den Gründungsmitgliedern gehören IBM, HP, Compaq und Microsoft. Inzwischen haben sich der Initiative mehr als 160 Unternehmen angeschlossen.

http://www.trustedcomputing.org

Die aktuelle Version 1.1b der „Main Specification“ vom 22.02.2002 (frei gegeben im Mai 2002) findet sich unter:

http://www.trustedcomputing.org/docs/main%20v1_1b.pdf (pdf, 1,7 MB)

Durch eine in mehreren Sprachen verfügbare „FAQ“-Liste von Ross Anderson kommt jetzt allerdings Wirbel in das Thema: Er vermutet hinter der Initiative den Versuch, mit in Hardware realisierten kryptografischen Mechanismen zum Digital Rights Management (DRM) die Nutzung manipulierter oder nicht lizenzierter Software und unerwünschter Daten (z.B. MP3-Files) zu kontrollieren sowie Nutzer-Informationen zentral zu registrieren – eine Breitseite auf den Datenschutz mit Zensurpotential.

http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

1.3 Windows 2000 zertifiziert

Im Oktober 2002 hat Microsoft für Windows 2000 die Sicherheitszertifizierung nach den Common Criteria bezüglich des Controlled Access Protection Profile und für Evaluation Assurance Level EAL-4 bestanden.

Hinweise für die erforderliche Konfiguration für einen mit dieser Zertifizierung konformen Betrieb von Windows 2000 gibt:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/w2kccwp.asp

1.4 „Backdoor“ im EFS

Unter Windows 2000 enthält das Encrypted File System (EFS) eine hässliche ungeplante Hintertür, wie die Fachzeitschrift c’t (23/2002, S. 33) berichtet: Bootet man beispielsweise einen mit EFS gesicherten Laptop mit der Startdiskette, kann man hinter dem Rücken des Rechnerinhabers das Zugriffspasswort ändern. Anschließend kann auf EFS-verschlüsselte Dateien frei zugegriffen werden.

Microsoft empfiehlt, diese Aushebelung der integrierten Dateiverschlüsselung in Windows 2000 durch die Verwendung eines höheren Syskey-Modus (2 oder 3) zu verhindern: Dann ist ein zusätzliches Passwort bzw. sogar eine Schlüsseldiskette beim Systemstart erforderlich.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/efs.asp

1.5 Sammelpatch IE 5.x-6.0

Microsoft hat mit dem Siegeszug des Internet Explorers die Browser-Schlacht für sich entschieden: In den meisten Unternehmen genießt der IE heute den Status des Standard-Browsers. Der große Funktionsumfang des IE gibt aus Sicht der IT-Sicherheit allerdings wenig Anlass zur Freude: ActiveX, JScript, VBScript und ActiveScripting eröffnen auch Angreifern großartige Möglichkeiten. Immer wieder werden zudem sicherheitsrelevante Programmierfehler entdeckt und „Exploits" – Programme, die die Nutzung dieser Schwächen exemplarisch vorführen – im Internet veröffentlicht.

Zuletzt gab Microsoft am 20.11.2002 einen aktuellen Sammelpatch für den Internet Explorer heraus, der zahlreiche, z.T. schwere Fehler der Versionen 5.x-6.0 (SP 1) korrigiert:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-066.asp

Software-Updates „hinken" den Entdeckungen findiger Programmierer zwangsläufig hinterher. Dass einige Fehler allerdings auch von dem aktuellen Patch nicht behoben sind, zeigt die von Thor Larholm gepflegte „unpatched"-Liste ungelöster Fehlerreports zum Internet Explorer:

http://www.pivx.com/larholm/unpatched

Eine Online-Prüfung auf von Angreifern nutzbare Konfigurations- und Programmierfehler für den Internet-Explorer findet sich auf den Webseiten der Zeitschrift c't:

http://www.heise.de/ct/browsercheck/e5demo.shtml

Sensibilisierung für die sichere Nutzung des Internet Explorers und Hinweise zur geeigneten Konfiguration bietet auch das von Secorvo erstellte Video „Safer Surfen mit dem Internet Explorer", das seit kurzem verfügbar ist:

http://www.secorvo.de/video

1.6 Mcert gegründet

Am 15.10.2002 wurde vom Präsidium des Branchenverbands Bitkom der Aufbau eines Computer-Notfall-Teams (CERT) beschlossen. Die Finanzierung dieses „Mittelstand-CERTs" übernehmen in den ersten drei Jahren BMWi, BMI, Bitkom sowie sieben Unterstützer aus der Industrie. Mit speziell aufbereiteten Warn- und Schwachstellenmeldungen sowie einer koordinierten Behandlung von Sicherheitsvorfällen und -problemen soll speziell der Mittelstand beim Thema IT-Sicherheit unterstützt werden.

Diese Entscheidung basiert unter anderem auf einer im Auftrag des BMWi erstellten Studie zu „CERT-Dienstleistungen für kleine und Mittlere Unternehmen (KMU)" vom 08.07.2001 (pdf, 479 kB):

http://www.bitkom.org/gbgateinvoker.cfm/Studie_CERT_KMU.pdf?gbAction=gbFileDownload&ObjectID=F93098A0-2DB0-4818-8334CEA5E3FFFB61&DownloadObject=documents&index=1&cacheLevel=0

Die konstituierende Sitzung zum offiziellen Projektstart und der Gründung einer Mcert-Betreiber-GmbH sowie der Berufung eines Mcert-Beirats ist am 03.12.2002 in Berlin geplant.

2 Secorvo News

2.1 Secorvo College aktuell

Alles wird teurer – jedenfalls fast alles. Ein kleines Unternehmen aus Karlsruhe schwimmt gegen den Strom: Wir senken die Teilnahmegebühren für Seminare von Secorvo College durchgängig um ca. 7 %. Denn es ist uns gelungen, Kosten für Druck und Versand unserer Prospekte durch verschiedene Maßnahmen deutlich zu senken. Diese Einsparungen geben wir an Sie weiter: Sie erhalten „schlankere" Post von uns – und sparen bei den Seminargebühren bis zu 140 €.

http://www.secorvo.de/college

2.2 Förderpreis Baden-Württemberg für Secorvo

Am 13.11.2002 wurde Secorvo von Ministerpräsident Erwin Teufel als zweiter Sieger des „Förderpreises des Landes Baden-Württemberg für junge Unternehmen 2002“ für vorbildliche unternehmerische Leistungen ausgezeichnet. Um diesen renommierten Preis hatten sich mehr als 630 Unternehmen aus Baden-Württemberg beworben.

http://www.secorvo.de/presse/pm21-foerderpreis-bw-2002.html

2.3 In neuem Gewand

Seit Ende November hat Secorvo ein neues „Outfit“: Unserem Internetauftritt haben wir eine gründliche Überarbeitung angedeihen lassen. Nicht nur Farbe, Form und Design sind frisch, sondern auch Struktur und Navigation der Seiten wurden neu gestaltet – wir hoffen, zu Ihrem Gefallen und Nutzen. Aber urteilen Sie selbst – wir freuen uns über Ihre Kommentare:

http://www.secorvo.de

2.4 IT-Grundschutz-Auditor

Mitte November 2002 erhielt Stefan Gora, Consultant bei Secorvo, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) seine Lizenz als IT-Grundschutz-Auditor. Herr Gora ist damit berechtigt, IT-Grundschutz-Audits für die Erlangung von IT-Grundschutz-Zertifikaten des BSI durchzuführen sowie IT-Grundschutz-Selbsterklärungen durch ein Testat zu bestätigen.

http://www.secorvo.de/leistungen/grundschutz-audit.html

3 Veranstaltungshinweise

Dezember 2002	
01.-05.12.	AsiaCrypt 2002 (IACR, Otago/NZ)
02.-03.12.	IsSec 2002 (Computas, Berlin)
03.-04.12.	Defense Lab (Live Hacking) (Secorvo College, Karlsruhe)
04.-05.12.	TrustD@y – IT-Sicherheit ist Chefsache (TimeContor, Berlin)
09.-13.12.	ACSAC 2002 (ACSA, Las Vegas)
13.12.	Trust in Electronic Signatures (ETSI, London)
Januar 2003	
15.-17.01.	Omnicard 2003 (inTIME, Berlin)
22.-23.01.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
22.-24.01.	IT-Defense (Cirosec, Leverkusen)
28.-29.01.	PKI – Public Key Infrastrukturen (Secorvo College, Karlsruhe)
30.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine automatische Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feed-Back an
redaktion-security-news@secorvo.de

Secorvo Security News
Januar 2003

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 1, 2. Jhrg. 2003
Stand 30. Dezember 2003

http://www.secorvo.de/security-news

Inhalt

Editorial: Besinnung auf ‚Basics‘

1 Security News

1.1 Neue Patch Suite für Internet Explorer

1.2 MBSA v1.1

1.3 Aktuelle SSH-Bugs

1.4 Sperrungsverfügung

1.5 ECCp-109 gelöst

1.6 NSA-Richtlinien für Windows XP und Cisco

1.7 Marmor, Stein und Eisen bricht...

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Awareness-Partnerschaft

2.3 Video-Lizenzen

2.4 DuD 2003 – IT-RM 2003

3 Veranstaltungshinweise

Impressum

Editorial: Besinnung auf ‚Basics‘

Der Technik-Hype ist nun auch in der IT-Sicherheit vorbei. Die Prävention durch innovative technische Lösungen hat in den vergangenen Jahren in vielen Unternehmen organisatorische Maßnahmen hintan stehen und bestehende Sicherheitskonzepte veralten lassen: Zu selten wurden Sicherheitskonzepte systematisch nachgeführt, Dokumentationen an Konfigurationsänderungen sicherheitsrelevanter Systeme begleitend angepasst oder Sicherheitsrichtlinien vor der Freigabe neuer Systeme aktualisiert – das dokumentieren Sicherheitsanalysen branchenübergreifend.

Auch Studien belegen diesen Trend: Bei einer Umfrage von silicon.de gaben nur 20 % der 483 befragten Unternehmen an, ein schriftliches IT-Sicherheitskonzept zu besitzen; nach der KES/KPMG-Studie existierte es immerhin bei 56 % von 260 Unternehmen; und Ernst & Young fand unter 459 befragten Managern gerade 57 %, die sich sicher waren, über ein IT-Sicherheitskonzept zu verfügen. Nach Aktualität und Pflegeprozess wurde nicht gefragt – ernüchternd daher eine weitere Zahl: Nur 40 % der Manager waren sicher, einen Angriff überhaupt zu bemerken.

Zum Glück haben sich die Prioritäten verschoben. Vielleicht aus Einsicht. Oder um Anforderungen des KontraG, einer Zertifizierung nach BS 7799 oder einem Grundschutz-Audit zu genügen. Aber sicher auch aufgrund knapper IT-Budgets stehen nun in vielen Unternehmen die Grundlagen der IT-Sicherheit wieder oben auf der „To Do“-Liste:

- die Überarbeitung von Sicherheitsrichtlinien und Security Policies,
- die systematische Vervollständigung des IT-Sicherheitskonzepts und
- die Sensibilisierung der Mitarbeiter durch Awareness-Maßnahmen.

Vielleicht wird 2003 ein „Jahr des Sicherheitsmanagements“.

1 Security News

1.1 Neue Patch Suite für Internet Explorer

Am 04.12.2002 hat Microsoft erneut einen Patch für den Internet Explorer veröffentlicht: Ein Fehler im Cross Domain Security Model ermöglicht es einem Angreifer, über eine manipulierte Webseite Zugriff auf lokale Dateien zu gewinnen und dort Programme zu starten. Der Fehler wurde von Microsoft zunächst als „moderat" eingestuft; zwei Tage später wurde die Einstufung auf „kritisch" korrigiert. Eine Installation des Patches wird dringend angeraten.

Betroffen ist der Internet Explorer in den Versionen 5.5 (mit Service Pack 2) und 6.0 (mit Service Pack 1). Weitere Informationen und der Software-Patch von Microsoft finden sich unter

http://www.microsoft.com/technet/security/bulletin/ms02-068.asp

1.2 MBSA v1.1

Im Rahmen des im Oktober 2001 öffentlichkeitswirksam gestarteten „Strategic Technology Protection Program" hat Microsoft ein hilfreiches Tool für die Online-Überprüfung installierter Microsoft Software auf fehlende Sicherheits-Updates und sicherheitsrelevante Konfigurationsfehler entwickelt: den „Microsoft Baseline Security Analyzer" (MBSA). Seit dem 04.12.2002 ist er in Version 1.1 (englische Fassung) verfügbar und kann unter

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp (2,7 MB)

abgerufen werden. Analysiert werden Windows NT 4.0, 2000 und XP, IIS ab v4.0, IE ab v5.01, SQL Server ab v7.0, Office ab v2000, Exchange ab v5.5 und Windows Media Player ab v6.4. Der MBSA erlaubt nicht nur eine lokale, sondern auch eine Remote Analyse.

1.3 Aktuelle SSH-Bugs

Die amerikanische Firma Rapid7 Inc. deckte am 16.12.2002 zahlreiche Fehler in unterschiedlichen Implementierungen des verbreiteten Secure Shell-Protokolls SSH auf. Die Fehler und die betroffenen SSH-Implementierungen sind im zuletzt am 09.01.2003 aktualisierten CERT-Advisory CA-2002-36 zusammengefasst.

http://www.cert.org/advisories/CA-2002-36.html

Als Schutzmaßnahme wird die Installation aktueller Programmversionen und Patches empfohlen.

1.4 Sperrungsverfügung

Am 06.02.2002 hatte die Bezirksregierung Düsseldorf nach zwei mündlichen Anhörungen im November und Dezember 2001 an rund 80 Internet-Zugangs-Provider in Nordrhein-Westfalen eine Sperrungsverfügung verschickt, in der sie unter Berufung auf § 18 Abs. 2 des Mediendienste-Staatsvertrags (MdStV). zur umgehenden Sperrung ausgewählter Internet-Seiten mit strafrechtlich relevanten, rechtsextremistischen Inhalten aufforderte.

Gegen diese äußerst umstrittene Verfügung hatten 38 Provider Widerspruch eingelegt. Denn unabhängig von der Frage der Verantwortlichkeit der Provider für die vermittelten Inhalte lassen sich Sperrungen durch einen Anbieter technisch leicht umgehen. Die Widerspruchsbescheide der Bezirksregierung wiesen – erwartungsgemäß – die Einprüche zurück. Regierungspräsident Jürgen Büssow wurde daraufhin am 25.10.2002 im Rahmen der Verleihung des „Big Brother Awards" die zweifelhafte Ehre einer „Tadelnden Erwähnung" zuteil.

Das Verwaltungsgericht Düsseldorf lehnte nun mit Beschluss vom 19.12.2002 drei dort anhängige Eilanträge von Internet-Providern ab. Damit sind die Verfügungen trotz erheblicher Zweifel am Sinn einer solchen Maßnahme rechtskräftig.

http://www.sperrungsanordnung.de

1.5 ECCp-109 gelöst

Am 15.10.2002 wurde eine weitere „Elliptic Curve Challenge“ der Firma Certicom gelöst. Die mit 10.000 $ dotierte Lösung der 1997 veröffentlichten Aufgabe der zweiten Schwierigkeitsstufe wurde von einem Team um Chris Monico, University of Notre Dame (Indiana) nach 549 Tagen gefunden. An der Suche waren zuletzt weltweit 10.300 Computer und 247 Teams beteiligt.

Bestimmt wurde der diskrete Logarithmus eines Punktes auf einer elliptischen Kurve über GF(*p*), mit einem *p* der Länge 109 bit.

http://www.nd.edu/~cmonico/eccp109

Der erforderliche Rechenaufwand lag in der theoretisch erwarteten Größenordnung – und damit um etwa den Faktor 100.000.000 unter dem Aufwand, der nach heutiger Kenntnis für einen erfolgreichen Angriff auf derzeit verwendete Elliptische Kurven über GF(*p*) mit 163 bit langen Werten *p* erforderlich wäre.

1.6 NSA-Richtlinien für Windows XP und Cisco

Das „Systems and Network Attack Center“ (SNAC) der National Security Agency der USA (NSA) hat Leitlinien für die sichere Konfiguration wichtiger Systeme (Windows NT, Windows 2000, Windows XP, Cisco Router) in amerikanischen Behörden entwickelt, die zum Download bereitgestellt werden:

http://www.nsa.gov/snac

Am 25.11.2002 wurde der 141-seitige „Guide to Securing Microsoft Windows XP“ (Stand: 30.10.2002) veröffentlicht:

http://www.nsa.gov/snac/winxp/guides/wxp-1.pdf (1,78 MB)

Am 10.12.2002 veröffentlichte die NSA ein Update des 291 Seiten starken „Cisco Router Security Configuration Guide“ (Stand: 27.09.2002):

http://www.nsa.gov/snac/cisco/guides/cis-2.pdf (1,44 MB)

1.7 Marmor, Stein und Eisen bricht...

Die von den Karlsruher Versicherungen und Secorvo unter der Schirmherrschaft des Karlsruher Oberbürgermeisters im Jahr 2000 initiierte „Karlsruher IT-Sicherheitsinitiative“, einem Forum für aktuelle und ganzheitliche Fragen der IT-Sicherheit, startet ihre diesjährigen Aktivitäten im Februar mit einer Vortragsveranstaltung am Donnerstag, **13.02.2003** um **18 Uhr**. **Hans-Jürgen Frase**, Geschäftsführer der LITCOS GmbH & Co. KG, wird über physischen Schutz für IT-Systeme vortragen.

Für das leibliche Wohl ist gesorgt. Der Kostenbeitrag beträgt 30 €; für Partner ist die Teilnahme unentgeltlich. Da wieder eine große Zahl von Teilnehmern erwartet wird, wird um Anmeldung – möglichst bis 06.02.2003 – an info@ka-it-si.de gebeten.

http://www.KA-IT-Si.de

2 Secorvo News

2.1 Secorvo College aktuell

IT-Sicherheit muss, allen neuen Techniken zum Trotz, immer noch (vielleicht sogar erst recht) vor allem als ein Management-Prozess verstanden werden, in den sich die Konzeption, Umsetzung, Freigabe, regelmäßige Prüfung und Überarbeitung von Sicherheitsmaßnahmen systematisch einbetten.

In unserem neu entwickelten **Seminar „IT-Security Management“** stellen wir die grundlegenden Elemente eines systematischen IT Security Managements vor, präsentieren „Best Practices“ und entwickeln mit Ihnen an einem Beispielunternehmen ein Management-System – von der Risiko-Analyse bis zur ROI-Berechnung.

Termin: **11.-12.02.2003** (Anmeldung).

http://www.secorvo.de/college/it-security-management.html

2.2 Awareness-Partnerschaft

Seit November 2002 hat Secorvo einen weiteren starken Partner: das für hochwertige e-Learning-Lösungen bekannte Unternehmen digital spirit AG mit Sitz in Berlin.

http://www.digital-spirit.de

Mit digital spirit bietet Secorvo Konzeption und Unterstützung bei Awareness-Kampagnen. Ein erstes konkretes Resultat der Partnerschaft hat offenbar den Nerv der Zeit getroffen: Das **Web based Training zum Thema IT-Sicherheit**, entwickelt von Medienpädagogen der Firma digital spirit mit fachlicher Unterstützung von Secorvo.

http://www.secorvo.de/leistungen/awareness.html

2.3 Video-Lizenzen

Die beiden Videos zu den Themen „Trojanische Pferde“ und „Safer Surfen“ werden vermehrt in Security-Awareness-Kampagnen großer Unternehmen eingesetzt. Dafür kann nun auch eine **Intranet-Lizenz ohne Nutzer-Begrenzung** zum Preis von 2.900 € (zzgl. MwSt.) erworben werden.

http://www.secorvo.de/video/

2.4 DuD 2003 – IT-RM 2003

Wie im vergangenen Jahr werden wir auch 2003 gemeinsam mit dem für sein außergewöhnliches Qualitätsniveau bekannten Veranstalter Computas drei Konferenzen mitgestalten. Zur Vormerkung in Ihrem Kalender schon einmal die Termine der beiden ersten Vernstaltungen:

- **DuD 2003** (Datenschutz und Datensicherheit): **05.-06.05.2003, Berlin**
- **IT-RM 2003** (IT-Risk Management): **19.-20.05.2003, Karlsruhe**

Das Programm und nähere Informationen zu diesen drei Konferenzen werden nach Abschluss der Planungen auf der Webseite der Firma Computas zu finden sein:

http://www.computas.de/konferen.html

3 Veranstaltungshinweise

Januar 2003	
22.-23.01.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
28.-29.01.	PKI – Public Key Infrastrukturen (Secorvo College, Karlsruhe)
30.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2003	
04.-05.02.	SAP-Sicherheit im Betrieb (Secorvo College, Karlsruhe)
11.-12.02.	IT-Security Management (Secorvo College, Karlsruhe)
13.02.	Marmor, Stein und Eisen bricht (KA-IT-Si, Karlsruhe)
18.-19.02.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
18.-20.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
24.-26.02.	Fast Software Encryption Workshop (IACR, Lund/SE)
25.-26.02.	Lotus Notes Security (Secorvo College, Karlsruhe)
25.-26.02.	10. DFN-CERT/PCA-Workshop (DFN-CERT, Hamburg)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feed-Back an
redaktion-security-news@secorvo.de

Secorvo Security News
Februar 2003

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 2, 2. Jhrg. 2003
Stand 30. Dezember 2003

http://www.secorvo.de/security-news

Inhalt

Editorial: Wie die Schildbürger die Signatur regulierten

1 Security News

1.1 Fortsetzungsgeschichte: IE und Windows Patches

1.2 Steuerdaten-Übermittlungsverordnung, StDÜV

1.3 NGSCBFW

1.4 The National Strategy to Secure Cyberspace

1.5 PKI-Forum bei OASIS

1.6 Vorratsspeicherung

1.7 Programm „DuD 2003“

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Neu: SSL-Zertifikate der PKI-1-Verwaltung

2.3 White Paper „VPN Basis-Interoperabilität“

3 Veranstaltungshinweise

Impressum

Editorial: Wie die Schildbürger die Signatur regulierten

Für Karl Simrock (1802-1876) wäre es ein gefundenes Fressen gewesen: Die Geschichte der Regulierung der elektronischen Signatur im Deutschland des 21. Jahrhunderts. Sie beginnt 1997 nach dreijähriger Reifung mit dem ersten nationalen Signaturgesetz der Welt, gewissermaßen dem dreieckigen Rathaus. Acht Seiten, ergänzt um eine zehnseitige Signaturverordnung, die alles Wesentliche in knappen Sätzen regeln – ganz untypisch deutsch und weltweit beachtet. Sogar die Verabschiedung eines 300 Seiten starken „Maßnahmenkatalogs“ ließ sich verhindern.

Die erhoffte Initialzündung für die Etablierung elektronischer Abläufe bleibt allerdings aus, denn das definierte Sicherheitsniveau ist so hoch, dass Wirtschaftlichkeit und Praktikabilität in Frage stehen. Zwar gibt es bald erste Zertifizierungsstellen, doch Anwendungen und Nutzer fehlen: Das dreieckige Rathaus hat keine Fenster.

Da kommt Ende 1999 die EU-Richtlinie mit mehr Markt: Statt technischer Festlegungen soll die Haftung der Anbieter hinreichende Sicherheit garantieren – das Dach wird abgedeckt, im Rathaus ist Licht. Nun regnet es aber hinein: Die Investitionen der Zertifizierungsanbieter drohen Makulatur zu werden. Prompt kommt das Dach wieder drauf: Zur fortgeschrittenen und qualifizierten Signatur gesellt sich im neuen Signaturgesetz die „freiwillige Akkreditierung“.

Damit es wieder hell wird, wird nun das Licht in Säcken ins Rathaus getragen: Die GDPdU fordert 2001 die „qualifizierte Signatur mit Anbieterakkreditierung“, das 3. VwVerfÄndG führt 2002 die „qualifizierte Signatur mit Einschränkung“ ein und die aktuelle StDÜV erfindet qualifizierte Zertifikate, die elf der Kriterien nicht erfüllen.

Glücklicherweise gab es im 19. Jahrhundert noch keine digitalen Signaturen. Sonst hätte die Regulierungswirklichkeit Simrocks Schildbürgern womöglich den literarischen Erfolg streitig gemacht.

1 Security News

1.1 Fortsetzungsgeschichte: IE und Windows Patches

Mit einem neuen Sammel-Patch vom 05.02.2003 (Update: 12.02.2003) dichtet Microsoft neu entdeckte, als „critical“ eingestufte Löcher im Internet Explorer, die einem Angreifer die Umgehung des Sicherheitsmodells und damit die Ausführung beliebigen Programmcodes auf der angegriffenen Maschine erlauben. Betroffen sind die Versionen 5.01, 5.5, 6.0 des IE.

http://www.microsoft.com/security/security_bulletins/ms03-004.asp

Der Patch schließt alle Sammel-Patches des Jahres 2002 ein:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;810847

Bereits Ende Januar (22.01.2003) veröffentlichte Microsoft ein Security Update für die Betriebssystemversionen Windows NT 4.0, die Terminal Server Edition, Windows 2000 und Windows XP, das einen als „critical“ eingestuften Fehler im (üblicherweise nur auf Servern aktivierten) Locator-Service behebt:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-001.asp

1.2 Steuerdaten-Übermittlungsverordnung, StDÜV

Am 28.01.2003 erließ der Bundesfinanzminister eine „Verordnung zur elektronischen Übermittlung von Steuererklärungen und sonstigen für das Besteuerungsverfahren erforderlichen Daten“ (Steuerdaten-Übermittlungsverordnung – StDÜV). Darin werden die Bedingungen für eine zulässige elektronische Übermittlung von Steuerdaten festgelegt:

http://www.dud.de/dud/documents/stduev-030128.pdf (pdf, 45 kB)

§ 7 StDÜV legt die Anforderungen an die in diesem Zusammenhang benötigten elektronischen Signaturen fest – und schafft damit neben einfachen, fortgeschrittenen, qualifizierten, qualifizierten mit Anbieterakkreditierung und qualifizierten mit Einschränkung eine neue, sechste Klasse von Signaturen, die sich von qualifizierten Signaturen durch den Verzicht auf elf ausgewählte Anforderungen unterscheidet.

1.3 NGSCBFW

„Next-Generation Secure Computing Base for Windows“ heißt seit dem 23.01.2003 die im August 2002 gestartete, bislang unter dem Codenamen „Palladium“ geführte und nicht unumstrittene Sicherheitsarchitektur von Microsoft, die ab 2005 Teil des Windows-Betriebssystems sein soll.

Alle geheimen Passwörter und Schlüssel sollen in einem in einer Hardware-Komponente verankerten Trusted Platform Module (TPM) vor unberechtigtem Zugriff Dritter geschützt werden. Die Ein-/Ausgabe-Kanäle sollen so um Authentifikationsmechanismen erweitert werden, dass kein Programm mehr Ein- oder Ausgaben vortäuschen oder abfangen kann – ein wirksames Handicap für Trojanische Pferde.

http://www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp

Welchen Preis hinsichtlich Flexibilität und Nutzbarkeit des Systems die Anwender für die unbestrittenen Sicherheitsgewinne zahlen müssen, ist dabei noch eine offene Frage.

1.4 The National Strategy to Secure Cyberspace

Im Februar 2003 veröffentlichte das Weiße Haus die Endfassung der „National Strategy to Secure Cyberspace“, deren Vorfassung am 17.09.2002 (nicht ganz freiwillig) öffentlich zur Diskussion gestellt worden war (siehe Secorvo Security News 4/2002).

http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (pdf, 980 kB)

Die Strategie verfolgt drei Ziele: den Schutz von Amerikas kritischen Infrastrukturen vor Cyber-Attacken, die Verringerung der Verletzlichkeit und die Minimierung von Schäden und Ausfallzeiten. Sie setzt fünf Prioritäten: Die Entwicklung eines nationalen Security Response Systems, eines Programms zur Verringerung der Verletzlichkeit, eines Awareness- und Trainings-Programms, den Schutz der Regierungsinfrastruktur sowie den Aufbau einer internationalen Sicherheitskooperation.

1.5 PKI-Forum bei OASIS

Das 1999 gegründete PKI-Forum, eine internationale Vereinigung der Anbieter von PKI-Lösungen, wurde am 04.11.2002 in OASIS (Organization for the Advancement of Structured Information Standards) integriert. OASIS ist ein 1993 gegründetes Konsortium von inzwischen mehr als 600 Unternehmen weltweit, das die Entwicklung offener technischer Standards fördert.

http://www.pkiforum.org
http://www.oasis-open.org

Am 07.01.2003 gründete OASIS ein „Technical Committee to Advance PKI Adoption for Secure Transactions“. Ziel dieser Arbeitsgruppe ist die Förderung von Public Key Infrastrukturen durch White Papers, Informationssammlungen und Standardisierungsaktivitäten, die der Lösungsinteroperabilität, der Orientierung am tatsächlichen Business-Bedarf und der Verbreitung digitaler Signaturen und Zertifikate dienen.

http://www.oasis-open.org/committees/pki/

1.6 Vorratsspeicherung

Im Zusammenhang mit dem Angebot von Flatrate-Internetzugängen ist eine Diskussion darüber entbrannt, ob die Speicherung von Verbindungsdaten (dynamische IP-Adresse, Datum, Uhrzeit) über das Ende der Nutzung hinaus zulässig ist, da sie zu Abrechnungszwecken nicht benötigt wird.

Sowohl ein für T-Online erstelltes Gutachten als auch die Datenschutz-Aufsichtsbehörde Darmstadt sind zu dem Ergebnis gekommen, dass eine solche Speicherung zulässig sei (Schreiben vom 14.01.2003):

http://www.dud.de/dud/documents/tdsl-rp-da-030114.pdf (pdf, 124 kB)

Ganz anders die Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vom 16.01.2003:

http://www.datenschutzzentrum.de/material/themen/presse/ipspeich.htm

Im gleichen Sinne äußert sich der Hamburgische Datenschutzbeauftragte, Dr. Hans-Hermann Schrader (28.01.2003):

http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/aktuelles/pressemeldung-2003-01-28-pdf,property=source.pdf (pdf, 56 kB)

1.7 Programm „DuD 2003“

Zum fünften Mal jährt sich die Fachkonferenz „Datenschutz und Datensicherheit“ – **DuD 2003** – am **05.-06.05.2003** in Berlin. Gemeinsam mit den Herausgebern der Fachzeitschrift „DuD“, Johann Bizer, Dirk Fox und Helmut Reimer, bietet der Veranstalter Computas eine zweitägige Konferenz mit Vorträgen namhafter Experten aus Politik, Industrie, Wissenschaft und Verwaltung zu zentralen, aktuellen Themen und (Streit-) Fragen des Datenschutzes und der IT-Sicherheit an.

http://www.computas.de/dud/dud2003.pdf (pdf, 276 kB)

Diese Tagung erfreut sich jährlich steigender Teilnehmerzahlen und konnte sich als „feste Größe“ unter den deutschen Datenschutz-Veranstaltungen etablieren. Für „Wiederholungsteilnehmer“ winken Staffelpreise – und bei Anmeldung über Secorvo (an info@secorvo.de oder per Fax an 0721/6105-455) zudem zur Feier des Jubiläums ein Crémant-d‘Alsace des Weinguts Raymond Kieffer – jedem Kenner von Computas-Veranstaltungen ein Begriff.

2 Secorvo News

2.1 Secorvo College aktuell

Die sichere Konfiguration der Microsoft-Betriebssysteme gibt es nicht „out of the box“. Erfahrung nutzen bedeutet hier die Sicherheit Ihrer Systeme wirksam zu erhöhen.

Inside Windows Security, Windows 2000 und XP, 25.-26.03.2003

Angriffe auf Rechnersysteme selbst zu erleben und durchzuführen erleichtert die realistische Abschätzung der Gefahren, denen Ihre IT-Systeme ausgesetzt sind.

Defense Lab – Live Hacking, Angriffstechniken, Gegenmaßnahmen, 01.-02.04.2003

2.2 Neu: SSL-Zertifikate der PKI-1-Verwaltung

Das BSI hat den Betrieb der PKI-1-Verwaltung im Januar 2003 um die Ausstellung von SSL-Zertifikaten erweitert. Dazu wurden von Secorvo eine SSL-Studie und ein Umsetzungskonzept erstellt:

http://www.secorvo.de/publikationen/bsi-ssl-studie1.4.zip (pdf/zip, 316 kB)

http://www.secorvo.de/publikationen/bsi-ssl-umsetzungskonzept1.4.pdf (335 kB)

2.3 White Paper „VPN Basis-Interoperabilität“

Seit Ende Januar ist das sechste Secorvo White Paper verfügbar, diesmal zum Thema „VPN Basis-Interoperabilität“. Eine Kurzfassung der Untersuchung, in der das paarweise Zusammenspiel der VPN-Geräte von sechs Herstellern mit einer Basis-Sicherheitskonfiguration untersucht wurde, erschien in der Oktoberausgabe der Zeitschrift iX.

http://www.secorvo.de/whitepapers

3 Veranstaltungshinweise

März 2003	
25.-26.03.	Inside Windows Security (Secorvo College, Karlsruhe)
26.-28.03.	Workshop on Privacy Enhancing Technologies 2003 (TU Dresden)
April 2003	
01.-02.04.	Defense Lab (Secorvo College, Karlsruhe)
08.-09.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
13.-17.04.	RSA Conference 2003 (RSA, San Francisco)
Mai 2003	
05.-06.05.	DuD 2003 (Computas, Berlin)
06.-07.05.	Public Key Infrastrukturen (PKI) (Secorvo, Karlsruhe)
08.05.	PKI für Fortgeschrittene (Secorvo, Karlsruhe)
13.-15.05.	BSI-Kongress 2003 (BSI, Bonn)
19.-20.05.	IT Risk Management (ITRM 2003) (Computas, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
März 2003

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch

Secorvo Security Consulting GmbH

Nr. 3, 2. Jhrg. 2003
Stand 28. März 2003

http://www.secorvo.de/security-news

Inhalt

Editorial: Von Keilen und groben Klötzen

1 Security News

1.1 In Memoriam Roger Needham

1.2 Biometrie mit Problemen

1.3 Sendmail-Bug bei „weitergereichten“ Mails

1.4 „Side-Channel“ Angriffe auf SSL und RSA

1.5 BVerfG urteilt zur TK-Überwachung

1.6 Eindringen per Intrusion Detection System

1.7 Krypto-Schwäche in Kerberos v4

1.8 Unendliche Geschichte: Windows-Patches

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Evaluierung der EU-Signaturrichtlinie

3 Veranstaltungshinweise

Impressum

Editorial: Von Keilen und groben Klötzen

Ein Mann, der sich für stark gehalten,
versuchte, einen Klotz zu spalten.

Geheimnisumwölkt und leicht verrucht lockt die Kryptografie Hobbyexperten wie das Lampenlicht die Sommermotten.

Doch schwang vergeblich er sein Beil,
der Klotz war gröber als der Keil.

Unter Kryptologen sind die Geschichten von vermeintlich „unbrechbaren neuen Verfahren“ Legende – ebenso wie ihre desillusionierende Kompromittierung.

Ein zweiter sprach: Ich werd’s schon kriegen! –
umsonst, der grobe Klotz blieb liegen.

Aber auch der umgekehrte Fall ist nicht selten: hoch intelligente und erfahrene Krypto-Experten, die sich an dem Versuch, ein neues Verfahren zu brechen, die Zähne ausbeißen.

Ein dritter kam nach Jahr und Tag,
dem glückt es auf den ersten Schlag.

Und dann gibt es den dritten Fall: Verfahren, die jahrelang genutzt werden, von deren Sicherheit Experten wie Laien überzeugt sind, die Eingang in Standards und Produkte gefunden haben – und eines Tages einem neuen kritischen Blick, der das danach so scheinbar Offensichtliche zu Tage fördert, zum Opfer fallen.

Diese Fälle sind zum Glück selten, auch wenn die jüngsten Erkenntnisse zu SSL, RSA und Kerberos gleich drei sehr prominente Verfahren betreffen.

War der nun wirklich gar so forsch?
Nein – nur der Klotz war seitdem morsch.

Zwar sind die Angriffe in realen Umgebungen nicht durchführbar. Aber sie zeigen: Erfahrung schützt vor Irrtum nicht. Und sie sind zugleich eine Mahnung an die enthusiastischen Verfechter des Open Source-Paradigmas: Auch die Veröffentlichung des Source-Codes verhindert keine Fehler. Wir werden noch viele davon kennen lernen – sofern wir ein wenig Geduld mitbringen.

1 Security News

1.1 In Memoriam Roger Needham

Einer der Pioniere der Computer-Sicherheit ist tot. Roger Needham, langjähriger Cambridge-Professor und zuletzt Managing Director von Microsoft Research Ltd. verstarb Anfang März im Alter von 68 Jahren.

Seine wohl bekannteste Arbeit ist das 1978 zusammen mit Michael Schroeder veröffentlichte Authentifikationsverfahren, das die wissenschaftliche Grundlage des Kerberos-Protokolls bildet, mit dem sich heute beispielsweise die Benutzer von Windows 2000 am Domänen-Controller anmelden.

http://research.microsoft.com/users/needham/

1.2 Biometrie mit Problemen

In zahlreichen Pilotversuche zum Einsatz biometrischer Verfahren bei der Personenkontrolle steht derzeit die Gesichtserkennung auf dem Prüfstand. Insbesondere die Sie gilt als sehr attraktiv, da ein Foto als biometrisches Merkmal in Ausweisdokumenten im Gegensatz etwa zu Fingerabdrücken allgemein akzeptiert ist.

Allerdings haben die Verfahren im praktischen Einsatz noch einige Probleme. Bei einem Pilotprojekt zur Überprüfung von Flugreisenden am Nürnberger Flughafen war das System dem menschlichen Auge des geschulten Personals weit unterlegen.

http://www.heise.de/newsticker/data/jk-18.03.03-006/

Im Verlauf eines ähnlichen Versuchs am Flughafen von Sydney gelang es zwei japanischen Reisenden sogar, ihre Pässe zu tauschen, ohne dass dies von der automatischen Gesichtskontrolle bemerkt wurde.

http://australianit.news.com.au/articles/0,7204,6048331^15306^^nbv^,00.html

1.3 Sendmail-Bug bei „weitergereichten“ Mails

Sicherheitslücken in Sendmail sind ja an sich nichts Neues. Viele Anwender schützen ihre Sendmail-Installation deshalb durch einen vorgelagerten Sicherheits-Proxy der Firewall, der eine direkte Verbindung vom Internet zu einem Sendmail-basierten Mailserver verhindert.

Der jüngst entdeckte Heap-Overflow tritt jedoch bei der Bearbeitung des Mail-Envelope-Headers auf und betrifft somit auch Sendmail-Installationen, die hinter einer Firewall Deckung suchen. Patches sind verfügbar und entfernen auch gleich die gefährlichen Header-Zeilen, so dass selbst eine weitergeleitete Mail keinen Schaden mehr anrichten kann.

http://www.cert.org/advisories/CA-2003-07.html

1.4 „Side-Channel“ Angriffe auf SSL und RSA

Gleich drei aktuelle Angriffe machen sich „Randinformationen“ von SSL- bzw. RSA-Implementierungen zu nutze. Als Testobjekt für die praktische Demonstration diente den Autoren OpenSSL – der Quelle vieler SSL-Lösungen. Daher sind höchstwahrscheinlich auch andere Implementierungen betroffen. Forscher der Eidgenössischen Technischen Hochschule Lausanne benutzen das Timing von schneller oder langsamer zurückgemeldeten Fehlermeldungen, um Hinweise zur Entschlüsselung von SSL-geschützten Nachrichten zu erhalten. Dieser ausgefeilte Angriff ist glücklicherweise nur unter sehr speziellen Umständen anwendbar und daher wenig praxisrelevant.

http://lasecwww.epfl.ch/memo_ssl.shtml

Zwei Stanford-Forscher messen die benötigte Zeit für die Ausführung der RSA-Operation, um den verwendeten geheimen Exponenten zu ermitteln. Hierüber könnte beispielsweise der geheime Schlüssel eines SSL-Webservers ermittelt werden.

http://crypto.stanford.edu/~dabo/abstracts/ssl-timing.html

Und tschechische Kryptologen werten die unterschiedlichen Reaktionen auf verschiedene Fehlerfälle, die während eines SSL-Verbindungsaufbaus auftreten können, um einen SSL-Sitzungsschlüssel zu ermitteln oder eine RSA-Signatur im Namen des SSL-Servers zu fälschen. Auch dieser Angriff ist nur von beschränkter Praxisrelevanz: Er erfordert Millionen von fehlgeschlagenen SSL-Verbindungen, die für aufmerksame Systemadministratoren nicht zu übersehen wären.

http://eprint.iacr.org/2003/052/

Für OpenSSL wurden umgehend Patches gegen alle drei Attacken bereit gestellt.

http://www.openssl.org/

1.5 BVerfG urteilt zur TK-Überwachung

Am 12.03.2003 hat das Bundesverfassungsgericht (BVerfG) zwei Verfassungsbeschwerden von Journalisten zurückgewiesen, deren Telefone im Zuge der Verfolgung schwerer Straftaten abgehört wurden. Beschwerdeführer waren das ZDF, zwei seiner journalistischen Mitarbeiter und eine für das Magazin „Stern“ tätige Journalistin, die Informationen zu verschiedenen Kriminalfällen recherchierten.

Da angenommen wurde, dass die Journalisten mit den Beschuldigten in telefonischem Kontakt stehen, ordnete das Amtsgericht Frankfurt a.M. auf Antrag der Staatsanwaltschaft die Auskunft über entsprechende Verbindungsdaten der Telefongespräche an. Die Verfassungsbeschwerden richteten sich gegen diese richterliche Anordnung der TK-Überwachung.

Obwohl das BVerfG sowohl den Eingriff in das Fernmeldegeheimnis als auch den Eingriff in die Presse- und Rundfunkfreiheit der Beschwerdeführer anerkannte, hatten die Verfassungsbeschwerden keinen Erfolg. Zur Begründung gab das Gericht an, dass auch schwer wiegende Grundrechtseingriffe als verhältnismäßig anzusehen sind. Denn „angesichts der Schwere der in Rede stehenden Straftaten“ hätten die Gerichte „dem Gebot der wirksamen Strafverfolgung zu Recht den Vorrang eingeräumt“.

http://www.bverfg.de/bverfg_cgi/pressemitteilungen/frames/bvg20-03

1.6 Eindringen per Intrusion Detection System

Ein Buffer Overflow bei der Analyse des mitgeschnittenen Datenverkehrs durch das Open-Source Intrusion Detection System (IDS) „snort“ ermöglichte es Angreifern, mittels einer vorgeblichen Attacke auf RPC-Dienste in Wirklichkeit den IDS Server anzugreifen. Entdeckt wurde die Sicherheitslücke vom kommerziellen IDS-Hersteller ISS Inc.

http://www.snort.org/

1.7 Krypto-Schwäche in Kerberos v4

Eine neu entdeckte Schwäche im altbekannten Kerberos v4 Protokoll ermöglicht verschiedene Angriffe durch Kerberos-Benutzer und durch Administratoren fremder Verwaltungsbereiche („Realms“). Wer noch Kerberos v4 einsetzt, sollte den empfohlenen Patch installieren – oder gleich zu Kerberos v5 wechseln.

http://web.mit.edu/kerberos/www/advisories

1.8 Unendliche Geschichte: Windows-Patches

Immer wieder einen Blick wert ist die Security Bulletin Liste von Microsoft. Neu hinzu gekommen sind kritische Sicherheitslücken in der Windows Script Engine und in der DOS/NT Namenskonvertierung sowie Denial-of-Service gegen ISA Server und RPC.

http://www.microsoft.com/technet/security/current.asp

2 Secorvo News

2.1 Secorvo College aktuell

Über fünf Jahre Erfahrung mit der Konzeption, dem Aufbau und dem erfolgreichen Betrieb von Public Key Infrastrukturen bündelt Secorvo in dem Seminar-Paket „PKI“ und „PKI für Fortgeschrittene“:

- PKI – Public Key Infrastrukturen, 06.-07.05.2003.
- PKI für Fortgeschrittene, 08.05.2003.

Einsteigern in das Thema IT-Sicherheit bietet Secorvo außerdem jetzt einen einwöchigen Intensivkurs:

- IT-Sicherheitsmanagement von A (wie Audit) bis Z (wie Zertifizierung), 12.-16.05.2003

Für Teilnehmer dieses Seminars ist der Eintritt zur Veranstaltung der Karlsruher IT-Sicherheitsinitiative am 15.05.2003 kostenfrei.

2.2 Evaluierung der EU-Signaturrichtlinie

Im Oktober 2002 hatte die Europäische Kommission eine Evaluationsstudie über „rechtliche und marktbezogene Aspekte der Anwendung der Richtlinie“ (zu elektronischen Signaturen) ausgeschrieben. Ziel der Studie ist es, den aktuellen Stand der praktischen Umsetzung der Signaturrichtlinie in den einzelnen Mitgliedsstaaten zu dokumentieren.

Ein internationales Konsortium unter der Leitung von Professor Jos Dumortier (KU Leuven, ICRI, Belgien) hat diese Ausschreibung gewonnen. Das Team aus Jos Dumortier, Patrick an Eecke (Belgien), Georgia Skouma (Belgien), Hans Nilsson (Schweden) und Stefan Kelm von Secorvo wird die Studie voraussichtlich im Juli 2003 vorlegen.

3 Veranstaltungshinweise

April 2003	
09.04.	Lampertz-Sicherheitstag (Lampertz, Speyer)
13.-17.04.	RSA Conference 2003 (RSA, San Francisco)
Mai 2003	
05.-06.05.	DuD 2003 (Computas, Berlin)
06.-07.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
08.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
13.-15.05.	BSI-Kongress 2003 (BSI, Bonn)
15.05.	Karlsruher IT-Sicherheitsinitiative (KA-IT-Si, Karlsruhe)
12.-16.05.	IT-Sicherheitsmanagement von Audit bis Zertifizierung (Secorvo College, Karlsruhe)
19.-20.05.	IT Risk Management (ITRM 2003) (Computas, Karlsruhe)
20.-21.05.	Lotus Notes Security (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
April 2003

Dirk Fox, Stefan Gora, Stefan Kelm
Hans-Joachim Knobloch

Secorvo Security Consulting GmbH

Nr. 4, 2. Jhrg. 2003
Stand 28. April 2003

http://www.secorvo.de/security-news

Inhalt

Editorial:
Am Zopf aus dem Sumpf

1 Security News

1.1 TCPA in der Kritik

1.2 Signaturbündnis geht an den Start

1.3 Bundestag verabschiedet neues Urheberrecht

1.4 CERT Summary 1/2003

1.5 CERT-Sicherheits-warnung „entwichen“

1.6 „Evil Flag“ für IP-Pakete

2 Secorvo News

2.1 Secorvo College aktuell

2.2 IT Risk Management

2.3 Let’s do the time warp again

2.4 Security Awareness Symposium 2003

3 Veranstaltungshinweise

Impressum

Editorial: Am Zopf aus dem Sumpf

Was dem einen der Lösungsweg, ist dem anderen eine Vermeidungsstrategie: Die Zurückführung eines Problems auf ein anderes. Mathematiker lösen mit dieser Methode komplexe Herausforderungen: Sie formulieren eine Problemstellung so um, dass sie auf eine andere, bereits gelöste, zurückgeführt werden kann. Die Entwickler von Sicherheitslösungen beherrschen diese Technik auch. Allerdings erwischen sie, so scheint es, dabei häufiger ungelöste Probleme, auf die sie die Fragestellung zurückführen.

Ein klassisches Beispiel ist die Erzeugung digitaler Signaturen. Theoretisch mag die Signatur unfälschbar sein. Tatsächlich ist sie aber immer nur so sicher wie der geheime Signierschlüssel: Kann ein Angreifer ihn in Erfahrung bringen, ist die Sicherheit perdu. Also speichert man ihn auf einer Smartcard – und führt das Problem damit auf den Schutz der PIN zurück. Die kann ein Angreifer jedoch oft leicht gewinnen, wie Forscher der Universität Bonn 2001 am Beispiel des Signtrust-Clients „eTrust“ anschaulich vorführten [Cremers, Spalka, Langweg 2001].

Ein anderes Beispiel ist die Jahrzehnte alte Vision eines sicheren Betriebssystems: Integer muss es sein und Veränderungen durch nicht autorisierte Programme verhindern. Allein durch Signieren der Software lässt sich das Problem jedoch nicht lösen – sondern bestenfalls auf die Authentizität des Prüfschlüssels verschieben. Die von Compaq, HP, IBM, Intel und Microsoft gegründete Trusted Computing Platform Alliance (TCPA) versucht es nun mit der Einführung einer Hardware-Verankerung von Schlüsseln und Zufallsgeneratoren.

Vor allzu kühnen Hoffnungen sei allerdings gewarnt. Denn die Angriffe auf die Xbox zeigen: Auch Hardware ist modifizierbar. Und noch sind wir alle keine Barone, die sich mit beherztem Griff an den eigenen Zopf aus dem Sumpf ziehen können.

1 Security News

1.1 TCPA in der Kritik

Gleich an mehreren Fronten kam die Trusted Computing Platform Alliance (TCPA) in den vergangenen Wochen unter Beschuss: Die Datenschutzbeauftragten des Bundes und der Länder äußerten ihre Skepsis, dass die TCPA Architektur zur Aushebelung des Datenschutzes missbraucht werden könnte und fordern die vollständige und ausschließliche Kontrolle der Anwender über ihre mit TCPA geschützten Systeme. In dieselbe Richtung zielen die vier Forderungen, die der Chaos Computer Club anlässlich der CeBIT an die TCPA stellte. Und Protect Privacy e.V. hat für die Kritiker ein Web-Forum etabliert.

Auf technischer Ebene wurde Anfang April der Sicherheitsmechanismus der Microsoft Xbox – von vielen als Testlauf für mögliche TCPA Mechanismen angesehen – ausgehebelt: durch einen Buffer Overflow im Spiel „007 Agent Under Fire“ ist es sogar ohne Hardware-Eingriff möglich, Linux auf der Xbox zu starten.

Bei aller Skepsis und negativen Schlagzeilen darf jedoch nicht übersehen werden, dass TCPA oder vergleichbare Architekturen – fehlerfrei und datenschutzkonform umgesetzt – einen wichtigen Schritt zu mehr Sicherheit darstellen können.

1.2 Signaturbündnis geht an den Start

Fast sechs Jahre nach Inkrafttreten des ersten Signaturgesetzes in Deutschland haben Staat und Wirtschaft am 03.04.2003 das „Bündnis für elektronische Signaturen“ gegründet.

Das von der Bundesregierung im Schulterschluss mit mehreren Großunternehmen initiierte Bündnis soll dem Markt für elektronische Signaturen zum lang ersehnten Durchbruch verhelfen: Deutschland sei „Vorreiter im Recht. Aber leider nicht in der Praxis.“, so Staatssekretär Wewer auf der Gründungsveranstaltung. Zu den Konvergenzzielen des Bündnisses zählen insbesondere die Standardkonformität technischer Komponenten sowie die Förderung multifunktionaler Chipkarten.

Bemerkenswert ist, dass Innen-, Wirtschafts- und Finanzministerium an der Gründung gemeinsam mitwirkten. Das ist ein wichtiges Signal, denn diese Ministerien waren in der Vergangenheit nicht immer einer Meinung, wenn es um die Förderung elektronischer Signaturen ging.

1.3 Bundestag verabschiedet neues Urheberrecht

Nach dem Signaturgesetz und einigen damit verbundenen Gesetzesänderungen befindet sich Deutschland nun auch im Bereich des Urheberrechts auf dem Weg in die Informationsgesellschaft: Der Bundestag hat am 11.04.2003 den „Gesetzesentwurf zur Regelung des Urheberrechts in der Informationsgesellschaft“ verabschiedet.

Ähnlich wie der in den USA bereits in Kraft getretene Digital Millenium Copyright Act (DMCA) soll auch das neue deutsche Recht das Eigentum an digitalen Daten besser schützen – so soll insbesondere das Umgehen von Kopierschutzsystemen zukünftig verboten sein. Lediglich für bestimmte private Zwecke sowie für die Forschung sollen Ausnahmen erlaubt werden, die jedoch recht ungenau gefasst wurden.

Damit ist die Diskussion um die Neugestaltung des Urheberrechts keineswegs beendet: Etliche Industrieverbände sowie private Initiativen haben bereits massive Kritik an der Neuregelung geäußert; die Bundesregierung selbst kündigte inzwischen eine weitere Urheberrechtsnovelle an.

1.4 CERT Summary 1/2003

Bei der Vielzahl an Sicherheitslücken und Hacker-Angriffen, die täglich in diversen

Medien veröffentlicht werden, ist es auch dem versierten Systemadministrator nahezu unmöglich, den Überblick zu behalten und die richtigen Entscheidungen effizient zu treffen.

Diesem Umstand trägt das CERT/CC mit dem CERT Summary Rechnung: Diese einmal pro Quartal herausgegebene Zusammenfassung listet stichwortartig diejenigen Sicherheitsvorfälle des vergangenen Quartals auf, denen das CERT/CC eine besondere Bedeutung zumisst. Damit stellt es eine echte Bereicherung im „Informationsdschungel“ dar.

Das Ende März veröffentlichte CERT Summary für das 1. Quartal 2003 beschreibt zehn Schwachstellen in verbreiteten Softwarepaketen und gibt Verweise auf weiter führende Informationen. Es finden sich Informationen zu Lücken in sendmail, Microsoft Windows, Samba, SSH, usw.; siehe dazu auch die Ausgaben 1-3/2003 der Secorvo Security News.

1.5 CERT-Sicherheitswarnung „entwichen“

Bereits seit 1988 gibt das US-amerikanische CERT Coordination Center (CERT/CC) in Pittsburgh aktuelle Sicherheitswarnungen zu Angriffen und Sicherheitslücken heraus – die sog. CERT Advisories.

Diese Advisories beschreiben – ohne eine „Anleitung zum Hacken“ darzustellen – Sicherheitslücken in Programmen und Betriebssystemen sowie Lösungsmöglichkeiten zu deren Beseitigung. Die Veröffentlichung dieser Advisories geschieht dabei in der Regel nach einer fest vorgegebenen Informationspolitik: Wird eine Schwachstelle entdeckt, wird der Hersteller informiert, um diesem die Behebung der Schwachstelle (z. B. durch entsprechende Patches) zu ermöglichen. Erst danach wird die Öffentlichkeit durch Herausgabe eines Advisories über die gefundene (und behobene) Sicherheitslücke informiert.

Diese Informationspolitik wird seit vielen Jahren kontrovers diskutiert. Gegner führen als Argumentation regelmäßig an, dass neue Sicherheitslücken unmittelbar und mit allen Details (full disclosure) veröffentlicht werden müssten, um die Hersteller zur Behebung der Lücken zu „zwingen“.

Im März nun ist es offenbar einem Hacker gelungen, drei im Entwurfsstadium befindliche Advisories zu „stehlen“ und die zwischen dem CERT/CC und den Herstellern diskutierten vertraulichen Informationen an die Öffentlichkeit zu bringen, bevor ein Advisory veröffentlicht werden konnte. Ob hieraus Schaden entstand, ist nicht bekannt; der Vorfall zeigt jedoch, wie kontrovers die Informationspolitik der CERTs zur Zeit diskutiert wird.

1.6 „Evil Flag“ für IP-Pakete

Von der Fachwelt lange erwartet erschien pünktlich am 1. April 2003 RFC 3514, in dem Steven Bellovin, Co-Director der IETF Security Area das „Security Flag in the IPv4 Header“ spezifiziert. Es nutzt ein seit 1981 unbelegtes Bit im Kopf von IP Paketen, um anzuzeigen, ob das Paket harmlos ist oder bösartigen Intentionen dient.

Sobald die namhaften Hersteller die Nutzung dieses sogenannten „Evil Flag“ in den IP-Stacks ihrer Betriebssysteme implementiert haben, ist es nur noch ein kurzer Weg zur perfekten Firewall.

2 Secorvo News

2.1 Secorvo College aktuell

Das neue Seminarprogramm 2003/2 von Secorvo College ist erschienen. Es wurde um einen einwöchigen Intensivkurs zum Thema „Information Security Management“ erweitert, dessen erste drei Tage getrennt gebucht werden können:

- Information Security Management von A(udit) bis Z(ertifizierung), **12.-16.05.2003**.

2.2 IT Risk Management

Vom **19.-20.05.2003** findet die Konferenz IT Risk Management 2003 unseres Partners COMPUTAS Giesela Geuhs GmbH in Karlsruhe statt. Topthema: Awareness.

2.3 Let's do the time warp again

Die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) startet am **15.05.2003** (18 Uhr) zu einer Zeitreise zu den Höhepunkten der Geschichte der IT-Sicherheit – und lädt anschließend zum „Schlemmer-Networking". Referent ist Dirk Fox, Geschäftsführer von Secorvo und Herausgeber der Zeitschrift „Datenschutz und Datensicherheit" (DuD).

2.4 Security Awareness Symposium 2003

Ein wirkungsvoller Informationsschutz steht und fällt mit der aktiven Unterstützung durch alle Mitarbeiter des Unternehmens. Häufig jedoch werden Sicherheitsmaßnahmen als Arbeitsbehinderung gesehen, wird die eigene Verantwortung nicht wahrgenommen oder werden vernünftige Risikoannahmen als realitätsfern abgetan – und damit Bedrohungen der Informationssicherheit durch Mitarbeiter mitverursacht.

Durch geeignete Security Awareness-Maßnahmen können sowohl das erforderliche Grundwissen vermittelt, die Sensibilität der Mitarbeiter für Informationssicherheit erhöht als auch Einstellungen und Verhaltensweisen nachhaltig verändert werden.

Ziel des Security Awareness Symposiums 2003, das Secorvo gemeinsam mit zwei Partnern, dem E-Learning-Spezialisten digital spirit ag und der Agentur Dauth, Kaun & Partner am **24.-25.06.2003** im Technologiepark Karlsruhe durchführt, ist ein intensiver Erfahrungsaustausch mit und zwischen Unternehmen, die Security Awareness-Kampagnen planen oder bereits umsetzen. Dafür konnten Referenten mehrerer Großunternehmen gewonnen werden.

3 Veranstaltungshinweise

Mai 2003	
05.-06.05.	DuD 2003 (Computas, Berlin)
06.-07.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
08.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
12.-16.05.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
13.-15.05.	BSI-Kongress 2003 (BSI, Bonn)
15.05.	Let's do the time warp again (KA-IT-Si, Karlsruhe)
19.-20.05.	IT Risk Management (ITRM 2003) (Computas, Karlsruhe)
20.-21.05.	Lotus Notes Security (Secorvo College, Karlsruhe)
Juni 2003	
24.-25.06.	Security Awareness Symposium 2003 (Secorvo, Karlsruhe)
24.-26.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News") an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Mai 2003

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch, Dörte Neundorf

Secorvo Security Consulting GmbH

Nr. 5, 2. Jhrg. 2003
Stand 28. Mai 2003

http://www.secorvo.de/security-news

Inhalt

Editorial:
Entsorgung von E-Müll

1 Security News

1.1 Signaturalgorithmen für Europa

1.2 PKI Challenge legt Abschlussbericht vor

1.3 Signaturbündnis Niedersachsen

1.4 ISIS-MTT-Compliance Criteria fertiggestellt

1.5 MS Windows Server 2003 Security Guide

1.6 MS Patchmanagement

1.7 Aktuelle Security Advisories von Cisco

1.8 Security Tools: “Top 75”

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Secorvo erstes ISIS-MTT-Prüflabor

2.3 Manche mögen’s heiß

3 Veranstaltungshinweise

Impressum

Editorial: Entsorgung von E-Müll

Viele, vielleicht die meisten der aktuellen Probleme in der IT-Sicherheit sind „uralt“: Neben Buffer Overflows und Computerviren beschäftigen uns auch Werbe-E-Mails – neudeutsch „Spam“ – seit Jahren. Zahlreiche Anbieter durchforsten heute Webseiten und Newsgroups automatisiert nach E-Mail-Adressen und nutzen diese Millionen-Verteiler für elektronische Postwurfsendungen. Inzwischen hat Spam für viele Nutzer die Grenze einer erträglichen Belästigung überschritten. Für Endbenutzer und Administratoren ist dieser tägliche E-Müll zur zeit- und ressourcenintensiven Belastung geworden. Provider versuchen Spam einzuschränken; auch gibt es für gängige Mail-Programme Filter, mit denen E-Mails auf „verdächtige“ Textstücke untersucht werden können.

Dank der Findigkeit der Werber haben diese Maßnahmen aber nur mäßigen Erfolg. Daher befassen sich mittlerweile weltweit Gesetzgebung und Rechtsprechung mit dem Phänomen. Jüngst zogen in Florida gar E-Mail-Vermarkter gegen Anti-Spam-Organisationen vor Gericht. Einige Länder bereiten Gesetze vor, nach denen das unerwünschte Versenden von Werbe-E-Mails unter Strafe gestellt werden soll. Auch der am 06.05.2003 vom Kabinett vorgelegte Entwurf für ein neues Gesetzes gegen den unlauteren Wettbewerb (UWG) definiert „Werbung mit elektronischen Nachrichten, bei der die Identität des Absenders ... verheimlicht wird“ als „unzumutbare Belästigung“ – ignoriert aber die Tatsache, dass solche E-Mails meist aus dem Ausland kommen und das UWG somit nicht greift.

Auch auf Tagungen wird das Thema intensiv diskutiert, so jüngst auf einer „Spam Conference“ des MIT, der DuD-Konferenz (05.-06.05.2003) sowie dem Anti-Spam-Kongress des eco-Forums (21.05.2003) Von einer Lösung des Problems, das zeigen die Diskussionen, sind wir allerdings noch weit entfernt. Daher ist eine weitere Zunahme von Spam zu befürchten.

1 Security News

1.1 Signaturalgorithmen für Europa

Bereits seit Dezember 1998 werden im Rahmen der europäischen Standardisierungsinitiative EESSI Standards entwickelt, die die Umsetzung und Implementierung der EU-Direktive zu elektronischen Signaturen aus dem Jahr 1999 fördern sollen. Zu den inzwischen verabschiedeten Dokumenten zählen beispielsweise Zertifikatsprofile, Richtlinien für Zertifizierungsinstanzen und Anforderungen an sichere Signaturerstellungseinheiten.

Mit dem „ETSI Special Report“ (ETSI SR 002 176 V1.1.1), an dessen Entstehung auch Secorvo aktiv beteiligt war, wurde am 27.03.2003 nun auch die überfällige Spezifikation der „Algorithms and Parameters for Secure Electronic Signatures“ verabschiedet. Inhaltlich ist das Dokument der Publikation der „Geeigneten Kryptoalgorithmen“ durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vergleichbar, die einmal jährlich gemäß Signaturgesetz die für die kommenden sechs Jahre als geeignet anzusehenden Kryptoalgorithmen und Parameter „amtlich“ festlegt.

1.2 PKI Challenge legt Abschlussbericht vor

Noch immer ist die Interoperabilität eine der größten Herausforderungen bei Aufbau und Betrieb von Public Key-Infrastrukturen. Diesem Umstand trug die „PKI Challenge“ Rechnung, ein von der Europäischen Kommission und der Schweizer Regierung gefördertes Projekt, das im Januar 2001 unter der Führung der EEMA (European Forum for Electronic Business) initiiert wurde.

Ein Konsortium aus 13 Herstellern, Dienstanbietern, Forschungseinrichtungen und Beratungsunternehmen entwickelte eine Infrastruktur zur Untersuchung technischer Interoperabilitätsaspekte der Public Key-Zertifizierung. Darin wurden zahlreiche Produkte gegen eine Referenz-Implementation getestet, auf die man sich zuvor geeinigt hatte. Der Testplan umfasste auch die Cross-Zertifizierung von CAs sowie die Verifikation von Zertifikaten durch Endbenutzeranwendungen. Der Abschlussbericht der PKI Challenge wurde am 29.04.2003 vorgelegt. Er enthält insbesondere technische Spezifikationen, die Beschreibung der durchgeführten Tests, der aufgetretenen Probleme sowie eine Reihe nützlicher Empfehlungen für den Aufbau von PKIs.

1.3 Signaturbündnis Niedersachsen

Das am 05.05.2003 veröffentlichte, vom Land Niedersachsen mit elf Unternehmen geschlossene „Bündnis für schnelle eSignatur-Lösungen Niedersachsen“ hat sich als Ziel gesetzt, flankierend zum Signaturbündnis der Bundesregierung bereits existierende Lösungen in Industrie und Verwaltung miteinander zu verknüpfen. Partner sind Cisco Systems, Deutsche Telekom, Microsoft Deutschland, BHW Bausparkasse, Empolis, Fujitsu-Siemens Computers, NordLB, Solvay, Volkswagen, die niedersächsischen Industrie- und Handelskammern und Sparkassen.

Mit der Initiative soll vor allem die private Nutzerakzeptanz gefördert werden. So können z. B. die mehr als 20.000 Mitarbeiterausweise der Volkswagen AG mit Signierfunktion zukünftig für elektronische Behördengänge genutzt werden.

1.4 ISIS-MTT-Compliance Criteria fertiggestellt

Die ISIS-MTT-Compliance-Criteria wurden am 26.05.2003 verabschiedet und am 27.05.2003 unter www.isis-mtt.org zum Download bereitgestellt. In diesem Dokument wird festgelegt, welche Kriterien ein Produkt erfüllen muss, um das Siegel „ISIS-MTT-konform“ und das entsprechende Logo führen zu dürfen.

Ziel der Siegelvergabe ist es, Anwendern schnell interoperable und damit einfach miteinander zu verwende Signatur- und Sicherheitsanwendungen zur Verfügung zu stellen.

Zum Erhalt des Siegels legen Hersteller oder Trustcenter-Betreiber in einem „Component Conformance Statement“ (CCS) fest, welchen Ausschnitt der ISIS-MTT-Spezifikation das Produkt erfüllt. Orientierung geben die in den Compliance Criteria festgelegten Produktklassen CA Server, OCSP Server, LDAP Server, VPN Server, Email-Client, SSL-Client, VPN-Client, Document-Signing Client, PKCS#11 Library, CSP und SigG conformant CSP. Zu den gewählten Funktionen ist ein Testbericht vorzulegen, der die mit Hilfe des von Secorvo entwickelten ISIS-MTT-Testbeds durchzuführenden Konformitäts-Tests belegt und dokumentiert.

Nach Prüfung des Berichtes durch ein zugelassenes Prüflabor (derzeit nur Secorvo) vergibt das ISIS-MTT-Board das Konformitätssiegel. Mit ersten Anträgen von interessierten Herstellern und Trustcenter-Betreibern wird in den kommenden Wochen gerechnet.

1.5 MS Windows Server 2003 Security Guide

Für Windows 2003 Server veröffentlichte Microsoft am 24.04.2003 einen „Security Guide“. In dem umfangreichen englischsprachigen Dokument werden zahlreiche ausführliche Hinweise zu Sicherungsmaßnahmen und dem Hardening von Systemen in Abhängigkeit vom Einsatzzweck (z. B. Domaincontroller, Fileserver etc.) gegeben. Sinnvolle Einstellungen werden vorgeschlagen und erläutert. Vervollständigt wird der Ratgeber durch Hilfsmittel wie Checklisten, Sicherheitsvorlagen und Skripte.

1.6 MS Patchmanagement

Das Tool HFNetChk des Herstellers Shavlik Technologies ermöglicht auf Microsoft-Betriebssystemen sowohl lokal als auch über das Netzwerk die Überprüfung des Patch-Levels. Die kürzlich freigegebene Version 4.0 erlaubt die Untersuchung einer Liste von Systemen (IP-Adressen) mit den Produkten Windows NT/2000/XP, IIS, MS-SQL Server, MS-Exchange Server, IE und MS-Office. Eine Funktion zum zentralen Download und dem Verteilen von Updates ist ebenfalls integriert.

Auf der HFNetChk-Engine basieren der Microsoft Baseline Security Analyzer (MBSA) und der Systems Management Server (SMS). Die kostenfreie Version von HFNetChkLT 4.0 kann bis zu 50 Systeme verwalten.

1.7 Aktuelle Security Advisories von Cisco

Nicht nur bei Microsoft werden mit schöner Regelmäßigkeit immer wieder neue Sicherheitslücken entdeckt – auch Netzwerkkomponenten, die ihr Dasein aus Sicht der meisten Anwender eher im Verborgenen fristen, sind davon betroffen und müssen ebenso wie Arbeitsplätze und Server in ein Patchmanagement einbezogen werden.

So veröffentliche Cisco am 08.05.2003 Advisories und Updates u. a. zu einem Buffer Overflow in der Administrationsoberfläche des ACS Authentifikationsservers und zu verschiedenen Schwächen im VPN 3000 Concentrator, die es im schlimmsten Fall erlauben, Firewalls per VPN-Gateway zu umgehen.

1.8 Security Tools: “Top 75”

Als Ergebnis einer Umfrage in der Newsgroup des Nmap Netzwerk-Scanners wurde eine Liste der 75 beliebtesten Sicherheits-Tools publiziert. Darin werden die Tools mit Bezugsquelle vorgestellt und bewertet. Diese Security Tools ermöglichen Administratoren, die Sicherheit ihrer Systeme und Netzwerke zu überprüfen – erleichtern allerdings auch die Durchführung von Angriffen.

2 Secorvo News

2.1 Secorvo College aktuell

Erstmalig führte Secorvo College vom 12. bis 16.05.2003 ein fünftägiges Seminar zum Information Security Management von A(udit) bis Z(ertifizierung) durch. Die positiven Rückmeldungen ermutigen uns, das Seminar erneut anzubieten – das nächste Mal in der Woche vom 22.-26.09.2003.

Vor der Sommerpause gibt es noch Gelegenheit zum Besuch zweier Seminare:

- Defense Lab – Life Hacking, Angriffstechniken und Gegenmaßnahmen, **17.-18.06.2003**
- IT-Sicherheit heute – Angriffe, Konzepte, Lösungen, **24.-26.06.2003**

2.2 Secorvo erstes ISIS-MTT-Prüflabor

Im Secorvo Security Labor werden seit 1999 IT-Sicherheitsprodukte im Kundenauftrag auf Funktionalität, Interoperabilität und Sicherheit geprüft. Vor der Beschaffung, Implementierung und Konfiguration komplexer Sicherheitslösungen werden zudem Integrationstests für Kundeninstallationen durchgeführt. Dafür stehen mehr als 300 Testinstallationen führender Sicherheitsprodukte (PKI, E-Mail, VPN, Firewall, Virenscanner etc.) bereit. Eine hohe Systematik bei der Testdurchführung und Dokumentation, sowie eine strikte Trennung der zu testenden Produkte durch Image-Dateien machen die Prüfergebnisse zudem reproduzierbar und übertragbar.

Am 14.05.2003 erhielt Secorvo vom ISIS-MTT-Board als erstes (und bisher einziges) Unternehmen die Zulassung als Prüflabor. Secorvo ist damit berechtigt, Konformitätstests für Hersteller von IT-Sicherheitssoftware und Betreiber von Trustcentern durchzuführen, auf deren Basis das ISIS-MTT-Board dann das ISIS-MTT-Konformitätssiegel vergibt.

2.3 Manche mögen's heiß

Nach einer spannenden Zeitreise durch die Geschichte der IT-Sicherheit (15.05.2003) lädt die Karlsruher IT-Sicherheitsinitiative, der die LuK GmbH & Co. oHG am 12.05. 2003 als neuer Partner beigetreten ist, zum nächsten Event: Am **03.07.2003** (18 Uhr) wird Oliver Stoll, Technical Director der WEB.DE AG, aus der Praxis des IT-Sicherheitsmanagements berichten – mit anschließendem Networking-Dinner am spanischen Buffet (u.A.w.g.).

3 Veranstaltungshinweise

Juni 2003	
17.-18.06.	Defense Lab (Secorvo College, Karlsruhe)
24.-25.06.	Security Awareness Symposium 2003 (Secorvo, Karlsruhe)
24.-26.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juli 2003	
03.07.	Manche mögen's heiß! (KA-IT-Si, Karlsruhe)
09.-10.07.	Einführung in die Praxis des betrieblichen DSB (Euroforum, Ffm)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News") an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Juni 2003

Dirk Fox, Stefan Gora, Stefan Kelm
Secorvo Security Consulting GmbH

Nr. 6, 2. Jhrg. 2003
Stand 30. Juni 2003

http://www.secorvo.de/security-news

Inhalt

Editorial: Keine Entwarnung

1 Security News

1.1 Bugs in Netzwerktreibern

1.2 Trojaner in vermeintlichem Windows-Update

1.3 Sicherheitslücken in Lotus Notes

1.4 Malware-Statistik

1.5 Validierung von Zertifikatsketten

1.6 Neuer Microsoft Guide

1.7 BSI-Studien zu Webservern

1.8 NIST-Empfehlung: MAC

1.9 USENIX Security Symposium 2003

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Lotus PKI White Paper

2.3 Awareness-Symposium

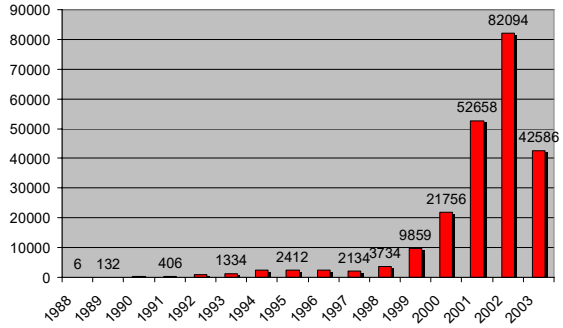
2.4 Forensik-Konferenz

3 Veranstaltungshinweise

Impressum

Editorial: Keine Entwarnung

IT-Sicherheit ist kein neues Thema. Und auch die Bedrohungen, die durch die weltweite Vernetzung von Rechnern und Servern entstanden sind, dürften keinen Verantwortlichen mehr überraschen. Dennoch staunen gelegentlich selbst Experten: Die Zunahme der den CERTs gemeldeten Sicherheitsvorfälle mutet dramatisch an. In nur vier Jahren hat sich deren Anzahl verzwanzigfacht (2003: nur erstes Quartal).



Dabei berücksichtigen diese Zahlen nur die beobachteten Angriffe. Trotz steigender Sensibilität für IT-Sicherheit und verbesserter Schutzmechanismen erscheint es unwahrscheinlich, dass die Zahl der unerkannten Angriffe nicht ähnlich stark zugenommen hat.

Viele Unternehmen tragen dieser Entwicklung durch Sensibilisierung und Schulung der Mitarbeiter sowie regelmäßige Auditierung ihrer Sicherheitsinfrastruktur Rechnung. In wachsendem Maße gilt die Aufmerksamkeit auch Intrusion Detection Systemen, die die Aufdeckung „unbekannter" Eindringmethoden versprechen, sowie Methoden der Forensik, der „digitalen Spurensicherung", um im Entdeckungsfall eine gerichtsfeste Beweissicherung vornehmen zu können. Obwohl die Bedeutung der IT-Sicherheit in vielen Unternehmen kontinuierlich zunimmt und Bedrohungen immer professioneller begegnet wird, erlauben die schiere Zahl der Angriffe und die ständige Perfektionierung von (meist frei verfügbarer) Angriffssoftware keine Entwarnung.

IT-Sicherheit bleibt eine Herausforderung.

1 Security News

1.1 Bugs in Netzwerktreibern

Bei immer mehr Ethernetkarten wird ein Programmierfehler entdeckt, der bereits Anfang diesen Jahres veröffentlicht wurde: Durch eine fehlerhafte Initialisierung der Treibersoftware kann es vorkommen, dass „alter" Netzwerkverkehr beim Senden von IP-Paketen in Füll-Bytes übertragen wird. Das CERT/CC pflegt eine Liste aller betroffenen Netzwerktreiber, die regelmäßig aktualisiert wird.

1.2 Trojaner in vermeintlichem Windows-Update

Über die Webseite http://www.windows-update.com wird derzeit ein Trojanisches Pferd verteilt: Die vermeintliche Windows-Update-Datei update0932.exe enthält den Trojaner zasil. Schlimmer noch: Greift man mit dem Internet-Explorer ohne den Sammelpatch MS03-020 auf diese Datei zu, genügt das Aufrufen der Webseite, um den Schädling zu installieren.

Die offizielle Update-Seite von Microsoft unterscheidet sich von der gefälschten nur durch einen Bindestrich...

1.3 Sicherheitslücken in Lotus Notes

Kritische Schwachstellen in Betriebssystemen wie Windows und Linux sowie verbreiteten Anwendungen wie Sendmail oder dem Internet Explorer werden häufig veröffentlicht (vgl. auch die zurückliegenden Ausgaben der Secorvo Security News).

Dass auch andere, nicht weniger verbreitete Programmpakete von solchen Problemen betroffen sind, zeigt ein „CERT Advisory" vom 26.03.2003, welches gleich acht verschiedene Sicherheitslücken in Lotus Notes und Lotus Domino beschreibt.

Die Lücken erlauben unterschiedliche Angriffe über das Internet – so z. B. einen Denial-of-Service-Angriff gegen den Domino Web Server. Betroffen sind alle Lotus-Clients bis Version 5.0.12 und Server bis Version 6.0.1.

Da Lotus-Umgebungen in vielen Unternehmen zu den Standardanwendungen gehören, ist das Einspielen der Patches dringend zu empfehlen. Weil nicht alle Fehler durch die Patches korrigiert werden, empfiehlt sich zusätzlich ein Schutz betroffener Server durch geeignete Firewallregeln (z. B. blockieren von Port 1352/TCP).

1.4 Malware-Statistik

Die Kaspersky-Labs veröffentlichen allmonatlich eine Malware-Statistik der am häufigsten auftretenden Viren, Würmer und Trojaner. Nach dem Mai-Überblick vom 02.06.2003 dominieren die Würmer Sobig (22 %), Lentin (16 %) und Klez (15%) die Statistik mit riesigem Abstand vor Fizzer, dem Viertplatzierten (0,7 %).

1.5 Validierung von Zertifikatsketten

Zu den anspruchsvollsten – und in der Praxis leider noch immer weitest gehend ungelösten – Problemen einer jeden PKI gehört die Gültigkeitsprüfung von kompletten X.509-Zertifikatsketten bzw. –pfaden. Diesem Problem widmet sich seit einiger Zeit das US-amerikanische National Institute of Standards and Technology (NIST) mit der „Public Key Interoperability Test Suite (PKITS)". Ausgehend von einer Testspezifikation sowie etablierten PKI-Standards (z. B. X.509 und RFC 3280) wurde am 15.05.2003 eine neue Version der Test-Suite (v1.07) mit ausführlicher Beschreibung (pdf/zip, 311 kB) veröffentlicht, welche Hunderte von Zertifikaten, Sperrlisten, PKCS12-Dateien und S/MIME-Nachrichten enthält. Sie sollen zunächst eigenen Tests dienen. In einer weiteren Stufe soll später

eine Referenzmenge der wichtigsten Tests definiert werden.

Vergleichbare Zertifikatspfad-Validierungen enthält auch das Mitte des vergangenen Jahres von Secorvo im Auftrag des TeleTrusT e.V. auf Open Source-Basis entwickelte ISIS-MTT Testbed, dessen Release 1.1 (Build 5) am 28.05.2003 freigegeben wurde.

1.6 Neuer Microsoft Guide

Seit dem 12.06.2003 ist ein neuer Ratgeber von Microsoft mit dem Titel „Improving Web Application Security“ (pdf, 5,8 MB) verfügbar. In dem über 900 Seiten starken englischsprachigen Dokument werden ausführliche Hinweise zur Konzeption und zum Betrieb sicherer Web-Applikationen gegeben. Gefährdungen und geeignete Schutzmaßnahmen werden allgemein und für Microsoft-Produkte vorgestellt. Der Guide enthält zusätzlich Checklisten und „How Tos“.

1.7 BSI-Studien zu Webservern

Zwei umfangreiche Studien hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) der Sicherheit der beiden derzeit verbreitetsten Webserver gewidmet: Microsofts Internet Information Server (IIS 4.0) und dem Open Source-Server Apache (v1.3 und v2.0).

Die beiden mehr als 150 Seiten starken Studien geben neben einer Einführung in die jeweilige Software eine Bewertung der Sicherheit der untersuchten Versionen und Hinweise für eine sichere Konfiguration und Administration. Da die den im April 2003 publizierten Ergebnissen zu Grunde liegenden Analysen bereits im November 2002 abgeschlossen wurden, müssen außerdem aktuelle Sicherheitshinweise der jeweiligen Hersteller berücksichtigt werden.

1.8 NIST-Empfehlung: MAC

Das US-amerikanische National Institute of Standards and Technology (NIST) arbeitet an einer Empfehlung für MAC-Algorithmen (Message Authentication Codes) auf der Basis von Blockchiffren. Der Draft der NIST Special Publication 800-38B vom November 2002 empfahl ursprünglich den Algorithmus RMAC als Ersatz für den durch eine „Konkatenations-Fälschung“ gebrochenen CBC-MAC (Cipher Block Chaining) des ISO-Standards 9797-1.

Aufgrund zahlreicher kritischer Kommentare sind anstelle der RMAC-Empfehlung nun EMAC und XCBC im Gespräch. Auf der Webseite des NIST findet sich seit dem 06.06.2003 eine Kurzbewertung der wesentlichen Eigenschaften aller drei MAC-Verfahren. Expertenkommentare sind explizit erbeten; die Kommentierungsfrist endet am 03.07.2003.

1.9 USENIX Security Symposium 2003

Bereits zum 12. Mal findet vom 04.-08.08.2003 mit dem USENIX Security Symposium eine der weltweit wichtigsten und innovativsten Sicherheitskonferenzen statt – diesmal in Washington, DC.

Auch in diesem Jahr besteht die Konferenz aus zwei parallelen Tracks: Neben der üblichen Vorstellung der eingereichten Konferenzbeiträge wird es wieder 90-minütige Spezialvorträge von eingeladenen Sprechern geben. Das Rahmenprogramm umfasst ferner ganztägige Tutorials, auf denen hochkarätige IT-Sicherheitsexperten detailliert zahlreiche Praxisthemen behandeln.

2 Secorvo News

2.1 Secorvo College aktuell

Ende Juni hat Secorvo College einen dritten Ausbildungspartner gewonnen: Neben der SAP AG und dem Bundesamt für Sicherheit in der Informationstechnik (BSI)

ergänzen die Seminare von Secorvo College von nun an auch das Weiterbildungsangebot der T-Systems International GmbH.

Zum Vormerken: Ende September findet zum zweiten Mal das fünftägige Intensiv-Seminar „Information Security Management“ statt. Neben einer Einführung in alle relevanten Standards ist ein großer Teil des Seminars „Best Practices“ gewidmet.

2.2 Lotus PKI White Paper

Ab sofort ist ein neues Secorvo White Paper zum Thema „Einsatz der Lotus Domino-PKI 6“ elektronisch verfügbar (pdf, 149 kB). Das 24 Seiten starke Dokument beschreibt kompakt, wie die aktuelle Version 6 von Lotus Notes / Domino zur Realisierung von Sicherheitslösungen auf der Basis von X.509-Zertifikaten genutzt werden kann. Es fasst die Ergebnisse von umfangreichen Tests im Secorvo Security-Labor zusammen und richtet sich vor allem an Projektleiter und Mitarbeiter, die für den Einsatz und die Nutzung von Notes im Unternehmen verantwortlich sind.

2.3 Awareness-Symposium

Mit knapp 60 Teilnehmern, spannenden Vorträgen und intensiven Diskussionen war das erstmalig von Secorvo durchgeführte „Security Awareness Symposium 2003“ ein großer Erfolg. Die Teilnehmerunterlagen können über die Webseite bestellt werden.

2.4 Forensik-Konferenz

Die Fachgruppe SIDAR (Security – Intrusion Detection and Response) der Gesellschaft für Informatik e. V. (GI) veranstaltet vom 24.-25.11.2003 die erste Tagung „IT-Incident Management & IT-Forensics“. Auf der Tagung werden alle Fragen rund um die Behandlung von IT-Sicherheitsvorfällen – von der Erkennung und Bewertung von Angriffen bis hin zur Beweissicherung – diskutiert. Stefan Kelm (Secorvo) ist Mitglied des Programmkomitees, welches um Einreichung von Konferenzbeiträgen bis zum 30.06.2003 bittet.

3 Veranstaltungshinweise

Juli 2003	
03.07.	"Manche mögen's heiß" - Event zum IT-Sicherheitsmanagement (KA-IT-Si, Karlsruhe)
09.-10.07.	Einführung in die Praxis des betrieblichen DSB (Euroforum, Ffm)
20.-23.07.	31st Annual International Conference on Computer Audit, Control and Security (ISACA, Singapore)
August 2003	
04.-08.08.	12th USENIX Security Symposium (USENIX, Washington D.C.)
26.-27.08.	Einführung in die Praxis des betriebl. DSB (Euroforum, Berlin)
September 2003	
22.-26.09.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
29.09.-02.10.	Informatik 2003 – Teiltagung Sicherheit (GI, Frankfurt)
30.09.-01.10.	SAP-Sicherheit im Betrieb (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de/

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Juli 2003

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch

Secorvo Security Consulting GmbH

Nr. 7, 2. Jhrg. 2003
Stand 24. Juli 2003

http://www.secorvo.de/security-news

Inhalt

Editorial: Vertrauensfrage(n)

1 Security News

1.1 Kreditkartenmissbrauch analysiert

1.2 CERT-Statistik Q2/2003

1.3 Bug in Microsofts HTML-Konverter

1.4 To Update or not to update …

1.5 Bremen „Europäischer eGovernment Champion“

1.6 Hosten Sie Schmuddel-Seiten?

1.7 Gefahr erkannt – Gefahr gebannt?

1.8 Denial of Service auf Ciscos IOS

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Neues Video zur „E-Mail Sicherheit“

2.3 PKI-Symposium 2003

3 Veranstaltungshinweise

Impressum

Editorial: Vertrauensfrage(n)

Zuviel Vertrauen ist häufig eine Dummheit,
zuviel Misstrauen immer ein Unglück.
Johann Nestroy

Leicht geht uns in der IT-Sicherheit das Wörtchen „Vertrauen“ über die Lippen: Wir sprechen von dem Sicherheitsziel „Vertraulichkeit“, von „Vertrauensinfrastrukturen“ und „vertrauenswürdigen Dritten”. Tatsächlich aber sind Schutzmaßnahmen nichts anders als „institutionalisiertes Misstrauen“: Wir schützen uns, weil wir hinsichtlich der Vertrauenswürdigkeit unserer zunehmend digitalen Welt so unsere Zweifel hegen.

Für diese vorsichtige Haltung gibt es viele gute Gründe. Allerdings: Im „wirklichen Leben“ gründen unser zwischenmenschlicher Umgang und unser Wirtschaftsleben auf dem Gegenteil – einer vorwiegend von Vertrauen geprägten Haltung unseren Kollegen, Kunden und Geschäftspartnern gegenüber. Das ist, wie wir heute wissen, nicht nur gut so, sondern auch volkswirtschaftlich bedeutsam: Die wirtschaftliche Entwicklung eines Landes wird inzwischen über „Vertrauensindizes“ prognostiziert.

Tatsächlich vertrauen wir fast täglich „blind“ – z. B. darauf, dass unser Gesprächspartner am Telefon auch derjenige ist, der zu sein er behauptet, dass ein Fax oder eine E-Mail vom angegebenen Sender stammt (wofür es technisch keinen Beleg gibt), und dass ein Gast oder Besucher die auf der Visitenkarte genannte Person ist. Das geht auch fast immer gut – und bestärkt uns in unserem Verhalten. Gefährlich wird es, wenn diese Vertrauensseligkeit ausgenutzt wird und dabei Schäden entstehen, wie z. B. im jüngst bekannt gewordenen Fall einer vermeintlichen Bestellung von 6.000 Kfz von Citroën durch das österreichische Innenministerium.

Dieses Dilemma ist die zentrale Herausforderung für die Informationssicherheit: Ihr muss das Kunststück gelingen, bei Kollegen und Mitarbeitern eine Prise gesunder Skepsis in das notwendige Grundvertrauen zu mischen – ohne Flexibilität und Kundenorientierung zu beeinträchtigen.

1 Security News

1.1 Kreditkartenmissbrauch analysiert

Das Bestellen von Waren und Dienstleistungen per Internet wird auch in Deutschland immer beliebter. In zunehmenden Maße wird dabei – nicht zuletzt aus Bequemlichkeit – auch die Zahlung über E-Mail oder Web-Formular abgewickelt, häufig unter Angabe der Kreditkartennummer.

Dass solche Transaktionen potenziell gefährlich sind, ist lange bekannt. Nun hat es zum ersten Mal eine Gruppe von Securityexperten aus dem „Honeynet"-Projekt geschafft, genauere Informationen über die Vorgehensweise der „Carders" beim Kreditkartenmissbrauch zu dokumentieren. Die Gruppe beobachtete über einen Zeitraum von mehreren Jahren verschiedene einschlägige Foren, insbesondere IRC-Netze, und veröffentlichte am 23.06.2003 ihre Ergebnisse in dem Bericht "Know Your Enemy: Automated Credit Card Fraud".

Besonders interessant ist die Darstellung heutiger „Carder"-Infrastrukturen, die inzwischen über stark automatisierte Tools verfügen sowie Informationen über Online-Händler verbreiten, die keine oder schwache Sicherheitsmechanismen einsetzen.

1.2 CERT-Statistik Q2/2003

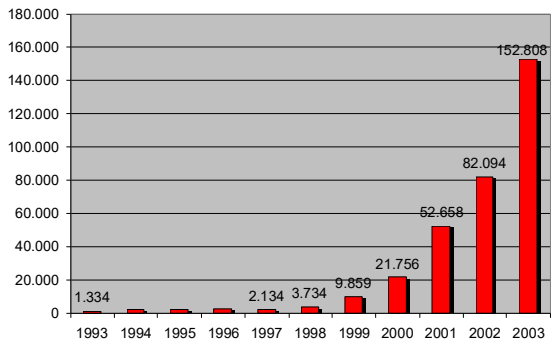


Abb. 1: Gemeldete Sicherheitsvorfälle des CERT/CC (2003: Prognose)

Am 15.07.2003 hat das CERT Coordination Center (CERT/CC) seine Quartalsstatistik veröffentlicht. Danach steigt die Zahl der berichteten Vorfälle nach wie vor steil – für die erste Jahreshälfte 2003 liegt der Wert knapp unter dem des Gesamtjahres 2002.

1.3 Bug in Microsofts HTML-Konverter

Das Konvertieren von Dateien in andere Formate ist eine Funktion des Microsoft Windows Betriebssystems. Sie ermöglicht Anwendungen z. B. die Anzeige und Speicherung von Dateien in HTML. Ein Fehler in der cut-and-paste Operation dieser Konverter-Routine wurde am 09.07.2003 publiziert. Er ermöglicht einem Angreifer, mit einer geeignet gestalteten HTML-E-Mail oder einer Webseite beliebigen Code auf dem Rechner des E-Mail-Empfängers respektive Web-Surfers (sofern dieser den Internet-Explorer verwendet) auszuführen.

Sicherheitseinstufung:

Windows 98/98 SE Windows NT 4.0 Server Windows 2000/XP	kritisch
Windows Server 2003	mittel

1.4 To update or not to update …

Seit dem 26.06.2003 ist das neue Windows 2000 Service Pack 4 verfügbar. Es enthält eine Vielzahl neuer Patches und alle Updates der vorhergehenden Service Packs. Die Installation verursacht allerdings in einigen Fällen Probleme: So warnt Microsoft vor Schwierigkeiten bei der Kombination von Terminaldiensten und dem .Net Framework 1.0 und einem Fehlverhalten des Key Management Service von Microsoft Exchange. Weitere Probleme traten beim Einsatz von Norton Internet Security 2001 auf: Nach der Installation von SP 4 war kein Internetzugriff mehr möglich. Symantec hat ein Update erstellt, welches mit der Option „Live-Update" *vor* der Installation des SP 4 heruntergeladen werden

sollte. In der Regel ist aus Sicherheitsgründen die Installation der aktuellsten Servicepacks zu empfehlen. Die Beispiele zeigen, dass dies jedoch nicht ohne vorausgehende Tests erfolgen sollte.

1.5 Bremen „Europäischer eGovernment Champion“

Bremen ist Sieger der Champions League des eGovernments: Aus dem Wettbewerb um den EU-Preis für vorbildliche Beispiele elektronischer Verwaltungsdienste ist bremen online services (bos), die eGovernment-Strategie der bremischen Verwaltung, am 08.07.2003 als Sieger in der Kategorie „Europäische Konkurrenzfähigkeit" hervorgegangen.

1.6 Hosten Sie Schmuddel-Seiten?

Die Spammer-Branche macht Ernst mit der Anonymität – zumindest mit der eigenen. Der am 11.07.2003 im Internet neu aufgetauchte Trojaner Migmaf erlaubt es, die Rechner nichts ahnender Remote- und Heim-Nutzer (bevorzugt solcher mit „always-on” DSL- oder Kabelmodem-Anschlüssen) nicht nur als Versender von Spam-Mails, sondern auch als Proxy-Server zu missbrauchen: Die Links in den verschickten Spam-E-Mails verweisen dabei nicht direkt auf den Webserver mit den beworbenen Inhalten, sondern auf einen der infizierten PCs; von dort leitet der Trojaner den Zugriff weiter.

Die Spammer sind dabei technisch auf der Höhe der Zeit: Per dynamischem DNS wird in Minutenabständen die IP-Adresse eines anderen missbrauchten PCs verwendet. Dadurch wird es Internet Service Providern praktisch unmöglich gemacht, die von den Spammern benutzten Systeme über eine IP-Filterung auszusperren.

Schutz vor dem beschriebenen Kapern durch Spammer (siehe Abb. 2) bietet eine sauber konfigurierte Personal Firewall.

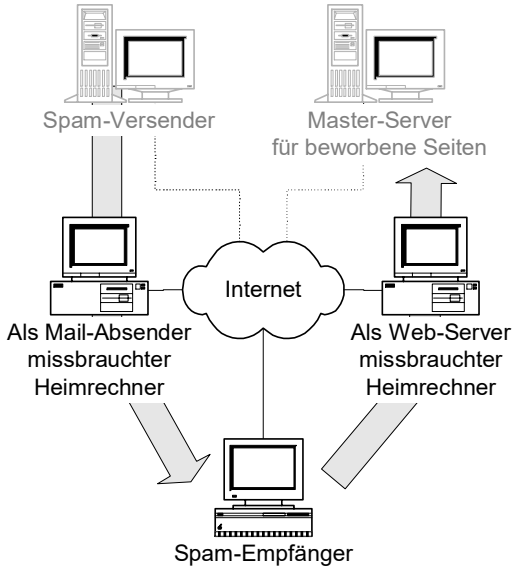


Abb. 2: Funktionsweise eines Trojaner-Spammers

1.7 Gefahr erkannt – Gefahr gebannt?

Zwei aktuelle Meldungen belegen, dass einige Sicherheitsprobleme trotz großer Publicity hartnäckig weiter bestehen:

Richard Smith – bekannt durch seine Untersuchungen über unerwünschte Zusatzinformationen in Office Dokumenten – meldete am 03.07.2003, dass noch immer viele Softwarehersteller ihre ActiveX-Controls als „sicher für Scripting“ markieren, obwohl sie bekannte Sicherheitsmängel aufweisen. Das legt den Verdacht nahe, dass sich die Prüfung dieser Hersteller auf „Absturzsicherheit“ beschränkt. Und die russische Softwarefirma ElcomSoft, deren Rechtsstreit mit Adobe weltweit Schlagzeilen machte, berichtet am 08.07.2003, dass auch zwei Jahre nach der ersten Veröffentlichung die von ElcomSoft entdeckten Sicherheitslücken in Acrobat und Acrobat Reader noch nicht beseitigt sind.

1.8 Denial of Service auf Ciscos IOS

Mit geeignet konstruierten IPv4-Paketen kann ein Denial-of-Service Angriff gegen

IOS-basierte Router von Cisco durchgeführt werden – das wurde am 16.07.2003 bekannt. Cisco stellt Vertragskunden Updates online zur Verfügung. Zur Erleichterung der Prüfung, ob eigene Geräte betroffen sind, hat Foundstone, Inc. eine Funktion zur Bestimmung der IOS-Version in das kostenfreie Tool SNS-Scan integriert.

2 Secorvo News

2.1 Secorvo College aktuell

Auf dem überarbeiteten Seminar „SAP-Sicherheit im Betrieb“ (30.09.-01.10.2003) beleuchten erfahrene Praktiker SAP-Systeme hinsichtlich der Stärken und Schwächen der Sicherheitsarchitektur und Sicherheitsfunktionalitäten von allen Seiten. Im Mittelpunkt stehen Konzepte und Maßnahmen zur Erreichung eines adäquaten Sicherheitsniveaus.

2.2 Neues Video zur „E-Mail Sicherheit“

Dass E-Mails offen wie eine „Postkarte” im Internet übertragen werden, gehört erfreulicherweise inzwischen fast zum Allgemeinwissen. Weniger bekannt ist allerdings, wie leicht es tatsächlich ist, mit frei verfügbaren Tools E-Mails abzuhören oder zu fälschen. Das ist vor allem deshalb bedenklich, weil immer mehr sensible Daten elektronisch übermittelt werden.

Um Mitarbeiter für einen bedachtsameren Umgang mit E-Mails zu sensibilisieren, hat Secorvo ein Lehrvideo entwickelt, das eindrucksvoll Angriffe auf elektronische Nachrichten demonstriert. Es hat eine Spielzeit von zehn Minuten und kann mit gängigen Flash-Playern abgespielt werden.

2.3 PKI-Symposium 2003

Noch ist das Programm in Vorbereitung – der Termin steht aber bereits: Das (vierte) „PKI-Symposium 2003“ wird am 07. und 08.10.2003 in Karlsruhe stattfinden. Über die Webseite können Sie sich schon jetzt einen Platz reservieren. Dort finden Sie auch Programme und Materialien der Symposien der Jahre 2000, 2001 und 2002.

3 Veranstaltungshinweise

August 2003	
04.-08.08.	12th USENIX Security Symposium (USENIX, Washington D.C.)
26.-27.08.	Einführung in die Praxis des betriebl. DSB (Euroforum, Berlin)
September 2003	
08.-10.09.	6th Internat. Symposium on Recent Adv. in Intrusion Detection RAID 2003 (CERT/CC, Pittsburg)
22.-26.09.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
29.09.-02.10.	Informatik 2003 – Teiltagung Sicherheit (GI, Frankfurt)
30.09.-01.10.	SAP-Sicherheit im Betrieb (Secorvo College, Karlsruhe)
Oktober 2003	
07.-08.10.	PKI-Symposium 2003 (Secorvo, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
August 2003

Dirk Fox, Hans-Joachim Knobloch,
Holger Mack, Dr. Markus Michels
Secorvo Security Consulting GmbH

Nr. 8, 2. Jhrg. 2003
Stand 25. August 2003

http://www.secorvo.de/security-news

Inhalt

Editorial:
„Eisberg rechts voraus!“

1 Security News

1.1 Yet Another Worm – was tun gegen Blaster & Co.?

1.2 Web-Application Hacking

1.3 Computerkriminalität statistisch

1.4 IT Security Benchmarks

1.5 Linux erhält Common-Criteria-Zertifikat des BSI

1.6 Bundesbank tritt European Bridge-CA bei

1.7 WBT Datenschutz

2 Secorvo News

2.1 Secorvo College aktuell

2.2 PKI-Woche 2003

3 Veranstaltungshinweise

Impressum

Editorial: „Eisberg rechts voraus!“

Der entsetzte Ruf vom Ausguck der Titanic, ausgestoßen am 14. April 1912 um 23:40 Uhr, steht für ein Ereignis, das die Welt erschüttert hat: den qualvollen und vermeidbaren Tod von über 1.500 Passagieren, verursacht durch die Hybris der Techniker, die das Schiff als „unsinkbar“ erklärten und nur 20 Rettungsboote vorsahen – zu wenig selbst für die Hälfte der Reisenden.

Haben wir aus diesem Unglück gelernt? Natürlich sind Unternehmens- und Behördennetze heute mit einer Firewall abgesichert. Was aber, wenn diese vom „Eisberg“ erwischt wird – durch einen unentdeckten Software-Fehler oder eine scheinbar harmlose Kommunikationsverbindung, die tatsächlich einen Trojaner auf Client-Systemen installiert, wie der aktuelle Blaster-Wurm?

Bei der Titanic mussten immerhin fünf Schotten volllaufen, bevor sie sank. Nur hatte niemand mit einem Eisberg gerechnet, der gleich fünf der Länge nach aufriss. In unseren Kommunikationsnetzen geben wir uns häufig mit einem Schott zufrieden – und glauben einfach nicht an den Eisberg. Wie Kapitän E.J. Smith: „*When anyone asks me how I can best describe my experience in nearly forty years at sea, I merely say, uneventful. (…) I never saw a wreck and never have been wrecked nor was I ever in any predicament that threatened to end in disaster of any sort.*“ (New York Times-Interview kurz vor der verhängnisvollen Jungfernfahrt der Titanic).

Kommt uns das nicht bekannt vor? „Bei uns ist noch nie etwas passiert.“ Stimmt vielleicht. Wenigstens hat es niemand bemerkt. Dürfen wir aber daraus Aussagen über die Zukunft ableiten? Da lohnt es, sich das Bonmot von Winston Churchill auf der Zunge zergehen zu lassen:

„*Der beste Zeitpunkt für eine Prognose ist kurz nach dem Ereignis.*“
Allerdings hilft sie dann nicht mehr viel.

1 Security News

1.1 Yet Another Worm – was tun gegen Blaster & Co.?

Wieder einmal treibt ein Wurm Publicity-trächtig sein Unwesen im Internet – diesmal quasi mit vorheriger Ansage. Die wichtigsten Maßnahmen, um sich vor den wohl unvermeidlichen Nachfolgern von Blaster, Slammer, Sobig & Co. zu wappnen, sind:

- Ein aktueller Virenscanner auf jedem (Windows-) PC gehört heute ebenso zum „Standard“ wie die Beherzigung einiger genereller Empfehlungen.
- Da vor allem Microsoft-Systeme im „Bull’s Eye“ der Virenschreiber stehen, ist das umgehende Einspielen kritischer Sicherheitsupdates hier besonders wichtig. Es wird mittlerweile von Microsoft durch einen E-Mail-Benachrichtigungsdienst unterstützt.
- PCs von Kleinunternehmen und Privatanwendern, ganz besonders solche mit „always-on“ Internetanschluss, müssen mit einer Personal-Firewall geschützt sein, die so konfiguriert ist, dass sie unerwartete Datenverbindungen nur nach manueller Freigabe zulässt oder generell blockiert.
- Unternehmen mit großen Netzen sollten Netzbereiche durch interne Firewall-Filter separieren. Im Fall eines Befalles ist es dann möglich, Würmer in kleineren Netzbereichen zu isolieren – wie Schotten im Ozeandampfer gegen eindringendes Wasser.

Gegen einen hässlichen Effekt der aktuellen Würmer ist kein Kraut gewachsen: Sobig verschickt seine Kopien unter Angabe falscher Absenderadressen, die er wie die Zieladressen auf einem infizierten System gefunden hat. Dadurch können Unbeteiligte in Verdacht geraten, Viren zu verschicken, auch wenn ihr System gar nicht infiziert ist. Technisch versierte Empfänger können zwar am E-Mail-Header erkennen, dass mit dem Transportweg der Nachricht etwas nicht stimmt. Doch auch diese versteckten Hinweise könnte schon die nächste Wurm-Generation verschleiern.

1.2 Web-Application Hacking

Firewalls und auch die verbreiteten Tools für Penetrationstests konzentrieren sich meist auf Angriffe auf der Netzwerkebene. Angriffe auf Anwendungsebene werden oft nicht erkannt. Kein Wunder, dass „Web-Application Hacking“ sich zunehmender Beliebtheit erfreut. Angriffe wie Cross-Site Scripting oder SQL Injection werden per HTTP-Protokoll getunnelt – gerne zynisch als „Firewall-friendly“ bezeichnet – und sind nur schwer von normalem Netzverkehr zu unterscheiden; teilweise entziehen sie sich sogar per SSL-Verschlüsselung dem Zugriff der Firewall.

Da andererseits Web-Applikationen in zunehmendem Maße für den Zugriff auf kritische Geschäftsdaten und Anwendungen eingesetzt werden, besteht dringender Handlungsbedarf. Leider ist die Suche nach Schwachstellen hier erheblich schwieriger zu automatisieren als auf Netzwerkebene, da Web-Applikationen häufig Eigenentwicklungen und die Schwachstellen damit meist „hausgemacht“ sind.

Eine dreiteilige Online-Artikelserie „Penetration Testing for Web Applications“ von Jody Melbourne und David Jorm, deren abschließender Teil am 20.08.2003 erschien, stellt typische Schwachstellen von Web-Applikationen vor und führt in das geeignete Vorgehen bei Penetrationstests ein. Zum gefahrlosen Erproben und Simulieren von Angriffen auf Web-Applikationen empfiehlt sich das freie Tool WebGoat.

1.3 Computerkriminalität statistisch

Das Bundeskriminalamt schlüsselt jährlich die erfassten Fälle von Computerkriminalität auf. Danach waren im Jahr 2002 zwei Drittel der insgesamt um 27,5 % auf 57.288

zurückgegangenen Fälle ein Betrug mittels rechtswidrig erlangter Debitkarten mit PIN.

Bei Computersabotage und Datenveränderung verzeichnet die Kriminalstatistik einen Anstieg um 54 % auf 1.327 Fälle. Die Aufklärungsquote erreicht im Durchschnitt respektable 50 %; bei Fällen von Datenveränderung und Computersabotage, die auch nicht autorisierte Zugriffe auf Rechner („Einbrüche“, „Hacking“) umfassen, lag sie mit 38 % unter dem Durchschnitt.

1.4 IT Security Benchmarks

Je stärker IT-Investitionen in den suchenden Blick der Controller geraten, desto wichtiger werden belastbare ROI-Nachweise. Dass solche Nachweise für die IT-Sicherheit besonders schwierig zu führen sind, ist ein offenes Geheimnis.

Ein viel versprechender Ansatz ist die Bestimmung von IT Security Benchmarks, die das erreichte Sicherheitsniveau und die Entwicklung der IT-Sicherheit im Unternehmen in Relation zu den Zielen bzw. im Vergleich zum Niveau anderer Unternehmen der Branche bewerten.

Das National Institute of Standards and Technology (NIST) hat am 12.08.2003 einen „Security Metrics Guide for Information Technology Systems“ veröffentlicht, der primär US-Behörden den Nachweis erleichtern soll, dass und in welchem Grad sie gesetzlichen Anforderungen an die IT-Sicherheit genügen.

Der Ansatz ist aber von weit allgemeinerem Interesse. Er beschreibt einen Prozess, mit dem – ausgehend von den Interessen der beteiligten Parteien, allgemeinen Organisationszielen und Sicherheitsleitlinien – eine passende IT Security Metrik entwickelt werden kann.

Im Anhang, der etwa zwei Drittel des knapp 100-seitigen Dokuments ausmacht, werden Beispielmetriken dargestellt, die auf dem bereits früher publizierten „Security Self-Assessment Guide for Information Technology Systems“ des NIST beruhen.

1.5 Linux erhält Common-Criteria-Zertifikat des BSI

Der „SuSE Linux Enterprise Server V8 with certification-sles-eal2 package“ der SuSE Linux AG hat am 28.07.2003 als erstes Open Source Betriebssystem ein Sicherheitszertifikat nach Common Criteria (CC) erhalten. Die Sicherheitsmechanismen dieser Linux-Version (User Identifikation, Authentifikation, Login-Prozess, ACLs, Rollen, User-Management etc.) wurden auf IBM xSeries 335 und 440 Systemen gemäß Zertifizierungslevel EAL2+ geprüft.

Details und nähere Informationen zu den geprüften Versionsständen der Komponenten des Linux-Softwarepakets finden sich im 55-seitigen Certification Report des BSI und in den 60-seitigen Sicherheitsvorgaben, nach denen evaluiert wurde. Anzumerken ist, dass keines der registrierten Protection Profiles nach CC zu Grunde gelegt wurde; die Linux-Version erfüllt lediglich eine Untermenge des Controlled Access Protection Profile.

Über die Aussagekraft einer CC-Zertifizierung hat Jonathan Shapiro (Johns Hopkins University) eine lesenswerte, ebenso kritische wie humorvolle Betrachtung verfasst.

1.6 Bundesbank tritt European Bridge-CA bei

Nach der SAP AG ist auch die Deutsche Bundesbank der European Bridge-CA beigetreten, einer Public Private Partnership unter der Leitung von TeleTrusT Deutschland e.V., an deren Konzeption auch Secorvo mitgewirkt hat. Damit können künftig Mitarbeiter der Bundesbank ohne weiteres S/MIME-Nachrichten mit den PKI-Nutzern der Bundesverwaltung, der Deutschen Bank AG, der SAP AG, der Siemens AG und der Telekom AG austauschen.

Die S/MIME-Interoperabilitätstests der Bridge-CA haben bereits weitere Unternehmen bestanden: BMW AG, Bundeswehr, Dresdner Bank AG, TC TrustCenter GmbH und Secartis AG.

1.7 WBT Datenschutz

Unter der fachlichen Mitwirkung von Dr. Johann Bizer, Herausgeber der Zeitschrift Datenschutz und Datensicherheit, hat der E-Learning-Spezialist digital spirit ein Web Based Training (WBT) zum Datenschutz im Unternehmen entwickelt.

2 Secorvo News

2.1 Secorvo College aktuell

Das fünftägige Intensivseminar „Information Security Management“ vom **22. bis 26.09.2003** erfreut sich schon jetzt zahlreicher Anmeldungen und verspricht daher nicht nur einen vertieften Einblick in Theorie und Praxis des ISM, sondern auch einen wertvollen Erfahrungsaustausch.

Die thematische Einführung an den beiden ersten Tagen des Seminars kann auch einzeln gebucht werden (aktuelle Seminarübersicht).

2.2 PKI-Woche 2003

Vom **06. bis 09.10.2003** steht der Technologiepark Karlsruhe unter dem Zeichen der „PKI-Woche 2003“. Sie beginnt mit dem Seminar „Public Key Infrastrukturen“, das eine umfassende, zweitägige Einführung in das Thema bietet, gefolgt vom schon traditionellen „PKI-Symposium“ mit Praxisberichten und aktuellen Themen, und schließt mit einem eintägigen Vertiefungsseminar am 09.10.2003 zu ausgewählten Themen der PKI-Realisierung.

Vier Tage intensives Erfahrungswissen, die auch getrennt gebucht werden können. Bis **02.09.2003** gilt der **Frühbucherrabatt**.

3 Veranstaltungshinweise

September 2003	
08.-10.09	5th Workshop on Cryptographic Hardware & Embedded Systems (CHES 2003, Köln)
16.-17.09.	Signatur Workshop 2003 (RegTP, Mainz)
22.-26.09.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
29.09.-02.10.	Informatik 2003 – Teiltagung Sicherheit (GI, Frankfurt)
30.09.-01.10.	SAP-Sicherheit im Betrieb (Secorvo College, Karlsruhe)
Oktober 2003	
	„PKI-Woche“ (Secorvo und Secorvo College)
06.-07.10.	Public Key Infrastrukturen (Secorvo College, Karlsruhe)
07.-08.10.	**PKI-Symposium 2003** (Secorvo)
09.10.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
07.-09.10.	ISSE 2003 (EEMA und TeleTrusT, Wien)
14.-15.10.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.10.	Defense Lab (Secorvo College, Karlsruhe)
November 2003	
10.-11.11.	ZertiFA 2003 (Computas, Köln)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
September 2003

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 9, 2. Jhrg. 2003
Stand 19. Oktober 2003

http://www.secorvo.de/security-news

Inhalt

Editorial: Happy Birthday

1 Security News

1.1 PGP in neuem Gewand

1.2 Kritischer RPC-Bug

1.3 Gefälschte eBay-Server

1.4 Trauen Sie Ihrem Browser?

1.5 Digitalbilder: Echt oder retuschiert?

1.6 GSM-Verschlüsselung unter Beschuss

1.7 Private Internet-Nutzung

2 Secorvo News

2.1 Secorvo College aktuell

2.2 „IT – Aber sicher!“

2.3 „ZertiFA 2003”

3 Veranstaltungshinweise

Impressum

Editorial: Happy Birthday

Der 01.09.2003 war für Secorvo ein besonderes Datum. Daher erlauben wir uns diesmal ein Editorial in eigener Sache: Auf den Tag genau am 01.09.1998 hat die Secorvo Security Consulting GmbH mit fünf Mitarbeitern das „Licht der Welt“ erblickt. Zwischen diesen beiden Daten liegen 1.826 ereignisreiche Tage: 167 erfolgreiche Projekte, 135 Publikationen, 133 öffentliche Vorträge, 58 Seminare von Secorvo College mit mehr als 600 überdurchschnittlich zufriedenen Teilnehmern (Note 1,45) aus mehr als 200 Unternehmen und Behörden, und weit über eine Million Webseitenzugriffe.

Secorvo entstand 1998 aus der Vision eines vollständig unabhängigen, ausschließlich den eigenen Kunden verpflichteten und auf IT-Sicherheit spezialisierten Beratungsunternehmens mit besonders kompetenten und erfahrenen Consultants, die durch aktives Engagement in Fachgremien, durch die Mitgestaltung von Normen und Standards der IT-Sicherheit und nicht zuletzt durch Publikationen und hochwertige Projektarbeit einen nachhaltigen Beitrag zur Verbesserung der IT-Sicherheit in Unternehmen und Behörden leisten.

Dieser Vision sind wir treu geblieben – und konnten sie auch in vielerlei Hinsicht Wirklichkeit werden lassen: So ist das Beratungsteam auf zehn anerkannte Experten für IT-Sicherheit angewachsen, Standards wie MailTrusT und ISIS-MTT wurden maßgeblich von Secorvo entwickelt, und namhafte mittelständische und zahlreiche große Unternehmen sowie Landes- und Bundesbehörden haben Secorvo in den vergangenen fünf Jahren mit herausfordernden Projekten betraut.

Dass dieser Erfolg möglich war, verdanken wir neben dem Engagement und dem Einsatz unseres inzwischen 16-köpfigen Teams vor allem den vielen Kunden, die auf Secorvo vertraut haben. Wir sind stolz darauf, deren hohe Erwartungen nicht enttäuscht zu haben – für die Zukunft Ansporn und Anspruch zugleich.

1 Security News

1.1 PGP in neuem Gewand

Am 16.09.2003 stellte die PGP Corp. in London ihr neuestes Software-Release – „PGP Universal“ – der Öffentlichkeit vor. Diese neue Version basiert auf der seit über einem Jahrzehnt bekannten und verbreiteten Verschlüsselungssoftware von Phil Zimmermann, unterscheidet sich aber konzeptionell erheblich von allen Vorgängerversionen: PGP Universal implementiert eine serverbasierte (proxy-artige) Lösung, die transparent und automatisch sämtliche E-Mails (oder solche für festgelegte Kommunikationspartner) ver- und entschlüsselt. Auch mit Kommunikationspartnern, die über kein Schlüsselpaar verfügen, kann man mit PGP Universal gesichert kommunizieren.

Die wichtigste Neuerung bilden sogenannte „Domain Policies“, die es ermöglichen, eine organisationsweite Security Policy zentral zu definieren und duchzusetzen. Damit ist PGP Universal insbesondere für Unternehmen und Behörden interessant. Eine Übersicht finden Sie in einem Beitrag von Dr. Rainer Gerling und Stefan Kelm in der Zeitschrift „DuD“ (10/2003).

Zum Vormerken für Interessierte: Secorvo bietet am 03.-04.12.2003 ein zweitägiges Seminar an, in dem der betriebliche Einsatz von PGP, auch der neuen Produktversion, im Detail beleuchtet wird.

1.2 Kritischer RPC-Bug

Eine neue, als sehr kritisch einzustufende Schwachstelle im RPC-Dienst der Betriebssysteme Windows NT 4.0, 2000, XP und 2003 wurde am 10.09.2003 vom Microsoft veröffentlicht. Sie erlaubt einem Angreifer, über das Protokoll Netbios durch einen Heap Overrun beliebigen Code auf dem Zielsystem auszuführen. Eine Erläuterung mit Patch findet sich im Microsoft Security Bulletin MS03-039.

Delikat: Seit dem 16.09.2003, nur sechs Tage nach Veröffentlichung, ist im Internet ein Exploit zu finden, dass diese Schwachstelle ausnutzt. Wir testeten den Angriffscode im Secorvo Security Labor: Ein Angreifer erhält damit über ein neu angelegtes Konto mit Administrationsberechtigungen vollen Zugriff auf das Zielsystem.

Nach den Erfahrungen der vergangenen Monate muss davon ausgegangen werden, dass diese Schwachstelle sehr bald auch von Würmern ausgenutzt werden wird. Ein umgehendes Einspielen des Patches ist daher dringend zu empfehlen.

1.3 Gefälschte eBay-Server

Wie am 08.09.2003 bekannt wurde, haben Betrüger einen gefälschten eBay-Webserver aufgebaut, um an die Daten von eBay-Kunden zu kommen. Der Trick: Mit einer scheinbar von eBay stammenden E-Mail versuchen sie, ihre Opfer auf den vorgeblichen eBay-Server zu locken. Tatsächlich enthält die E-Mail mit dem korrekt aussehenden Link keinen Text, sondern ein Bild – das mit einer völlig anderen URL hinterlegt ist.

1.4 Trauen Sie Ihrem Browser?

Die Aufdeckung kritischer Schwachstellen in Betriebssystemen und Anwendungen ist leider mittlerweile an der Tagesordnung. Meist handelt es sich dabei um Programmierfehler („Bugs“), die es erlauben, z. B. den Rechner zum Absturz zu bringen oder lokale Dateien auszulesen. Dass immer wieder auch konzeptionelle Sicherheitslücken entdeckt werden, deren Ursache im mangelhaften Design der Software zu finden ist, ist oft weniger geläufig.

Ein prominentes Beispiel für derartige Schwachstellen sind die vom Dartmouth PKI Lab durchgeführten Forschungen zum Thema „Web Spoofing“. Nachdem dieser Begriff bereits 1996 zum ersten Mal in der Literatur auftauchte, testeten die Forscher aus Dartmouth in den vergangenen Jahren

vor allem die gängigen Browser auf Lücken und konnten dabei beeindruckende Ergebnisse erzielen: So gelang es ihnen – unter Verwendung von JavaScript auf präparierten Webseiten – einen Mozilla-Browser so zu überlisten, dass der Benutzer glaubte, eine sichere SSL-Verbindung zu nutzen. Tatsächlich waren sämtliche Fenster, Icons und Links „gefälscht"; sogar die Eingaben auf der Tastatur wurden überwacht.

Etliche detaillierte Lösungsvorschläge der Forscher, die schon Anfang 2002 publiziert wurden, haben leider bis heute keinen Einzug in die Anwendungen gehalten.

1.5 Digitalbilder: Echt oder retuschiert?

Dass Fotos mit zunehmenden Fortschritten in der digitalen Bildbearbeitung mehr und mehr an Beweiskraft verlieren, ist offenkundig. Ein neuer Ansatz zur Rettung der Authentizität digitaler Bilder versucht nun, anhand statistischer Eigenschaften des per Wavelet-Transformation mathematisch umgeformten Bildes Originalaufnahmen von manipulierten Bildern zu unterscheiden.

Dieser Ansatz trifft auch die Steganografie: Sie steht nun vor der Herausforderung, ein Verfahren zu finden, das bei veränderten Bildern die Statistik wieder „richtet".

1.6 GSM-Verschlüsselung unter Beschuss

Vom Israel Institute of Technology (Technion) in Haifa wurde am 03.09.2003 ein Angriff auf die GSM-Verschlüsselung veröffentlicht, der effizienter ist als alle bisher publizierten Attacken auf den Kryptoalgorithmus A5. Die Methode der Forschungsgruppe um Eli Biham reiht sich ein in den Trend, bei der Kryptanalyse zusätzliche Informationen zu nutzen – in diesem Fall aus Verbindungsaufbau und Fehlerkorrektur. Merke: Ein guter Algorithmus alleine ist höchtens die „halbe Miete" – das Einsatzumfeld ist ebenso von Bedeutung.

1.7 Private Internet-Nutzung

Die private Nutzung des dienstlichen Internetzugangs ist eines der derzeit heftigst diskutierten Themen. Zwar ist die Besteuerung als „Geld werter Vorteil" vom Tisch. Doch bei erlaubter oder auch nur geduldeter privater Nutzung unterliegt der Betrieb erheblichen Einschränkungen aus Telekommunikations- (TKG) und Teledienstedatenschutzgesetz (TDDSG), da der Arbeitgeber zum geschäftsmäßigen Anbieter von Telekommunikationsdiensten wird – auch, wenn er die Leistungen unentgeltlich bereitstellt. Denn Inhalts- und Verbindungsdaten einer privaten Kommunikation genießen den strengen Schutz des Fernmeldegeheimnisses (Art. 10 GG, § 87 TKG).

Zwei aktuelle Leitfänden zu diesem Thema klären die Rechtslage und unterstützen mit Mustervereinbarungen die betriebliche Regelung: Der Leitfaden „Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz" des Bundesdatenschutzbeauftragten (14.03.2003) und der BITKOM-Leitfaden „Die Nutzung von E-Mail und Internet im Unternehmen" (21.08.2003).

2 Secorvo News

2.1 Secorvo College aktuell

Die erste Oktoberwoche ist „PKI-Woche": In einer zweitägigen Einführung in Public Key Infrastrukturen vom **06.-07.10.2003** und einem eintägigen Vertiefungsseminar PKI für Fortgeschrittene am **09.10.2003** bietet Secorvo einen vertieften Einblick aus umfassender Beratungserfahrung in die Grundlagen und ausgewählte Herausforderungen der Konzeption und des Aufbaus von PKIs.

Seit der Ankündigung von NAI im Oktober des vergangenen Jahres, die PGP-Produktlinie einzustellen, war es um PGP stiller geworden. Nun hat sich die neue PGP Corporation mit neuen Produktversionen zurückgemeldet (siehe oben).

Anfang Dezember (**03.-04.12.2003**) stellen wir in unserem Seminar „PGP & Co. Im betrieblichen Einsatz“ vor, was sich hinter OpenPGP und den aktuellen Konzepten verbirgt, wie PGP sich zum Schutz von E-Mails und zur Verschlüsselung von Dateien in der Unternehmenspraxis einsetzen lässt und was PGP von anderen PKI-Lösungen unterscheidet.

Wegen der großen Nachfrage werden wir das Fünf-Tages-Intensivseminar „Information Security Management von A(udit) bis Z(ertifizierung)“ am **03.-07.11.2003** ein drittes Mal durchführen. Das Seminar vermittelt die wesentlichen Grundlagen eines verlässlichen Sicherheitsmanagements auf technischer und organisatorischer Ebene und liefert konkrete Hilfestellungen für Konzeption und Umsetzung in der Praxis.

http://www.secorvo.de/college

2.2 „IT – Aber sicher!“

Am **30.10.2003** wird Lutz Bleyer, Leiter Zentrale Security der Fiducia AG, im Rahmen des nächsten Events der „Karlsruher IT-Sicherheitsinitiative“ (KA-IT-Si) die Security Awareness-Kampagne der Fiducia „IT – Aber sicher!“ vorstellen. Beginn 18 Uhr, anschließend „Badisches Buffet“.

2.3 „ZertiFA 2003”

Um Licht ins Dunkel des Zertifikate-Dschungels zu bringen, haben Dr. Johann Bizer und Dirk Fox, Herausgeber der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“ mit COMPUTAS, einem für hochwertige Security-Konferenzveranstaltungen bekannten Anbieter, eine neue Fachtagung konzipiert. Auf der „ZertiFA 2003“ am **10. und 11.11.2003** im Kölner Hotel Hilton werden Zertifikate und Gütesiegel von BS 7799 über BSI-Grundschutz- und Datenschutzaudits bis ITSEC- und CC-Zertifizierungen vorgestellt und vor dem Hintergrund aktueller Erfahrungsberichte diskutiert.

3 Veranstaltungshinweise

September 2003	
29.09.-02.10.	Informatik 2003 – Teiltagung Sicherheit (GI, Frankfurt)
Oktober 2003	
06.-07.10.	Public Key Infrastrukturen (Secorvo College, Karlsruhe)
09.10.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
14.-15.10.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.10.	Defense Lab (Secorvo College, Karlsruhe)
30.10.	„IT – Aber sicher!“ (KA-IT-Si, Karlsruhe)
November 2003	
03.-07.11.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
10.-11.11.	ZertiFA 2003 (Computas, Köln)
11.-13.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
18.-19.11.	Inside Windows Security (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Oktober 2003

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 10, 2. Jhrg. 2003
Stand 22. Oktober 2003

http://www.secorvo.de/security-news

Inhalt

Editorial: WYSIWY – B?

1 Security News

1.1 „U-Bahn-Spoofing" in Hamburg

1.2 Neue EU-Studien

1.3 IT-Grundschutz kompakt

1.4 Security Tools (Update)

1.5 Top 20 Security Bugs

1.6 Spam-Bounces – die Kehrseite der Medaille

1.7 Fehler in OpenSSL

1.8 Hacker stiehlt Spielequellcode

2 Secorvo News

2.1 Secorvo College aktuell

2.2 „Anti-Spam-Symposium"

3 Veranstaltungshinweise

Impressum

Editorial: WYSIWY – B?

In festem Vertrauen auf unsere Erfahrung und Aufmerksamkeit sind wir überzeugt, dass bei kompetenter Nutzung des Internet nichts passieren könne – jedenfalls nicht uns. Schließlich vertrauen wir nicht naiv auf die Gutartigkeit der E-Mail-Anhänge unbekannter Absender, selbst bei bekannten Adressen sind wir skeptisch und öffnen sie nicht. HTML-formatierte E-Mails betrachten wir grundsätzlich nur in reinem Textformat, da sie über Web Bugs heimlich Rückmeldungen an den Sender auslösen können. Spam isolieren und löschen wir nach kurzer Prüfung – die „keep me off that list"-Option geflissentlich ignorierend. Und Updates sowie Sicherheits-Patches beziehen wir nur aus verlässlicher Quelle via CD.

Auch außerhalb des Firmennetzes nutzen wir das Internet ausschließlich mit (Personal) Firewall. ActiveX- und VisualBasic-Script-Komponenten filtern wir heraus, Flash-Intros werden übersprungen, PlugIns nicht automatisch installiert. Und wenn's ums Geld geht, sind wir noch vorsichtiger: Kreditkartennummern vertrauen wir keiner Webseite an, Passwort-Login und Online-Banking gibt es nur bei SSL-Verbindungen. Dabei prüfen wir: Ist das Zertifikat gültig? Wurde es für die gewählte Webseite ausgestellt? Ist der Schlüssel lang genug?

Zwar ist das Internet so nur noch mit Einschränkung nutzbar. Die Perfidie der Angreifer haben wir dennoch unterschätzt. So gehen wir meist davon aus, dass die Konfigurationsoberfläche kein Potemkinsches Dorf ist – haben wir doch das Credo „What You See is What You Get" tief verinnerlicht.

Wer aber garantiert uns, dass der Mechanismus vieler Werbe-Banner, eine Interaktionsbox zu simulieren, uns nicht beim Homebanking die SSL-Verbindung nur vortäuscht? Dass die URL-Anzeige im Browser auch den verbundenen Server anzeigt? Dass eine E-Mail vom angegebenen Sender stammt? Sollte das World Wide Web so zum „What You See is What You Believe", werden, wäre das der Anfang vom Ende dieses effizienten Mediums.

1 Security News

1.1 „U-Bahn-Spoofing" in Hamburg

Das News-Forums Symlink dokumentierte am 06.10.2003 eine Manipulation der Infobildschirme der Hamburger U-Bahn (siehe Fotos). Hacker hatten die Texte der eingeblendeten Nachrichten abgefangen und modifiziert. Dabei machten sie sich zu Nutze, dass die in vielen U-Bahn-Waggons installierten Windows95-Systeme ihre Meldungen an bestimmten U-Bahnhöfen über ungesicherte WLAN-Verbindungen beziehen. Auch wenn diese Aktion sicherlich mehr Unterhaltungswert als Gefährdungspotenzial besitzt, dokumentiert sie die inhärenten Sicherheitsprobleme heutiger WLAN-Lösungen.

1.2 Neue EU-Studien

Die im Juli 2003 von der EU-Kommission vorgelegte Studie "Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview" kommt zu dem Ergebnis, dass sich das Gleichgewicht zwischen Privatsphäre einerseits und Sicherheit andererseits durch moderne Kommunikationstechniken und staatliche Reaktionen auf Kriminalität und Terrorismus zu Ungunsten des individuellen Datenschutzes verschoben hat. Zugleich wurden die Vorbehalte hinsichtlich des Schutzes der Privatsphäre und der Sicherheit als Haupthindernis für die Akzeptanz von e-Commerce-Angeboten identifiziert. Die Studie untersuchte insbesondere die Auswirkungen der neuen Kommunikationstechnologien, z. B. die „elektronischen Spuren", die man im Internet oder beim Telefonieren mit dem Handy hinterlässt und die für andere Zwecke als die Strafverfolgung missbraucht werden könnten.

In einer zweiten, gerade fertig gestellten Studie trägt die europäische Kommission der in Art. 12 der EG-Richtlinie zu elektronischen Signaturen geforderten Prüfung der „Durchführung dieser Richtlinie" Rechnung.

Der Prüfbereicht "The legal and market aspects of electronic signatures" kommt zu dem Ergebnis, dass die Richtlinie in fast allen Mitgliedsstaaten (sowie den Beitrittskandidaten) umgesetzt wurde, variierende Interpretationen einzelner Artikel jedoch zu teils großen Unterschieden in der Anwendung sowie der nationalen Gesetzgebung geführt haben. Er identifiziert eine Reihe von Problemfeldern, die auf EU-Ebene Beachtung finden sollten, um die gewünschte Harmonisierung elektronischer Signaturen zu erreichen. Stefan Kelm, Security Consultant bei Secorvo, war als Autor an der Erstellung dieser Studie beteiligt.

1.3 IT-Grundschutz kompakt

Am 18.09.2003 wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) der „Leitfaden IT-Sicherheit" (IT-Grundschutz kompakt) publiziert (415 kB). In der 48-seitigen Broschüre werden die häufigsten Versäumnisse und die wichtigsten Sicherheitsmaßnahmen überschaubar und verständlich dargestellt. Ergänzt wird der Leitfaden durch eine Einführung zum IT-Grundschutzhandbuch sowie kurze Checklisten für die wichtigsten Bereiche.

1.4 Security Tools (Update)

Seit dem 01.10.2003 ist v2.5 beta 38 von Cain & Abel verfügbar. Das Multifunktionstool, welches viele Angriffsmöglichkeiten wie ARP-Spoofing und eine Reihe von Passwortcrackern enthält, bietet nun wie L0phtCrack die Möglichkeit, gesniffte SMB-Hashes direkt an den Passwortcracker zu übergeben. Dadurch können schwache Benutzerpassworte bei NT 4.0 oder Windows 2000 im NTLM-Standard-Modus innerhalb von Stunden geknackt werden.

Der verbreitete Portscanner Nmap, der ständig weiterentwickelt wird, liegt seit dem 06.10.2003 in Version 3.48 vor und enthält nun über 650 Signaturen zur Erkennung von Diensten und Betriebssystemen.

1.5 Top 20 Security Bugs

Die von SANS in Zusammenarbeit mit internationalen Unternehmen erstellte und jährlich aktualisierte Liste der 20 häufigsten Sicherheitsschwächen unter Windows (10) und Unix/Linux (10) wurde am 08.10.2003 publiziert. An dieser Fassung haben das US-Department of Homeland Security sowie Sicherheitsbehörden aus Großbritannien und Kanada mitgewirkt.

1.6 Spam-Bounces – die Kehrseite der Medaille

Nicht nur Würmer à la Sobig verwenden gefälschte, aber real existierende E-Mail-Absender (vgl. Security News 8/2003), sondern auch immer mehr Spam-E-Mail-Versender segeln unter falscher Flagge. Da sich unter abertausenden Spam-Adressaten viele finden, die gar nicht existieren, gerade in Urlaub sind oder sich über die Spam-Mail beschwerden wollen, landen Abwesenheitsnotizen, Fehlermeldungen („Bounces“) und Beschwerden in der Mailbox des vermeintlichen Absenders – zumindest so lange, bis diese überquillt.

Am 09.10.2003 brachen die Mail-Server des zu QSC gehörenden Providers Ginko unter der Last solcher Spam-Bounces ein.

1.7 Fehler in OpenSSL

Am 30.09.2003 wurde eine mit hohem Risiko bewertete Schwachstelle im ASN.1-Parser publiziert, der sich in allen auf OpenSSL basierenden Implementierungen findet: Beim Einlesen manipulierter Zertifikate im Rahmen der SSL/TLS-Client-Authentifikation treten Pufferüberläufe auf, die einen Denial-of-Service Angriff auf SSL-Server ermöglichen. Ob auch die Ausführung von beliebigem Code möglich ist, ist noch unklar.

Besonders schwer wiegt der Fehler dadurch, dass die Überläufe auch dann auftreten, wenn ein bösartiger Client sein Zertifikat unverlangt sendet. Wer OpenSSL im Einsatz hat, sollte daher umgehend auf die entsprechend gesicherten Versionen 0.9.6k bzw. 0.9.7.c aktualisieren.

Die zu dieser Sicherheitslücke publizierten Advisories fördern nebenbei zu Tage, in wie vielen kommerziellen Produkten dieser Code enthalten ist. Die illustere Liste reicht von Cisco Routern und PIX Firewalls über den Apple Macintosh bis zu Novell.

OpenSSL ist nicht die einzige Open Source Crypto-Software, die aktuelle Sicherheitslücken vermeldet: Auch zu den beiden Secure-Shell Implementierungen LSH und OpenSSH wurden seit Mitte September mehrere Advisories publiziert.

1.8 Hacker stiehlt Spielequellcode

Üblicherweise erfährt die Öffentlichkeit wenig über erfolgreiche Einbrüche von Hackern und den angerichteten Schaden. In einem nun bekannt gewordenen Fall war dies anders: Ein Hacker, der möglicherweise eine Sicherheitslücke in Outlook nutzte, konnte um den 19.09.2003 Zugriff auf den Quellcode des noch unveröffentlichten zweiten Teils des populären Spiels Half-Life erlangen und verbreitete den Code anschließend im Internet.

Im Verlauf des vom Hersteller Valve Software bestätigten Vorfalls wurden von dem oder den Angreifern u. a. „Keystroke-Logger“, die per Software alle Tastendrücke des Benutzers aufzeichnen, auf Rechnern von Valve-Mitarbeitern installiert. Damit ein Spieler, der den internen Aufbau des Spiels kennt, keinen unfairen Vorteil daraus ziehen kann, müssen nun Teile von Half-Life 2 umgeschrieben werden. Dadurch wird sich das Erscheinen des Spiels über das für die Branche so wichtige Vorweihnachtsgeschäft hinaus verzögern.

Das Beispiel zeigt, dass die veröffentlichten Sicherheitsschwächen wichtiger Anwendungen (wie Outlook oder Internet Explorer) und Betriebssysteme keineswegs ein „theoretisches“ Problem darstellen, sondern zu erheblichen, wenn auch oft unveröffentlichten Schäden führen.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminar „IT-Security Management“ – buchbar als zweitägiges Intensiv- oder einwöchiges Grundlagenseminar (**03.-04.11.** bzw. **03.-07.11.2003**) – führt in Aufbau, Prozesse und Strukturen des Sicherheitsmanagements ein. Am Beispiel eines fiktiven Unternehmens werden Standards und rechtliche Rahmenbedingungen konkret.

Eine aktuelle „Standortbestimmung“ der IT-Sicherheit leistet das Seminar „IT-Sicherheit heute“ (**11.-13.11.2003**), das sich als inhaltliche Auffrischung und Einstieg in das Themengebiet eignet.

Nach den Würmer- und Virenattacken der vergangenen Monate aktueller denn je: Die sichere Konfiguration des Betriebssystems Windows (NT/2000/XP). Insider-Einblicke gewährt das Seminar „Inside Windows Security“ am **18.-19.11.2003**.

Hilfestellung für die Einführung von E-Mail-Verschlüsselung im Unternehmen und viele Tipps aus der Beratungspraxis bietet das Seminar E-Mail-Sicherheit am **25.-26.11. 2003**.

2.2 „Anti-Spam-Symposium“

Mit einem „Anti-Spam-Symposium“ am **18.-19.11.2003** greift die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) die Diskussion des angemessenen Umgangs mit unerwünschten E-Mail-Nachrichten („Spam“) in Unternehmen auf. Namhafte Referenten werden diese Frage aus rechtlicher, technischer und organisatorischer Perspektive beleuchten. Das Symposium, für das Microsoft als Sponsor gewonnen werden konnte, richtet sich an alle mit Abwehrmaßnahmen gegen Spam befassten Verantwortlichen in Unternehmen und Behörden – IT-Leiter, Management, Techniker und Datenschutzbeauftragte (Heise-Ticker).

Programm und Anmeldung unter
http://www.anti-spam-symposium.de

3 Veranstaltungshinweise

Oktober 2003	
30.10.	„IT – Aber sicher!“ (KA-IT-Si, Karlsruhe)
November 2003	
03.-04.11.	IT-Security Management (Secorvo College, Karlsruhe)
03.-07.11.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
10.-11.11.	ZertiFA 2003 (Computas, Köln)
11.-13.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
18.-19.11.	Anti-Spam-Symposium (KA-IT-Si, Karlsruhe)
18.-19.11.	Inside Windows Security (Secorvo College, Karlsruhe)
24.-25.11.	IT Incident Management & Forensik (GI, Stuttgart)
25.-26.11.	E-Mail-Sicherheit (Secorvo College, Karlsruhe)
Dezember 2003	
03.-04.12.	PGP & Co. im Betrieb (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News

November 2003

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 11, 2. Jhrg. 2003
Stand 21. November 2003

http://www.secorvo.de/security-news

Inhalt

Editorial:
Wer misst, misst Mist

1 Security News

1.1 Neuer BfD im Amt

1.2 EU-Spam illegal

1.3 (K)eine Linux-Backdoor

1.4 Noch mehr fehlerhafte ASN.1-Dekodierer

1.5 Macht Microsoft ernst?

1.6 VPN Key Cracker

1.7 Happy Birthday, Malware

1.8 Stichwort: „Regression Bug“

1.9 „RFID-Wanzensucher“

1.10 Bluetooth Security

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Whitepaper Information Security Management

2.3 ISIS-MTT Siegel für Entrust Authority™

2.4 Video „E-Mail Security“

3 Veranstaltungshinweise

Impressum

Editorial: Wer misst, misst Mist

Der vom allgegenwärtigen Spardruck ausgelöste Trend, Leistungen und Kostentreiber im Unternehmen durch Kennzahlen transparent zu machen, hat mit Balanced Scorecards und Benchmarks nach dem Management die IT erfasst.

Nun ist auch die IT-Sicherheit in den Fokus des „Erbsenzählens“ geraten. Zunächst einmal ist das nicht besonders verwunderlich. Denn IT-Sicherheit kostet Geld, und je besser sie funktioniert, desto weniger sichtbar ist sie – je schlechter sie funktioniert, desto kritischer wird sie beäugt. In beiden Fällen stehen die Kosten unter Rechtfertigungsdruck.

Hinzu kommt ein der Unternehmensleitung nicht immer leicht verständlich zu machendes, aber elementares Faktum: IT-Sicherheit ist kein „binärer Zustand“ – die beliebte „Sind wir sicher?“-Frage konnte noch kein IT-Sicherheitsverantwortlicher eindeutig mit „Ja“ oder „Nein“ beantworten (jedenfalls nicht ohne rot zu werden).

Die Wirklichkeit liegt – wie so oft – zwischen den Extremen. Wo aber liegt sie genau? Sind wir gut genug, um den Anforderungen von KontraG, GmbHG und Basel II zu genügen? Tun wir das Erforderliche? Entsprechen unsere Maßnahmen dem „Stand der Technik“? Wirken unsere Maßnahmen? Und nicht zuletzt: Werden wir besser?

Die Fragen sind nicht neu. Aber bisher haben wir es uns geleistet, sie unbeantwortet zu lassen. Den Kostendruck sollten wir nun als Chance nutzen, die IT-Sicherheit über Metriken zu einer Entwicklungsgröße im Unternehmen zu machen. Das ist eine anspruchsvolle Aufgabe, denn es fehlt an akzeptierten Messgrößen und Bewertungsschemata. Immerhin gibt es Beispiele, und erste Normierungsversuche, wie die jüngsten Publikationen des NIST und der CESG zeigen. Bei der Umsetzung sollten wir jedoch immer Einstein im Kopf behalten:

Nicht alles, was zählt, kann gezählt werden,
und nicht alles was gezählt werden kann, zählt.
Albert Einstein (1879-1955)

1 Security News

1.1 Neuer BfD im Amt

Am 14.11.2003 wurde nach langem politischen Ringen hinter den Kulissen und mit mehrmonatiger Verzögerung der von den Grünen vorgeschlagene ehemalige stellvertretende Hamburgische Datenschutzbeauftragte Peter Schaar vom Bundestag als Nachfolger von Joachim Jacob zum Bundesbeauftragten für den Datenschutz (BfD) gewählt.

Dafür, dass ihm die Arbeit nicht ausgeht, wollen die Parteikollegen sorgen: Nach dem rechtspolitischen Sprecher der Bundestagsfraktion, Jerzy Montag, soll geprüft werden, Verschlüsselungsschlüssel zukünftig beim BfD zu hinterlegen.

1.2 EU-Spam illegal

Mit Artikel 13 („Unerbetene Nachrichten“) der EU-Datenschutzrichtlinie für elektronische Kommunikation vom 12.07.2002 (Amtsblatt der EG L 201/47, 31.07.2002) wurden per E-Mail, Fax oder SMS verschickte Nachrichten zum Zweck der Direktwerbung für illegal erklärt, wenn sie ohne „Opt-Out“-Hinweis oder unter Verschleierung der Absenderidentität gesendet werden. Die Richtlinie fordert sogar – sofern keine Kundenbeziehung besteht – aktives „Opt-In“ als Voraussetzung. Die Richtlinie war bis zum 31.10.2003 in nationales Recht umzusetzen. Die Bundesregierung verpasste (auch) diesen Termin – damit gilt sie jetzt als übergeordnetes Recht.

Allerdings dürfte die Richtlinie ein „zahnloser Tiger“ bleiben: Spammer agieren – sofern überhaupt feststellbar – fast immer aus Ländern außerhalb der EU.

1.3 (K)eine Linux-Backdoor

Am 05.11.2003 entdeckte eine Gruppe von Linux-Kernel-Entwicklern, dass jemand versucht hatte, eine Hintertür in die 2.6er Entwicklungsversion des Linux-Kernels einzubauen. Dem Quellcode wurden zwei Programmzeilen hinzugefügt, die es einem normalen Benutzer ermöglicht hätten, Administrationsberechtigung zu erlangen.

Die Änderung betraf allerdings nicht die „heilige“ Kernel-Source-Referenz, sondern die an anderer Stelle exportierten Dateien im Concurrent Versioning System (CVS). Nach Angaben von Bitkeeper, dem Hersteller der Kernel-Source-Verwaltungssoftware, wäre eine Änderung des Referenzcodes unverzüglich festgestellt worden.

1.4 Noch mehr fehlerhafte ASN.1-Dekodierer

Dass auch Sicherheitssoftware Opfer von Fehlern in gemeinsam genutzten Funktionsbibliotheken sein kann, zeigen mehrere Schwachstellen, die kürzlich – wie in den Security News 10-2003 berichtet – in OpenSSL, mittlerweile aber auch in verschiedenen anderen SSL- und S/MIME-Produkten gefunden wurden.

Quelle dieser Bugs ist die „Abstract Syntax Notation“ (ASN.1), die beschreibt, wie z. B. X.509-Zertifikate und geschützte S/MIME-Nachrichten für den Transport zu kodieren sind. Fehler in der ASN.1-Kodierung können bei zahlreichen Implementierungen zu Pufferüberläufen oder Denial-of-Service-Angriffen führen. Da diese Schwachstellen innerhalb von verbreiteten Krypto-Bibliotheken entdeckt wurden, sind weit mehr Hersteller von diesem Problem betroffen, als ursprünglich berichtet. Entsprechend aktualisierte Listen findet man beim CERT/CC.

1.5 Macht Microsoft ernst?

Die Anzeichen mehren sich, dass Microsoft künftig tatsächlich Sicherheit über Funktionalität stellen wird: In einer E-Mail an BugTraq warnt Microsoft-Mitarbeiter Michael Howard, Co-Autor von „Writing Secure Code“, am 12.11.2003, dass die sicherere Grundkonfiguration des angekündigten Windows XP SP 2 zu fehlerhaftem Verhalten von Anwendungen führen kann.

1.6 VPN Key Cracker

Dass eine Schwäche des Internet Key Exchange Protokolls (IKE) eine Kompromittierung des häufig in IPsec-VPNs verwendeten „Preshared Key“ ermöglicht, ist seit April 2003 bekannt. Inzwischen gibt es auch Tools, die derartige Angriffe unterstützen, wie z. B. ikecrack. Seit Version 2.5 beta36 hat auch das beliebte Multifunktions-Sniff- und -Crack-Tool Cain eine solche Funktion, den „IKE Aggressive Mode Pre-Shared Keys Cracker“, integriert.

Seit dem 07.11.2003 ist der Scanner ike-probe verfügbar, der prüft, ob ein VPN-Gateway anfällig für diese Attacke ist.

1.7 Happy Birthday, Malware

Genau 20 Jahre war es am 03.11.2003 her, dass Fred Cohen im Rahmen seiner Doktorarbeit den ersten experimentellen Computervirus entwickelte. Was damals noch als theoretisches Hirngespinst erscheinen konnte, hat sich in der Zwischenzeit zur realen Plage und Bedrohung entwickelt und Anti-Virus-Software als ganz neue Produktklasse entstehen lassen.

Microsoft hat nun härtere Bandagen angelegt und am 05.11.2003 5 Mio. US $ Kopfprämien für Hinweise ausgesetzt, die zur Ergreifung der Viren-Entwickler von Blaster und Sobig führen. Angeblich häufen sich derzeit in Bagdad die Selbstanzeigen...

1.8 Stichwort: „Regression Bug“

„Regression Bug“ nennt es der Softwareentwickler, wenn sich bei einer beabsichtigten Verbesserung ein neuer oder gar ein alter, eigentlich schon behobener Fehler wieder einschleicht.

Auf ein Paradebeispiel dafür hat am 11.11.2003 Microsoft hingewiesen: Wer das am 09.09.2002 veröffentlichte Service Pack 1 (SP 1) zum Internet Explorer 6 nach dem am 20.06.2003 erschienenen SP 4 für Windows 2000 installiert, führt damit einen schwerwiegenden Fehler bei der Auswertung von SSL-Serverzertifikaten wieder ein, der einem SSL-Server die Ausstellung weiterer gültiger Zertifikate ermöglicht.

1.9 „RFID-Wanzensucher“

Am 06.11.2003 wurde der FoeBuD e.V., bekannt durch die jährliche Verleihung der BigBrother Awards für „Datenkraken“, von der Stiftung bridge mit einen Ideenpreis ausgezeichnet. Mit dem Preisgeld von 15.000 € wird nun ein Warngerät zum Aufspüren von RFID (Radio Frequency Identification) Transponderchips entwickelt.

Dahinter verbirgt sich ein ernsthaftes Datenschutzproblem: RFID Chips, die es erlauben, berührungslos einen eindeutigen ID-Code auszulesen, sind inzwischen so miniaturisiert, dass sie mit bloßem Auge kaum noch zu erkennen sind. Sie werden, auf Verpackungen oder Waren befestigt, von vielen als die „Wunderwaffe“ zur weiteren Rationalisierung von Logistik und Warenwirtschaft angesehen. Einmal mit einer Person in Verbindung gebracht, eröffnen sich faszinierende Möglichkeiten der Profilerstellung – vom Einkaufsverhalten im Laden (Bewegungsmuster) bis hin zur Verfolgung des Lebenszyklus einer Verpackung. Der Drang zum raschen Einsatz dieser neuen Technik könnte dabei wieder einmal der Beherrschung von Missbrauchsmöglichkeiten davoneilen (FoeBuD-Positionspapier vom 19.11.2003).

1.10 Bluetooth Security

Adam Laurie veröffentlichte am 11.11.2003 in BugTraq eine kurze, vierseitige Übersicht über aktuelle Angriffe und sicherheitsrelevante (Implementierungs-) Fehler in Bluetooth-Geräten. Die Anfälligkeit für Backdoor-Angriffe, SNARF-Attacken und das sogenannte „Bluejacking“ wies er für mehrere verbreitete Handy-Typen nach.

Zwar verfügt Bluetooth über zahlreiche, konzeptionell vergleichsweise gute Sicherheitsmechanismen; deren Wirksamkeit hängt allerdings in der Praxis von der Qualität der jeweiligen Implementierung ab.

2 Secorvo News

2.1 Secorvo College aktuell

Anfang November 2003 ist das Seminarprogramm von Secorvo College für das erste Halbjahr 2004 erschienen. Im Seminarkalender 2004 finden Sie eine ganzjährige Terminübersicht. In das Jahr 2004 startet Secorvo College mit zwei zentralen Themen: Information Security Management am **19.-23.01.2004** (auch als zweitägiges Seminar buchbar) und Public Key Infrastrukturen (PKI) vom **27.-28.01. 2004** – mit zusätzlichem Vertiefungstag am **29.01.2004**.

2.2 Whitepaper Information Security Management

Einen Überblick über die aktuelle Fassung des britischen Standards zur Informationssicherheit, BS 7799, gibt das am 06.11. 2003 erschienene White Paper von Jörg Völker: BS 7799 – Von „Best Practice“ zum Standard (pdf, 376 kB).

2.3 ISIS-MTT Siegel für Entrust Authority™

Nach eingehenden Tests im offiziellen ISIS-MTT-Prüflabor von Secorvo wurde dem „Entrust Authority™ Security Manager 7.0 for Windows" des kanadischen Unternehmens Entrust am 05.11.2003 als weltweit erstem Produkt das ISIS-MTT-Siegel in der Produktklasse „CA Server“ verliehen. Damit ist nun von unabhängiger Seite bestätigt, dass (und wie) Anwender mit dieser Software ISIS-MTT-konforme PKI-Zertifikate und Sperrlisten ausstellen können.

2.4 Video „E-Mail Security“

Das von Secorvo entwickelte Video „E-Mail Sicherheit“ steht nun auch, vertont mit einem „Native Speaker“, in englischer Sprache zur Verfügung. Diese Version ist als Intranet-Lizenz erhältlich und kann über die Secorvo-Webseiten bestellt werden.

3 Veranstaltungshinweise

November 2003	
25.-26.11.	E-Mail-Sicherheit (Secorvo College, Karlsruhe)
Dezember 2003	
03.-04.12.	PGP-Lösungen im Betrieb (Secorvo College, Karlsruhe)
08.-09.12.	IsSec 2003 (Computas, Berlin)
08.-10.12.	IT-Security- und Risk-Management (ZfU, Zürich)
Januar 2004	
19.-23.01.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
20.-21.01.	Einführung in die Praxis des betr. DSB (Euroforum, München)
27.-28.01.	Public Key Infrastrukturen (Secorvo College, Karlsruhe)
29.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2004	
03.-04.02.	DFN-CERT Workshop "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Dezember 2003

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 12, 2. Jhrg. 2003
Stand 23. Dezember 2003

http://www.secorvo-security-news.de

Inhalt

Editorial: Patchwork

1 Security News

1.1 CERT für den Mittelstand

1.2 Biometrie-Fiasko

1.3 Murphy hat doch recht

1.4 Lücke in Zertifikatskette

1.5 Neue Version des GSHB

1.6 Einbruch bei Debian

1.7 Satelliten-Dialer

1.8 Bürgerkarte in Österreich

1.9 VDEW setzt auf ISIS-MTT

1.10 ENISA beschlossen

2 Secorvo News

2.1 Secorvo College aktuell

2.2 DuD elektronisch

2.3 Video “trojan horse”

3 Veranstaltungshinweise

Impressum

Editorial: Patchwork

Was haben aktuelle Softwareversionen und neumodische Jeans gemeinsam? Ganz einfach: Beide sind nur mit Löchern echt.

Mittlerweile haben wir uns daran gewöhnt: Ein neues Programm ist ein unsicheres Programm. Nicht etwa, weil es nicht funktioniert oder ständig abstürzt – das war früher – sondern weil es mit Sicherheitslöchern ausgeliefert wird. Erst nach mehrmaligen Nachbesserungen reift es – Patch für Patch – zu einer Programm- oder Betriebssystemversion, die mit gutem Gewissen für den Produktivbetrieb frei gegeben werden kann.

Diese Entwicklung hat dazu geführt, dass sich die „Organisation der Flicken“ (Patchmanagement) zu einer neuen Disziplin der IT-Security gemausert hat, der das amerikanische NIST im vergangenen Jahr sogar eine Special Publication (SP 800-40) widmete. Keine einfache Disziplin. Nicht genug damit, dass ein rechtzeitiges Einspielen von Patches die Kenntnis von Sicherheitsloch und Flicken voraussetzt: Ohne Tests sollte ein Patch nicht in den operativen Betrieb „entlassen“ werden. Nicht selten verursachen Patches unerwünschte Seiteneffekte – es kann passieren, dass von systemspezifischen Bibliotheken abhängige Anwendungsprogramme anschließend den Dienst versagen. Bei einigen Software-Anbietern erlischt zudem die Betriebsgarantie, sobald das System unter modifiziertem Betriebssystemcode betrieben wird. Und die Zeit zwischen der Entdeckung eines Programmfehlers und der Verfügbarkeit eines „Exploits“ im Internet schrumpft kontinuierlich. Der Patch-Bezug selbst ist auch nicht frei von Fallen: Zahlreiche Empfänger sind den jüngsten, vermeintlich von Microsoft stammenden „Patch-E-Mails“ auf den Leim gegangen.

Zwar wissen wir nicht, ob die Sicherheits-Löcher wie die der Jeans kunstvoll und mit Vorsatz hineingerissen wurden. In einem unterscheiden sich Jeans und Programme jedoch sicher: Die Löcher in letzteren sind keine vorübergehende Modeerscheinung.

1 Security News

1.1 CERT für den Mittelstand

Computer Notfallteams (CERTs) existieren – auch in Deutschland – bereits seit einem Jahrzehnt. Meist richten sich die Dienstleistungen dieser CERTs, wie etwa die Bearbeitung von Sicherheitsvorfällen oder die Herausgabe von Sicherheitsbulletins, an größere Unternehmen. Auch Behörden und Forschungseinrichtungen betreiben eigene Notfallteams.

Bislang nicht bedient wurden jedoch klein- und mittelständische Unternehmen; dies hatte vor allem finanzielle Gründe. Diesem Umstand trug jetzt der Branchenverband BITKOM Rechnung: Am 09.12.2003 entließ er ein von einer Tochtergesellschaft getragenes Notfallteam für den Mittelstand, kurz Mcert, in den Echtbetrieb. Für eine Jahresgebühr ab € 50 (Basic) oder etwas individueller ab € 300 (Professional) stellt das Mcert Kunden z. B. Warnmeldungen über Software-Schwachstellen zur Verfügung. Zwar unterscheidet sich die Beispielmeldung kaum von den bis heute kostenlos verfügbaren Angeboten anderer CERTs (DFN-CERT, RUS-CERT, etc.), ein CERT mit klarem Mittelstands-Fokus wurde jedoch schon lange erwartet.

1.2 Biometrie-Fiasko

Am 27.11.2003 veröffentlichte das BSI den Abschlussbericht des Projekts BioFace, in dessen Verlauf vier verschiedene Gesichtserkennungssysteme beim BKA getestet wurden. Das ernüchternde Ergebnis: die Falsch-Rückweisungs-Rate (FRR) lag zwischen 64 % und 99,7 %. Das Urteil: Für einen Einsatz bei der Zutrittskontrolle „in keiner Weise akzeptabel“.

Ungeachtet solcher technischen Resultate haben just am selben Tag die Innen- und Justizminister der EU die Integration eines Chips in Visa und Aufenthaltstitel beschlossen – auf dem zukünftig Gesicht und Abdrücke zweier Finger gespeichert werden.

1.3 Murphy hat doch recht

Am 26.11.2003 führte eine für extrem unwahrscheinlich gehaltene Kette von Ereignissen zum ersten „unbeabsichtigten Distributed Denial-of-Service Angriff“ auf große Teile des europäischen DNS.

Die Chronologie: Anfang November wurde die Nord-Route des Transatlantik-Unterseekabels TAT-14 unterbrochen. Während der mehrwöchigen Reparaturarbeiten trat am 25.11.2003 auch bei der redundanten Süd-Route des Kabels ein Kabelbruch auf. Dadurch wurden die Europa-Verbindungen des amerikanischen Providers above.net gestört. Als dann am 26.11.2003 die Auto-Update Funktion der verbreiteten Personal-Firewall Software ZoneAlarm nach dem Server des Herstellers Zone Labs suchte, warteten europäische DNS-Server vergebens auf eine Antwort aus den USA – denn die DNS-Server von Zone Labs sind über above.net angebunden. Die Last der in kurzen Abständen vieltausendfach wiederholten DNS-Anfragen zwang kurz danach verschiedene DNS-Server in die Knie – ein neuer Beleg für die Unumstößlichkeit von Murphy’s Law.

Zone Labs wurde übrigens unabhängig von diesen Ereignissen am 15.12. vom Firewall-Marktführer Check Point übernommen.

1.4 Lücke in Zertifikatskette

Ab dem 07.01.2004 kann es zu Problemen mit SSL-Zertifikaten kommen, die von der VeriSign International Server CA – Class 3 ausgestellt wurden. Grund: Die Gültigkeit des Zertifikats einer unterhalb der VeriSign-Root-CA operierenden „intermediate CA“ läuft ab. Zwar hat VeriSign bereits 2001 auf dieses Problem hingewiesen und das Zertifikat bis 2011 verlängert. Das nun ablaufende Zertifikat befindet sich jedoch noch immer auf vielen Clients, vor allem Internet-Browsern. Das Problem lässt sich Server-seitig durch Übermitteln der neuen Zertifikatskette beim Verbindungsaufbau oder Client-seitig durch Download des neuen CA-Zertifikats beheben.

1.5 Neue Version des GSHB

Am 16.12.2003 erschien im Bundesanzeiger-Verlag die 5. Ergänzungslieferung zum IT-Grundschutzhandbuch des BSI. Darin wurden einige der Bausteine aktualisiert und Bausteine zu Outsourcing, IIS, Apache Webserver, Exchange/Outlook 2000 und der Archivierung von Daten ergänzt. Die Online-Version des neuen GSHB wird Ende Januar 2004 verfügbar sein.

Außerdem wurden zum 01.12.2003 das Prüfschema zur Durchführung einer Zertifizierung nach IT-Grundschutz, die Aufgaben des Zertifizierers und das Lizensierungsschema für IT-Grundschutz-Auditoren überarbeitet.

1.6 Einbruch bei Debian

Am 21.11.2003 wurde eine Kompromittierung verschiedener Server des Linux-Distributionsprojekts Debian entdeckt. Die Rekonstruktion des Vorfalls ergab, dass die Angreifer sich mit einem abgehörten Passwort eines Debian-Entwicklers auf einer Maschine anmeldeten und sich anschließend mit einem lokalen Root-Exploit Superuser-Rechte verschafften.

Hauptursache: Nachlässiges Patchmanagement. Denn die vom Root-Exploit ausgenutzte Sicherheitslücke im Linux-Kern war seit September bekannt und in Entwicklerversionen des Kernels schon eliminiert, wurde aber erst nach dem Vorfall im Kernel 2.4.23 beseitigt und auf den Debian-eigenen Servern gestopft.

1.7 Satelliten-Dialer

Mit ungebremster Kreativität legen sich die Dialer-Anbieter ins Zeug. Wie auf der Informationsseite dialerschutz.de ausführlich dargestellt, werden inzwischen sogar Verbindungen über Satelliten (Vorwahl 0088) von Dialer-Programmen genutzt. Die Kosten liegen bei gut 3 € pro Minute.

Mit Wirkung vom 14.12.2003 erklärte die RegTP daher Dialer, die nicht die registrierungspflichtige Vorwahl (0)9009 nutzen, als illegal: Für den geprellten „Nutzer“ entfällt damit die Zahlungspflicht.

1.8 Bürgerkarte in Österreich

Was in vielen europäischen Ländern noch immer ein Wunschtraum ist, soll in Österreich jetzt Wirklichkeit werden: die Einführung einer digitalen Bürgerkarte, mit der landesweit Behördengänge online und in abgesicherter Form erledigt werden können.

Das Konzept der Bürgerkarte genügt den Anforderungen des österreichischen Signaturgesetzes, gestattet jedoch explizit, dass „neue Speichermedien wie etwa USB-Tokens oder Handy-SIMs ebenfalls bürgerkartenfähig sein können.“ Es wurde bewusst darauf verzichtet, die in der Praxis noch immer wenig verbreiteten evaluierten „sicheren Signaturerstellungseinheiten“ zu fordern. Die Anerkennung derartiger elektronischer Signaturen durch andere EU-Mitgliedsstaaten könnte zwar daran scheitern (wie jüngst in der Studie der EU-Kommission erläutert), der praktische Nutzen der Karte steigt damit jedoch erheblich.

1.9 VDEW setzt auf ISIS-MTT

Am 01.09.2003 haben die sechs Spitzenverbände der deutschen Stromwirtschaft unter Führung des VDEW in einer gemeinsamen Erklärung die Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr innerhalb der Branche festgelegt. Mit Blick auf die Interoperabilität setzt das VEDIS Projekt dabei auf eine X.509-PKI und das Austauschformat S/MIME in der Ausprägung nach ISIS-MTT.

1.10 ENISA beschlossen

Das EU-Parlament hat am 20.11.2003 die Einrichtung einer Europäischen Agentur für Netzwerk- und Informationssicherheit (ENISA) beschlossen. Schon im Januar soll die zunächst auf fünf Jahre geplante und mit einem Budget von € 24,3 Mio. ausgestattete Behörde die Arbeit aufnehmen. Sitz und Besetzung sind noch umstritten.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminarangebot von Secorvo College startet im Januar mit dem fünftägigen Intensivseminar „Information Security Management von A(udit) bis Z(ertifizierung)“ (**19.-23.01.2004**), dessen erste beiden Tage (**19.-20.01.2004**) auch separat gebucht werden können. Konkretisiert werden die rechtlichen Anforderungen und Standards am Beispiel eines fiktiven Unternehmens.

Das Seminar „Public Key Infrastrukturen (PKI)“ (**27.-28.01.2004**) führt in Grundlagen, Aufbau und Organisation von Schlüsselinfrastrukturen ein – vor dem Hintergrund der Erfahrung von Secorvo aus zahlreichen PKI-Projekten. Für Experten folgt am **29.01.2004** eine eintägige Vertiefung („PKI für Fortgeschrittene“).

Im Februar (**10.-11.02.2004**) werden im „Live Hacking Lab“ spektakuläre und trickreiche Angriffe auf verbreitete Systeme und Anwendungen durchgeführt und analysiert.

2.2 DuD elektronisch

Zukünftig wird es die Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“ auch in digitaler Form geben. In den Genuss einer pdf-Fassung des Jahrgangs 2003 kommt vorab jeder, der die DuD bis zum **31.01.2004** über Secorvo mit einem speziellen Bestellformular abonniert.

2.3 Video “trojan horse”

Aufgrund des großen Erfolgs des viel gelobten Videos „E-Mail-Sicherheit“ und zahlreicher Anfragen wird ab Februar 2004 auch das Video „Trojanische Pferde“ in einer grundlegend überarbeiteten Fassung als Flash-Video in deutscher und englischer Sprache (mit „Native Speaker“) erhältlich sein. Beide wurden bereits von der Linde AG und der T-Systems als Unternehmenslizenz für den Einsatz im Intranet erworben.

3 Veranstaltungshinweise

Dezember 2003	
24.12.	Bescherung
Januar 2004	
19.-20.01.	IT-Security Management (Secorvo College, Karlsruhe)
19.-23.01.	Information Security Management (Secorvo College, Karlsruhe)
20.-21.01.	Einführung in die Praxis des betr. DSB (Euroforum, München)
27.-28.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
29.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2004	
03.-04.02.	Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
10.-11.02.	Live Hacking Lab (Secorvo College, Karlsruhe)
März 2004	
02.-03.03.	Lotus Notes Security (Secorvo College, Karlsruhe)
09.-10.03.	Einführung in die Praxis des betr. DSB (Euroforum, München)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News

Januar 2004

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 1, 3. Jhrg. 2004
Stand 27. Januar 2004

http://www.secorvo-security-news.de

Inhalt

Editorial: Paradigmatisch

1 Security News

1.1 Viren „prosaisch“

1.2 Zertifikatskettenlücke II

1.3 Sicherheitslücke Backup

1.4 11. DFN-CERT Workshop

1.5 Microsoft-Tool reinigt Office-Dokumente

1.6 ASN.1 zum Dritten...

1.7 MBSA 1.2 in Deutsch

1.8 BDSG-Übergangsfrist

2 Secorvo News

2.1 Secorvo College aktuell

2.2 PKI in Windows XP/2003

2.3 SSN – der 2. Jahrgang

3 Veranstaltungshinweise

Impressum

Editorial: Paradigmatisch

Die Paradigmen der Informatik sind zahlreich. Ihre Volatilität aber leider hoch: Kein Jahr, in dem nicht ein neuer vermeintlicher „Paradigmenwechsel“ die Gazetten erobert. Dabei lohnt es zumindest in der IT-Sicherheit, sich gelegentlich auf bewährte Prinzipien zu besinnen und diese zur Analyse und Bewertung bestehender Sicherheitslösungen heranzuziehen.

Zwar kommen diese Prinzipien scheinbar primitiv in ihrer Allgemeinheit und zudem lächerlich bekannt daher – konsequent umgesetzt finden sie sich jedoch selten:

- **No Single Point of Failure**: Die Sicherheit keines Systems darf allein an einem Glied der Kette hängen: Reißt es, muss es eine zweite Schutzebene geben, die mindestens bis zur erfolgreichen Alarmierung hält. Leider finden sich immer noch in vielen Unternehmen nicht abgeschottete sensible Teilnetze – eingeschleppte Würmer können dort das Gesamtnetz lahm legen. Ebenso sind einstufige Firewalls hilflos, wenn sich in der Firmware ein Fehler findet – eine zweite „Verteidigungslinie“ eines anderen Herstellers brächte Abhilfe.
- **Least Privilege**: Jedem genau so viele Rechte, wie zur Aufgabenerfüllung erforderlich – nicht mehr, nicht weniger – und konsequenter Rechteentzug bei Aufgabenwechsel, damit keine „Rechtekumulation“ das Sicherheitskonzept unterläuft.
- **Checks and Balances**: Reviews und getrennte Rollen bei Konzeption und Umsetzung, verteilte Berechtigungen statt zentraler Einzelzuständigkeit – nur so lässt sich missbrauchbare „Machtkonzentration“ systematisch verhindern.

Keine Frage: Eine konsequente Umsetzung dieser Prinzipien ist aufwändiger als ihre Vermeidung. Was aber ist gefährlicher als ein vermeintlich „wasserdichtes“ Sicherheitskonzept mit Loch?

1 Security News

1.1 Viren „prosaisch“

Offenbar haben Autoren von Viren und Trojanern derzeit das technisch Machbare ausgereizt – sie besinnen sich wieder auf eine althergebrachte Disziplin ihrer „Kunst“ – das Tarnen und Täuschen.

So waren in den vergangenen Jahren allenfalls die Spam-Mails der Nigeria Connection amüsant zu lesen. Viren- und Trojaner-E-Mails konnte der geübte Blick hingegen schnell aufgrund der simplen Strickart aussortieren. Das hat sich mit aktuellen Schädlingen wie Sober.C, vor dem das BSI am 22.12.2003 warnte, und Xombe geändert. Deren Wirts-E-Mails tarnen sich als „Windows XP Service Pack“ zum Ersatz eines angeblich abgelaufenen „Beta Service Packs“, als Gegengift für den „Trojaner services.exe“, der „nicht einmal per Taskmanager beendet werden kann“[1], oder als Mitteilung über eine erfolgte Strafanzeige wegen „illegaler Downloads“ – samt korrekter Telefonnummer der Kripo Düsseldorf (allein die inkriminierte IP-Adresse gehört zu einem freien Adressblock in Brasilien).

Diese extrem plausibel gestalteten Anschreiben dürften auch manch skeptischen Empfänger zum Öffnen des Dateianhangs verleiten. Vermutlich erregt nicht einmal (mehr) der Hinweis Verdacht, dass vor der Installation ein eventuell vorhandener Virenscanner zu deaktivieren ist.

1.2 Zertifikatskettenlücke II

Wie in den Secorvo Security News 12/2003 vorausgesagt, hatten am 07.01.2004 diverse Browser wegen des ablaufenden VeriSign-CA-Zertifikats Probleme mit SSL-Zertifikaten. Dass dies nicht das einzige Problem blieb, war einer VeriSign-Sperrliste (CRL) zu verdanken, die zum selben Zeitpunkt auslief. Die Verfügbarkeit des Servers crl.versign.com brach daraufhin wegen der großen Zahl von Windows-PCs ein, die eine neue Sperrliste zu laden versuchten. VeriSign verzehnfachte kurzfristig die Server-Kapazität und entschuldigte sich für diesen Fauxpas.

Pikantes Randdetail: Symantec empfahl in diesem Zusammenhang seinen Kunden, die Sicherheitspolicy zu lockern – und die Prüfung zurückgezogener Zertifikate unter Windows zu deaktivieren.

1.3 Sicherheitslücke Backup

Wie am 09.01.2004 bekannt wurde, hat jetzt auch ein Backup-Programm Federn lassen müssen: Zur Durchführung der Datensicherung legt der Open Transaction Manager (OTM) von Veritas NetBackup Professional 3.5 eine Netzwerkfreigabe an. Da diese Berechtigung auf „Jeder/Vollzugriff“ eingestellt ist, können Unbefugte darauf während des Sicherungsvorgangs ohne Einschränkung über das Netzwerk zugreifen und Dateien und Ordner in der OTM Cache-Datei einsehen.

Eine Beschreibung der Schwachstelle und ein Workaround finden sich auf der Website des Herstellers. Alternativ wird ein Update auf Version 3.6 empfohlen.

1.4 11. DFN-CERT Workshop

Anfang Februar ist es wieder soweit: zum elften Mal wird im Kongresszentrum (CCH) in Hamburg der zweitägige DFN-CERT/PCA-Workshop stattfinden. Das auch diesmal sehr viel versprechende Programm dürfte auch 2004 wieder mehr als 350 Teilnehmer aus Forschung, Unternehmen und Behörden anlocken. Aktuelle Vorträge aus den Themengebieten PKI, Intrusion Detection, Chipkarten, sicheres Linux, ARP-Spoofing etc. stehen auf der Agenda. Auch Secorvo ist mit einem Beitrag vertreten: Stefan Kelm wird gemeinsam mit Dr. Rainer W. Gerling zum Thema „E-Mail-Verschlüsselungsproxies in der Praxis“ vortragen.

[1] Fußnote für Unix-Anwender: Dies entspricht in etwa dem „Trojaner /sbin/init“.

1.5 Microsoft-Tool reinigt Office-Dokumente

Dass Restinformationen in Office-Dateien verräterische Details früherer Dokumentenversionen mitliefern können, weiß mittlerweile auch Tony Blair, dessen am 30.01.2003 im Word-Format veröffentlichtes Irak-Dossier von der Presse genüsslich seziert wurde. Auch aus diesem Grund werden Dokumente zunehmend im PDF-Format publiziert. Für MS-Office-Nutzer, die ihre Dateien bedenkenlos direkt weitergeben möchten, veröffentlichte Microsoft am 05.01.2004 ein Remove Hidden Data Add-In Tool – verfügbar allerdings nur für Office XP und 2003.

Pikantes Randdetail auch hier: Sollte die Software nicht funktionieren, empfiehlt Microsoft, die Sicherheitspolicy zu lockern – und allen lokal installierten Makros in Add-Ins und Templates das Vertrauen auszusprechen.

1.6 ASN.1 zum Dritten...

Zunächst verursachte die fehlerhafte Dekodierung missgestalteter ASN.1-Protokollnachrichten Sicherheitslücken in SNMP-Modulen diverser Netzwerk-Produkte, dann in Sicherheitssoftware wie OpenSSL, die ASN.1-kodierte S/MIME-Nachrichten und X.509-Zertifikate auswertet. Forscher der Universität Oulu konnten nun nachweisen, dass auch Internet-Telefonie und Videokonferenzen nach dem Standard H.323 betroffen sind – das zugehörige Signalisierungsprotokoll H.225 kodiert seine Protokollnachrichten ebenfalls nach ASN.1.

Brisant werden diese Fehler dadurch, dass sie nicht nur in H.323-Produkten im engeren Sinne auftreten können, sondern auch in Firewalls, die H.225-Nachrichten für die Network Address Translation (NAT) interpretieren und modifizieren müssen. Am 13.01.2004 gab Cisco ein entsprechendes Security Advisory zu IOS und weiteren H.323-Produkten heraus. Microsoft veröffentlichte am selben Tag als Abhilfe für den hauseigenen ISA Server einen Hotfix, der allerdings mit Bedacht angewendet werden sollte: Ersten Berichten zufolge beendet der Hotfix ohne weitere Nachfrage die Dienste des ISA Servers.

Spätestens jetzt sollten Hersteller ihre Implementierungen aller Protokolle, die auf ASN.1 basieren, auf den Prüfstand stellen.

1.7 MBSA 1.2 in Deutsch

Die neue Version 1.2 des Baseline Security Analyzer (MBSA, siehe SSN 1/2003) von Microsoft für NT, 2000, XP, 2003, IIS und SQL-Server ist seit dem 19.01.2004 auch in deutscher Sprache verfügbar – und sollte nun auch für deutsche Versionen einwandfreie Analyseergebnisse liefern. Einzig die Patch-Beschreibung erfolgt nach wie vor in englischer Sprache und auch die ermittelten Links verweisen leider auf die amerikanischen Referenzseiten.

1.8 BDSG-Übergangsfrist

Am 23.05.2004 endet die Übergangsfrist, die die Neufassung des Bundesdatenschutzgesetzes (BDSG) vom Mai 2001 (in der aktuellen Fassung vom 14.01.2003) für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten einräumt, die vor dem 23.05.2001 begonnen wurde.

Die Novellierung umfasst einige grundsätzliche Änderungen, wie die Aufnahme der Prinzipien der Datensparsamkeit und Datenvermeidung, die Überarbeitung der „10 Gebote“ der technischen und organisatorischen Maßnahmen (Anlage zu § 9) sowie die Einführung eines noch gesetzlich auszugestaltenden Datenschutzaudits.

Unternehmen, die mehr als vier Arbeitnehmer mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, müssen innerhalb eines Monats schriftlich einen (internen oder externen) Datenschutzbeauftragten bestellen. Zudem sind eine Übersicht meldepflichtiger automatisierter Verarbeitungsverfahren und der jeweils Zugriffsberechtigten zu erstellen. Verstöße werden mit Bußgeldern von bis zu 250.000 € belegt.

2 Secorvo News

2.1 Secorvo College aktuell

Für Kurzentschlossene gibt es noch einige wenige freie Plätze auf dem Seminar Public Key Infrastrukturen (27.-28.01.2004) und der eintägigen Vertiefung PKI für Fortgeschrittene (29.01.2004).

Einen „eigenhändigen" Einblick in aktuelle Angriffstechniken erhalten Sie in der ausgeklügelten Laborumgebung des Live Hacking Lab, einer Kooperationsveranstaltung mit der schweizerischen Compass Security Network Computing AG (10.-11.02.2004).

Wegen der großen Nachfrage bietet Secorvo College das fünftägige Intensiv-Seminar Information Security Management von A(udit) bis Z(ertifizierung) ein zusätzliches Mal am 08.-12.03.2004 an.

http://www.secorvo.de/college

2.2 PKI in Windows XP/2003

Die aktualisierte und auf Windows XP und Windows 2003 Server erweiterte Fassung des mehr als 20.000 Mal herunter geladenen Secorvo White Papers „PKI-Unterstützung in Windows 2000" von Holger Mack liegt nun auch in englischer Sprache vor. Darin werden die PKI-Funktionalitäten der aktuellen Windows Versionen dargestellt und ihre Anwendung und Anwendbarkeit in der Praxis untersucht sowie die Unterschiede der PKI-Unterstützung in Windows 2000 und den Nachfolgern Windows 2003/XP verdeutlicht.

2.3 SSN – der 2. Jahrgang

Wer das vergangene Jahr unter der Security-Brille nochmals Revue passieren lassen möchte, findet jetzt den 2. Jahrgang der Secorvo Security News in einer PDF-Datei zusammengefasst – dem Trend zum Abnehmen nach den Feiertagen folgend auch als schlanke Zip-Datei.

3 Veranstaltungshinweise

Januar 2004	
27.-28.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
29.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2004	
03.-04.02.	Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
10.-11.02.	Live Hacking Lab (Secorvo College, Karlsruhe)
März 2004	
02.-03.03.	Lotus Notes Security (Secorvo College, Karlsruhe)
08.-09.03.	IT-Security Management (Secorvo College, Karlsruhe)
08.-12.03.	Information Security Management (Secorvo College, Karlsruhe)
09.-10.03.	Einführung in die Praxis des betr. DSB (Euroforum, München)
April 2004	
20.-21.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
27.-29.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Februar 2004

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 2, 3. Jhrg. 2004
Stand 25. Februar 2004

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Virendialektik

1 Security News

1.1 E-Mail Ping-Pong

1.2 Firewall-Intelligenz-Bugs

1.3 Tunnelrisiken

1.4 CERT-Statistiken

1.5 Sicherheitsrisiko IPv6?

1.6 Jetzt auch Microsoft...

2 Secorvo News

2.1 Secorvo College aktuell

2.2 KA-IT-Si-Event

2.3 Neues Video

2.4 Der Klassiker: DuD 2004

3 Veranstaltungshinweise

Impressum

Editorial: Virendialektik

Es ist also die Geschichte der Natur wie der menschlichen Gesellschaft, aus der die Gesetze der Dialektik abstrahiert werden. (...) 1. das Gesetz des Umschlagens von Quantität in Qualität (...)

Friedrich Engels, „Dialektik der Natur“ (1873-1882)

Seit Ende der 80er Jahre (des vergangenen Jahrhunderts) gibt es Viren, und seitdem auch Virenscanner – nichts wirklich Neues also. Die Schwerpunkte haben sich über die Jahre verschoben – es waren erst die Boot-, dann die Macro- und schließlich die E-Mail-Viren, die unausrottbar schienen. Dennoch lagen die Scanner regelmäßig vorn, denn die Verbreitungsgeschwindigkeit war weit geringer als das Update-Tempo der Antivirensoftware. Und auch die von Scannern verursachten Ablaufverzögerungen konnten trotz immer umfangreicherer Viren-Signatur-Dateien durch die Geschwindigkeitsfortschritte neuer Rechnergenerationen kompensiert werden.

Mit dem Virus „MyDoom“ und seinen Varianten droht nun aber die zunehmende Quantität in eine neue Qualität umzuschlagen. Der Verbreitungsmechanismus versucht, alle Register zu ziehen: Wechselnde Betreff-Zeile, E-Mail-Absenderadresse von Kollegen, sprachlich korrekte Nachrichten mit plausiblem „Subject“ und Textinhalt, gezippter Anhang – und gestartet wurde der Virus am Wochenende, zu einer Zeit, zu der der Arbeitseifer auch der Virenjäger weltweit gedämpft ist. Der Erfolg: Erstmals seit geraumer Zeit verbreitete sich ein Virus schneller als die neuen Virensignaturen der Anti-Viren-Software.

Aber auch die Angriffs-Wellen, die entdeckte Schwachstellen auslösen, werden immer steiler: Die Zeitspanne von der Entdeckung einer Schwachstelle bis zur Verfügbarkeit eines „Exploits“ und dessen Massenmissbrauch wird ständig kürzer. Sollte es zutreffen, dass seit dem 13.02.2004 Teile des Quellcodes von Windows NT/2000 im Internet kursieren, könnte auch bei den Exploits ein Qualitätssprung bevorstehen – hoffen wir, dass Microsoft seine Hausaufgaben gemacht hat.

1 Security News

1.1 E-Mail Ping-Pong

Weltweit litten seit dem 26.01.2004 Millionen Computernutzer unter dem E-Mail-Wurm MyDoom. Immerhin waren zumindest Unternehmensnetze dank zügiger Aktualisierung der zentralen Virenschutz-Gateways nach ein bis zwei Tagen überwiegend vor dem Virus geschützt.

Dabei trat allerdings eine in den Auswirkungen schwer wiegende Nebenwirkung von Viren wie MyDoom, Sobig und Co., die sich mit falschen, aber existierenden Absenderadressen verbreiten, zu Tage: Virenschutz-Gateways schicken meist automatisch eine Viren-Warnung an den vermeintlichen Versender der virenverseuchten E-Mail. So kann trotz ausreichenden Virenschutzes das „Echo“ des Wurms die E-Mailboxen überquellen lassen. Einzelne Lösungen senden sogar eine Kopie der verseuchten E-Mail im Anhang zurück.

Das Ping-Pong-Spiel, das entsteht, wenn zwei solche Gateways aufeinander treffen, kann man sich leicht ausmalen. Den Anbietern von Virenschutz-Gateways ist daher dringend zu raten, bei der Entdeckung von Würmern, die für falsche Absenderadressen bekannt sind, keine automatischen Antwort-E-Mails zu erzeugen.

1.2 Firewall-Intelligenz-Bugs

In den vergangenen Wochen wurden gleich mehrere Schwachstellen in Check Points Firewall-1 entdeckt, die den voreingestellten „Eigenintelligenz“-Eigenschaften der Firewall zuzuschreiben sind:

- Am 26.01.2004 wurde der ASN.1-Bug in H.323-Modulen, vor dem wir zuletzt in den SSN 1/2004 gewarnt haben, auch in der Firewall-1 aufgespürt.
- Am 04.02.2004 wurde ein Pufferüberlauf beim VPN-Verbindungsaufbau gemeldet, über den älteren Produkttypen Code untergeschoben werden kann.
- Am selben Tag wurde ein weiterer Pufferüberlauf im HTTP Security Server der Firewall gemeldet, der versucht, mittels „Application Intelligence“ Angriffe auf Anwendungsebene abzuwehren.

Durch diese Schwachstellen kann ein Angreifer potenziell die ganze Firewall „knacken“. Es ist zu befürchten, dass mit der Integration immer komplexerer intelligenter Sicherheitsfunktionen in Firewall-Produkte auch Schwachstellen dieser Art häufiger auftreten werden. Vielleicht erlebt dann die klassische P-A-P Firewall-Architektur mit getrennten Maschinen für Paketfilter und Application-Gateway eine unerwartete Renaissance.

1.3 Tunnelrisiken

Das sogenannte „Tunneln“ von Netzwerkpaketen ist schon seit geraumer Zeit als kritische Schwachstelle vieler Kommunikationsprotokolle bekannt: Angreifer nutzen hierbei die Möglichkeit, Informationen in verbreiteten Standardprotokollen – z. B. HTTP – zu „verstecken“, um beispielsweise zentrale Firewalls zu umgehen.

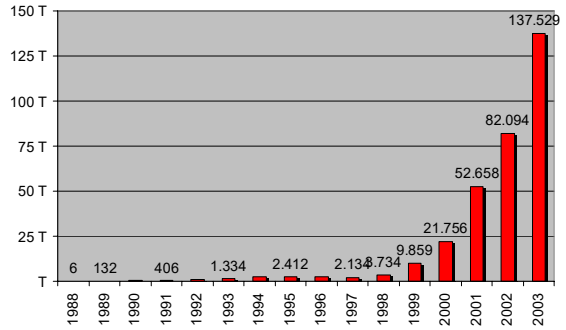
Bislang wurden vor allem die Protokolle HTTP und HTTPS als Tunnelmedien verwendet. Etliche Tools hierfür sind im Internet zu finden. Dass auch jedes andere Protokoll prinzipiell zum Tunneln missbraucht werden kann, demonstrierte die schweizerische Compass Security AG mit der Entwicklung eines DNS-Tunnel-Clients, den sie kostenlos zur Verfügung stellt.

Mit Hilfe dieses Clients ist es möglich, beliebige Netzwerkpakete in reguläre DNS-Anfragen und –Antworten einzupacken. Da DNS (Domain Name Service) zur Umwandlung von Hostnamen in IP-Adressen das zentrale Kommunikationsprotokoll im Internet darstellt, wird es auch von vielen Unternehmens-Firewalls nicht blockiert.

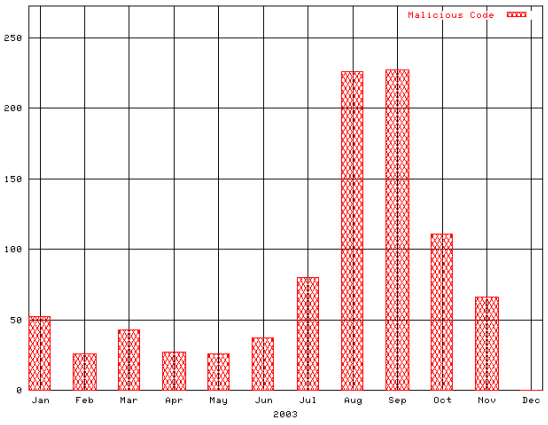
Der von Compass programmierte Client beinhaltet keinerlei Schadensroutinen und kann daher zur Überprüfung der eigenen Infrastruktur genutzt werden.

1.4 CERT-Statistiken

Kurz nach Erscheinen der Security News 1/2004 aktualisierte das CERT Coordination Center an der Carnegie Mellon University am 22.01.2004 die Statistik der gemeldeten Vorfälle: Danach stieg deren Zahl im Jahr 2003 erneut um fast 70 %.



Auch das European CSIRT Network pflegt eine öffentliche CERT-Statistik mit interessanten Ergebnissen. So zum Beispiel die folgende Zählung der je CERT im vergangenen Jahr monatlich durchschnittlich bearbeiteten Fälle bösartigen Codes, die einen extremen Anstieg ab Juli belegt:



1.5 Sicherheitsrisiko IPv6?

In einer Kolumne vom 14.01.2004 äußerte sich der Sicherheits-Experte Simson Garfinkel skeptisch über den von IPv6, der nächsten Generation des Internet-Protokolls zu erwartenden Sicherheitsgewinn. Zwar seien in IPv6 IPsec-Verschlüsselung und andere neue Sicherheitsfunktionen enthalten. Andererseits aber wird jede umfangreiche neue Protokoll-Implementierung unweigerlich auch zahlreiche neue Programmierfehler und Sicherheitsprobleme mit sich bringen.

Wie zum postwendenden Beweis von Garfinkels These wurde am 04.02.2004 ein Denial-of-Service Angriff per IPv6 auf OpenBSD entdeckt – ein Betriebssystem, das für den hohen Stellenwert der Sicherheit bei seiner Entwicklung bekannt ist. Die Lücke wurde am 08.02.2004 gestopft.

Fast zeitgleich wurde beim 47. RIPE Meeting am 26.-30.01.2004 die Forderung erhoben, IPv6-Adressen in die weltweiten DNS Root-Nameserver einzutragen. Dabei wurde als technisches Problem primär die Verlängerung der DNS-Antworten gesehen – nicht aber der nicht unwahrscheinliche Ausfall ganzer nationaler Top-Level-Domains, verursacht durch eine IPv6-Schwachstelle. Diesen Fall mag man sich auch lieber nicht vorstellen.

1.6 Jetzt auch Microsoft...

Der schon in den SSN 11/2003 diskutierte Fehler in der ASN.1-Bibliothek (Abstract Syntax Notation 1) wurde am 10.02.2004 auch in den Microsoft-Betriebssystemen NT 4.0, 2000 und XP entdeckt. Dabei kann ein Pufferüberlauf ausgelöst und beliebiger Code ausgeführt werden. Ähnliche Fehler sind auch bei anderen ASN.1-Implementierungen bekannt geworden.

Die Installation des entsprechenden, von Microsoft bereitgestellten Patches wird dringend angeraten. Während der Endredaktion dieser Security News wurde bereits das erste Exploit veröffentlicht...

2 Secorvo News

2.1 Secorvo College aktuell

Wegen der großen Nachfrage bieten wir das Seminar Information Security Management von A(udit) bis Z(ertifizierung) an einem zusätzlichen Termin, vom **08.-12.03.2004** an. Die ersten beiden Tage bilden eine inhaltlich abgeschlossene Ein-

heit und können getrennt als Seminar IT-Security Management (**08.-09.03.2004**) gebucht werden.

http://www.secorvo.de/college

2.2 KA-IT-Si-Event

Das nächste Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) findet am **31.03.2004** im Karlsruher Technologiepark statt. Dirk Fox, Herausgeber der Fachzeitschrift DuD, wird Anspruch und Wirklichkeit des Datenschutzes in der Unternehmenspraxis beleuchten: Drahtseilakt zwischen Genie und Wahnsinn. Beginn 18 Uhr, anschließend Buffet-Networking.

2.3 Neues Video

Seit Anfang Februar ist das neueste Secorvo-Lehrvideo in deutscher und englischer Sprache verfügbar – das Thema: „Trojanische Pferde“. Dabei handelt es sich um eine professionell überarbeitete Version des seit 2002 erhältlichen und sehr nachgefragten Videos. Dank der verwendeten Flash-Technologie ist es äußerst ressourcenschonend. Die Intranet-Version wird zudem mit Steuerungsmöglichkeit (Stopp, Vor- und Zurückspulen) geliefert. Weitere Sprachversionen sowie Themen für neue Videos sind zur Zeit in Vorbereitung.

2.4 Der Klassiker: DuD 2004

Schon zum sechsten Mal findet am **03.-04.05.2004** die Fachkonferenz DuD 2004 in Berlin statt, die der für seine hochwertigen Konferenzen bekannte Veranstalter COMPUTAS gemeinsam mit den Herausgebern der Fachzeitschrift Datenschutz und Datensicherheit (DuD) konzipiert und organisiert. Nicht nur jährlich steigende Teilnehmerzahlen belegen, dass dieses etablierte Forum von und für Experten aus Unternehmen, Behörden und der Politik für viele Datenschutzbeauftragte und IT-Sicherheitsverantwortliche zum „Muss“ geworden ist: In diesem Jahr lagen schon lange vor Programmveröffentlichung zahlreiche Anmeldungen vor.

3 Veranstaltungshinweise

März 2004	
02.-03.03.	Lotus Notes Security (Secorvo College, Karlsruhe)
08.-09.03.	IT-Security Management (Secorvo College, Karlsruhe)
08.-12.03.	Information Security Management (Secorvo College, Karlsruhe)
09.-10.03.	Einführung in die Praxis des betr. DSB (Euroforum, München)
31.03.	Drahtseilakt zwischen Genie und Wahnsinn (KA-IT-Si, Karlsruhe)
April 2004	
20.-21.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
27.-29.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Mai 2004	
03.-04.05.	Datenschutz und Datensicherheit – DuD 2004 (COMPUTAS, Berlin)
04.-05.05.	Inside Windows Security (Secorvo College, Karlsruhe)
11.-12.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
13.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
März 2004

Dirk Fox, Stefan Gora, Stefan Kelm
Secorvo Security Consulting GmbH

Nr. 3, 3. Jhrg. 2004
Stand 22. März 2004

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial:
Rechtsfalle Privatnutzung

1 Security News

1.1 Qualifizierte Massen-Signaturen

1.2 ENISA: Holpriger Start

1.3 NGWT – Next Generation Worm Tricks

1.4 Einstufungs(s)pannen bei Sicherheitslücken

1.5 „Security“ schützt vor Lücken nicht

1.6 Raubkopieverbreitung über Firmensysteme

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Chefsache IT-Sicherheit

2.3 Microsoft erhält ISIS-MTT-Konformitätssiegel

3 Veranstaltungshinweise

Impressum

Editorial: Rechtsfalle Privatnutzung

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Abs. 1 bezeichneten Unternehmens unbefugt (...) eine der in Abs. 1 (...) bezeichneten Handlungen gestattet (...).

Verletzung des Post- oder Fernmeldegeheimnisses, § 206 StGB

Zwar ist die Kuh des “geldwerten Vorteils” bei privater Nutzung von WWW und E-Mail im Unternehmen vom Eis. Dennoch hängt ein Damokles-Schwert über allen Unternehmen, die der Privatnutzung keinen Riegel vorgeschoben haben – als unvermeidliche Konsequenz des verfassungsrechtlich verankerten Fernmeldegeheimnisses. Die Auswirkungen sind dramatisch – und in vielen Unternehmen nicht einmal bekannt: Lassen sich private E-Mails nicht eindeutig identifizieren oder ausschließen, dann unterliegen auch Spam-E-Mails dem selben Schutz wie private Post. Als Service-Provider seiner Mitarbeiter ist der Arbeitgeber nämlich zur (unverstümmelten) Zustellung jeder Nachricht verpflichtet. Ein Löschen unliebsamer, oft mit schädlichen Dateianhängen (Viren) versehener E-Mails ist ein strafbewehrter Verstoß gegen § 206 StGB.

Aus dieser Konsequenz gibt es kein Entrinnen: Denn auch per Verzichtserklärung kann ein Grundrecht nicht abgetreten werden, mithin kann kein Mitarbeiter den Arbeitgeber zum Eingriff ermächtigen. Zumal die Freiwilligkeit einer solchen Zustimmung im Arbeitsverhältnis in Zweifel steht. Selbst eine stillschweigende Duldung privater Nutzung genügt, damit der Arbeitgeber zum Internet-Service-Provider mutiert. Bleibt nur eines: Wer zentral filtern will, muss die private Nutzung explizit verbieten – und die Einhaltung des Verbots regelmäßig prüfen.

1 Security News

1.1 Qualifizierte Massen-Signaturen

Ein in der PKI-Praxis noch immer kontrovers diskutiertes Problem ist die Fragestellung, wie sich fortgeschrittene oder „qualifizierte“ elektronische Signaturen nach EU-Richtlinie und deutschem Signaturgesetz mit Signaturen durch Server bzw. juristische Personen in Einklang bringen lassen. Obgleich dieses Thema bereits seit mehreren Jahren diskutiert wird, kam es erst im Zusammenhang mit der zum 01.01.2004 erforderlichen Umsetzung der EG-Richlinie zu elektronischen Rechnungen wieder auf dem Tisch.

Da dieses Problem nicht nur die Zertifizierungsdiensteanbieter, sondern auch die nationalen Aufsichtsbehörden (in Deutschland die RegTP) betrifft, hat sich die österreichische Aufsichtsstelle für elektronische Signaturen dieses Themas angenommen und am 16.03.2004 einen interessanten Entwurf eines „Positionspapiers zu Fragen der elektronischen Rechnung und der Serversignatur“ vorgelegt. Das Papier enthält konkrete Empfehlungen für die Gestaltung von Massensignaturen, die in ähnlicher Form auch in anderen EU-Ländern umsetzbar sein dürften.

1.2 ENISA: Holpriger Start

Die europäische Sicherheitsagentur ENISA (European Network Information Security Agency) mit provisorischem Sitz in Brüssel ist seit dem 18.03.2004 online. Ihre Aufgabe liegt unter anderem darin, die EU-Mitgliedsstaaten in Fragen der Netzwerk-Sicherheit zu beraten. Ihr Hauptsitz soll gemäß Beschluss vom 13.12.2003 in Griechenland aufgebaut werden. Derzeit ist die Stelle des Direktors ausgeschrieben.

Ein kritischer Blick auf den Webserver legt die Empfehlung nahe, auch die Stelle eines Administrators mit Grundkenntnissen in Webserver-Sicherheit auszuschreiben. Vielleicht würde dann die wenig vorbildliche Informationsfreigabe unterbunden: Unter anderem sind private IP-Adresse, ein Logfile und Skripte des Servers einsehbar.

1.3 NGWT – Next Generation Worm Tricks

Die inhaltlich immer glaubwürdigeren Massen-E-Mails mit Trojanern im Anhang waren ein Thema der SSN 01/2004. Seit einigen Wochen verbergen Würmer den schädlichen Anhang in Passwort geschützten Archiven (.zip, .rar) vor dem Zugriff der Antiviren-Software. Das zugehörige Kennwort wird im Text der E-Mail mitgeliefert – und tatsächlich von unzähligen Empfängern bereitwillig zum Aktivieren des anhängenden Schadprogramms eingetippt.

Darauf haben einige Hersteller von Antivirenlösungen reagiert: Sie entnehmen vor dem Scannen der E-Mail automatisiert die Passwörter und entdecken so Viren und Würmer auch in passwortgeschützten Anhängen. Das ist den Virenprogrammierern nicht verborgen geblieben: Seit Bagle.N werden die Kennwörter daher jetzt als Bild im gif-Format angehängt.

Will man nicht ständig mit den technischen Lösungen der Kreativität der Angreifer hinterherhinken, bleibt als einziger Ausweg eine wirkungsvolle und nachhaltige Mitarbeitersensibilisierung.

1.4 Einstufungs(s)pannen bei Sicherheitslücken

Oft fällt es Herstellern offenbar schwer, die Bedeutung von Sicherheitslücken richtig einzustufen. Zwei aktuelle Beispiele belegen dies: So wurde ein am 09.03.2004 von Microsoft veröffentlichtes Outlook-Update, welches eine mögliche Systemübernahme behebt, zunächst nicht als „kritisch“ bewertet. Und die aktuelle Version des ISS Internet Scanner schätzt die NT-Schwachstelle „NtservicesExeDos“ als „mittel“ ein – obwohl betroffenen Systemen keine Netzdienste mehr zur Verfügung stehen.

Daher ist bei Angaben von Herstellern und Tools zur Relevanz von Schwachstellen Vorsicht angeraten: Die Angaben sollten nur als Empfehlung verstanden werden und nie die eigene Bewertung ersetzen.

1.5 „Security“ schützt vor Lücken nicht

Über sicherheitskritische Schwachstellen in Programmen und Betriebssystemen wird in schöner Regelmäßigkeit berichtet. Sicherheitswarnungen, von Notfallteams „Advisories“ genannt, werden oft als Reaktion auf öffentlich diskutierte Sicherheitslücken publiziert. Vielfach handelt es sich dabei um Erkenntnisse von Security-Experten, die in verbreiteten Systemen gezielt nach Sicherheitslücken suchen.

Dass dabei insbesondere auch die Hersteller von Sicherheitsprodukten unter die Lupe genommen werden, verwundert nicht. Auch hier werden die Experten regelmäßig fündig: Allein im Februar diesen Jahres wurde eine Reihe von teils äußerst kritischen Lücken entdeckt. Betroffen waren u.a. Produkte wie ZoneAlarm, Symantec Firewall/VPN, Symantec Antivirus und Norton Internet Security. Ursache der Bugs waren „alte Bekannte“ wie Buffer Overflows oder Race Conditions.

Als besonders brisant erwiesen sich dabei Fehler, die in der noch recht jungen Produktklasse der so genannten „Intrusion Prevention Systeme“ gefunden wurden, deren Ziel – im Unterschied zu IDS – nicht das Erkennen, sondern die Verhinderung von Angriffen ist. So hat ein Angreifer in diversen ungepatchten Produkten des Herstellers ISS (Internet Security Systems) die Möglichkeit, eigene Code-Sequenzen ausführen zu lassen. Und die Fachzeitschrift c’t kommt in Ausgabe 5/2004 beim Test von Symantecs Gateway Security 5400 gar zu dem Ergebnis, der Schutz durch das Produkt sei „eher niedrig einzuschätzen“.

Noch kritischer ist eine Schwachstelle, die in Hardware-Sicherheitsmodulen (HSM) der Firma nCipher entdeckt wurde: Dort ist es einem lokalen Angreifer u.U. möglich, Zugriff auf kryptographische Schlüssel zu erhalten, die ja gerade durch diese Hardware besonders geschützt sein sollen.

Merke: Auch Hersteller von Security-Produkten sind nicht vor Sicherheitslücken gefeit. Daher sollten gerade diese Lösungen vor dem Produktiveinsatz intensiven Analysen unterzogen werden.

1.6 Raubkopieverbreitung über Firmensysteme

Die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. berichtet von der bislang weltweit größten Razzia gegen Raubkopierer. Dabei wurden vom 16. bis 18.03.2004 allein in Deutschland mehr als 800 Firmen, Rechenzentren und Privatwohnungen durchsucht. Zur Verbreitung der illegalen Kopien, die einen geschätzten Verlust in Höhe eines zweistelligen Millionen-Euro-Betrags verursacht haben, wurden offenbar im großen Stil Systeme von Rechenzentren, Firmen und Privatpersonen missbraucht. Unternehmensserver standen dabei wegen deren performanter Internetanbindung und der hohen Speicherkapazitäten im Fokus des nun ausgehobenen Hacker-Rings, der systematisch fremde Systeme übernommen und missbraucht haben soll.

Erheblich dürften auch die durch die Beschlagnahmungen entstanden Schäden in den betroffenen Unternehmen sein.

2 Secorvo News

2.1 Secorvo College aktuell

Anfang April (06.04.2004) bietet Secorvo College erstmalig einen eintägigen Intensiv-Workshop an, in dessen Verlauf typische Hacker-Vorgehensweisen gemeinsam durchgespielt werden: „Dem Hacker über die Schulter geschaut“. Um intensive praktische Übungen und Diskussionen sicherzustellen, ist die Teilnehmerzahl auf fünf Sicherheitsverantwortliche beschränkt.

Grundlegend überarbeitet, erweitert und aktualisiert wurde das nun dreitägige Seminar „E-Mail-Sicherheit“ (20.-22.04. 2004), das seit 1999 zahlreich besucht und kontinuierlich weiter entwickelt wurde. Erstmalig werden nun auch Server-basierte Verschlüsselungslösungen ausführlich behandelt.

Ende April (27.-29.04.2004) folgt der „Klassiker“: Das Seminar „IT-Sicherheit heute“ gibt einen Einblick in die zentralen Themen und aktuellen Fragestellungen der IT-Sicherheit – geeignet sowohl für einen intensiven thematischen Einstieg als auch als Auffrischung.

http://www.secorvo.de/college

2.2 Chefsache IT-Sicherheit

Mit einer halbtägigen Roadshow zum Thema IT-Sicherheit richten sich die IHKs in Baden-Württemberg derzeit an mittelständische Unternehmen. Die Veranstaltung klärt über zentrale IT-Risiken auf und stellt Lösungswege vor.

In Karlsruhe findet die Roadshow am 31.03.2004 in Zusammenarbeit mit der „Karlsruher IT-Sicherheitsinitiative“ in den Räumen der IHK statt. Die Partner der Initiative begleiten die Roadshow mit einer Ausstellung zum Thema. Im Anschluss referiert Dirk Fox, Geschäftsführer von Secorvo und Herausgeber der Zeitschrift „Datenschutz und Datensicherheit (DuD)“, über Anspruch und Wirklichkeit des Datenschutzes – einem „Drahtseilakt zwischen Genie und Wahnsinn“. Der Eintritt ist frei.

2.3 Microsoft erhält ISIS-MTT-Konformitätssiegel

Am 16.03.2004 hat der Microsoft Windows 2003 Certificate Service nach Prüfung durch das Secorvo Prüflabor vom ISIS-MTT-Board das ISIS-MTT-Konformitätssiegel erhalten. Damit ist die Microsoft-CA das dritte Produkt, dessen ISIS-MTT-Konformität in einem vereinheitlichten Testverfahren nachgewiesen wurde.

3 Veranstaltungshinweise

März 2004	
30.-31.03.	D-A-CH Security 2004 (GI, BITKOM, TeleTrusT; Basel)
31.03.	Chefsache IT-Sicherheit und Drahtseilakt zwischen Genie und Wahnsinn (IHK Karlsruhe)
April 2004	
06.04.04	Dem Hacker über die Schulter geschaut (Secorvo College)
20.-22.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
27.-29.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Mai 2004	
03.-04.05.	Datenschutz und Datensicherheit – DuD 2004 (COMPUTAS, Berlin)
04.-05.05.	Inside Windows Security (Secorvo College, Karlsruhe)
10.-13.05.	Netzwerk Sicherheits-Forum 2004 (ComConsult, Königswinter)
11.-12.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
13.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
April 2004

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 4, 3. Jhrg. 2004
Stand 19. April 2004

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Rechtsfalle revisited

1 Security News

1.1 Overflow in Ethereal

1.2 Cisco Global Exploiter

1.3 TKG im Bundesrat

1.4 Neue ISIS-MTT Version

1.5 Windows versus Linux

1.6 SigG Novelle

1.7 VPN-Sicherheitslücken

2 Secorvo News

2.1 Secorvo College aktuell

2.2 IT-Sicherheitsforum 2004

2.3 Midvision 2004

3 Veranstaltungshinweise

Impressum

Editorial: Rechtsfalle revisited

Alles sollte so einfach wie möglich gemacht werden, aber nicht einfacher.

Albert Einstein

Die Implikationen einer Privatnutzung von WWW- und E-Mail-Diensten im Unternehmen liegen zahlreichen Verantwortlichen im Magen, das haben die vielen Reaktionen auf das Editorial der SSN 03/2004 eindrucksvoll bestätigt. Die Zuspitzung auf § 206 StGB hat jedoch das Gesamtproblem stark verkürzt:

Festzuhalten ist: Als unproblematisch gilt die automatisierte zentrale Löschung von schädlichen Anhängen (Viren, trojanischen Pferden), da hier das mutmaßliche Einverständnis des Empfängers angenommen werden kann – § 87 TKG verpflichtet Provider sogar zu Schutzmaßnahmen.

Kritisch hingegen ist das zentrale Löschen von vermeintlichem Spam – sogar bei ausschließlich dienstlicher Nutzung: Ohne explizites Einverständnis des Nutzers oder eine geeignete Betriebsvereinbarung verstößt der Arbeitgeber gegen § 303a StGB:

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Spamabwehr erfordert jedoch keineswegs zwingend die zentrale Löschung:

- Das Abweisen von E-Mails am SMTP-Gateway, z. B. durch IP-Blocking, vermeidet ein Filtern und Löschen.
- Ein Aussortieren Spam-verdächtiger E-Mails in einen Quarantäne-Bereich ist nach herrschender Meinung untadelig.
- Wird Spam-verdächtige E-Mail vom zentralen Filter lediglich markiert und erfolgt die Löschung erst beim Empfänger, ist dies sogar bei zulässiger Privatnutzung unbedenklich.

In jedem Fall empfiehlt sich der Abschluss einer Betriebsvereinbarung – und eine Filter- und Löschlösung unter Nutzerkontrolle.

1 Security News

1.1 Overflow in Ethereal

Eines der Standard-Tools, die sowohl von Security-Experten als auch von Hackern eingesetzt werden, ist seit Jahren der sehr mächtige und kostenlos verfügbare Sniffer Ethereal. Er ermöglicht es, den kompletten Netzwerkverkehr mitzuschneiden, um beispielsweise Protokolle zu überwachen oder Verbindungen zu rekonstruieren.

Wie zuletzt in den SSN 03/2004 thematisiert, sind jedoch auch viele Sicherheits-Tools nicht frei von Schwachstellen. Nun hat es Ethereal „erwischt“: Am 22.03.2004 wurden gleich vier teilweise kritische Schwachstellen aufgedeckt, die – wen wundert es – ihre Ursache u. a. in einem „klassischen“ Buffer Overflow haben. Da das Tool sehr Hardware-nah programmiert wurde, sind von den Fehlern nicht nur Windows-, sondern auch alle Unix-Varianten betroffen. Administratoren, die Ethereal einsetzen, sollten nur noch die mittlerweile verfügbare korrigierte Version 0.10.3 verwenden, um nicht Opfer eines zweifellos bald kursierenden Exploits zu werden.

1.2 Cisco Global Exploiter

Unter der Bezeichnung „Cisco Global Exploiter“ ist seit kurzem ein Tool zur Überprüfung von neun bekannten Cisco-Schwachstellen verfügbar. Das Perl-Skript vereinfacht die Untersuchung von Routern und Switches auf Schwachstellen, kann aber – selbst von technisch unversierten „Skript-Kiddies“ – auch für Angriffe missbraucht werden. Ein Update von Systemen mit diesen Schwachstellen wird daher dringend empfohlen.

Die am 07.04.2004 publizierte Schwachstelle – eine fest in der Software verankerte UserID/Kennwort Kombination der Management-Lösungen Wireless Lan Solution Engine und Hosting Solution Engine – dürfte bald auch Teil des Exploits sein.

1.3 TKG im Bundesrat

Nicht zuletzt dank des Engagements der Branchenverbände, insbesondere eco und VATM, hatte die Bundesregierung in letzter Sekunde die umstrittene Vorratsspeicherung von Verbindungsdaten für die Sicherheitsbehörden aus der Novelle des Telekommunikationsgesetzes (TKG), die am 12.03.2004 vom Deutschen Bundestag verabschiedet wurde, herausgenommen. Sogar eine Entschädigung der Diensteanbieter bei Überwachungsmaßnahmen ist vorgesehen. Wie erwartet kam am 02.04.2004 prompt die von mehreren Bundesländern angekündigte Ablehnung im Bundesrat (BR-Drs. 200/04). Erschreckend die Änderungswunschliste der Länder:

- Verpflichtung von TK-Anbietern zur 6-monatigen Speicherung von Verkehrsdaten,
- Verpflichtung der Mobilfunkbetreiber zur Erhebung der Kunden-Bestandsdaten bei Prepaid-Karten,
- Möglichkeit eines Zugriffs auf personenbezogene PINs und Passwörter,
- Streichung der Entschädigung für Auskünfte im automatisierten Verfahren.

Auch die Einschränkung der Verpflichteten auf Unternehmen, die TK-Dienste für die Öffentlichkeit anbieten und mindestens 1.000 Teilnehmer versorgen, ist wieder auf dem Tisch. Damit könnten doch noch alle Unternehmen, die eine Privatnutzung ihrer TK-Dienste zulassen, in den Kreis der Verpflichteten aufrücken.

1.4 Neue ISIS-MTT Version

Am 16.03.2004 verabschiedete das ISIS-MTT Board die neue Version 1.1 der PKI-Interoperabilitätsspezifikation. Wichtigste Neuerung ist die Aufnahme des Profils für XML-Signatur und -Verschlüsselung als neuer Teil 8 von ISIS-MTT. Daneben wurden teils unnötig strenge Profilierungsanforderungen gelockert, um die Interoperabilität mit weit verbreiteter Anwendungssoftware zu verbessern.

Die Bedeutung des Standards ISIS-MTT hat in den vergangenen Monaten weiter zugenommen. So ist ISIS-MTT inzwischen obligatorischer Baustein des E-Government-Frameworks SAGA und, in der neuen Version 1.1, technische Grundlage für das Signaturbündnis. Ebenfalls am 16.03.2004 wurde auf der Grundlage eines Prüfberichts von Secorvo das ISIS-MTT Siegel in der Produktklasse „CA Server“ für die Certificate Services des Microsoft Windows Server 2003 verliehen.

1.5 Windows versus Linux

Eine am 19.03.2004 erschienene Studie von Forrester Research versucht, die seit mehreren Jahren heiß diskutierten Frage, ob Windows oder Linux das sicherere Betriebssystem sei, methodisch sauber zu beantworten. Über ein Jahr untersuchte Forrester Sicherheitslücken und Patches und legte als Vergleichsmetrik die Schwere bekannt gewordener Sicherheitslücken und die Zeit zwischen Bekanntgabe und Behebung zu Grunde. Das Ergebnis: Microsoft veröffentlichte Patch-Releases am schnellsten, hatte aber die meisten Sicherheitslücken der höchsten Einstufung (nach NISTs ICAT Database for Severe Computer Vulnerabilities).

Dieser Ansatz, mit dem sich Vorteile für Windows und Debian-Linux ergaben, wurde am 06.04.2004 postwendend von den großen Linux-Distributoren kritisiert, da sämtliche Lücken über einen Kamm geschoren würden, ohne auf die spezifischen Auswirkungen einzugehen. Zugleich belohnt die Metrik Hersteller, die die Bekanntgabe von Sicherheitslücken so lange wie möglich hinauszögern – und schüttet damit Öl in die seit einigen Jahren schwelende Debatte über den richtigen Zeitpunkt der Veröffentlichung von Sicherheitslücken.

Neben der Erkenntnis, dass bis zu allgemein akzeptierten Metriken für IT-Sicherheit noch ein Stück Weges vor uns liegt, ist anzunehmen, dass der Disput um die Studie zumindest den Absatz des 899 US $ teuren Dokuments fördert.

1.6 SigG-Novelle

Am 01.04.2004 wurde der mit Spannung erwartete Entwurf des SigG-Änderungsgesetzes nebst Begründung veröffentlicht. Der Großteil der vorgesehenen Änderungen bzw. Klarstellungen dient dazu, den Weg für eine einfache, weitest gehend elektronische Beantragung und Ausgabe von Signaturkarten zu ebnen.

Dadurch sollen die etablierten Verfahren für die Ausgabe von EC-, Bank- oder Versicherungskarten auch für Signaturkarten nutzbar gemacht werden – um der elektronischen Signatur endlich zum lange ersehnten Durchbruch zu verhelfen.

1.7 VPN-Sicherheitslücken

Gleich mehrere Implementierungen von ISAKMP/IKE, dem Schlüsselaustauschdienst für IPsec-VPNs, gerieten in den vergangenen Wochen in die Kritik:

- Am 17.03.2004 wurde eine Denial-of-Service Attacke gegen den ISAKMP-Dienst von OpenBSD veröffentlicht.
- Cisco veröffentlichte am 08.04.2004 ein Advisory, wonach einige IOS-Router und Catalyst-Switches durch missgeformte ISAKMP/IKE-Pakete gezielt zum Absturz gebracht werden können.

Den Vogel abgeschossen hat der mittlerweile auch in Linux integrierte ISAKMP-Dienst „Racoon“ des KAME-Projekts, der, wie am 07.04.2004 gemeldet wurde, zwischen September 2001 und April 2004 unbemerkt bei der ISAKMP-Variante mit RSA-Signatur zwar die verwendeten Zertifikate, nicht aber die eigentliche Signatur über die ausgetauschten Protokolldaten überprüft hat.

Dies bestätigt – im Nachhinein – Niels Ferguson und Bruce Schneier, die bereits Anfang 2000 vor der zu hohen Komplexität des IPsec-Standards warnten.

2 Secorvo News

2.1 Secorvo College aktuell

Auf vielfachen Wunsch haben wir das Seminarangebot von Secorvo College um ein Intensivseminar zum Datenschutz erweitert. Einen umfassenden Überblick über die im Mai 2001 neu geregelten Anforderungen des BDSG und unsere Erfahrungen mit der praktischen Umsetzung aktueller Datenschutzanforderungen in Unternehmen erhalten Sie – kurz vor Ablauf der BDSG-Übergangsfrist (vgl. SSN 01/2004) – erstmalig am 18.05.2004.

2.2 IT-Sicherheitsforum 2004

Das IT-Sicherheits-Forum der ComConsult Akademie zählt seit einigen Jahren zu den herausragenden Events der IT-Sicherheit. Das Programm 2004 beinhaltet aktuelle Vorträge zu Themen wie IDS in der Praxis, Sicherheit von Webanwendungen, Patch-Management und XML-Sicherheit. Abgerundet wird die Veranstaltung durch drei ganztägige Tutorien sowie diverse Praxis-Workshops. Stefan Kelm wird über Aufgaben und Strategien von CERTs referieren.

2.3 Midvision 2004

Die IT-Fachmesse für den Mittelstand, Midrange Welt und Midvision 2004, wird in diesem Jahr am 13.-14.05.2004 zum zweiten Mal in der Neuen Messe Karlsruhe stattfinden – diesmal mit dem thematischen Schwerpunkt „IT-Sicherheit“ und einem begleitenden zweitägigen Kongress. Auch die Karlsruher-IT-Sicherheitsinitiative (KA-IT-Si) ist vertreten: Mit Ausstellern, einem Event am 13.05.2004 und zwei Vorträgen auf dem begleitenden Fachkongress.

2.4 DuD 2004

Der Fachkonferenz DuD 2004 (03.-04.05. 2004) „droht“ ein neuer Teilnehmerrekord: schon jetzt haben sich mehr als 80 Teilnehmer angemeldet (Anmeldung).

3 Veranstaltungshinweise

April 2004	
27.-29.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Mai 2004	
03.-04.05.	Datenschutz und Datensicherheit – DuD 2004 (COMPUTAS, Berlin)
04.-05.05.	Inside Windows Security (Secorvo College, Karlsruhe)
10.-13.05.	IT-Sicherheits-Forum 2004 (ComConsult, Königswinter)
13.-14.05.	Midvision 2004 (KA-IT-Si/KMKG, Karlsruhe)
11.-12.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
13.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
18.05.	Datenschutz kompakt (Secorvo College, Karlsruhe)
Juni 2004	
14.-15.06.	IT-Security Management (Secorvo College, Karlsruhe)
14.-18.06.	Information Security Management (Secorvo College, Karlsruhe)
29.-30.06.	Security Awareness Symposium 2004 (Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Mai 2004

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 5, 3. Jhrg. 2004
Stand 28. Mai 2004

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Vom Wichtigen

1 Security News

1.1 RSA-576 faktorisiert

1.2 TCP-Schwachstelle

1.3 Kommt DNSSEC?

1.4 T-Online-Authentifikation

1.5 Sicherheitsloch Schutzsoftware

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Security Awareness Symposium 2004

3 Veranstaltungshinweise

Impressum

Editorial: Vom Wichtigen

Das Wichtigste im Leben ist, zu wissen, was das Wichtigste ist.

Otto Milo (Aphoristiker, 1902-1980)

Es ist wie im „wirklichen Leben“: Entscheidungen über Maßnahmen der IT-Sicherheit sind eine tägliche Herausforderung. Denn natürlich sind Zeit und Mittel begrenzt und damit Prioritätensetzungen unvermeidlich.

Begrenzt ist aber auch die Perspektive der beiden wichtigsten Entscheider – die des Verantwortlichen für IT-Sicherheit und die der Budget-verantwortlichen Geschäftsleitung. Schlimmer: Beide haben eine unterschiedliche Perspektive – und das liegt auch noch in der Natur der Sache.

Ein typischer Fall: Der IT-Leiter wählt für eine kritische Netz-Komponente ein Produkt mit Austausch-Garantie innerhalb weniger Stunden. Als die Geschäftsleitung das erfährt, wird sie blass: Die betroffene geschäftskritische Anwendung verträgt eine Ausfallzeit von nur wenigen Minuten.

Kern des Problems: Die Geschäftsleitung interessiert nur das Risiko, der IT-Sicherheitsverantwortliche kümmert sich um das Sicherheitsniveau. Das ist nicht dasselbe: Die Risikoperspektive zielt auf eine fallbezogene Kosten-Nutzen-Entscheidung, ob ein Risiko in Kauf genommen, transferiert (Versicherung, Outsourcing) oder durch Vorbeugung reduziert wird, nicht aber auf eine Verbesserung des Sicherheitsniveaus.

Denn das geschäftliche Risiko leitet sich nicht (allein) aus realen Bedrohungen ab, sondern muss die Kritikalität der betroffenen Anwendung für das Kerngeschäft berücksichtigen. Sicherheitsbeauftragte kennen aber häufig die maximalen Ausfallzeiten nicht, die sie für ein IT-System garantieren müssen, und der Geschäftsleitung sind die konkreten Bedrohungen der genutzten Systeme und Daten oft unbekannt.

Risiko-adäquate Prioritätensetzung in der IT-Sicherheit gelingt daher nur mit Kenntnis des „Business Impact“ betroffener IT-Systeme und Daten einerseits und deren realer Bedrohungen andererseits.

1 Security News

1.1 RSA-576 faktorisiert

Am 27.04.2004 ging die Nachricht durch die Ticker, dass die 576-bit-Challenge der Firma RSA gelöst sei. Tatsächlich wurde die 174 Dezimalstellen lange Zahl bereits am 03.12.2003 zerlegt. Die Faktorisierung gelang einem Team der Universität Bonn um Professor Franke mit Unterstützung durch das Institut für Experimentelle Mathematik in Essen und das BSI. Die verteilte Berechung erfolge auf einem Linux-Cluster mit 144 PCs (400 MHz, Pentium II) und verwendete den General Number Field Sieve-Algorithmus – mit einem Aufwand von umgerechnet 13.200 MIPS-Jahren.

Interessant dabei: Dieser Faktorisierungserfolg bestätigt die Prognose, die Secorvo vor drei Jahren auf der Basis der Faktorisierungserfolge der vergangenen 30 Jahre gestellt hat (siehe Bild), und die weit weniger dramatisch ausfiel als viele Expertenwarnungen und die Erwartung des BSI. Danach wäre 2004 erstmals die Faktorisierung einer 630 bit langen Zahl zu erwarten gewesen – was nun eher unwahrscheinlich erscheint. Selbst die frühestens für das Jahr 2020 vorausgesagte Faktorisierung eines 1024 bit langen RSA-Schlüssels könnte sich daher noch als zu pessimistische Befürchtung erweisen – allen Warnern zum Trotz, die seit Jahren Schlüssellängen von 2048 bit und mehr empfehlen oder gar das baldige Ende von RSA prophezeihen.

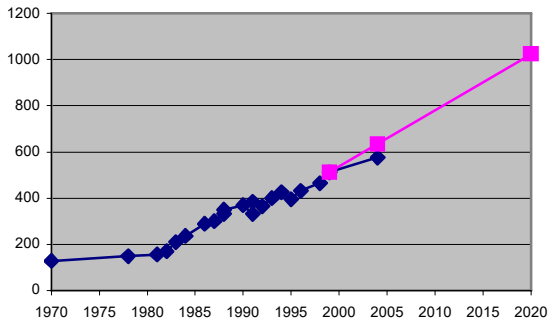


Bild: Secorvo-Prognose 2001 [BoFT_02]

1.2 TCP-Schwachstelle

Das im September 1981 in RFC 793 spezifizierte TCP (Transmission Control Protocol) ist heute das zentrale Protokoll des Internet. Da überrascht es, dass erst im Jahr 2004 eine inhärente Schwachstelle dieses Protokolls aufgedeckt wird: Der Standard erlaubt – aus guten Gründen – bestehende TCP-Verbindungen durch ein Reset-Paket (RST) abzubrechen. Diese Eigenschaft wird zur Schwachstelle, wenn das RST-Paket nicht vom einem der beiden Verbindungspartner gesendet wird, sondern von einem Dritten. Besonders kritisch ist, wenn so Verbindungen gekappt werden, über die Backbone-Router im Internet ihre Routing-Informationen austauschen. Der Angreifer muss allerdings die 32 bit lange, zum Schutz gegen dererlei Attacken zufällig gewählte so genannte Sequence-Number kennen – und dazu entweder die Verbindung belauschen oder sie erraten.

Am 20.04.2004 schlug nun das US-CERT aufgrund einer am gleichen Tag veröffentlichten Studie von Paul Watson Alarm: Häufig akzeptieren TCP-Implementierungen jede Sequence-Number in einem Fenster von 64 kB Größe. Hierdurch wird der effektiv zu durchsuchende Schlüsselraum für den Angreifer von 2^{32} auf 2^{16} Möglichkeiten reduziert. Er muss also maximal 65.536 Pakete schicken – anders als 1981 ist das heute eine Angelegenheit von nur wenigen Minuten.

Fast zeitgleich wurde von der IETF am 19.04.2004 ein Internet-Draft veröffentlicht, der diese Schwachstelle beheben soll. Pikanterweise hat Cisco ein Patent auf das dort beschriebene Verfahren eingereicht. Dieses Vorgehen wurde prompt von Open-Source-Vertretern kritisiert. In OpenBSD findet sich ein anderer Ansatz zur Behebung der Schachstelle: Dort wird die ebenfalls vom Angreifer zu ratende Quell-Portnummer nicht fortlaufend, sondern ebenfalls zufällig gewählt. So gewinnt man die fehlenden 16 bit des effektiven Schlüsselraums wieder zurück.

1.3 Kommt DNSSEC?

Eines der wichtigsten Kommunikationsprotokolle im Internet ist das Domain Name System (DNS), welches für die Zuordnung von IP-Adressen und Hostnamen verantwortlich ist. Dass DNS – genau wie alle anderen verbreiteten Protokolle, die sich des DNS bedienen – über keinerlei Sicherheitsmechanismen verfügt, ist seit Jahren bekannt; bereits Mitte der 90er Jahre wurde daher die IETF-Arbeitsgruppe DNSSEC gegründet, um das Protokoll abzusichern.

Erste technische Drafts zu DNSSEC wurden bald veröffentlicht; ebenso schnell kam man jedoch zu der Einsicht, dass zur Einführung von DNS – insbesondere auf Ebene der Root-Nameserver – vor allem organisatorische Probleme zu überwinden sind. Im Jahr 2000 untersuchte die DENIC eG mit Untersützung von Secorvo die flächendeckende Einführung von DNSSEC innerhalb der Top Level Domain .de. Die Studie kam zu dem Ergebnis, dass DNSSEC im großen Stil noch nicht einsetzbar war. Jüngst legte auch das BSI eine Studie vor, die zu vergleichbaren Resultaten kommt.

Immerhin: Der erste Schritt auf Anwendungsseite ist getan. Die neueste Version 9.3 des im Internet am häufigsten eingesetzten Nameservers BIND unterstützt die DNSSEC-Protokolle. Auch liefen erste erfolgreiche Pilotprojekte. Nun bleibt abzuwarten, ob einerseits andere Hersteller nachziehen und andererseits die wichtigen Betriebsprozesse zur Einführung von DNSSEC so etabliert werden können, dass auch Top Level Domains und die Root-Nameserver DNSSEC anbieten können. Dann erst entfalten Security-Protokolle wie SSL ihre volle Wirkung.

1.4 T-Online-Authentifikation

Die Authentifikation beim Zugriff auf E-Mail-Postfächer erfolgt bei T-Online implizit über das Einwahl-Login. Ein zusätzliches Passwort wird daher beim Zugriff auf die Mailbox nicht mehr benötigt.

Das verursacht bei T-DSL-Router-Zugängen, die von mehreren Personen genutzt werden, ein Problem: Beim Zugriff auf die T-Online-Mailbox werden automatisch die E-Mails des T-DSL-Inhabers abgerufen. Schlimmer: Gelingt es einem Nachbarn (oder „war driver“), sich in ein via T-DSL mit dem Internet verbundenes WLAN einzuklinken, hat er unmittelbaren Zugriff auf den Mail-Account des WLAN-Betreibers.

Seit Kurzem bietet T-Online daher die Möglichkeit, für den E-Mail-Account einen POP3-Passwortschutz einzurichten.

1.5 Sicherheitsloch Schutzsoftware

In den vergangenen Wochen waren wieder mehrere Sicherheitsprodukte Thema von Security Advisories. Am 13.05.2004 wurden schwer wiegende Schwachstellen der verbreiteten Norton Personal Firewall und von Norton Internet Security (Symantec) in verschiedenen Versionen aufgedeckt. Manipulierte DNS- und NetBIOS-Pakete können Heap oder Buffer Overflows und damit die Ausführung beliebigen Codes verursachen. Das Einspielen von Updates oder die Aktivierung der LiveUpdate-Funktion ist daher dringend angeraten. Nachdem am 24.05.2004 auch ein fehlerhaftes ActiveX-Control in Norton Antivirus bekannt wurde, das die Ausführung beliebigen Codes erlaubt, folgte am 26.04.2004 der Virenscanner von F-Secure: Er erkennt die aktuelle Sobig.G-Variante nicht in LHA-komprimierten Dateien – und kann über manipulierte LHA-Anhänge zum Absturz gebracht werden. Zum Schutz vor diesen Angriffen sollten die vom Hersteller für die Client- und die Serverkomponenten bereit gestellten Patches installiert werden.

Schließlich wurde am 15.05.2004 der aktuelle Source Code von Ciscos Router- und Switch-Betriebssystem IOS v12.3 im Internet publiziert. Zwar ist der Code inzwischen nicht mehr auf den Seiten von Securitylab verfügbar; mit gezielten Angriffen auf neue Schwachstellen sollte in den kommenden Wochen jedoch gerechnet werden.

2 Secorvo News

2.1 Secorvo College aktuell

Gerne hätten wir unser Ausbildungsangebot zur IT-Sicherheit schon 1999 vom Start weg mit einem international anerkannten Abschluss vervollständigt. Weil jedoch alle international verbreiteten Zertifikate sich inhaltlich entweder an der eingeschränkten Perspektive der Revision bzw. an spezifisch amerikanischen, insbesondere rechtlichen Rahmenbedingungen orientieren oder auf eine Multiple-Choice-Prüfung beschränken, bieten wir nun einen eigenen Ausbildungsgang zum „IT Security Professional“ an.

Der Ausbildungsgang orientiert sich an der an Hochschulen bewährten Kombination aus Pflicht- und Wahlveranstaltungen: Die Teilnahme an fünf Seminaren von Secorvo College, darunter „IT-Sicherheit heute“ und je ein Seminar aus den Bereichen „Grundlagen“, „Lösungen“ und „Systeme“ qualifiziert zum „IT Security Professional“.

Mit einer theoretischen und praktischen Prüfung, die ab 2005 mindestens zweimal jährlich angeboten wird, können Sie das Zertifikat zum „Certified IT Security Professional“ erwerben.

http://www.secorvo.de/college

2.2 Security Awareness Symposium 2004

Inzwischen steht das Programm des diesjährigen zweiten Security Awareness-Symposium am 29.-30.06.2004. Nach Fiducia, Münchener Rück, RWE, SAP und der Schweizerischen Armee (2003) werden in diesem Jahr BASF, BMW, FinanzIT und T-Systems über ihre Awareness-Aktivitäten berichten. Weiter steht die Frage der Nachhaltigkeit der Sensibilisierung im Mittelpunkt der Veranstaltung, zu der sich schon jetzt Sicherheitsverantwortliche zahlreicher Unternehmen angemeldet haben. Die Teilnahmegebühr liegt bei 390 € (zzgl. MwSt.).

3 Veranstaltungshinweise

Juni 2004	
07.-08.06.	IT Risk Management 2004 (COMPUAS, Köln)
13.-18.06.	16th Computer Security Incident Handling Conference, Budapest (FIRST, Budapest)
14.-15.06.	IT-Security Management (Secorvo College, Karlsruhe)
14.-18.06.	Information Security Management (Secorvo College, Karlsruhe)
22.-23.06.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.-30.06.	Security Awareness Symposium 2004 (Secorvo, Karlsruhe)
August 2004	
09.-13.08.	USENIX Security Symposium (San Diego)
September 2004	
21.-22.09.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Juni 2004

Dirk Fox, Stefan Gora,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 6, 3. Jhrg. 2004
Stand 28. Juni 2004

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Chefsache

1 Security News

1.1 „Phishing“ auf dem Vormarsch

1.2 Studie von silicon.de

1.3 Happy Birthday, Diffie!

1.4 Hilfe bei Wurmbefall

1.5 MS Antivirus-Guide

1.6 Fluggastdaten in die USA

1.7 PC/SC Draft 2.0

1.8 WLAN-Router-Attacken

1.9 Home Made Router-Security

1.10 SQL-Injection in Oracle E-Business Suite

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Nexus erhält ISIS-MTT-Konformitätssiegel

3 Veranstaltungshinweise

Impressum

Editorial: Chefsache

„IT-Sicherheit ist Chefsache“: Eine oft genutzte, als Slogan missbrauchte, zur Phrase gedroschene – aber tatsächlich zutreffende Behauptung. Allerdings meist falsch oder sogar gänzlich unverstanden. Über 55% der Befragten einer aktuellen Studie von silicon.de bewerten sie als „wichtig“ oder sogar „sehr wichtig“ (32%). Da lohnt ein kritischer Blick.

Zunächst einmal ist die Aussage trivial: Handelt es sich bei IT-Sicherheit um eine Angelegenheit, um die sich ein Unternehmen kümmern muss, dann liegt die Verantwortung dafür natürlich bei der Unternehmensleitung – wo auch sonst.

Tatsächlich hat die Aussage größere Tragweite. Kaum ein Unternehmen, bei dem heute nicht zumindest einzelne, wenn nicht zentrale oder gar alle Geschäftsprozesse in erhebliche Abhängigkeit von Teilbereichen der eingesetzten Informationstechnik geraten sind. Die zuvor verwendeten (manuellen) Prozesse wurden fast immer vollständig abgelöst – daher existieren nur noch sehr selten Ersatzprozesse für den Fall des Ausfalls. Nur noch wenige Unternehmen würden heute einen eintägigen IT-Ausfall problemlos „wegstecken“, fast alle könnte ein einwöchiger Ausfall in eine Existenz bedrohende Schieflage bringen.

Nur: Die wenigsten Unternehmen kümmern sich um dieses Problem so, wie es die „Sorgfalt eines ordentlichen Geschäftsmanns“ (§ 43 GmbHG) „und gewissenhaften Geschäftsleiters“ (§ 93 AktG) gebieten. Das Aktienrecht fordert sogar explizit und zwingend die Einrichtung eines Überwachungssystems zur Erkennung von „den Fortbestand des Unternehmens gefährdenden Entwicklungen“ (KontraG, § 91 AktG).

Zwar kann die Geschäftsleitung das Thema delegieren. Wählt sie jedoch nicht sorgfältig geeignete Mitarbeiter dafür aus, gibt sie die für die Umsetzung erforderlichen Mittel nicht frei oder kontrolliert sie nicht die Qualität des Ergebnisses, verletzt sie ihre Sorgfaltspflicht – und haftet im Schadensfall.

1 Security News

1.1 „Phishing“ auf dem Vormarsch

Die Fälle von Betrugsversuchen durch so genanntes „Phishing“ nehmen auch im deutschsprachigen Raum zu. E-Mails, die angeblich von E-Business-Angeboten wie z. B. Ebay oder einer Direktbank stammen, fordern den Benutzer dazu auf, seine Accountdaten zu überprüfen. Klickt der Empfänger auf den in der E-Mail enthaltenen Link, landet er auf einer Webseite, die wie die Originalseiten aussieht – tatsächlich aber von Betrügern angelegt wurde. Dabei nutzen einige „Phisher“ Sicherheitsschwächen von Browsern, wie z. B. die am 18.06. 2004 gemeldete Schwachstelle von Opera, mit der die dem Benutzer angezeigte URL manipuliert werden kann.

Fällt der Empfänger auf den Bluff herein und gibt bereitwillig Konto- oder Kreditkartennummer, PIN und womöglich eine TAN ein, kann der Angreifer selbst auf den Account zugreifen. Dabei lassen sich „Phishing“-E-Mails leicht erkennen: Seriöse Anbieter versenden grundätzlich keine E-Mails dieser Art.

1.2 Studie von silicon.de

Nach einer Pause von drei Jahren hat silicon.de am 04.06.2004 eine zweite umfangreiche Studie zur IT-Sicherheit auf der Basis von über 1.000 Fragebögen vorgelegt. Zahlreiche Ergebnisse sind wenig überraschend, interessant allerdings das eine oder andere Detail:

- Dramatisch erscheint der Anstieg der Angriffe mit Trojanischen Pferden: Gaben in der ersten Studie nur 20% der Befragten Sicherheitsvorfälle mit Trojanern an, stieg die Zahl in der aktuellen bereits auf 42%.
- Direkt auf den Schutz des Netzwerks folgt als zweitwichtigster Faktor einer effektiven IT-Sicherheit das Sicherheitsbewusstsein der Mitarbeiter: fast 90% der Befragten stuften es als „sehr wichtig“ (63%) oder „wichtig“ ein. Auch die große Resonanz auf das 2. Deutsche Security Awareness Symposium (29.-30.06.2004) bestätigt diesen Trend.
- Als „Daumengröße“ zur Abschätzung des Investitionsvolumens für IT-Sicherheit scheint sich ein Wert von 5-10% des IT-Budgets einzuschwingen: Mehr als ein Drittel der befragten Unternehmen liegt in diesem Bereich, ein weiteres Drittel knapp darüber oder darunter.

1.3 Happy Birthday, Diffie!

Der (Mit-) Entdecker der Public Key Kryptographie Whitfield Diffie feierte am 05.06. 2004 seinen 60. Geburtstag. Auch von uns ein herzliches Prosit auf Diffie, der – mittlerweile in der Funktion des Chief Security Officer von Sun – seit seiner bahnbrechenden Entdeckung zusammen mit Martin E. Hellman Mitte der 70er Jahre weder seine Haarpracht noch seinen Spaß an (Datenschutz-motivierten) Cracks verloren hat.

1.4 Hilfe bei Wurmbefall

Nach Feststellung eines Viren- oder Wurmbefalls stellt sich die Frage „Was tun?“ Aus Sicherheitsperspektive ist die Empfehlung eindeutig: System-Image bzw. Backup zurückspielen oder das System neu aufsetzen. In manchen Fällen können die Schädlinge auch durch das Starten des Betriebssystems im abgesicherten Modus und anschließendem manuellen Entfernen beseitigt werden.

Alternativ können spezielle Virus Removal Tools wie Stinger des Herstellers NAI hilfreich sein – die sicherste Methode bleibt aber ein Neuaufsetzen der betroffenen Systeme. Das effektivste Verfahren ist jedoch der vorbeugende Einsatz aktueller Virenscanner und die regelmäßige Aktualisierung der zugehörigen Viren-Informationsdatenbank.

1.5 MS Antivirus-Guide

Von Microsoft wurde am 15.06.2004 ein „Antivirus Defense-in-Depth Guide“ zur Verfügung gestellt. Warum das englischsprachige, 90seitige pdf-Dokument als ausführbare MSI-Installer-Datei zum Download angeboten wird, entzieht sich allerdings dem Verständnis.

Das umfassende Werk enthält nicht sehr viel Neues: Neben den hinlänglich bekannten Standardmaßnahmen werden einige sinnvolle weitere Schutzmöglichkeiten wie z. B. der Einsatz von Software Restriction Policies aufgezeigt.

1.6 Fluggastdaten in die USA

Am 17.05.2004 hat die EU-Kommission entgegen den Protesten von Datenschützern und dem Europäischen Parlament der vom US-Kongress zum Schutz vor Terroristen geforderten Übermittlung von Flugpassagierdaten an die USA zugestimmt, die bereits seit Monaten praktiziert wird. 34 Datenfelder je Passagier dürfen nun 3,5 Jahre von den zuständigen US-Behörden gespeichert werden – nach Ansicht der Kritiker ein eklatanter Verstoß gegen die EG-Datenschutzrichtlinie.

1.7 PC/SC Draft 2.0

Totgesagte leben länger: Die 1997 mit der Vision eines vereinheitlichten und Plattform-unabhängigen Standards für Smart-Cards, Lesegeräte und Anwendungen angetretene PC-SC-Workgroup veröffentlichte schon im Dezember 1997 die erste Spezifikation PC/SC v1.0. Seitdem war es ruhig um diesen wichtigen Standard. Anfang Juni 2004 wurde nun Version 2.0 der Spezifikation zum „public review“ frei gegeben.

1.8 WLAN-Router-Attacken

Viele der mittlerweile weit verbreiteten DSL- und WLAN-Router werden ohne weiter gehende Sicherheitseinstellungen betrieben. Den Benutzern ist dabei offenbar nicht klar, dass sie so ein „Bürgerfunknetz“ betreiben, das ohne ihr Wissen auch von Dritten verwendet und für Angriffe missbraucht werden kann. Treten im ersten Fall „nur“ zusätzliche Verbindungskosten auf, ist der zweite wesentlich schwerwiegender. Denn kann ein Unternehmen als Quelle eines Angriffs mit Hilfe seines Providers einen ungeschützten DSL-Zugang identifizieren, wird sich der Geschädigte mit Klagen und Schadensersatzforderungen zunächst an den Betreiber des Anschlusses wenden.

Doch auch vermeintlich sicher konfigurierte Systeme können anfällig sein: Der Router WG602v1 des Herstellers Netgear enthielt eine undokumentierte Hintertür in Form eines fest programmierten Administratorzugangs. Die Schwachstelle wurde am 04.06.2004 durch ein Update der Firmware behoben. Nur wenige Tage später, am 18.06.2004, wurde allerdings eine weitere Zugangsmöglichkeit über das Netzwerk-Management-Protokoll SNMP bekannt, über die die Konfiguration verändert und das System unbrauchbar gemacht werden können. Das Einspielen der aktuellen Firmware wird daher dringend empfohlen.

1.9 Home Made Router-Security

Da die Firmware zahlreicher Router und anderer Netzwerkgeräte auf Programmcode basiert, der unter der GNU General Public License (GPL) entwickelt wurde, haben sich einige Hersteller inzwischen dazu durchgerungen, Teile Ihres Quellcodes oder zumindest Bibliotheken zur Verlinkung mit eigener Software ebenfalls zu publizieren. Wer über das entsprechende technische Know-How verfügt, kann damit das Betriebssystem seines Routers anpassen und weitere, durch die Hardware unterstützte Sicherheitsfunktionen wie etwa virtuelle LANs implementieren.

So werden beispielsweise für das Modell WRT54G des Herstellers Linksys der Quellcode und zusätzliche kommerzielle und selbst entwickelte Firmware-Versionen

angeboten sowie offene Firmware-Versionen in Projekten wie OpenWRT weiterentwickelt.

1.10 SQL-Injection in Oracle E-Business Suite

Die Oracle E-Business Suite 11i ist, wie am 03.06.2004 gemeldet wurde, für einen Angriff durch SQL-Injection verletzlich. Ebenso betroffen ist Oracle Apps in allen 11er Versionen. Einem versierten Angreifer kann es so gelingen, mit seinem Browser in den Eingabefeldern SQL-Befehle absetzen, die direkt vom Applikationsserver an die Datenbank übertragen und ausgeführt werden. Zur Abhilfe werden ein Update und der Einsatz von Filterungstechniken auf Applikationsebene empfohlen.

2 Secorvo News

2.1 Secorvo College aktuell

Nach der Sommerpause in den Monaten Juli und August, die in diesem Jahr wieder zu zahlreichen internationalen Security-Events an attraktiven Urlaubsorten lädt – darunter Turku, Las Vegas, San Diego, Toulouse, Sophia Antipolis und Klagenfurt – startet das College-Programm des zweiten Halbjahrs 2004 im September mit Seminaren zu Lotus Notes Security und Public Key Infrastrukturen.

http://www.secorvo.de/college

2.2 Nexus erhält ISIS-MTT-Konformitätssiegel

Am 27.05.2004 hat der Certificate Manager 5.3 von Nexus nach Prüfung durch das Secorvo Prüflabor vom ISIS-MTT-Board das ISIS-MTT-Konformitätssiegel als CA-Server erhalten. Damit liegt nunmehr das vierte Produkt vor, dessen ISIS-MTT-Konformität in einem vereinheitlichten Testverfahren nachgewiesen wurde. Weitere Produkte werden derzeit auf ISIS-MTT-Konformität untersucht.

3 Veranstaltungshinweise

Juni 2004	
29.-30.06.	Security Awareness Symposium 2004 (Secorvo, Karlsruhe)
Juli 2004	
12.-13.07.	Foundations of Computer Security FCS'04 (Turku)
24.-29.07.	Black Hat Briefings (Black Hat, Las Vegas)
August 2004	
09.-13.08.	USENIX Security Symposium (USENIX, San Diego)
23.-26.08.	19th IFIP International Information Security Conference (Toulouse)
September 2004	
15.-17.09.	7th International Symposium on Recent Advances in Intrusion Detection – RAID (Sophia Antipolis)
20.-21.09.	Elektronische Geschäftsprozesse – EGP 2004 (Klagenfurt)
21.-22.09.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Juli 2004

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 7, 3. Jhrg. 2004
Stand 22. Juli 2004

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial:
Abschied von der Sicherheit

1 Security News

1.1 Phishing mit Frames

1.2 802.11i WLAN Security

1.3 Online-Banking-Trojaner

1.4 Digitale Spurensuche

1.5 Spurenverwischung

1.6 Grundschutztool 3.1

1.7 MD5-Passwort-Cracker

2 Secorvo News

2.1 IT Security Professional

2.2 White Paper: Poststelle

3 Veranstaltungshinweise

Impressum

Editorial: Abschied von der Sicherheit

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts.

Gene Spafford,
Scientific American, 3/1989

Immer wieder gerne hervorgekramt und oft gebetsmühlenartig wiederholt – die vermeintliche Weisheit, dass 100%ige Sicherheit nicht erreichbar ist. Aber was sagt uns das? Häufig muss diese Einsicht als Rechtfertigung für Resignation herhalten: Wenn es ohnehin nicht sicher geht, warum dann überhaupt Aufwand betreiben?

Dabei ist die Erkenntnis irreführend. Tatsächlich gibt es 100%ige Sicherheit nicht. Viel schlimmer: Sicherheit gibt es nicht. Sofern man sie als einen Zustand versteht, der sich nicht partiell erreichen lässt – „ein bisschen schwanger“ geht eben auch nicht.

Zielführender, als die Sicherheit zu messen, ist daher die Bewertung des Schutzniveaus. Damit werden differenzierte Aussagen möglich – die Frage „Haben wir das Notwendige getan?“ lässt sich im Gegensatz zu „Sind wir sicher?“ mit Blick auf die realistischen Bedrohungen einerseits und die getroffenen Schutzmaßnahmen andererseits detailliert beantworten.

Allein auf diesem Weg ist eine sachgemäße Reaktion auf perfide neue Angriffsmuster, wie PWSteal.Refest oder Frame-Phishing möglich: Nur wer mit seinem System nicht im Administrator-Modus surft, einen Browser ohne Sicherheitslöcher und mit reduzierten „Features“ nutzt, sich mit einer Personal Firewall sichert, einen aktuellen Virenscanner verwendet, Security-Patches einspielt und die Sicherheitsmechanismen des Betriebssystems konfiguriert, hat seine Hausaufgaben gemacht.

Danach darf man wieder auf die Hersteller schimpfen – oder über die Unsicherheit der (IT-) Welt im Allgemeinen klagen. Wenn man dann noch Grund dazu hat.

1 Security News

1.1 Phishing mit Frames

Wie in den SSN 06/2004 berichtet, nehmen die Fälle von Phishing erheblich zu. Die verwendeten Techniken werden immer perfider: Mit einem neuen Trick gelingt es, die Eingabedaten eines Browser-Fensters, z. B. einer Online-Banking-Anwendung, an den Server eines anderen Fensters zu senden. Zwar sollten Cross-Domain-Sicherheitsmechanismen den Zugriff auf Frames anderer Domänen verhindern – das funktioniert jedoch bei den verbreitetsten Browsern (Internet Explorer, Netscape, Mozilla) nicht. Eine Demonstration dieser gravierende Schwachstelle ist seit dem 02.07.2004 online beim heise-Verlag zu finden. Opera war der erste Browser, bei dem dieses Sicherheitsloch am 19.07.2004 kurzfristig gestopft wurde; inzwischen gibt es Updates für alle gängigen Browser.

1.2 802.11i WLAN Security

Am 24.06.2004 wurde der lange erwartete Standard IEEE 802.11i verabschiedet, der verbesserte und erweiterte Sicherheitsmechanismen für Wireless LANs festlegt. Im Rahmen des Get IEEE 802 Programms wird der neue Standard übrigens ab Ende 2004 frei im Internet verfügbar sein.

Anfang des Jahres 2001 waren im Vorgänger-Standard Wireless Equivalent Privacy (WEP) schwer wiegende Sicherheitslücken gefunden worden. Daher nahmen einige Hersteller, die des Wartens auf den WEP-Nachfolger überdrüssig waren, schon Anfang 2003 unter der Bezeichnung WPA (WiFi Protected Access) einen Teil der jetzt verabschiedeten Neuerungen vorweg: die Authentifikation von WLAN-Clients durch RADIUS-Server nach 802.1x und eine TKIP/RC4-Verschlüsselung, die die bekannten Schwachstellen von WEP ausbügelt. Die wesentlichen Erweiterungen von IEEE 802.11i – inoffiziell auch „WPA2“ genannt – gegenüber WPA sind

- die Verwendung von CCMP/AES alternativ zu TKIP/RC4 als Standard-Verschlüsselungsverfahren,
- die Unterstützung sicherer „Ad-hoc“-WLANS und
- Methoden für die sichere Übergabe eines Clients zwischen Access-Points sowie für eine sichere Abmeldung.[1]

Aufgrund der Verwendung von AES erfordert der Wechsel zu 802.11i in der Regel einen Hardware-Upgrade von Access-Points und WLAN-Karten – oder einen schnellen Rechner, der der Netzwerkkarte die Ver- und Entschlüsselung abnimmt. Wer seine WLAN-Hardware erst in diesem Jahr gekauft hat, kann Glück haben und kommt möglicherweise mit einem Firmware-Upgrade aus – dank der langen Vorlaufzeit des Standards konnten Hersteller ihre Chips seit Ende 2003 anpassen.

Leer gehen die Besitzer älterer Geräte des 11-Mbit/s-Standards 802.11b aus. Ihnen wird meist nichts anderes übrig bleiben, als ihr WLAN durch ein darüber gestülptes VPN abzusichern. Wer auf den 54-Mbit/s-Standard 802.11g wechseln will, sollte darauf achten, dass die gewählte Lösung zumindest WPA unterstützt und die Hardware für 802.11i vorbereitet ist.

1.3 Online-Banking-Trojaner

Wie unter anderem am 02.07.2004 vom BSI und schon am 29.06.2004 von SANS berichtet wird, existiert ein neuer besonders heimtückischer Trojaner namens PWSteal.Refest. Er nistet sich als Browser Helper Object in den Internet Explorer ein und schneidet gezielt Daten mit, die verschlüsselt an die Domänen citibank.de, deutsche-bank.de und weitere Online-Banking-Server übertragen werden. Dabei werden die Daten vor der Verschlüsselung im Klartext abgegriffen und an einen Rechner im Internet versendet. Bester Schutz: ein anderer Browser, z. B. Mozilla.

[1] Bei WPA kann ein Angreifer alle angemeldeten Clients ungehindert abmelden.

1.4 Digitale Spurensuche

Eine noch recht junge Disziplin der Informationssicherheit ist die digitale oder IT-Forensik. Ziel einer forensischen Analyse ist es, Systemeinbrüche nicht nur generell zu erkennen, sondern die digitalen Spuren des bzw. der Angreifer im Detail zu analysieren, um Rückschlüsse auf Vorgehensweise, Schäden sowie ggf. die Identität des Angreifers ziehen zu können.

IT-Forensiker werden mittlerweile durch eine Vielzahl mächtiger, oft kostenlos verfügbarer Tools unterstützt. Zwei dieser Tools, die auch von Secorvo bei forensischen Analysen eingesetzt werden, sind am 02.06.2004 in neuen Versionen erschienen: Das „Sleuth Kit“ sowie das zugehörige grafische Frontend „Autopsy“. Bei beiden Programmen handelt es sich um seit mehreren Jahren etablierte frei verfügbare UNIX-Tools, die sich vor allem auch hervorragend zur Analyse von Windows-PCs eignen.

Da eine erfolgreiche forensische Analyse neben geeigneten Tools auch eine entsprechende Expertise voraussetzt, findet man in jüngster Zeit immer mehr unterstützende Literatur zu dem Thema: zwei aktuelle White Paper (vom 26.06.2004 und vom 16.05.2004) dokumentieren auf anschauliche Weise die forensische Analyse eines Windows-PCs.

1.5 Spurenverwischung

Es mehren sich die Gründe für Hacker und Virenautoren, nervös zu werden: Anfang Juli 2004 gingen mehrere Meldungen über Fahndungserfolge und Haftstrafen aus Australien und Spanien durch die Presse.

Kurz darauf wurde am 04.07.2004 mit Bagle.ad der erste Computerwurm entdeckt, der seinen eigenen Quellcode mit verschickt. Böse Zungen vermuten, dass dies nicht als Nachhilfe für Möchtegern-Virenautoren gedacht war, sondern zum „Spurenverwischen“: Der Quellcode genügt damit nicht mehr als Beweis, dass ein Virenautor dingfest gemacht wurde.

1.6 Grundschutztool 3.1

Die überarbeitete Version 3.1 des BSI Grundschutztools ist am 05.07.2004 erschienen. Eine Demoversion kann von der Webseite des BSI geladen werden. Die Einzel-Lizenz kostet 765 €, ein Update 68,10 €. Neben einigen Änderungen der Datenbankroutinen wurden unter anderem die wichtigen neuen Bausteine Apache Webserver, Microsoft Exchange/Outlook und Internet Information Server ergänzt. Grundsätzlich ist es nun, wie Version 3.0 mit Servicepack 2, komplett zweisprachig (deutsch, englisch).

1.7 MD5-Passwort-Cracker

Am 03.07.2004 wurde über Slashdot der Dienst passcracking.com publik gemacht, der aus MD5-Hashes die zugehörigen Passwörter zurückrechnen kann – solange sie aus maximal acht Kleinbuchstaben oder Ziffern bestehen. Zu diesem Zweck hat das System die Hash-Werte aller 36^8 möglichen Passwörter vorberechnet. Diese Daten würden normalerweise gut 61 Terabyte Festplattenplatz füllen. Mit einem auf der Crypto 2003 veröffentlichten, optimierten Time/ Memory-Tradeoff kann der benötigte Speicherplatz jedoch zu Lasten einer deutlich höheren Rechenleistung beim Wiederfinden der richtigen Lösung auf eine vertretbare Größe beschränkt werden.

Ein auf demselben Prinzip beruhender „Advanced Instant NT Password Cracker“ wurde nach 200.000 Anfragen innerhalb von nur einer Woche wieder vom Netz genommen, ist aber seit dem 14.07.2004 wieder verfügbar.

Diese Entwicklung sollte auch die letzten Zweifler bewegen, hinreichend sichere Passwörter zu wählen. Zugleich wird deutlich, wie wichtig es ist, Kryptoalgorithmen nicht ad-hoc zu implementieren, sondern sie in etablierte, von Experten untersuchte Verfahrensweisen einzubetten: Unix-typisch „gesalzene“ Passwörter kann das Programm nämlich nicht knacken.

2 Secorvo News

2.1 IT Security Professional

Der von Secorvo College seit Anfang Mai angebotene Ausbildungsgang zum IT Security Professional erfreut sich wachsender Beliebtheit: Inzwischen haben zwei Teilnehmer den Ausbildungsgang absolviert; für den ab 2005 eine Abschlussprüfung mit Zertifikat (Certified IT Security Professional – CISP) angeboten wird.



Noch eine aktuelle Terminänderung: Das eintägige Seminar PKI für Fortgeschrittene wird im Anschluss an das PKI-Seminar am **30.09.2004** stattfinden.

2.2 White Paper: „Poststelle“

Das Modell der „virtuellen Poststelle“, das das Konzept eines Ende-zu-Ende-Schutzes für E-Mail durch die Idee einer zentralen Ver- und Entschlüsselungsinstanz ersetzt, findet immer mehr Anhänger – und wird inzwischen auch von mehreren Herstellern unterstützt. Die Vor- und Nachteile dieses Ansatzes und die größten Stolperfallen diskutieren Holger Mack und Dr. Markus Michels im neuen Secorvo White Paper „Praktischer Einsatz von E-Mail-Gateways“.

3 Veranstaltungshinweise

Juli 2004	
24.-29.07.	Black Hat Briefings (Black Hat, Las Vegas)
August 2004	
09.-13.08.	USENIX Security Symposium (USENIX, San Diego)
11.-13.08.	Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004 (Cambridge/Boston)
15.-19.08.	Crypto 2004 (IACR, Santa Barbara)
September 2004	
15.-17.09.	7th International Symposium on Recent Advances in Intrusion Detection – RAID (Sophia Antipolis)
20.-21.09.	Elektronische Geschäftsprozesse – EGP 2004 (Klagenfurt)
21.-22.09.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)
28.-29.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
30.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
August 2004

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 8, 3. Jhrg. 2004
Stand 23. August 2004

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: DES – Ein Nachruf

1 Security News

1.1 WinXP SP 2 verfügbar

1.2 Déjà-vu bei Check Point

1.3 Acrobat ohne Netz

1.4 Biometrische Realität

1.5 Sicherheitsloch in PuTTY

1.6 Musterrichtlinien des BSI

1.7 MD5: Keine Panik

1.8 Bluetooth-Distanzangriff

1.9 WPA im Verdacht

1.10 SANS XP Survival Guide

1.11 BSI-Kongress 2005

2 Secorvo News

2.1 Secorvo College aktuell

2.2 25. SSN-Jubiläum

3 Veranstaltungshinweise

Impressum

Editorial: DES – Ein Nachruf

"NIST determined that the strength of the DES algorithm is no longer sufficient to adequately protect Federal government information."

Jetzt ist es amtlich: Das NIST hat am 26.07.2004 offiziell angekündigt, den DES-Standard FIPS 46-3 zurückzuziehen.

Erinnern wir uns: Seit 1977 prägte der DES – vom National Bureau of Standards als FIPS 46-1 publiziert –, das weltweit erste standardisierte Verschlüsselungsverfahren, sowohl die Kryptoanalyse als auch die Diskussion über die Rolle des amerikanischen Geheimdienstes NSA, zeitweilig in „No Such Agency" umgetauft. Der DES entstand 1975 aus einer Entwicklung des IBM-Kryptologen Feistel, der Lucifer-Cipher. Tatsächlich reduzierte die NSA für den Standard die ursprüngliche Schlüssellänge von 128 auf 64 bit – und machte weitere 8 bit zu Paritätsbits. Schon damals war diese Schlüssellänge von 56 bit Stein des Anstoßes; mit der Geheimhaltung des Entwurfs der S-Boxen aber nährte die NSA zudem den Verdacht, eine Hintertür im Algorithmus verborgen zu haben.

Biham und Shamir gelang 1990 eine Attakke auf den DES; sie war theoretisch bedeutsam, aber nicht praxisrelevant. Erst die Koordination von mehreren 10.000 PCs über das Internet, die in Idle-Zeiten DES-Schlüssel durchprobierten, versetzte dem DES Ende 1997 den „Todesstoß": Die erste DES-Challenge wurde so in 140 Tagen gelöst. Schließlich schockte Mitte 1998 der DES-Cracker der EFF, der ein Cluster von Spezialchips verwendete, die Krypto-Welt: In weniger als drei Tagen war der Key der zweiten DES-Challenge gefunden. Abgelöst wurde der DES mit der Veröffentlichung des Advanced Encryption Standard 2001 (FIPS 197). Der mehrjährige Auswahlprozess fand in der Fachöffentlichkeit statt – und wurde selbst von kritischen Beobachtern wie Bruce Schneier als sachlich und fair bewertet. Mit dem DES hat die Krypto-Gemeinde nun nicht allein einen Algorithmus, sondern auch ein verbindendes, lieb gewonnenes Feindbild verloren.

1 Security News

1.1 WinXP SP 2 verfügbar

Nach einigen Verzögerungen ist am 10.08.2004 das lange angekündigte Servicepack 2 für Windows XP erschienen. Neben zahlreichen Bugfixes enthält es insbesondere im Bereich Sicherheit einige Neuerungen: Unter anderem wurde die Funktionalität der Personal Firewall erweitert, und sicherheitsrelevante Einstellungen können nun übersichtlich im „Security Center“ eingesehen werden.

Die verbesserten Funktionen der Personal Firewall sind allerdings nicht ganz „State-of-the-art“, da beispielsweise ausgehende Verbindungen nicht überwacht werden. Ein gewisser Basisschutz ist durch die Firewall jedoch gegeben; für sensible Bereiche wird dennoch der Einsatz einer dedizierten Personal Firewall empfohlen. Die Virenschutz-Meldungen im Security Center hängen maßgeblich von den integrierten Produkten von Drittherstellern ab – und nicht alle Hersteller liefern diese Meldungen.

Microsoft scheint jedenfalls auf dem richtigen Weg zu sein. Allerdings: Nur wenige Tage, nachdem das SP 2 erschien war, tauchten bereits die ersten Probleme auf: Offenbar gibt es Schwierigkeiten, die knapp 270 Megabyte große Datei fehlerfrei zu installieren. Es wird von Systemabstürzen und Datenverlusten berichtet. Microsoft selbst veröffentlichte jetzt eine (leider nicht sortierte) Liste von über 200 Anwendungsprogrammen, die nach der Installation unter Umständen nicht mehr richtig funktionieren.

Pikanterweise finden sich auf dieser Liste auch Microsoft-Lösungen wie Word und Outlook. Microsoft macht also offenbar gründlich ernst mit dem eigenen Anspruch, nunmehr mehr auf die Sicherheit als auf Abwärtskompatibilität zu setzen. Fazit: Für dieses Servicepack gilt einmal mehr: Vor dem Roll-Out ausgiebig innerhalb einer geschlossenen Testumgebung prüfen.

1.2 Déjà-vu bei Check Point

Am 28.07.2004 wurde von ISS auf eine Sicherheitsschwäche beim VPN-Verbindungsaufbau von Check Points Produktlinie VPN-1 hingewiesen – ein Déjà-vu-Erlebnis in doppelter Hinsicht: Nicht nur, dass die Schwachstelle einmal mehr in den ASN.1-Bibliotheken liegt, auf die schon häufig, in den SSN zuletzt im Januar hingewiesen wurde. Auch das aktuelle Advisory von Check Point hat auffällige Ähnlichkeit einem früheren vom Mai 2004.

1.3 Acrobat ohne Netz

Seit dem 12.08.2004 wurden in kurzer Folge mehrere Sicherheitslücken in Adobes Acrobat veröffentlicht, die auch den Reader und sowohl Windows- als auch Unix-Versionen betreffen. Da der Acrobat Reader auf Arbeitsplätzen praktisch aller Betriebssysteme inzwischen zur Standardausstattung gehört, wird ein Wechsel auf die aktuelle Version angeraten, obwohl die Funktionenvielfalt der neueren Versionen die Wahrscheinlichkeit einer Sicherheitslücke zweifellos grundsätzlich erhöht.

1.4 Biometrische Realität

Am 06.08.2004 wurde von BSI, BKA und Fraunhofer-IGD der öffentliche Abschlussbericht der Studie „BioFinger“ zu Fingerabdruck-Systemen in überarbeiteter Form (Erstfassung: 20.05.2004) veröffentlicht. Die Studie attestiert dem besten System eine Falschakzeptanzrate von 0,1% – bei einer Falschzurückweisungsrate von 2%. Übersetzt heißt das: Damit nur jeder tausendste Attentäter in ein Flugzeug kommt, müssen bei jedem voll besetzten Jumbo sechs bis acht Passagiere unfreiwillig am Boden bleiben.

Möglich, dass Studienergebnisse dieser Art dazu beigetragen haben, dass die Forderung der USA, ab Oktober nur noch Pässe mit digitalen Fingerprint-Daten zuzulassen, am 10.08.2004 vom US-Kongress für ein Jahr zurückgestellt wurde.

1.5 Sicherheitsloch in PuTTY

Am 03.08.2004 wurde ein kritischer Fehler in dem bei Administratoren sehr beliebten Telnet/SSH-Client PuTTY entdeckt. Er erlaubt es einem Angreifer, via Spoofing oder über einen gehackten Server beliebigen Code auf dem Client-System auszuführen. Der Autor Simon Tatham empfiehlt dringend ein Upgrade auf Version 0.55.

1.6 Musterrichtlinien des BSI

Das BSI stellte am 07.06.2004 Musterrichtlinien zur IT-Sicherheit als Teil des BSI-Grundschutzhandbuchs elektronisch bereit. Sie umfassen ein Übersichtsdokument und neun Beispielkonzepte und –Richtlinien, die sich an unterschiedliche Adressatenkreise richten und eine Hilfestellung bei der Entwicklung eigener Security Policies bieten sollen. Die einzelnen Regelungsvorschläge wurden um zahlreiche Referenzen auf die entsprechenden Maßnahmen des Grundschutzhandbuchs (GSHB) ergänzt. Leider sind diese Querbezüge weder in der Word- noch der pdf-Version des Dokuments mit den Maßnahmenbeschreibungen des GSHB verlinkt, was die Nutzung aufwändig gestaltet.

1.7 MD5: Keine Panik

Auf der diesjährigen Kryptographen-Konferenz Crypto 2004 (15.-19.08.2004) kündigten chinesische Wissenschaftler an, sie hätten Kollisionen in den Hash-Algorithmen MD4, MD5 und SHA-0 entdeckt. Diese Ankündigung sorgte unter Krypto-Experten für einige Aufregung; es gab sogar Gerüchte, die Angriffe ließen sich auf heutige Algorithmen wie den SHA-1 übertragen.

Tatsächlich scheinen die Wissenschaftler Kollisionen gefunden zu haben, die denselben Hashwert zu unterschiedlichen Eingangswerten liefern. Der Weg zu einem praktikablen Angriff ist dennoch weit. So hatte Hans Dobbertin bereits 1996 Kollisionen für den MD5 beschrieben. Der Algorithmus gilt seitdem als unsicher – gebrochen wurde er indes bis heute nicht.

1.8 Bluetooth-Distanzangriff

Einer Gruppe von WLAN- und Bluetooth-Experten gelang am 03.08.2004 ein sogenannter Snarf-Angriff mit einem modifizierten Bluetooth-Adapter und einer Hochleistungsantenne über eine Distanz von 1,8 km. Die Annahme, dass Bluetooth nur im Abstand von maximal 100-150 m für Angriffe genutzt werden kann, ist damit widerlegt. Bluetooth sollte in Handys daher im Hidden-Modus betrieben oder besser gänzlich deaktiviert werden.

1.9 WPA im Verdacht

Der WLAN-Sicherheitsstandard WPA(2), über den in den letzten SSN berichtet wurde, kam am 26.07.2004 ins Gerede. Bei näherem Hinsehen entpuppte sich der beschriebene Angriff jedoch als „ganz normale“ Wörterbuch-Attacke auf das hinter WPA liegende RADIUS-Protokoll, die durch ein starkes EAP-Authentifikationsprotokoll und gut gewählte Shared-Secrets zwischen RADIUS-Server und WLAN-Access-Point verhindert werden kann.

1.10 SANS XP Survival Guide

Die „Lebenserwartung“ eines ungeschützten und mit dem Internet verbundenen PCs ist innerhalb eines Jahres von durchschnittlich 40 auf unter 20 Minuten gesunken. Das SANS Internet Storm Center ermittelt diesen Erwartungswert aus monatlich mehr als 1 Mio. Einzelmessungen. Im Mai wurde mit acht Minuten ein historischer Tiefststand erreicht. Als Anleitung für eine sichere Anfangskonfiguration und einen einigermaßen sicheren Betrieb empfiehlt sich der von SANS herausgegebene XP Survival Guide („Surviving the first day“).

1.11 BSI-Kongress 2005

Der 9. IT-Sicherheitskongress des BSI am 10.-12.05.2005 wird wie gewohnt in Bonn (Bad Godesberg) stattfinden. Anfang August hat das Programmkomitee den „Call for Papers“ veröffentlicht: Interessierte sind

aufgerufen, bis zum 08.10.2004 eine Kurzzusammenfassung (vier Seiten) mit Gliederung ihres Beitrags einzureichen.

2 Secorvo News

2.1 Secorvo College aktuell

Auf vielfachen Teilnehmerwunsch ergänzen wir – erstmalig am 23.09.2004 – unser Seminar Lotus Notes Security um einen Workshop, dessen Inhalte in Abstimmung mit den Teilnehmern aus folgendem Themenpool ausgewählt werden:

- Gruppen und Gruppenkonzepte
- ID-Administrationswerkzeuge
- Log Files
- Passwort Synchronisation
- Roaming User
- Antispam und Antivirus
- ECL
- Security Best Practices
- Betriebssystem-Sicherheit
- Notes Security Architecture Exposed

Dieser Workshop kann zusammen mit dem Seminar Lotus Notes Security oder separat gebucht werden; Frühbucher zahlen bis zum 31.08.2004 nur 580 € (zzgl. MwSt.). Weitere Auskünfte erteilt Frau Bradatsch (bradatsch@secorvo.de, 0721/6105-500).

http://www.secorvo.de/college

2.2 25. SSN-Jubiläum

Die vorliegende Ausgabe der Secorvo Security News ist die 25. – und unser Anspruch an Inhalt und Qualität entspricht nach wie vor dem, den wir im Editorial der Erstausgabe im Juli 2002 formulierten.

Seitdem hat uns viel Lob erreicht, und zahlreiche Unternehmen verbreiten die News inzwischen über ihr Intranet. Das freut und ehrt uns. Einer unveränderten Publikation der News als vollständiges .pdf stimmen wir grundsätzlich zu – und freuen uns über eine kurze Benachrichtigung: als Balsam für unsere Motivation.

3 Veranstaltungshinweise

September 2004	
20.-21.09.	Elektronische Geschäftsprozesse – EGP 2004 (Klagenfurt)
21.-22.09.	Lotus Notes Security (Secorvo College, Karlsruhe)
23.09.	Lotus Notes Security – Advanced (Secorvo College, Karlsruhe)
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)
28.-29.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
30.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Oktober 2004	
12.-13.10.	Live Hacking Lab (Secorvo College, Karlsruhe)
26.-27.10.	Inside Windows Security (Secorvo College, Karlsruhe)
November 2004	
02.-04.11.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
09.-11.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
22.-26.11.	Information Security Management (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
September 2004

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 9, 3. Jhrg. 2004
Stand 22. November 2004

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Schicksal Patchen

1 Security News

1.1 Erfahrungen mit XP SP 2

1.2 Abenteuer E-Banking

1.3 Es geht auch ohne...

1.4 Hacme Bank v1.0

1.5 Laws of Vulnerabilities

1.6 Frechheit siegt...

1.7 Gefahr durch VxWorks?

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Und da waren es sechs...

2.3 Secorvo wächst

3 Veranstaltungshinweise

Impressum

Editorial: Schicksal Patchen

Vor gut sieben Jahren erheiterte die angeblich von Bill Gates provozierte Pressemitteilung von General Motors, die in 13 Punkten beschrieb, was wäre, wenn Autos mit einer Technologie wie der von Microsoft gebaut würden. Drei Kostproben: „Wenn man bestimmte Manöver ausführt, z. B. eine Linkskurve, stellt sich das Auto ab und weigert sich, neu zu starten. Man muss dann den Motor neu installieren." Oder: „Das Airbag-System würde bei jedem Unfall fragen: ‚Sind Sie sicher?' bevor es auslöst." Und: „Man muss den <Start>-Knopf drücken, um den Motor auszuschalten."

Tatsächlich: Zwischen der Qualität eines Autos und der von Software lagen Welten. Ein Daimler mit Bluescreen? Ein Porsche, der selbstständig bootet? Ein BMW, der ‚Die Anwendung reagiert nicht' meldet? Undenkbar. Warum aber war und ist Software nicht so fehlerarm wie ein Auto?

Der Grund ist einfach: Die präzise Produktion von Achsen, Kolben und Getrieben hat im Maschinenbau eine weit über 100jährige Tradition. Anders als die Softwaretechnik – sie existiert noch keine 20 Jahre. Denn allen theoretischen Ansätzen zum Trotz gebiert noch immer Erfahrung den größten Fortschritt. So versagten Fahrzeuge vor 80 Jahren – bei niedrigerer Geschwindigkeit und Belastung – weit häufiger als heute.

Vermutlich wäre GM heute zurückhaltender mit ihrer Replik. Denn in modernen Fahrzeugen werkeln inzwischen bis zu 50 vernetzte Kleinstrechner, um Antrieb, Beleuchtung, Sicherheitseinrichtungen und Steuerung zu koordinieren und an die Umgebungsbedingungen anzupassen. Der Preis: 2003 war die Fahrzeugelektronik Pannenursache Nr. 1. Wir werden also weiterhin damit leben müssen, dass Software Fehler enthält – im Schnitt 20 je 1.000 Programmzeilen, darunter auch Sicherheitslücken. Damit bleibt bis auf Weiteres das „Flicken" (Patchen) eine wichtige Security-Disziplin. Allerdings unter verschärften Randbedingungen: Exploits sind inzwischen im Schnitt nach 5,8 Tagen verfügbar.

1 Security News

1.1 Erfahrungen mit XP SP 2

Im Schnitt treten bei 10 % aller Systeme nach der Installation des Service Pack 2 für Windows XP Probleme auf – das jedenfalls behauptet eine am 31.08.2004 veröffentlichte Studie des Asset Management Providers AssetMetrix auf der Basis von 340 befragten Unternehmen mit insgesamt 44.000 PCs. Dabei fanden sich signifikante Unterschiede zwischen kleineren und großen Netzen: Bei weniger als 100 Arbeitsstationen gab es bei gut 12 % der Systeme Probleme, während in grösseren Netzen nur etwa 6 % betroffen waren.

SANS führt derzeit ebenfalls eine (Online-) Umfrage zu Erfahrungen mit SP 2 durch. Zwischenstand: 42 % der knapp 2.100 Befragten hatten keine Schwierigkeiten, dafür aber 10 % große, nicht lösbare Probleme – und 12 % mussten ihre Systeme komplett neu aufsetzen. Trotz des nicht vernachlässigbaren Anteils negativer Erfahrungen raten wir aus Sicherheitsgründen weiterhin zur SP 2-Installation – jedoch erst nach intensiven Tests.

1.2 Abenteuer E-Banking

Das Erkennen von Phishing-E-Mails ist für viele Online-Banking-Anwender eine Herausforderung, nicht zuletzt wegen der perfide verfeinerten Tarntechniken der Absender. Wiederholt wurde von Fällen berichtet, in denen Kunden bereitwillig PIN und TANs preisgaben – und die Transfers der Täter erst in letzter Sekunde von der Bank rückgängig gemacht werden konnten. SANS publizierte am 10.09.2004 sechs Empfehlungen für Webseitenanbieter zur Erkennung von Phishing-Angriffen. Ein absolutes Muss für Entwickler ist Gunter Ollmanns 42seitiger Phishing Guide vom 23.09.2004.

Weit dramatischer jedoch ist die Wirkung des am 07.09.2004 erstmalig dokumentierten Trojaners Bizex-E, der eine knapp drei Wochen alte Schwachstelle des Internet Explorers ausnutzt – und systematisch PIN- und TAN-Eingaben abfängt. Für je einen Kunden der Dresdner Bank und der Postbank ist belegt, dass auf diesem Weg die PIN und eine gültige TAN entwendet und damit je ein vierstelliger €-Betrag auf ein Konto in Lettland überwiesen wurden. Beide Überweisungen konnten von den Banken noch gestoppt werden. Weitere vielleicht „erfolgreiche“ Fälle sind, auch bei anderen Banken, höchst wahrscheinlich.

Gegen Angriffe dieser Art hilft vor allem die Verwendung eines möglichst Fehler freien und restriktiv konfigurierten Browsers. Dafür ist seit Jahren (bekanntermaßen) der Internet Explorer nicht erste Wahl. Diese Überzeugung vertritt nun auch das BSI – zumindest kann man das Interview mit Sprecher Michael Dickopf zu diesem Anlass (Berliner Zeitung vom 10.09.2004) so lesen. Das Portal www.bsi-fuer-buerger.de empfiehlt unverblümter: „Um auf Nummer sicher zu gehen: Wechseln Sie den Browser“.

1.3 Es geht auch ohne...

Eine wichtige Ursache zahlreicher erfolgreicher Viren-, Wurm- und Trojaner-Attacken sind die administrativen Berechtigungen vieler Windows-PC-Nutzer. Erst diese hohe Berechtigungsstufe erlaubt die Installation und Deinstallation beliebiger Software. Daher wird schon lange empfohlen, Anwender nur mit eingeschränkten Rechten auszustatten. Neben dem Widerstand der Nutzer gegen den Rechteentzug sind Probleme mit Anwendungen, die Daten in Systemverzeichnisse schreiben oder auf geschützte Bereiche der Registry zugreifen, häufigstes Umsetzungshindernis.

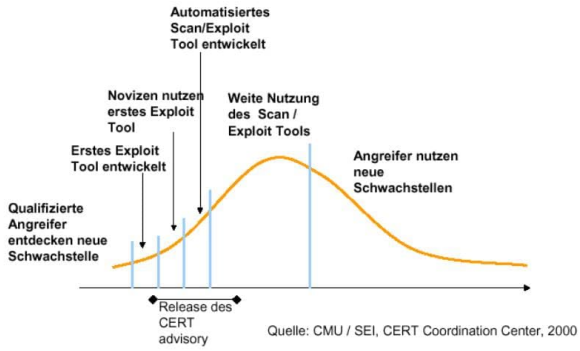
Oft gibt es jedoch eine (undokumentierte) Möglichkeit, die betroffene Anwendung auch ohne Administrationsrechte zu betreiben. Angeregt durch einen Beitrag in c’t 15/2004 wurde solchen Problemlösungen die Webseite www.noadmin.de gewidmet. Zur Zeit können dort in einem Forum Tipps ausgetauscht werden; der Aufbau einer umfassenden Datenbank ist geplant.

1.4 Hacme Bank v1.0

Von Foundstone wurde am 08.09.2004 das kostenfreie Tool Hacme Bank veröffentlicht, eine Webapplikation, in die typische Schwachstellen integriert wurden. Gedacht ist es zur Schulung von Systemverantwortlichen und Entwicklern: Sie sollen die Schwachstellen mit geeigneten Analysetools entdecken. Solchermaßen sensibilisiert werden sie anschließend Schwachstellen in eigenen Applikationen hoffentlich selbst erkennen bzw. schon in der Entwicklungsphase vermeiden.

1.5 Laws of Vulnerabilities

Unter dem Titel "Laws of Vulnerabilities" publizierte Gerhard Eschelbeck, CTO von Qualsys, auf den diesjährigen Black Hat Briefings am 28.07.2004 in Las Vegas die Ergebnisse einer Auswertung von 6,5 Mio. Device Scans. Danach benötigen Unternehmen ab dem Bekanntwerden schwer wiegender Schwachstellen derzeit im Schnitt 62 Tage, um die Hälfte ihrer internen Systeme zu patchen, und 21 Tage für die Hälfte der direkt vom Internet aus erreichbaren Systeme.



Da die Zeitspanne zwischen Bekanntwerden einer Schwachstelle und der Verfügbarkeit eines Exploits oder der Ausnutzung durch einen Wurm immer kürzer wird – nach Symantecs aktuellem Security Thread Report vom 22.09.2004 schrumpfte sie in der ersten Jahreshälfte 2004 auf sechs (!) Tage – sollte ein wirksames Patch-Management derzeit ganz oben auf der Agenda des Security-Managements geführt werden.

1.6 Frechheit siegt...

Die marktführende Online-Handelsplattform Ebay wurde Ende August für einige Stunden außer Betrieb gesetzt – allerdings nicht durch eine Distributed Denial of Service Attacke, wie man vermuten könnte. Eine Privatperson hatte ganz dreist beim Provider intergenia die Domänen ebay.de und amazon.de bestellt. Der automatisierte KK-Antrag zur Übertragung der Domäne wurde von Amazon abgelehnt. Von Ebay kam jedoch keine Reaktion, und so wurde der korrekte DNS-Eintrag durch den der Webseite der Privatperson ersetzt.

Merke: Nicht nur in komplexen Anwendungen, sondern auch in einfachsten Prozessen kann der Wurm drin sein – und nicht unerhebliche Umsatzausfälle verursachen.

1.7 Gefahr durch VxWorks?

Frank Denis publizierte am 04.09.2004 auf der Mailing-Liste full disclosure eine kritische Schwachstelle von Storage Devices, die einen Controller von Engenio (ehemals LSI Logic) verwenden. Diese Devices werden u.a. in Fibre-Channel Switches von Brocade und in Storage-Systemen der Hersteller Storagetek (D series) und IBM (DS4xxx series, ehemals FAStT) sowie weiteren, wie SGI und Teradata eingesetzt.

Durch den Fehler kann das Device mit Hilfe spezieller IP-Pakete zum Absturz gebracht werden; in bestimmten Fällen ist ein Datenverlust möglich. Je nach Einsatzumfeld können die Auswirkungen eines solchen Angriffs erheblich sein. Vor diesem Hintergrund stimmen die Reaktionen der betroffenen Hersteller sehr nachdenklich: Nicht genug damit, dass die schon Mitte Juni durch Frank Denis informierten Hersteller trotz mitgesandtem funktionierenden Exploit, sofern überhaupt, erst nach mehreren Wochen reagierten. Sollte der Fehler, wie Storagetek behauptet, dem verwendeten Betriebssystem VxWorks zuzuordnen sein, dann könnten zahlreiche weitere Systeme betroffen sein. Der Hersteller Windriver war jedoch angeblich nicht bereit, sich des Falls ohne Lizenznachweis anzunehmen.

2 Secorvo News

2.1 Secorvo College aktuell

Die “Herbstsaison” hat begonnen. Mit dem gefragten „Live Hacking Lab“, das wir gemeinsam mit der Schweizer Compass Security und einem umfangreichen Laboraufbau durchführen, lassen wir Sie zwei Tage lang, vom **12.-13.10.2004**, einen Blick in die Hexenküche aktueller Angriffsmethoden werfen – von Spoofing und Sniffing über inside-out-Attacken bis hin zu SQL-Injektion und Cross-Site-Scripting.

Daran schließt sich am **14.10.2004** ein eintägiger Aufbauworkshop an, der Internet-Angriffe, LAN-Attacken und Penetrationstests vertieft.

http://www.secorvo.de/college

2.2 Und da waren es sechs...

Am 01.09.2004 konnte Secorvo auf sechs erfolgreiche Unternehmensjahre zurückblicken. Über 200 erfolgreiche Projekte, mehr als 650 zufriedene Teilnehmer aus über 220 namhaften Unternehmen, die an Seminaren von Secorvo College teilgenommen hatten, über 150 Fachpublikationen und mehr als 160 Fachvorträge sowie 1,5 Mio. Webseitenzugriffe auf Artikel, White Paper und 25 Security News dokumentieren unsere Entwicklung – auf die wir auch ein wenig stolz sind.

2.3 Secorvo wächst

Aufgrund der in den vergangenen Monaten erheblich gestiegenen Zahl von Projektanfragen erweitern wir unser Team. Ab dem 01.10.2004 wird Petra Barzin uns verstärken. Sie bringt neun Jahre Berufserfahrung in der IT-Sicherheit mit und hat sich u.a. als Autorin der Signatur-Interoperabilitätsspezifikation und der RFC 3039 (Qualified Certificates) sowie als Mitentwicklerin der SecuDE-Bibliothek einen Namen gemacht.

3 Veranstaltungshinweise

September 2004	
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)
Oktober 2004	
12.-13.10.	Live Hacking Lab (Secorvo College, Karlsruhe)
14.10.	Live Hacking Lab – Aufbauworkshop (Secorvo College)
26.-27.10.	Inside Windows Security (Secorvo College, Karlsruhe)
November 2004	
02.-04.11.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
09.-10.11.	Computer Forensic Symposium (Secorvo/VICCON, Karlsruhe)
09.-11.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
22.-23.11.	IT-Security Management (Secorvo College, Karlsruhe)
22.-26.11.	Information Security Management (Secorvo College, Karlsruhe)
Dezember 2004	
06.-07.12.	IsSec/ZertiFA 2004 (COMPUTAS, Berlin)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Oktober 2004

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 10, 3. Jhrg. 2004
Stand 22. November 2004

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Auf Phishfang

1 Security News

1.1 Neue SANS Top 20

1.2 Scanner ausgetrickst

1.3 Linux strikes back

1.4 JPEG-of-Death

1.5 Erfolgreiche Bug Bounty

1.6 Samba Bug

1.7 Pufferüberlauf dank XML

1.8 Vorsicht bei Browser-Eingaben

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Neues Video in Arbeit

2.3 IsSec und ZertiFA 2004

2.4 DuD 2005

3 Veranstaltungshinweise

Impressum

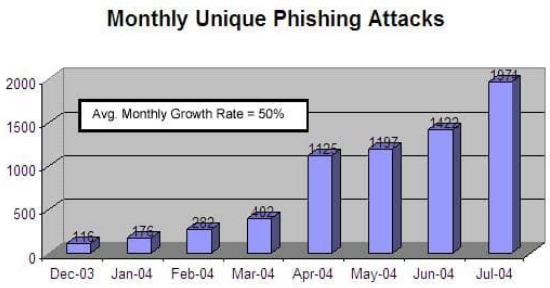
Editorial: Auf Phishfang

Erhoffe das Beste und sei gefasst auf das Schlimmste. (Anonymus)

Seit einem Jahr ist das gezielte Abgreifen von persönlichen Authentifikationsdaten in Mode. Im Hacker-Jargon wird das Ergattern von „hacked accounts“, so genannten „phishes“, seit 1996 als „phishing“ bezeichnet. Damals waren AOL-Accounts das Ziel; Phishes galten in Hackerkreisen als digitale Währung.

Mit dem Aufkommen von Spam haben sich Vorgehensweise und Angriffsziel geändert: In vermeintlich von einer Bank stammenden E-Mails, die das Corporate Design des Geldinstituts täuschend echt nachbilden, werden die Empfänger aufgefordert, eine verlinkte Webseite zu besuchen und dort ihre Authentifikationsdaten einzugeben, wie User-ID, PIN und TANs. Perfider noch ist verstecktes Phishing via Cross Site Scripting, mit Hidden Frames oder URL Obfuscation.

Bislang sind vor allem amerikanische Banken und Privatnutzer von diesen Angriffen betroffen. In Deutschland sind nur wenige Fast-Schadensfälle bekannt – die Überweisungen konnten noch rechtzeitig gestoppt werden. Das muss aber nicht so bleiben: Der Phishing Attack Trend Report der Anti-Phishing Working Group vom 30.08.2004 weist für den Zeitraum von Dezember 2003 bis Juli 2004 einen monatlichen Anstieg der Phishing-Angriffe um im Mittel 50 % aus.



Außer Aufklärung ist bisher kein Kraut dagegen gewachsen. Nur ein Positives lässt sich der neuen Plage abgewinnen: Vielleicht steigt durch Phishing die Sensibilität der Nutzer – auch in den Unternehmen.

1 Security News

1.1 Neue SANS Top 20

Am 08.10.2004 erschien Version 5.0 der SANS Top 20: Einer Liste der 20 kritischsten Internetschwachstellen, je zehn für Windows- und für Unix-Systeme, inklusive einer Auflistung der wichtigsten Patches. Sie wird jährlich aus den Einschätzungen zahlreicher internationaler Sicherheitsexperten zusammen gestellt. Diesmal auf Platz eins: die Standard-Installation von HTTP-Servern und die BIND-Implementierung des DNS. Auch eine deutsche Version der Top 20 ist verfügbar.

1.2 Scanner ausgetrickst

Jeder Virenscanner beherrscht heute die Analyse von .zip-Dateien. Am 18.10.2004 veröffentlichte iDefense jedoch eine perfide Methode, mit der sich diese Funktion bei vielen gängigen Virenscannern austricksen lässt: Setzt man im Header der .zip-Datei die Größenangabe der Originaldatei auf Null, überspringen diese Scanner das Archiv – die Dekompression beim Empfänger funktioniert jedoch weiterhin. Ein Update der Virenscanner-Software ist sehr zu empfehlen.

1.3 Linux strikes back

Nachdem Microsoft in Anzeigen und mit Veröffentlichungen zu belegen versucht, dass Linux das unsicherere Betriebssystem ist, hat sich nun Nicholas Petreley, ehemals Redakteur der Zeitschrift LinuxWorld, an einen Sicherheitsvergleich gewagt – sicherlich auch als Replik auf die umstrittene Studie von Forrester Research vom 19.03.2004 (siehe SSN 04/2004). Das Ergebnis der von Petreley am 25.10.2004 publizierten Studie, in der er 40 aktuelle Schwachstellen von Windows Server 2003 und Red Hat Enterprise Linux Advanced Server v3 verglich: Unter Anlegung gleicher Maßstäbe waren nur 10 % der Red Hat Bugs als schwer wiegend einzustufen, jedoch 50 % der Windows-Bugs.

Aus diesem Ergebnis ist nicht – und schon gar nicht generell – abzuleiten, dass Linux sicherer ist als Windows, wohl aber, dass in der Momentaufnahme von Petreley deutlich mehr der veröffentlichten Microsoft-Schwachstellen schwerwiegend waren. Über die nicht veröffentlichten und die unentdeckten Schwachstellen lässt sich nur spekulieren.

1.4 JPEG-of-Death

Bilder können nicht nur verbotenen und jugendgefährdenden Inhalts sein, sondern auch ein Trojanisches Pferd enthalten – das belegt Microsofts Warnmeldung vom 14.09.2004 (aktualisiert am 12.10.2004). Durch einen kritischen Fehler, der alle Betriebssystem- und Anwendungsprogrammversionen von Microsoft betrifft, kann das Öffnen von manipulierten (JPEG-) Bildern einem Angreifer die Ausführung beliebigen Programmcodes ermöglichen.

Seit dem 29.09.2004 sind solche Bilder unter der martialischen Bezeichnung „JPEG-of-Death“ in Umlauf, die den JPEG-of-Death-Exploit enthalten. Sie schieben dem System durch einen Buffer-Overflow einen kleinen Trojaner unter. Der Angreifer erhält über das Netzwerk Zugriff auf die Kommandozeile des angegriffenen Systems und kann es so kontrollieren. Um den Trojaner zu aktivieren genügt das bloße Ansehen eines manipulierten Bildes – auf einer Webseite, als Anhang oder sogar innerhalb einer E-Mail. Die Schwachstelle betrifft auch das weniger gebräuchliche Windows Metafile-Format (.emf/.wmf), wie ein weiteres Exploit von K-OTIK belegt.

Als Gegenmaßnahme sollten umgehend die Microsoft-Patches MS04-28 und MS04-32 installiert werden, da inzwischen schon „Baukästen“ zur Herstellung derartiger Bilder über das Internet verbreitet werden. Auch ein Update des Virenscanners kann helfen: Zahlreiche Hersteller haben ihre Signaturen angepasst und erkennen jetzt auch manipulierte Bilder.

1.5 Erfolgreiche Bug Bounty

Das Konzept des Bug Bounty Programms der Mozilla-Gemeinde vom 05.08.2004, für die Entdeckung jeder relevanten Schwachstelle eine Belohnung von 500 $ in bar auszuloben, scheint aufzugehen. Die ersten Prämien wurden am 14.09.2004 ausgezahlt – und die festgestellten Schwachstellen umgehend behoben. Ein Update auf die jeweils aktuellen Versionen von Mozilla, Thunderbird und Firefox wird empfohlen.

1.6 Samba Bug

Noch immer wirkt er weiter: Der am 30.09.2003 erstmals veröffentlichte Fehler im ASN.1-Parser von OpenSSL (SSN 10/2003), der in vielen Implementierungen eingesetzt wird – und von zahlreichen vergleichbaren Fehlern anderen in verbreiteten Produkten begleitet wurde (siehe SSN 11/2003, 1/2004, 2/2004, 8/2004). Am 13.09.2004 wurde ein solcher Bug in smbd festgestellt: Durch entsprechend präparierte Pakete können sowohl der Dämon als auch das Serversystem über das Netzwerk „abgeschossen“ werden. Die Installation des zur Verfügung gestellten Patches oder ein Update auf die aktuelle Version 3.0.7 wird dringend empfohlen.

1.7 Pufferüberlauf dank XML

Als Sprache für die Kodierung komplexer Datenelemente hat XML mittlerweile ASN.1 und proprietäre Formate in vielen Bereichen verdrängt. Dies ist sicherlich auch der Erwartung zu verdanken, dass XML-Datenstrukturen einfacher zu handhaben sein sollten als solche in ASN.1.

Zumindest aus dem Blickwinkel der Sicherheit müssen an dieser Erwartung mittlerweile Abstriche gemacht werden: Am 12.10.2004 veröffentlichte Microsoft den Patch für eine Sicherheitslücke bei der XML-Verarbeitung durch das hauseigene WebDAV-Modul, und am 26.10.2004 meldete ein Security-Alert, dass sich in aktuellen Versionen der weit verbreiteten XML-Bibliothek libxml2 des Gnome-Projekts ein halbes Dutzend Pufferüberläufe finden lassen. Tags darauf wurde Version 2.6.15 von libxml2 veröffentlicht, die diese Lücken stopfen soll.

Möglicherweise ist dies der Anfang einer zweiten Folgefehler-Geschichte, wie wir sie im ASN.1-Bereich erleben mussten (s.o.) – dann wäre zu befürchten, dass ähnliche Fehler in einer Implementierung nach der anderen entdeckt werden.

1.8 Vorsicht bei Browser-Eingaben

Dass JavaScript und andere aktive Inhalte sicherheitskritisch sein können, ist bekannt. Am 20.10.2004 wurden jetzt zwei weitere Probleme veröffentlicht, diesmal im Zusammenhang mit dem so genannten „tabbed browsing“, einer Funktionalität vieler Browser, mehrere Webseiten innerhalb eines Browserfensters darzustellen.

Tabbed Browsing kann immer dann problematisch sein, wenn JavaScript aktiviert ist: Die Eingaben, die ein Benutzer scheinbar auf der Webseite z.B. seiner Online-Bank tätigt, können durch geeignet manipulierte Skripte auf anderen Servern landen, wenn entsprechende Webseiten gleichzeitig (innerhalb eines anderen „Tabs“) im Browser angezeigt werden. Betroffen sind alle gängigen Browser in den aktuellen Versionen (siehe auch SSN 7/2004).

Solange keine Patches der Hersteller verfügbar sind, schützen nur die bekannten Verhaltenstipps: JavaScript nach Möglichkeit deaktivieren, URLs immer direkt aufrufen (nicht über Links) sowie andere Seiten (Tabs) schließen, bevor vertrauliche Daten wie Passwörter, PIN oder TAN in ein HTML-Formular eingegeben werden.

Ähnliche Probleme sind seit Jahren im Zusammenhang mit Java-Applets bekannt: Falls Java aktiviert ist, hat der Benutzer keine Kontrolle darüber, wann ein Java-Applet im Browser abläuft. Es kann auch erst dann gestartet werden, wenn der Benutzer längst auf anderen Webseiten „unterwegs“ ist.

2 Secorvo News

2.1 Secorvo College aktuell

Dreimal haben Sie in diesem Jahr noch Gelegenheit, von unseren Erfahrungen zu profitieren – auf dem Grundlagenseminar "IT-Sicherheit heute" vom **09.-11.11.2004**, der Einführung in das "IT-Security Management" vom **22.-23.11.2004** und dem einwöchigen Intensivseminar "Information Security Management" vom **22.-26.11.2004**. Auf Grund der großen Nachfrage empfehlen wir Ihnen bei Interesse eine baldige Anmeldung unter

http://www.secorvo.de/college

2.2 Neues Video in Arbeit

Nach dem großen Erfolg unserer Flash-Videos „Trojanisches Pferd" und „E-Mail-Sicherheit" zur Sensibilisierung der Mitarbeiter haben wir auf Kundenwunsch mit der Entwicklung eines neuen Videos zum Thema „Passwortsicherheit" begonnen. Das zehnminütige Video zeigt die Leistungsfähigkeit heutiger Passwort-Cracker, motiviert für die Verwendung hinreichend sicherer Passworte und zeigt, wie sich gute Passworte bilden und merken lassen.

Die Fertigstellung des Videos ist für Mitte Januar geplant; gerne können Sie ein Exemplar vormerken lassen.

2.3 IsSec und ZertiFA 2004

Anfang Dezember (**06.-07.12.2004**) finden die traditionellen COMPUTAS-Fachkonferenzen IsSec und ZertiFA im Herzen Berlins statt – in diesem Jahr als gemeinsame Veranstaltung unter dem Vorsitz von Stefan Kelm, Johann Bizer und Dirk Fox.

2.4 DuD 2005

Für Ihren Kalender: Die Konferenz DuD 2005 – Datenschutz und Datensicherheit findet vom **18.-19.04.2005** in Berlin statt.

3 Veranstaltungshinweise

November 2004	
09.-11.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
22.-23.11.	IT-Security Management (Secorvo College, Karlsruhe)
22.-26.11.	Information Security Management (Secorvo College, Karlsruhe)
23.-24.11.	Einführung in die Praxis des DSB (Euroforum, Wiesbaden)
Dezember 2004	
05.-09.12.	Asiacrypt 2004 (IACR, Jeju Island/Korea)
06.-07.12.	IsSec/ZertiFA 2004 (COMPUTAS, Berlin)
09.-10.12.	Einführung in die Praxis des DSB (Euroforum, Düsseldorf)
16.12.	Nächstes KA-IT-Si-Event (KA-IT-Si, Karlsruhe)
Januar 2005	
25.-26.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
27.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
November 2004

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 11, 3. Jhrg. 2004
Stand 06. Dezember 2004

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Weniger ist weniger

1 Security News

1.1 Phishing revisited

1.2 IT-Grundschutzprofile

1.3 Internetspionage per Satellit

1.4 Erste Bank mit IT-Grundschutz-Zertifikat

1.5 SigG-Novelle

1.6 DNS-Ping-Pong

1.7 PDA-Forensik

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Lead Auditor

2.3 Forensik-Symposium

2.4 Delegation und Haftung

2.5 DuD 2005

3 Veranstaltungshinweise

Impressum

Editorial: Weniger ist weniger

Denken wir an Überwachung, so fallen uns Kameras, Abhöranordnungen und Lauschangriff, E-Mail-Filterung und Strafverfolgungsbehörden ein. Die Welt des „Großen Bruders“ hört, sieht und liest mit – und uns beschleichen klamme Gefühle, wenn wir uns eine Rundherumbeobachtung vorstellen.

Tatsächlich aber trügt unsere Wahrnehmung. Denn die Kernbedrohung unserer gesellschaftlichen Freiheit schlummert in einer weit weniger sichtbaren Gefahr. Sie kommt auf viel leiseren Sohlen daher – als die uns Deutschen vielleicht besonders eigene Neigung zur Dokumentation, zur Sammlung und Verschriftlichung, die dazu führt, dass wir das Mögliche archivieren – manchmal mehr als zulässig, fast immer mehr als erforderlich. Das gilt bei weitem nicht nur für Behörden – auch deutsche Unternehmen sind Weltmeister im Speichern, und vergessen das Löschen.

In seiner Grundsatzentscheidung zum Volkszählungsgesetz hat das Bundesverfassungsgericht 1983 so treffend formuliert: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, (...) kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“

Heute sollte man hinzufügen: Wer weiß, dass Vorgänge dokumentiert, gespeichert und zukünftig möglicherweise in ganz anderem Kontext ausgewertet werden, *wird* gehemmt *sein*, selbstbestimmt zu entscheiden. Aus dieser Perspektive könnten sich Ermächtigungen der Strafverfolgungsbehörden, sofern sie verhältnismäßig bleiben, als weit harmloser erweisen als etwa das geplante Anti-Diskriminierungsgesetz, das lückenlose Entscheidungsdokumentationen zur Folge haben dürfte.

„Liberty dies by inches”, konstatierte der kürzlich verstorbene Rechtsexperte Heinz Schueler schon 1979. Wie recht er hatte.

1 Security News

1.1 Phishing revisited

Die Perfidie von Phishing-Attacken nimmt weiter zu. Erste Phisher sind jetzt eine Ehe mit Schadprogrammen eingegangen. So wurde am 03.11.2004 eine Phishing-E-Mail gemeldet, deren aktiver Anhang die „hosts"-Datei im Windows-Verzeichnis system32/drivers/etc modifiziert. In dieser Datei werden IP-Adressen fest zugeordnet; üblicherweise findet sich hier nur die Lokalhost-Adresse 127.0.0.1. Werden in dieser Datei beliebigen Hostnamen, z.B. Webadressen, feste IP-Adressen zugewiesen, sind sie damit „fest verdrahtet": Der Browser bemüht dann nicht das DNS-Protokoll, um die korrekte Adresse zu finden, sondern nimmt die hier eingetragene – der ahnungslose Surfer sieht im Browserfenster die richtige WWW-Adresse, wird aber auf eine falsche Seite umgelenkt, ohne dass das für ihn erkennbar wäre.

1.2 IT-Grundschutzprofile

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 17.11.2004 auf ihrer Webseite drei Grundschutz-Profile jeweils für kleine, mittlere und große Unternehmen veröffentlicht, die die Umsetzung des BSI-Grundschutzhandbuchs vereinfachen sollen.

Analog zum „Leitfaden IT-Sicherheit kompakt" enthält die Handreichung für kleine Unternehmen eine Checkliste, die eine gute Hilfestellung darstellt. Bei den Profilen für mittlere (112 S.) und große Unternehmen (117 S.) werden die Vorgehensweise im Detail sowie sinnvoller Weise auch der Einsatz des Grundschutz-Tools vorgestellt. Praxisnah werden beim Profil für große Unternehmen zusätzlich mögliche Problemfälle und Lösungsmöglichkeiten aufgezeigt.

1.3 Internetspionage per Satellit

Laut einer aktuellen Untersuchung von Forschern der Ruhr-Universität Bochum konnten bei satellitengestützten Internetverbindungen einiger Provider unverschlüsselte Daten von und über andere Nutzer recht einfach in Erfahrung gebracht werden.

Es wird empfohlen, die auch sonst im Internetverkehr üblichen Sicherheitsmaßnahmen wie die Verwendung von verschlüsselten Protokollen zu nutzen.

1.4 Erste Bank mit IT-Grundschutz-Zertifikat

Das BSI konnte am 16.11.2004 die Vergabe des ersten IT-Grundschutz-Zertifikats an eine Bank vermelden: die PSD-Bank Westfalen-Lippe e. G. mit Sitz in Münster hat als erste Bank eine IT-Grundschutz-Zertifizierung erfolgreich durchgeführt.

1.5 SigG-Novelle

Am 19.11.2004 hat der Bundestag in zweiter und dritter Lesung das deutsche Signaturgesetz (SigG) novelliert. Zentrale Änderung: Für die Beantragung eines qualifizierten Signaturschlüssel-Zertifikats genügt nunmehr ein PIN-TAN-basierter Prozess – der eigenhändig unterschriebene Antrag mit Vorlage des Personalausweises ist bei bestehenden Kunden nicht mehr erforderlich. Damit kommt die Novelle einer zentralen Forderung der deutschen Banken entgegen, die eine Vereinfachung der Prozesse gefordert hatten, um ihre Bankkarten zu Signaturkarten aufwerten zu können.

Die Bundesregierung erhofft sich mit diesem Schritt eine erhebliche Ausweitung der nach wie vor nur marginalen Verbreitung qualifizierter Signaturen in Deutschland; freilich fehlen trotz dieser Verfahrensvereinfachung noch immer die seit vielen Jahren versprochenen Anwendungen für „Otto Normalsignierer", die für ihn einen erkennbaren Zusatznutzen darstellen und einen Technikwechsel rechtfertigen.

1.6 DNS-Ping-Pong

Dass auch in Protokollen aus der “Ur-Zeit” des Internet immer wieder Schwachstellen entdeckt werden, wird inzwischen niemanden mehr überraschen. Häufig handelt es sich dabei zum Glück nicht um konzeptionelle Schwachstellen, die einen Austausch aller Implementierungen des Protokolls erfordern würden, sondern um Programmierfehler. Manchmal jedoch sind davon dank „Code-Wiederverwendung“ zahlreiche Produkte betroffen.

So erging es nun auch dem vielleicht wichtigsten Protokoll – DNS, dem Domain Name System. Am 09.11.2004 warnte das britische NISCC in einem Advisory, dass verschiedene Hersteller das DNS-Protokoll in ihren Produkten fehlerhaft implementieren. Danach reagieren DNS-Server unter Umständen auf die einer DNS-Anfrage folgende Antwort mit einer erneuten DNS-Antwort. Dadurch können sehr schnell „DNS-Stürme“ ausgelöst werden, sofern zwei von diesem Fehler betroffene DNS-Server beteiligt sind – ein Szenario, das in großen Firmen-Netzwerken nicht unwahrscheinlich sein dürfte.

Analog zu bereits 1996 berichteten ähnlichen Problem auf UNIX-Systemen könnten Server durch geeignet Pakete auch dazu gebracht werden, sich selbst entsprechende Anfragen zu senden.

1.7 PDA-Forensik

IT-Forensik wird als Teildisziplin der IT-Sicherheit immer wichtiger. In forensischen Analysen tauchen dabei immer häufiger Untersuchungen zu Mini-Organizern auf, auch Personal Digital Assistants (PDAs) genannt, da diese vor allem im Firmenumfeld an Bedeutung gewinnen.

Dieser Entwicklung trägt jetzt das US-amerikanische National Institute of Standards and Technology (NIST) Rechnung: In den am 10.11.2004 vorgestellten „Guidelines on PDA Forensics“ erläutert das NIST die spezifischen Merkmale einer PDA-Analyse (u.a. am Beispiel von Palm OS und Pocket PC), führt in forensische Vorgehensweisen ein und stellt einige Tools vor, auf die in einem umfangreichen Begleitdokument im Detail eingegangen wird.

2 Secorvo News

2.1 Secorvo College aktuell

Im neuen Jahr startet Secorvo College mit einem zweitägigen Seminar zu Public Key Infrastrukturen (PKI) (25.-26.01.2005), an das sich am 27.01.2005 ein eintägiges PKI-Vertiefungsseminar für Fortgeschrittene anschließt. Im Februar folgen das Grundlagenseminare IT-Sicherheit heute (15.-17. 02.2005) sowie das fünftägige Schlüsselseminar zum Information Security Management (21.-25.02.2005), dessen erste drei Tage auch getrennt gebucht werden können. Erstmals wird am 21.-22.06.2005 auch die Prüfung zum „Certified IT-Security Professional“ abgenommen.

http://www.secorvo.de/college

2.2 Lead Auditor

Am 15.11.2004 wurde Jörg Völker, Autor eines der mit über 13.000 Downloads meistgelesenen Secorvo Whitepaper zum Information Security Management, als Lead Auditor nach dem Information Security Management (ISM) Standard BS 7799 zertifiziert. Das berechtigt ihn zur Durchführung von offiziellen Audits gemäß BS 7799, zur Vorbereitung auf oder der Abnahme von einer offiziellen BS 7799-Zertifizierung, die inzwischen auch in Deutschland zunehmend in den Fokus der Informationssicherheit stehen.

2.3 Forensik-Symposium

Am **01.-02.03.2005** veranstaltet Secorvo im Rahmen der Karlsruher IT-Sicherheitsinitiative ein Computer Forensik Symposium: ausgewiesene Experten aus unterschiedlichen Bereichen (BKA, Interpol, Recht und Technik) versprechen eine eineinhalb tägi-

ge intensive Beschäftigung mit forensischen Fragestellungen. Nicht zuletzt besteht im Rahmen des gemeinsamen Dinners ausreichend Möglichkeit zum Erfahrungsaustausch. Eine frühzeitige Anmeldung wird empfohlen.

2.4 Delegation und Haftung

Nicht nur Geschäftsführer, sondern auch IT-Leiter, IT-Sicherheitsverantwortliche und Datenschutzbeauftragte tragen eine erhebliche Verantwortung für den reibungslosen und gesetzeskonformen Betrieb der Informationstechnik eines Unternehmens.

Was bedeutet das im Falle eines Vorfalls? Wer haftet unter welchen Voraussetzungen gegenüber wem? Muss der IT-Leiter bei Regressforderungen mit seinem Vermögen gerade stehen?

Die Vielzahl der zu diesen Fragen kursierenden Behauptungen, Gerüchte und Befürchtungen ersetzt Professor Dr. Michael Bartsch auf der kommenden Veranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **16.12.2004** (Beginn: 18 Uhr) durch belastbare Fakten.

Wir freuen uns, mit Prof. Bartsch nicht nur einen ausgewiesenen Experten in diesen Fragen, sondern auch einen brillianten Redner gewonnen zu haben – wer schon einmal das Vergnügen hatte, ihn zu hören, wird diesen Termin nicht verpassen wollen; allen anderen sei er wärmstens empfohlen. Im Anschluss an Vortrag und Diskussion haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim kulinarischen Ausklang – "Buffet-Networking", sozusagen.

2.5 DuD 2005

Schon wirft sie ihre Schatten voraus: Die Konferenz „Datenschutz und Datensicherheit“ (DuD), seit sechs Jahren von COMPUTAS in enger Kooperation mit den Herausgebern und Autoren der Fachzeitschrift DuD veranstaltet. Zum Vormerken in Ihrem Kalender: **18.-19.04.2005**, Berlin.

3 Veranstaltungshinweise

Dezember 2004	
05.-09.12.	Asiacrypt 2004 (IACR, Jeju Island/Korea)
06.-07.12.	IsSec/ZertiFA 2004 (COMPUTAS, Berlin)
09.-10.12.	Einführung in die Praxis des DSB (Euroforum, Düsseldorf)
16.12.	Verantwortung, Delegation und Haftung (KA-IT-Si, Karlsruhe)
Januar 2005	
25.-26.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
27.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2005	
15.-17.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
21.-25.02.	Information Security Management (Secorvo College, Karlsruhe)
März 2005	
01.-02.03.	Computer Forensik Symposium 2005 (KA-IT-Si, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News

Dezember 2004

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 12, 3. Jhrg. 2004
Stand 22. Dezember 2004

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Bekenntnis

1 Security News

1.1 Immer wieder MD5

1.2 WLAN-Schnorrer erwischt

1.3 Neues ISIS-MTT-Profil

1.4 NSA-Guide zu MacOS X

1.5 PGP Global Directory

1.6 Trojanisierte Fahrräder

1.7 Schwachstelle PHP

1.8 RFID-Studie online

1.9 Phisher auf der Lauer

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Näher am Zug

2.3 Verstärkung

3 Veranstaltungshinweise

Impressum

Editorial: Bekenntnis

Ohne Sicherheit ist keine Freiheit.
Wilhelm von Humboldt (1767-1835)

Seit mehr als zwei Jahren ziert dieses Zitat unsere Webseite. Warum? Eine berechtigte Frage, ist doch der Zusammenhang nicht ganz offensichtlich.

Sicherheit als Vorbedingung von Freiheit? Das klingt befremdlich, schränken Sicherheitsmaßnahmen doch meist unseren persönlichen Freiraum ein, wie Gepäckkontrollen am Flughafen, videoüberwachte öffentliche Räume oder Ausweiskontrollen an der Grenze. Über die Verhältnismäßigkeit solcher Maßnahmen muss selbstverständlich politisch gestritten werden – unbestritten ist allerdings, dass erst ein durch die „innere Sicherheit“ geschütztes friedliches Zusammenleben eine freie Entfaltung ermöglicht.

Eine ähnliche Entwicklung lässt sich im Internet beobachten. So lange das Netz nur ausgewählten Nutzergruppen zugänglich war, funktionierte diese neuartige offene Kommunikation durch Selbstregulierung – sogar ein wenig über das Geburtsjahr des WWW hinaus. Mit der wachsenden Verbreitung und der Entdeckung immer neuer Nutzungsmöglichkeiten war es jedoch vorbei mit der friedlichen Kommunikation. Viren, Würmer, Trojaner, Angriffsprogramme und Spam konterkarierten den Nutzwert des neuen Mediums. Inzwischen ist die Nutzung des Internet ohne wirksame Sicherheitsmechanismen praktisch nicht mehr möglich. Nur wer Viren scannt, Angriffe an der Firewall abfängt und Spam filtert, kann die kommunikativen Freiheiten eines Daten- und Dokumentenaustauschs frei von Verzögerung, Qualitätsverlust und Medienbruch genießen.

Ohne Sicherheit ist keine Freiheit. Ob man für diese Erkenntnis den Hauptvertreter des deutschen Humanismus bemühen sollte, sei dahingestellt. Tatsächlich geht es vielleicht gar nicht passender. Im Zweifel sollten Sie es mit Johannes Rau halten: „Trau keinem Zitat, dass Du nicht selbst aus dem Zusammenhang gerissen hast.“

1 Security News

1.1 Immer wieder MD5

Am 06.12.2004 geriet der Hash-Algorithmus MD5 wieder einmal in die Schlagzeilen, als der Wissenschaftler Dan Kaminsky ein Papier („MD5 To Be Considered Harmful Some Day“) veröffentlichte, in dem er praktische Angriffe auf den Algorithmus dokumentiert – durch die Konstruktion geeigneter „Kollisionen“ sei es möglich, zu verschiedenen Bitfolgen (u.a. auch Binärcode) denselben MD5-Hash zu generieren. Ein von ihm gleichzeitig veröffentlichtes Tool untermauert seine Behauptungen.

Dieser Report hat die schon vor Jahren geführten Diskussionen um MD5 wieder belebt: Prinzipielle Schwachstellen sind seit Anfang der 90er Jahre bekannt, das RSA Labs Bulletin vom 12.11.1996 riet bereits von der weiteren Verwendung ab, und die erste Algorithmenempfehlung des BSI zum Signaturgesetz von 1998 enthielt MD5 gar nicht erst. Viele der veröffentlichten Angriffe hatten aber lange eher akademischen Wert. Auch Kaminiskys Veröffentlichung musste sich diesen Vorwurf gefallen lassen – Fakt bleibt jedoch, dass MD5 schon längst nicht mehr eingesetzt werden sollte.

1.2 WLAN-Schnorrer erwischt

Wie die Zeitung Die Welt am 11.11.2004 berichtete, wurde in Bielefeld ein „WLAN-Schnorrer“ verhaftet. Der Mann fiel der Polizei dadurch auf, dass er in seinem geparkten Auto offensichtlich im Internet surfte. Tatsächlich bediente er sich eines ungesicherten WLAN-Access-Points. Der Laptop wurde beschlagnahmt, zusätzlich erfolgte eine Anzeige wegen Verdachts auf Ausspähen von Daten. Sollte es sich um ein ungeschütztes WLAN gehandelt haben, dürfte die Strafbarkeit fraglich sein – nach § 202a StGB liegt der Tatbestand des Ausspähens nur vor, wenn die Daten „gegen unberechtigten Zugang besonders gesichert sind“.

1.3 Neues ISIS-MTT-Profil

Am 01.12.2004 verabschiedete das ISIS-MTT Board Version 1.0 des Profils für Zertifikate zu Authentifikationszwecken. Dieses u.a. mit Unterstützung von Microsoft und Sun entstandene Profil fasst die Anforderungen zusammen, die in verschiedenen Systemumgebungen – von SSL-gesicherten Web-Anwendungen bis zur Anmeldung an Linux-Rechner – an ISIS-MTT konforme Zertifikate zur Authentifikation gestellt werden.

1.4 NSA-Guide zu MacOS X

Bereits am 15.10.2004 aktualisierte das Systems and Network Attack Center (sic!) der National Security Agency (NSA) seinen Security Configuration Guide für Apples Betriebssystem MacOS X. Neben Suns Solaris 8 ist MacOS derzeit das einzige Nicht-Windows-Betriebssystem, für das die NSA einen entsprechenden Security Guide veröffentlicht. Für die Anwender von Apple-Systemen sicher ein hilfreiches Dokument – denn auch Systeme, die nicht wie Windows im „Bull’s Eye“ der Hacker stehen, erfordern die gleiche Sorgfalt bei Konfiguration und Betrieb.

1.5 PGP Global Directory

Bereits seit vielen Jahren existiert ein mehr oder weniger gut funktionierendes globales Netz von öffentlichen Keyservern zum Austausch von PGP-Schlüsseln. Die Server synchronisieren sich dabei in der Regel untereinander, um ihre Datenbestände abzugleichen. Auch die Firma PGP, Inc. betreibt einen solchen Verzeichnisdienst, hat sich aber in der Vergangenheit nur unregelmäßig an der Synchronisation mit den anderen Keyservern beteiligt.

Jetzt geht PGP mit dem „PGP Global Directory“ einen Schritt weiter: Jeder PGP-Key, der über ein Web-Interface an den Server übermittelt wird, muss vom Schlüsselinhaber authentisiert werden. Hierfür wird dem Inhaber automatisch eine E-Mail geschickt, die er beantworten muss, bevor

sein Key in die Datenbank aufgenommen wird; dies wird alle sechs Monate wiederholt. Die E-Mail-Adresse wird dabei aus dem PGP-Key extrahiert, bei dem es sich jedoch nicht um einen älteren („v3“) Schlüssel handeln darf.

Grundsätzlich handelt es sich hierbei um einen sinnvollen Mechanismus, da er verhindert, dass (wie auf anderen Keyservern leider der Fall) unzählige Schlüssel hochgeladen werden, hinter denen kein „echter“ Benutzer steckt. Andererseits hat es bereits Beschwerden von PGP-Nutzern gegeben, deren Keys von Dritten an den Server übermittelt wurden – jene erhielten anschließend E-Mails des Keyservers, die sie als Spam einstuften...

1.6 Trojanisierte Fahrräder

Unter dem Stichwort Hack a Bike haben findige Hacker die Miet-Fahrräder des Call a Bike-Angebots der Deutschen Bahn manipuliert. Dazu wurde die Firmware der elektronischen Fahrradschlösser bei etwa 200 Rädern in Berlin durch eine eigene Version mit Hintertür-Entsperrcode ersetzt.

Einzelheiten des Hacks sind in einer am 17.12.2004 anonym auf den CCC-Webseiten veröffentlichten Technologieanalyse dargestellt. Die Hacker bescheinigen darin dem System – außer, dass die Sperren gegen ein Auslesen der Firmware nicht aktiviert waren – ein „sehr gutes technisches Design“. Der Aufwand zum Brechen des Systems war offenbar deutlich höher als die Kosten Dutzender Fahrräder. Dass ihn die Hacker dennoch in Kauf nahmen, dürfte daran liegen, dass der Call-a-Bike-Chef den Code in einem Artikel als „nicht zu knacken“ bezeichnet hatte.

1.7 Schwachstelle PHP

Das am 17.04.2004 von Stefan Esser initiierte Hardened-PHP Projekt hat es sich zur Aufgabe gemacht, den Nutzern der besonders für CGI-Skripte beliebten Skriptsprache PHP mehr Sicherheit zu geben. Ein Hauptaugenmerk des Projekts liegt auf dem Schutz des Skript-Programmierers vor eigenen Fehlern und Unsauberkeiten. Aber auch Schwachstellen in PHP selbst treten bei der Arbeit an Hardened-PHP zu Tage. So zählt Esser in einem Advisory vom 15.12.2004 insgesamt sieben PHP-Schwachstellen auf; sie wurden in den am selben Tag veröffentlichten aktuellen PHP-Versionen beseitigt.

1.8 RFID-Studie online

Seit dem 20.12.2004 ist die BSI-Studie zu Risiken und Chancen des Einsatzes von RFID-Systemen (RIKCHA) vollständig online abrufbar. Die Studie fasst die Grundlagen der RFID-Technologie zusammen, betrachtet grundlegende Angriffsmöglichkeiten und Abwehrmaßnahmen und bietet Ausblicke auf Anwendungsfelder und künftige Entwicklungen.

1.9 Phisher auf der Lauer

Zu den neuen Tricks beim „Phishing“ nach Passwörtern gehört das am 08.12.2004 in einem Advisory der dänischen Firma Secunia veröffentlichte „Phishing mit Fenstern“, auf das praktisch alle aktuellen Browser herein fallen, solange Javascript aktiviert ist – d.h. faktisch leider bei fast allen Besuchern von Internet-Seiten.

Dabei lauert auf einer unbemerkt zum Phishing missbrauchten Seite ein Skript darauf, dass der Nutzer einen Link aktiviert, der ein neues Fenster zur Eingabe vertraulicher Daten öffnet. Ist der Name dieses Fensters dem Angreifer bekannt, kann das Skript den Inhalt des neuen Fensters dieses Namens augenblicklich mit einem gefälschten Formular überschreiben. Mittlerweile wird diese Methode auch beim bekannten c’t-Browsercheck demonstriert.

Vor dieser Phishing-Variante können die Anbieter von Homebanking- und E-Commerce-Seiten ihre Nutzer allerdings aktiv schützen, indem der Server bei jedem Aufruf einen neuen, nicht vorhersagbaren Fensternamen verwendet. Dann kann der Phisher lauern, bis er schwarz wird...

2 Secorvo News

2.1 Secorvo College aktuell

Für 2005 wurde das Weiterbildungsangebot von Secorvo College um mehrere Seminare erweitert. So haben wir das erfolgreiche Live Hacking Lab (26.-28.04. 2005) zu einem dreitägigen Seminar ausgebaut. Hinzu kommen zwei neue, thematisch ergänzende Seminare, die aktuelle Themen der Bedrohungsentwicklung aufgreifen: die Angriffe auf Web-Anwendungen und das Thema Computer Forensik (Web Application Security, 02.-04.05.2005 und Spurensuche im Web, 23.-25.05. 2005). Zwei weitere neue Seminare stellen die Systemsicherheit in den Mittelpunkt: IT-Sicherheit für Windows-Administratoren (07.-08.06.2005) und IT-Sicherheit für Unix-Administratoren (09.-10.06.2005).

2.2 Näher am Zug

Anfang Januar wird Secorvo neben dem Karlsruher Stadtgarten ein neues Domizil beziehen – in Fußweite vom Hauptbahnhof. Ab dem 10.01.2005 erreichen Sie uns daher unter der folgenden neuen Anschrift, Telefon- und Faxnummer:

Ettlinger Straße 12-14
D-76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

2.3 Verstärkung

Mitte November ist das Secorvo-Team erneut gewachsen. Jochen Schlichting verstärkt mit seinen Schwerpunkten Sicherheitspolicies, -architekturen, -analysen, Forensik und Systemsicherheit unser Consulting-Team. Er bringt mehr als zehn Jahre Berufserfahrung in der IT-Security Beratung mit. Natalie Mareth hat sich mit eSecurity-Lösungen und digitalen Signaturen beschäftigt. Ihre Kernaufgabe ist die Entwicklung eines neuen Service-Angebots – über das in einer der nächsten Security News mehr verraten wird.

3 Veranstaltungshinweise

Januar 2005	
25.-26.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
27.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2005	
14.-18.02.	RSA-Konferenz (San Francisco)
15.-17.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
21.-25.02.	Information Security Management (Secorvo College, Karlsruhe)
März 2005	
01.-02.03.	Computer Forensik Symposium 2005 (KA-IT-Si, Karlsruhe)
02.03.	Datenschutz kompakt (Secorvo College, Karlsruhe)
02.-03.03.	DFN-CERT Workshop (Hamburg)
15.-16.03.	D-A-CH Security (Darmstadt)
31.-01.04.	Black Hat Briefings (Amsterdam)
April 2005	
05.-07.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
05.-08.04.	Sicherheit 2005 (GI, Dortmund)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Januar 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 1, 4. Jhrg. 2005
Stand 28. Januar 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial:
Von Hasen und Igeln

1 Security News

1.1 Aktualisiertes IT-Grundschutzhandbuch des BSI

1.2 Anti-Spyware Tool

1.3 Anfänger für Office...

1.4 DoS gegen VoIP bei IOS

1.5 Microsoft lässt Patches intensiver testen

1.6 Apple Security Update

1.7 Einheitliche Sperrung

1.8 Anti-Phishing

1.9 12. DFN-CERT Workshop

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Forensik Symposium

2.3 DuD 2005

2.4 Teamverstärkung

3 Veranstaltungshinweise

Impressum

Editorial: Von Hasen und Igeln

Sie erinnern sich? Es war einmal an einem Sonntagmorgen im Herbst... ein Märchen der Gebrüder Grimm, erzählt an Ihrem Kinderbett, oder dem Ihrer Kinder.

Haben Sie nicht auch geschmunzelt über die List des Igels, der den Wettlauf gegen den körperlich weit überlegenen Hasen gewinnt, indem er sich in die Ackerfurche duckt und abwechselnd mit seiner Frau „Ich bin schon da!“ ruft, sobald der Hase das Ziel vermeintlich als Erster erreicht?

Zu denken hat mir damals gegeben, dass mein Großvater zu sagen pflegte: "Wahr muss die Geschichte sein, mein Sohn, sonst könnte man sie ja nicht erzählen.“

Und tatsächlich, da stellt sich, Jahrzehnte später, mit Blick auf das wirkliche Leben ein Déjà-vu ein. Der IT-Nutzer ruft: „Ich brauche einen sicheren Internetzugang“ – und Sie starten, installieren Firewall, Virenscanner und Spamfilter. Sie sind noch nicht fertig, da ruft er schon: „Ich brauche einen sicheren Laptop“ – und Sie sorgen für einen VPN-Tunnel, Personal Firewall und Festplattenverschlüsselung. Es ist noch nicht alles lauffähig, da ruft er bereits: „Meine E-Mails will ich auf meinem BlackBerry lesen“ – verschlüsselt natürlich. Und Sie rennen los und...

Eigentümlich nur, dass mir dabei meine kindliche Sympathie für den ob seiner krummen Beine verhöhnten und sich listig rächenden Igel ein wenig abhanden gekommen ist. Spielt nicht der Hase fair, indem er sich an die Regeln hält und alles gibt? Und ist nicht in Wahrheit der Igel grausam, nicht der erst hochnäsige Hase?

Auch aus diesem Märchen lässt sich also etwas fürs Leben lernen:

Erstens: Wenn die Igel nicht gestorben sind, leben sie noch heute. Zweitens: Eine höhere Geschwindigkeit löst nicht das Problem, sondern verkürzt die Lebenserwartung des Hasen.

Und drittens: Wer nicht auf dem Feld verenden möchte, sollte sich gelegentlich auch einmal in die Ackerfurche ducken.

1 Security News

1.1 Aktualisiertes IT-Grundschutzhandbuch des BSI

Am 10.01.2005 wurde eine aktualisierte Version des Grundschutzhandbuchs auf den Webseiten des BSI im PDF-Format zum Download bereit gestellt. Die HTML-Version soll in Kürze folgen. Neu hinzu gekommen sind die Bausteine „Router und Switches“, „S/390 und zSeries“ sowie „PDA“; der Baustein Sicherheitsgateway (Firewall) wurde überarbeitet. Das Grundschutzhandbuch deckt damit weitere wichtige Systeme ab – wird damit aber zugleich immer umfangreicher und komplexer. Daher wird über eine Ersetzung der inzwischen eher untertriebenen Bezeichnung „Grund“-Schutz diskutiert.

Fakt ist: Wer nach IT-Grundschutz zertifiziert ist, hat in der Regel ein hohes IT-Sicherheitsniveau erreicht. Kombiniert mit adäquatem Sicherheitsmanagement und ergänzenden Maßnahmen für besonders gefährdete Systeme sorgt Grundschutz für einen umfassenden Schutz der Unternehmens-IT.

1.2 Anti-Spyware Tool

Unter den am 11.01.2005 von Microsoft veröffentlichten Sicherheitspatches für XP findet sich die Beta-Version eines Anti-Spyware-Tools (MAS). Es erlaubt sowohl eine kontinuierliche als auch eine Anlass bezogene Untersuchung des PC auf verdächtige Programme.

Durch den Kauf der Firma Giant Ende 2004 verfügt Microsoft nun nicht nur über spezielles Spyware-Know-How, sondern auch über ein Programm, das grundsätzlich als umfassende Schädlingserkennungs-Engine ausgelegt ist: Es untersucht Registry und Systembibliotheken auf bekannte Spyware, prüft ausgewählte Konfigurationseinstellungen und arbeitet mit einer aktualisierbaren Signaturdatenbank – das Grundgerüst eines jeden Virenschutzprogramms.

Daher sprießen bereits die Gerüchte, Microsoft wolle doch noch in den Virenschutz-Markt einsteigen. Genährt wird dieser Verdacht dadurch, dass die genannten Sicherheitspatches – etwas versteckt – ein zweites Tool enthalten: ein „Malicious Software Removal Tool“, das nicht allein die in der Vergangenheit für ausgewählte Viren bereit gestellten Deinstallationstools zusammenfasst, sondern zusätzlich im Hintergrund versucht, ein erneutes Auftauchen dieser Viren zu erkennen.

1.3 Anfänger für Office...

...statt Office für Anfänger: In einem am 10.01.2005 bei der International Association for Cryptologic Research eingereichten Papier enthüllt ein Forscher aus Singapur, dass Microsoft bei der Verschlüsselung von Dokumenten in Office dieselbe Schlüsselfolge mehrfach verwendet. Dies gilt unter Kryptologen als typischer Anfängerfehler und sorgt dafür, dass Dokumente trotz starker 128-Bit RC4-Verschlüsselung unter Umständen leicht entschlüsselt werden können.

Bei Motoren gilt die alte Weisheit „Hubraum ist durch nichts zu ersetzen, außer durch mehr Hubraum!“. Bei Entwurf und Review eines Sicherheitskonzepts gilt dies analog – für langjährige Erfahrung.

1.4 DoS gegen VoIP bei IOS

Wie nicht anders zu erwarten, weisen auch moderne Voice-over-IP Systeme Schwachstellen auf. Da es sich dabei „nur“ um IT-Systeme handelt, trifft man auch hier auf bekannte Lücken durch fehlerhafte Implementierungen und Protokollschwächen. Jüngstes Beispiel ist ein von Cisco am 19.01.2005 veröffentlichtes Security Advisory: Bei Telephony Service (ITS), Call-Manager Express (CME) und Survivable Remote Site Telephony (SRST) bestimmter IOS-Versionen kann mit präparierten Nachrichten ein Reboot des Systems ausgelöst werden. Per „Dauerbeschuss“ lässt sich so ein ausgewachsener Denial-of-Service-Angriff durchführen. Es wird empfohlen, die aktuellen Updates baldigst einzuspielen.

1.5 Microsoft lässt Patches intensiver testen

Wie die Zeitschrift eWeek am 12.01.2005 berichtete, startet Microsoft ein „Security Update Validation Program“: Zukünftig sollen Sicherheitspatches nicht nur von Microsoft selbst und wenigen Großkunden getestet, sondern an weitere externe Beta-Tester verteilt werden. Hierdurch sollen in der Vergangenheit aufgetretene Problemfälle vermieden und die Qualität der Patches – und damit auch die Sicherheit – gesteigert werden. Das Programm verdient weitere Beobachtung; der Erfolg wird sich an den bei künftigen Patches auftretenden Problemen erweisen müssen.

1.6 Apple Security Update

Nicht nur Windows braucht Patch Management: Am 25.01.2005 veröffentlichte Apple das erste Security Update des Jahres für das hauseigene Betriebssystem Mac OS X.

Dabei wurde zugleich die vorher Datumsbasierte Bezeichnung der Security Updates auf eine laufende Nummer (2005-001) umgestellt – eine ebenso einfache wie wirkungsvolle Maßnahme, um Anwendern die Prüfung zu erleichtern, ob alle Updates bereits eingespielt wurden.

1.7 Einheitliche Sperrung

Die Regulierungsbehörde für Telekommunikation und Post (RegTP) hat am 21.12.2004 dem Sperr e. V. – Verein zur Förderung der Sicherheit in der Informationsgesellschaft – die bundeseinheitliche Telefonnummer 116 116 für die Sperrung von EC-, Kredit- Handy-, Krankenkassen- und Kundenkarten zugeteilt. Die Rufnummer muss 180 Tage ab Zuteilung, also ab Anfang Juli 2005 (im Inland entgeltfrei) erreichbar sein.

1.8 Anti-Phishing

Am 20.01.2005 veröffentlichte die Anti-Phishing Workung Group einen Report über die erkannten Phishing-Aktivitäten im Dezember 2004. Demnach werden die meisten der gefälschten Server zum ab„phish“en von Passwörtern nicht, wie man vielleicht erwarten könnte, in Osteuropa, Fernost oder Offshore-Steuerparadiesen installiert, sondern in den USA.

Diese Server waren durchschnittlich nur 5,9 Tage am Netz – daher ist bei Phishing-Attacken vor allem die erste Woche nach deren Auftreten kritisch. Daraus erklärt sich auch, dass einschlägige E-Mails oft an überdeutlichen Hinweisen auf ihre vorgeblich besondere Dringlichkeit zu erkennen sind.

Einen anderen Weg der Phishing-Detektion gehen, wie am 21.01.2005 gemeldet wurde, die Entwickler des Mozilla Mail-Clients Thunderbird: Sie wollen den Anwender warnen, wenn er eine in der Mail enthaltene URL anklickt, bei der z. B. anstelle des im Text angezeigten Hostnamens eine IP-Adresse hinterlegt ist. Umstritten ist jedoch, wie diese Warnung einem Endanwender verständlich vermittelt werden kann...

1.9 12. DFN-CERT Workshop

Die wichtigste deutsche Security-Konferenz wirft wieder einmal ihre langen Schatten voraus: Bereits zum zwölften Mal wird am 2. und 3. März im Kongresszentrum (CCH) in Hamburg der zweitägige DFN-CERT/ PCA-Workshop stattfinden. Das auch diesmal sehr viel versprechende Programm dürfte auch 2005 wieder deutlich mehr als 300 interessierte Teilnehmer aus Forschung, Unternehmen und Behörden anlocken und zum Diskutieren anregen.

Als eingeladener Sprecher konnte Lance Spitzner gewonnen werden, der vor allem für das Projekt „Honeynet“ verantwortlich zeichnet. Auch die anderen Vorträge versprechen interessante Themen auf hohem Niveau.

2 Secorvo News

2.1 Secorvo College aktuell

Secorvo College startet in das Jahr 2005 nicht nur mit einem um vier neue Seminare

erweiterten Angebot, sondern auch mit verkürzten Reisezeiten für Sie: Das neue Domizil von Secorvo liegt in Fußweite vom Karlsruher Hauptbahnhof (300 m) und fünf Autominuten von der A5.

Die Seminare im Februar geben einen Überblick über die IT-Sicherheit heute und vertiefen das zunehmend wichtige Thema Information Security Management (Anmeldung).

http://www.secorvo.de/college

2.2 Forensik Symposium

Secorvo veranstaltet im Rahmen der Karlsruher IT-Sicherheitsinitiative und in Kooperation mit Viccon am 01.-02.03.2005 das Computer Forensik Symposium 2005. Die systematische „virtuelle Spurensicherung" hat in den beiden vergangenen Jahren mit der Zunahme erfolgreicher Angriffe auf die IT-Infrastrukturen von Unternehmen spürbar an Bedeutung gewonnen. Das Programm des Symposiums beleuchtet das Thema erstmals von allen Seiten – aus der Perspektive der Strafverfolgung, der Unternehmenspraxis, der Technik und der „best practices".

2.3 DuD 2005

Inzwischen steht das Programm der diesjährigen siebten Konferenz „Datenschutz und Datensicherheit – DuD 2005", konzipiert und geleitet von den Herausgebern der Fachzeitschrift DuD. Sie findet am 18.-19.04.2005 in alter Tradition im Berliner Dorint-Hotel Schweizerhof statt; eine rechtzeitige Anmeldung wird empfohlen (die Teilnehmerzahl ist auf 100 begrenzt).

2.4 Teamverstärkung

Seit Mitte Januar ergänzt Ralph Wiedemann das Secorvo-Team: Er bringt mehrjährige Berufserfahrung als IT-Sicherheitsverantwortlicher, Berater und Projektleiter für IT-Security mit und verstärkt unser Know-How rund um Firewalls, PKI-basierte VPNs, Security-Audits, Intrusion Detection und Security Policies.

3 Veranstaltungshinweise

Februar 2005	
15.-17.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
21.-22.02.	IT-Security Management (Secorvo College, Karlsruhe)
21.-25.02.	Information Security Management (Secorvo College, Karlsruhe)
März 2005	
01.-02.03.	Computer Forensik Symposium 2005 (KA-IT-Si, Karlsruhe)
02.03.	Datenschutz kompakt (Secorvo College, Karlsruhe)
02.-03.03.	DFN-CERT Workshop (DFN-CERT, Hamburg)
15.-16.03.	D-A-CH Security 2005 (GI/OCG/ BITKOM/SI/TTT, TU Darmstadt)
April 2005	
05.-07.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
05.-08.04.	Sicherheit 2005 (GI, Regensburg)
12.-13.04.	Lotus Notes Security (Secorvo College, Karlsruhe)
14.04.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
18.-19.04.	Datenschutz und Datensicherheit – DuD 2005 (COMPUTAS, Berlin)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe
Tel. +49 721 225 171-0
Fax +49 721 225 171-100

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Februar 2005

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 2, 4. Jhrg. 2005
Stand 25. Februar 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Wer dreimal lügt...

1 Security News

1.1 SHA-1 – Gebrochen?

1.2 SigG-Algorithmen

1.3 Riskmanagement-Studie

1.4 Neue Schläuche bei RFID

1.5 Netfilter IP-Tables 1.3

1.6 Nessus übernommen

1.7 Suse mit EAL 4-Zertifikat

1.8 VoIP Security

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Forensik kompakt

2.3 DuD – das Programm

3 Veranstaltungshinweise

Impressum

Editorial: Wer dreimal lügt...

Wieder einmal wird eine (Krypto-)Sau durchs Dorf getrieben. Diesmal haben die Hashfunktionen Jagdsaison. Zum zweiten Mal steht der „Secure Hash Standard“ (SHA) des NIST auf der Abschussliste: Schon 2004 geisterten Gerüchte durch die Gazetten, SHA sei gebrochen. Tatsächlich waren Schwachstellen der ursprünglichen, vom NIST bereits 1995 ersetzten Version SHA-0 gefunden worden. „Hilfe, der Wolf kommt!“ – der erste Fehlalarm.

Jetzt hat es jedoch den SHA-1 erwischt. Bruce Schneier löste am 15.02.2005 mit einem Eintrag in seinem Blog („SHA-1 has been broken“) die zweite Welle der „Hilfe, der Wolf kommt!“-Alarme aus. Vier chinesische Forscher hatten ein kryptographisch bemerkenswertes Ergebnis angekündigt: Mit einem Aufwand von 2^{69} sei es möglich, SHA-1-Kollisionen zu finden. Dies ist allerdings ein Aufwand, der deutlich jenseits eines praktikablen Angriffs liegt – und nur zwei beliebige, keineswegs sinnvolle Zeichenfolgen liefert, die denselben Hash-Wert besitzen. Zweiter Fehlalarm.

Die Erfahrung der vergangenen Jahre hat jedoch gezeigt, dass ein solcherart angeschossener Algorithmus schon bald tatsächlich erlegt sein kann. Fatal wäre allerdings, wenn der SHA das Schicksal des Hashalgorithmus MD5 teilen würde: Auch beim MD5 gab es zwei Fehlalarme; der dritte Alarm Mitte 2004, nach dem Kollisionen mit einem Workstation-Cluster in weniger als einer Stunde konstruiert werden können, wurde überhört: Noch immer verwenden zahlreiche kryptographische Anwendungen und Produkte den MD5 als Hash-Algorithmus.

Sollte ein dritter, berechtigter „Hilfe, der Wolf kommt!“-Alarm beim SHA-1 ungehört verhallen, droht allerdings ein GAU – denn zum SHA-1 gibt es derzeit fast keine standardisierte und vor allem in Anwendungsstandards wie z. B. S/MIME berücksichtigte Alternative.

Der einzige Unterschied zwischen dieser Geschichte und dem Gleichnis mit dem Wolf: Die „Hilfe“-Rufer würden überleben.

1 Security News

1.1 SHA-1 – Gebrochen?

Ausgelöst durch einen Weblog-Eintrag des Krypto-Experten Bruce Schneier verbreitete sich am 15.02.2005 wie ein Lauffeuer die Nachricht, dass es einem renommierten chinesischen Forscherteam um Xiaoyun Wang gelungen ist, die Krypto-Hashfunktion SHA-1 zu brechen. Die Aufregung ist verständlich, wenn man bedenkt, dass SHA-1 ein zentraler Baustein für PKI-Zertifikate und -Anwendungen wie z.B. digitale Signaturen, SSL oder S/MIME ist.

Das Papier von Wang und Kollegen ist noch nicht öffentlich verfügbar. Soweit die Fakten mittlerweile bekannt sind, bedeutet „gebrochen", dass ein theoretischer Durchbruch gelungen ist: Der Aufwand zum Finden zweier verschiedener Klartexte, die denselben 160-Bit SHA-1-Hashwert besitzen, konnte von 2^{80} für eine Brute-Force-Attacke auf 2^{69} Schritte verringert werden. Letzteres erscheint z.B. im Vergleich mit dem mehr als vier Jahre dauernden „Brute-Forcing" von 2^{64} RC-5 Schlüsseln deutlich jenseits des heute praktisch Machbaren.

Zweifel an der Sicherheit des SHA-1 waren bereits aufgekommen, als auf der Expertenkonferenz Crypto 2004 mehrere Forschergruppen neue Angriffe auf Hashfunktionen vorstellten. Als Reaktion hierauf kündigte das NIST, Urheber des SHA-1, bereits am 25.08.2004 an, spätestens 2010 den SHA-1 zugunsten der designierten Nachfolger SHA-224 bis SHA-512 (jüngster SHA-Standard vom 01.08.2002) auslaufen zu lassen.

Das Dilemma für den Anwender ist, dass derzeit praktisch keine Alternativen zur Verfügung stehen: MD4 und MD5 wurden effektiv gebrochen (siehe auch SSN 12-04), RIPEMD-160 ist kaum verbreitet und nach ähnlichen Prinzipien aufgebaut wie SHA-1 (also eventuell auch ähnlich anfällig), und die jüngeren Algorithmen SHA-224/256/384/512 (auch als „SHA-2" bezeichnet) wurden bislang erst in wenige Produkte integriert.

Handlungsbedarf besteht also, aber Panik ist nicht angezeigt. Selbst wenn die Attacke in Einzelfällen praktisch umsetzbar wäre, erlaubt sie es nicht, einen zweiten Klartext zu finden, der zu einem vorgegebenen Hashwert – z.B. aus einem existierenden CA-Zertifikat – passt, sondern erzeugt „nur" zwei zunächst zufällige Zeichenfolgen so, dass deren Hashwerte (und damit auch die Signaturen) übereinstimmen. Somit sind bereits geleistete Signaturen ohnehin nicht gefährdet.

Am dringlichsten sind die Hersteller von Signaturanwendungen gefordert, alternative Hash-Algorithmen in ihre Produkte aufzunehmen. Als einer der ersten Hersteller hat PGP am 18.02.2005 die Gelegenheit ergriffen, ein Update anzukündigen.

1.2 SigG-Algorithmen

Noch ohne Kenntnis der neuesten Ergebnisse zum SHA-1 gab die RegTP am 02.01.2005 die Übersicht über geeignete Algorithmen nach dem Signaturgesetz bekannt. Wie auch durch das NIST wird darin dem SHA-1 eine (nun möglicherweise zu überdenkende) Lebenszeit bis 2010 gegeben. Zulässige Alternativen als Hashfunktion sind RIPEMD-160 und SHA-2.

1.3 Riskmanagement-Studie

Das Institut für Wirtschafts- und Verwaltungsinformatik von Prof. Dr. Hampe an der Universität Koblenz führt ab dem 24.02. 2005 eine Delphi-Studie zum IT Riskmanagement durch. Ziel dieser Studie ist es, Trends und Entwicklungen im Bereich des IT Risk Managements zu ermitteln. Die Studie richtet sich ausschließlich an Fachexperten, daher ist eine Teilnahme nur mit den folgenden Login-Daten möglich: Kennung: itrm, Passwort: mrti. Für weitere Informationen steht die Projektleiterin, Frau Meletiadou (0261/287-2535) zur Verfügung.

1.4 Neue Schläuche bei RFID

Am 28.01.2005 veröffentlichte ein Forscherteam der Johns Hopkins University

und der RSA Laboratories die – auch praktisch umgesetzte – Analyse eines RFID-Chips von Texas Instruments, der u.a. in Wegfahrsperren häufig eingesetzt wird.

Angesichts der Verwendung eines 40-Bit-Schlüssels, der eine Brute-Force-Suche ermöglicht, ließe sich dies als alter Wein (oder eher Essig) in neuen RFID-Schläuchen abtun. Bemerkenswert daran sind jedoch mehrere Punkte: Die Bereitschaft zur Kooperation des Herstellers (anstelle eines leider häufigen peinlichen Schweigens oder Abstreitens), die von den Autoren beschriebene Black-Box Rekonstruktion des im Chip verwendeten Algorithmus und die Überlegungen, wie man sich als Träger eines RFID-Chips vor unbeabsichtigtem Auslesen der darauf gespeicherten Daten schützen kann. Letzteres könnte eine neue Klasse von Produkten oder Werbe-Giveaways hervorbringen: einfach zu handhabende Faradaysche-RFID-Hüllen – womit sich der Kreis zu den Schläuchen schließt.

1.5 Netfilter IP-Tables 1.3

Das Netfilter-Team um Harald Welte hat am 12.02.2005 die Version 1.3 von iptables freigegeben. Die im Linux Kernel integrierten Funktionen ermöglichen eine stateful Paketfilterung und eine Reihe weiterer (Firewall)-Funktionen. In Version 1.3 wurden Bugs beseitigt und die Performance nochmals verbessert.

1.6 Nessus übernommen

Der verbreitete OpenSource-Scanner Nessus wurde unter die Hoheit von Tenable Network Security als offiziellem Sponsor gestellt. Tenable ist der Hersteller der kostenpflichtigen Windows32-Variante des Security Scanners (NeWT Pro), die kostenfreie Variante NeWT ist auf das lokale Subnetz beschränkt.

Nach einer Benutzerregistrierung kann Nessus weiterhin kostenfrei unter Linux und anderen Unix-Plattformen eingesetzt werden. Allerdings werden aktuelle Plugins von Tenable erst nach einer Wartezeit von sieben Tagen zur Verfügung gestellt. Wer die Plugins sofort einsetzen möchte, muss den „Direct Feed Update Service“ zum Preis von 1.200 $ pro Jahr buchen. Die unter der Gnu Public Licence (GPL) von der Community erstellten Plugins sind auch weiterhin ohne Verzögerung und kostenfrei erhältlich.

1.7 Suse mit EAL 4-Zertifikat

Am 15.02.2005 teilte die atsec information security GmbH mit, dass sie für Suse's Linux Enterprise Server 9 (SLES 9) den Prozess der Evaluierung nach Common Criteria (CC) EAL 4+ abgeschlossen habe und ein entsprechendes Zertifikat folgen werde.

EAL 4+ ist ein hohes Evaluationslevel; diese Stufe wird auch für Chipkarten nach dem Signaturgesetz (SigG) verlangt. Eine fundierte Beurteilung einer CC-Evaluierung ist jedoch nur unter Berücksichtigung des der Prüfung zu Grunde liegende Kriterienkatalogs („Protection Profile“) möglich, in dem die Prüfanforderungen definiert sind.

SLES 9 wurde in diesem Fall gegen das Schutzprofil „Controlled Access Protection Profile (CAPP)“ geprüft, welches insbesondere Anforderungen an die Zugriffskontrolle definiert. Auch Windows 2000 wurde bereits gegen CAPP EAL 4 evaluiert – genau diese Evaluierung führte jedoch vor einigen Jahren zu massiver Kritik an dem Schutzprofil: Bei genauerer Betrachtung gilt es nämlich nicht in üblichen Netzwerk-Umgebungen wie dem Internet („*The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers...*“).

1.8 VoIP Security

Am 07.02.2005 wurde unter der Federführung von Tippingpoint die Voice Over IP Security Alliance (VOIPSA) ins Leben gerufen. Die Gruppe hat sich zum Ziel gesetzt, das Thema Security im Bereich VoIP vorwärts zu bringen.

Vom National Institute of Standards and Technology (NIST) ist seit dem 03.01.2005

ein Whitepaper zum Thema "Security Considerations in Voice over IP Systems" verfügbar. Neben technischen Grundlagen werden insbesondere die Sicherheitsfunktionen der Protokolle und auch die Integration mit weiteren Schutzmechanismen wie Firewalls und VPN dargestellt.

2 Secorvo News

2.1 Secorvo College aktuell

Im April stehen zahlreiche Seminarangebote auf der Agenda von Secorvo College:

- drei aktuelle Seminare zur Systemsicherheit: Sichere E-Mail-Kommunikation (05.-07.04.) Lotus Notes Security (12.-13./14.04.) und Inside Windows Security (19.-20.04.2005), sowie
- eine in Zusammenarbeit mit dem Unternehmen Compass Security Network Computing AG (Schweiz) entwickelte „Hands on" Seminarreihe: Live Hacking Lab (26.-28./29.04.2005) und Web-Application Security (02.-04.05. 2005).

Veranstaltungsprogramme, das vollständige Seminarangebot mit weiteren Terminen und ein Anmeldeformular finden Sie auf den Webseiten von Secorvo College.

2.2 Forensik kompakt

In der kommenden Woche findet das erste Computer Forensik Symposium der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) bei Secorvo in Karlsruhe statt (01.-02.03. 2005). Themen sind die Sichtweisen und Erfahrungen von Staatsanwaltschaft, BKA und betroffenen Unternehmen sowie die Vorstellung von Forensik Tools und deren praktischem Einsatz. Die zahlreichen Anmeldungen versprechen spannende Diskussionen. Für Kurzentschlossene gibt es noch einige wenige freie Plätze.

2.3 DuD – das Programm

Das Programm der Fachkonferenz „Datenschutz und Datensicherheit" (DuD, 18.-19. 04.2005) ist jetzt verfügbar.

3 Veranstaltungshinweise

März 2005	
01.-02.03.	Computer Forensik Symposium 2005 (KA-IT-Si, Karlsruhe)
02.-03.03.	DFN-CERT Workshop (DFN-CERT, Hamburg)
15.-16.03.	D-A-CH Security 2005 (GI/OCG/ BITKOM/SI/TTT, TU Darmstadt)
April 2005	
05.-07.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
05.-08.04.	Sicherheit 2005 (GI, Uni Regensburg)
12.-13.04.	Lotus Notes Security (Secorvo College, Karlsruhe)
14.04.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
18.-19.04.	Datenschutz und Datensicherheit – DuD 2005 (COMPUTAS, Berlin)
19.-20.04.	Inside Windows Security (Secorvo College, Karlsruhe)
26.-28.04.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.04.	Live Hacking Spezial (Secorvo College, Karlsruhe)
Mai 2005	
02.-04.05.	Web-Application Security (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
März 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch und Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 3, 4. Jhrg. 2005
Stand 29. März 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial:
Vom Suchen und vom Finden

1 Security News

1.1 Kollidierende Zertifikate

1.2 Haftungsrisiken

1.3 NIST SP 800-53

1.4 Microsoft im Fadenkreuz

1.5 Kompass der IT-Sicherheitsstandards

1.6 Knack' den Knacker

1.7 Data-Mining the NSA

2 Secorvo New

2.1 Secorvo College aktuell

2.2 security-finder.de

3 Veranstaltungshinweise

Impressum

Editorial: Vom Suchen und vom Finden

Nicht erst seit der Proklamation des „lebenslangen Lernens" wissen wir: Die Halbwertzeit unserer Kenntnisse ist oft überraschend kurz. Erst recht im Gebiet IT-Sicherheit müssen wir immer wieder feststellen, dass manch mühsam erworbene und lieb gewonnene Erkenntnis durch neue Entwicklungen Makulatur wird. Nicht nur Hashfunktionen, Verschlüsselungsverfahren und kryptoanalytische Erkenntnisse jagen einander, auch neue Technologien halten uns in Atem – und die Security-Ticker in Bewegung. Da bleibt wenig Anderes, als mit der Entwicklung zu gehen, denn Stagnation in Sicherheitsfragen kann schwer wiegende Folgen haben.

Wie aber bleibt man „auf dem Laufenden"? Unter den Bedingungen knapper Zeitressourcen helfen allein aktuelle, konzentrierte, verständliche und fundierte Informationsmaterialien. Nur: Wo findet man die?

Meist geht inzwischen der Griff zur Tastatur statt zum Buch. Das zeigt eine aktuelle Befragung von 400 DAX-30-Managern: Für 94% ist das Internet die wichtigste Informationsquelle, 84% verbringen eine bis vier Stunden wöchentlich mit der Informationsrecherche (imc, 2005).

Zwar gilt auch für das Internet das Bibelwort: *„... wer da suchet, der findet"* (Matthäus, 7. Kapitel, Vers 8). Nur findet er nicht unbedingt auch das Gesuchte. Denn eines verrät keine Suchmaschine: Ob ein gefundenes Dokument informativ, verständlich und fachlich fundiert ist. Diesem Mangel kann man nur mit viel Leseaufwand begegnen.

Auch wir mussten uns dieser Herausforderung stellen. So ist bei Secorvo ein Informationspool aus vielen hundert ausgewählten Dokumenten entstanden. Den Zugriff auf diese „virtuelle Bibliothek" ermöglichen wir nun unter http://www.security-finder.de/ – den Lesern der Security News bis zum 10. April 2005 unentgeltlich (Login: „SSN-01", Passwort: „security-finder"). Wir freuen uns auf Ihre Rückmeldungen.

1 Security News

1.1 Kollidierende Zertifikate

Für viel Wirbel hat am 01.03.2005 die Publikation eines Forscherteams gesorgt, dem es gelungen ist, zwei unterschiedliche X.509-Zertifikate zu erzeugen, die denselben MD5-Hashwert liefern. Obwohl die Existenz von MD5-Kollisionen schon seit geraumer Zeit bekannt ist, waren praktische Angriffe selten – bis jetzt: Lenstra, Wang und de Weger präsentierten zwei Beispielzertifikate mit unterschiedlichem Public Key aber demselben MD5-Hashwert.

Die praktischen Auswirkungen dieses Angriffs sind dennoch gering: Ein Angreifer müsste eine vertrauenswürdige Zertifizierungsinstanz (CA) dazu bringen, das vorbereitete Zertifikat zu signieren, ohne eine Änderung daran vorzunehmen. Jede „vernünftig“ arbeitende CA wird jedoch vor allem kritische Felder wie die Seriennummer und das Gültigkeitsdatum des Zertifikats selbst ausfüllen.

Weiter erlaubt das Verfahren nicht die Konstruktion einer Kollision zu einem bereits vorliegenden Zertifikat. Damit sind insbesondere bereits ausgestellte Zertifikate nicht auf diese Weise angreifbar. Schließlich müssen die Zertifikatsparameter eine Bitlänge besitzen, die ein ganzzahliges Vielfaches von 512 ist.

Aber vor allem: Welchen Nutzen hätte ein Angreifer von zwei Zertifikaten zu von ihm selbst konstruierten Public Keys? Schlimm wäre, wenn er Zertifikatsparameter ändern könnte, um z.B. den Public Key einer zweiten Identität zuzuordnen oder aus einem End-User- ein CA-Zertifikat zu machen – dies ermöglicht das Konstruktionsverfahren jedoch nicht.

Nach eigenen Aussagen versucht das Forscherteam jetzt, vergleichbare Zertifikate auf SHA-1-Basis zu finden. Doch obwohl SHA-1 stark „angekratzt“ ist, scheint dies deutlich aufwändiger zu sein. Wer allerdings noch immer MD5 einsetzt, ist nicht nur nicht sicher, sondern selbst Schuld.

1.2 Haftungsrisiken

Vom Bitkom ist am 10.03.2005 ein Leitfaden zum Thema Haftungsrisiken erschienen. Das Dokument stellt recht übersichtlich die wichtigsten rechtlichen Anforderungen zusammen und unterscheidet insbesondere nach strategischen, konzeptionellen und operativen Aufgaben. Für verschiedene Zielgruppen wie Geschäftsführung/-Vorstand und IT-Leitung/-Sicherheitsbeauftragte werden in einer Matrix die jeweiligen Pflichten und der Bedarf den Rechtsgrundlagen, potentiellen Schäden und Ansprüchen Dritter gegenüber gestellt. Der Leitfaden bietet einen guten Einstieg in das Thema und zeichnet sich durch klare Strukturierung und übersichtliche Darstellung aus.

1.3 NIST SP 800-53

Am 07.03.2005 wurde die NIST Special Publication 800-53 „Recommended Security Controls for Federal Information Systems“ veröffentlicht. Sie stellt in guter, sehr detaillierter und umfassender Form die möglichen Ausprägungen von Sicherheitsmaßnahmen dar, die im Rahmen der Sicherheitsarchitektur einer Organisation notwendig sind. NIST SP 800-53 korrespondiert dabei mit dem im Dezember 2003 publizierten Standard FIPS-199 „Standards for Security Categorization of Federal Information and Information Systems“.

Das 121 Seiten starke Dokument differenziert Maßnahmen in den drei Kategorien Management, Organisation/Betrieb sowie Technik mit insgesamt 17 Teilbereichen. Passend dazu gibt es drei Ergänzungsdokumente, in denen die Sicherheitsmaßnahmen für drei unterschiedliche Grundsicherheitsniveaus (low/moderate/high) zusammen gestellt werden. Es ist zu erwarten, dass diese in den USA zukünftig verstärkt zur Bewertung des erreichten Sicherheitsniveaus heran gezogen werden.

Für Ende 2005 ist der Standard FIPS-200 "Minimum Security Controls for Federal Information Systems" angekündigt, der die Empfehlungen der SP 800-53 für US-amerikanische Organisationen ablösen soll.

1.4 Microsoft im Fadenkreuz

Wie bereits am 09.02.2005 vom Antivirus-Hersteller Sophos gemeldet versucht der Trojaner Bankash.A neben seiner eigentlichen „Tätigkeit", Zugangskennungen zum Online-Banking auszukundschaften, auch die am 20.01.2005 erschienene Beta-Version des Windows AntiSpyware Tools von Microsoft zu deaktivieren.

Dies könnte ein erstes Indiz sein, dass sich bei Sicherheits-Software das fortsetzt, was bei Betriebssystemen gang und gäbe ist: Andere Lösungen sind vielleicht nicht viel sicherer als Microsofts (apropos: am 12.03.2005 erschien das erste Sicherheitsupdate zu Firefox 1.0, am 23.03.2005 schon das zweite), aber allein auf Grund ihrer Verbreitung stehen Microsoft-Produkte im Fadenkreuz der Hacker und werden häufiger und schneller angegriffen.

1.5 Kompass der IT-Sicherheitsstandards

Auch am 10.03.2005 wurde vom Bitkom ein Leitfaden für mittelständische Unternehmen mit dem Titel „Kompass der IT-Sicherheitsstandards" veröffentlicht. Das Dokument bietet einen gelungenen Überblick wichtiger Standards wie ISO 17799, BS 7799-2, IT-Grundschutz, Cobit, ITIL sowie weiterer für spezifischere Sicherheitsaspekte. Durch ein Klassifizierungsschema ist je nach Art des Unternehmens und der IT-Relevanz sehr übersichtlich dargestellt, welche Felder der jeweilige Standard abdeckt und für welche Personen und Rollen er angewendet werden kann.

1.6 Knack' den Knacker

Das Passwort Recovery Tool Cain&Abel ist wegen seines mächtigen Funktionsumfangs und der eingängigen Bedienoberfläche bei Penetrations-Testern und IT-Forensikern vermutlich ebenso beliebt wie bei Hackern jeglicher Couleur. Ironie des Schicksals: Am 18.03.2005 wurde bekannt, dass Cain&Abel bis Version 2.65 anfällig für einen Buffer-Overflow ist, wenn es beim Abhören eines VPN-Verbindungsaufbaus auf manipulierte IKE-Pakete stößt.

Nimmt man einmal an, dass viele Angreifer es mit dem Patch-Level ihrer Werkzeuge nicht anders halten als die meisten ihrer Opfer, könnte man vor diesem Hintergrund auf die Idee verfallen, präventiv „vergiftete" Pakete im eigenen Netz auszustreuen...

1.7 Data-Mining the NSA

Dem österreichischen Verein Quintessenz ist es nach eigenen Angaben aufgrund eines Konfigurationsfehlers gelungen, ein vollständiges Archiv der „Biometrics Consortium List" zur erlangen, welches ca. 60 MB Text sowie 2 GB an Fachdokumenten und Präsentationen enthält. Insgesamt haben 2.500 Personen bzw. Organisationen an der Mailingliste mitgewirkt.

Unter dem Aufmacher „Datamining the NSA – Part I" wird derzeit mit Hilfe von Werkzeugen des Data-Minings höchst aufschlussreich und sehr detailliert nachgewiesen, in welchem Ausmaß über die letzten zehn Jahre hinweg mit dieser Mailingliste von US-amerikanischen Organisationen versucht wurde, den Biometriebereich systematisch zu beeinflussen. Die Diagnose: Ziel war ein patentfreier, universaler Standard, der eine technologische Unabhängigkeit der USA von nicht-amerikanischen Patentgebern sicherstellt.

Laut Quintessenz ist die Auswertung bisher erst bis zum Jahre 1996 erfolgt; daher kann noch nicht beurteilt werden, inwieweit die Entwicklung biometrischer Technologien und der Einsatz in Deutschland und Europa in den letzten Jahren „Impulse" durch diese Mailingliste erfahren haben.

2 Secorvo New

2.1 Secorvo College aktuell

Zusammen mit dem Schweizer Spezialisten Compass Security – Gewinner des 24-Stunden-Hacker-Contest 2004 des Schweizer Fernsehens – bieten wir Ihnen im April und Mai in vier technisch aufwändigen

Labor-Schulungen einen vertieften Einblick in die wichtigsten aktuellen Angriffsmethoden auf IT-Systeme – live und unter Ihrer aktiven Beteiligung vorgestellt. In den vier Labor-Seminaren wechselt die Arbeit im Übungslabor mit Referatsblöcken, in denen die wesentlichen theoretischen Hintergründe und Schutzmethoden vermittelt werden:

- Live-Hacking Lab (**26.-28.04.**)
- Live-Hacking Spezial (**29.04.**)
- Web Application Security (**02.-04.05.**)
- Spurensuche im Web (**23.-25.05.**).

2.2 security-finder.de

Seit Mitte März 2005 bietet Secorvo einen neuen Service: Den Zugang zur über mehr als zehn Jahre gewachsenen Secorvo-eigenen Know-How-Datenbank mit vielen Hundert ausgesuchten Dokumenten zu Fragestellungen der Datensicherheit und des Datenschutzes. Getreu dem Anspruch der Security News, eine „Schneise in die Informationsflut“ zu schlagen, bietet der Security-Finder den Zugang zu nach Wichtigkeit und Aktualität ausgewählten Dokumenten – jeweils mit Kategorisierung, inhaltlicher Zusammenfassung und Bewertung.

„Finden statt suchen“: Statt mühsamen Durchforschens von Suchmaschinenergebnissen führt der Security-Finder strukturiert direkt zum passenden Dokument. Besonders wertvolle Funde können per Mausklick in die private Bibliothek übernommen werden, und regelmäßig wird per E-Mail über Neuzugänge informiert.

Der Preis für den Zugang zum Security-Finder orientiert sich am Modell einer Loseblattsammlung: Der Zugang zum „Grundwerk“ kostet einmalig 299 €, das Jahresabonnement 149 €. Bis zum 30.06.2005 kostet der Zugang nur 249 € (Grundwerk) und das Jahresabonnement 124 €. (Preise für Unternehmenszugänge auf Anfrage).

Leser der Security News erhalten bis zum 10.04.2005 freien Zugang unter der ID „SSN-01“ (Passwort: „security-finder“).

3 Veranstaltungshinweise

April 2005	
05.-08.04.	Sicherheit 2005 (GI, Uni Regensburg)
12.-13.04.	Lotus Notes Security (Secorvo College, Karlsruhe)
14.04.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
18.-19.04.	Datenschutz und Datensicherheit – DuD 2005 (COMPUTAS, Berlin)
19.-20.04.	Inside Windows Security (Secorvo College, Karlsruhe)
26.-28.04.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.04.	Live Hacking Spezial (Secorvo College, Karlsruhe)
Mai 2005	
02.-04.05.	Web-Application Security (Secorvo College, Karlsruhe)
10.-11.05.	Datenschutzkongress 2005 (Euroforum, München)
10.-12.05.	IT-Sicherheitskongress 2005 (BSI, Bonn)
22.-26.05.	Eurocrypt 2005 (IACR, Aarhus/DK)
23.-25.05.	Spurensuche im Web (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de/

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
April 2005

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch,
Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 4, 4. Jhrg. 2005
Stand 25. April 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Verschwörung!

1 Security News

1.1 Datenschutz: Toll Collect

1.2 Hacken mit Google

1.3 MS Windows 2003 SP 1

1.4 Immer wieder: DNS-Gift

1.5 Un-Sicherheitsfeature

1.6 Wegmarke bei ISIS-MTT

1.7 WinZIP-Verschlüsselung

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Security Awareness Symposium 2005

3 Veranstaltungshinweise

Impressum

Editorial: Verschwörung!

Die Geschichte ist schnell erzählt: Für einen großen Kongress eines Sicherheits-Bundesamtes wird ein für kritische Kommentare bekannter Informatik-Professor um einen Vortrag über biometrische Sicherheitssysteme gebeten. Der Text ist geliefert, das Programm gedruckt – da kommt die Ausladung durch den Präsidenten, begründet mit „neuen Entwicklungen“. Der Brüskierte wendet sich an die Presse.

Zunächst nur ein Vorgang grober Unhöflichkeit unter Beamten. Aber: Der Beirat des Kongresses erfährt von der Ausladung aus der Zeitung, weiß nichts von „neuen Entwicklungen“, die im Programm unterzubringen sind. Ein Schelm, wer Arges dabei denkt: Fiebert doch der Innenminister bekanntlich nach biometrischen Merkmalen im Ausweis. Sollte da auf Veranlassung von oben ein Kritiker mundtot gemacht werden? „Zensur“, schreien die Kritiker. „Zu kurz gedacht“, erwidern Besonnene: Es sei doch dumm, Kritik und Professor medial so aufzuwerten. War es dann ein schwacher Moment des Präsidenten, der Versuch, in voraus eilendem Gehorsam befürchteten Minister-Groll abzuwenden? Nein, zu billig.

Dahinter steckt mehr. Schließlich war der Vortrag perfekt platziert: Um 9 Uhr am Morgen nach dem intensiv besuchten Empfang des ersten Kongressabends – nur Unverdrossene hätten die Reihen gefüllt. Da drängt sich eine andere Erklärung auf: Der Präsident, im Herzen Biometrie-Verächter, wollte der Kritik eine größere Bühne geben, sich selbst aber aus der ministeriellen Schusslinie halten. Jedoch: Auch dieser Verdacht hinkt. Die Kritik des Kritikers ist dünn, knapp (fünf Seiten) und akademisch, keine Bedrohung für den neuen Personalausweis. Versuchte der Präsident also, die Biometriekritik durch öffentliche Aufwertung magerer Argumente zu schwächen? Ist der Kritiker gar Agent der Biometrie-Industrie?

Tatsächlich diente die Farce ganz anderen Zwecken: Sie lenkte ab vom aufkeimenden Verschwörungsverdacht zur Rolle der NSA beim SHA-1-Design! (Warum bloß ist der SHA-1 nun Thema des Ersatzvortrags ...?)

1 Security News

1.1 Datenschutz: Toll Collect

Am 19.04.2005 hat Peter Schaar, der Bundesdatenschutzbeauftragte (BfD) den 20. Tätigkeitsbericht für die Jahre 2002-2004 vorgelegt. Darin äußert er sich unter anderem ausführlich zur Umsetzung des Datenschutzes im LKW-Mautsystem Toll Collect.

Dieses von der Toll Collect GmbH im Auftrag des Bundes nach dem Autobahnmautgesetz (ABMG) errichtete und seit Januar 2005 störungsfrei betriebene Mautsystem unterliegt strengen Datenschutzanforderungen. So dürfen beispielsweise von den ca. 300 Autobahn-Mautbrücken ausschließlich mautpflichtige Fahrzeuge erfasst werden; Fotos und Kennzeichen von PKW sind sofort zu löschen. Denn das ABMG berechtigt Toll Collect nur zur Nutzung von Daten, die für die Mauterhebung erforderlich sind. Die Erfassung von Daten, mit denen sich beispielsweise Bewegungsprofile erstellen oder Fahrzeuge von Straftätern verfolgen ließen, ist nicht erlaubt. Das Gesetz lässt daran keinen Zweifel: „Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig“ (§§ 4 Abs. 2, 7 Abs. 2 ABMG).

Um diese datenschutzrechtlichen Anforderungen in dem hoch komplexen Mautsystem umzusetzen, das täglich durchschnittlich 700.000 mautpflichtige LKW erfasst und kontrolliert, wurden zahlreiche Löschfunktionen für nicht erforderliche oder nicht mehr benötigte Fahrzeugdaten implementiert. An der Konzeption, Umsetzung und Kontrolle dieser Datenschutzmechanismen war Secorvo maßgeblich beteiligt.

Der BfD kommentiert das Ergebnis seiner Überprüfung des Datenschutzes bei Toll Collect in seinem Tätigkeitsbericht abschließend wie folgt: „Ich habe mich davon überzeugt, dass die Grundlagen für eine Umsetzung der datenschutzrechtlichen Anforderungen des Gesetzes in den Funktionalitäten des Systems auch geschaffen wurden.“ (S. 181). Wie sagt der Schwabe: „Ned gschumpfe isch gnug globd.“

1.2 Hacken mit Google

Bereits in den späten 1980er-Jahren diskutierten Sicherheitsexperten, dass damals aktuelle Suchmaschinen wie Gopher oder FTPsearch auch von Angreifern zur Recherche sensitiver Informationen – beispielsweise Passwortdateien – missbraucht werden könnten. Obwohl heutige Suchmaschinen wie Google ungleich mächtiger sind als ihre virtuellen Vorfahren, wurde diese Gefahr lange nicht untersucht.

Inzwischen betreibt der Sicherheitsexperte Johnny Long seit einiger Zeit eine viel beachtete Webseite, auf der Hunderte von Beispielen dafür zu finden sind, wie Google zum Suchen und Finden von z.B. Passwortdateien, versteckten Verzeichnissen, Logdateien, Software- und Betriebssystem-Schwachstellen, Login-Portalen, Datenbanken, Kreditkarteninformationen, oder Netzwerkdruckern, teilweise sogar automatisiert eingesetzt werden kann. In einem White Paper beschreibt Long die wichtigsten Beispiele und effektive Gegenmaßnahmen. Weiter geht sein soeben erschienenes Buch „Google Hacking for Penetration Testers“, das in keiner Bibliothek fehlen sollte.

1.3 MS Windows 2003 SP 1

Der am 30.03.2005 von Microsoft veröffentlichte Service Pack 1 (SP1) für Windows 2003 Server integriert alle sicherheitsrelevanten Patches der Jahre 2003-2005 bis einschließlich MS05-015. Darunter finden sich der Security Configuration Wizard (SCW) für eine vereinheitlichte und prozessorientierte Sicherheitsadministration, die Post-Setup Security Updates (PSSU) zur Blockade von Netzwerkverkehr bei einer Erstinstallation (schützt bis zur Patcheinspielung), die Windows Firewall (WF), die für jedes Interface über Group Policies administrierbar ist und die Data Execution Prevention (DEP) zum Schutz vor Speicherüberläufen.

Des weiteren wurden die Standard-Sicherheitseinstellungen restriktiver vordefiniert; damit sind Windows Server zukünftig hoffentlich auch sicherer konfiguriert.

1.4 Immer wieder: DNS-Gift

Seit dem 03.03.2005 gingen beim SANS-Institut zahlreiche Berichte über erfolgreiche „Cache Poisoning"-Angriffe auf diverse DNS-Server ein. Wieder hatten Angreifer die schon auf der USENIX 1995 publizierte DNS-Schwachstelle ausgenutzt. Neu war indes die Art der Angriffe: Gezielt wurden bekannte Lücken verschiedener Anwendungen genutzt: Zunächst wurden anfälligen DNS-Servern unter Windows NT4 bzw. 2000 sowie Gateways von Symantec gefälschte DNS-Einträge (Zuordnung von Hostnamen zu IP-Adressen) „untergejubelt". Anschließend wurden für bestimmte Hostnamen die IP-Adressen von Webservern geliefert, die dann über Schwachstellen des Internet Explorer versuchten, Spyware zu installieren. Vom SANS existiert eine detaillierte Analyse (deutsche Fassung), die auch Gegenmaßnahmen für Betroffene beschreibt.

Dieser Angriff zeigt nicht nur, dass unzureichendes Patch-Management immer wieder die Ausnutzung lange bekannter Schwachstellen ermöglicht. Sondern er lässt auch die Rufe nach DNSSEC wieder lauter werden. Mehrere Studien, u.a. von Secorvo und vom BSI, beschäftigten sich in den vergangenen Jahren mit der globalen Einführung von DNSSEC, rieten aber aus organisatorischen und technischen Gründen zur Zurückhaltung. Einige der identifizierten Mängel wurden jüngst in aktuellen RFCs korrigiert – mittelfristig führt sicherlich kein Weg an DNSSEC vorbei.

1.5 Un-Sicherheitsfeature

Ein am 01.04.2005 online veröffentlichter (und ernst gemeinter) Beitrag in der Zeitschrift c't ruft in Erinnerung, dass Zugriffsschutz und Denial-of-Service zwei Seiten einer Medaille sein können. So unterstützen viele Festplatten die im ATA-Standard vorgesehene Möglichkeit, den Zugriff auf die gespeicherten Daten durch ein Passwort in der Firmware des Laufwerks zu sperren. Dieses Passwort soll automatisch vom BIOS des Rechners, in dem die Festplatte eingebaut ist, gesetzt und verwendet werden. Weil jedoch viele BIOS-Hersteller das ATA-Passwort nicht unterstützen, wird nicht nur der mögliche Schutzeffekt nicht erzielt, sondern Trojanern & Co. die Möglichkeit gegeben, die Festplatte durch den Eintrag eines eigenen Passworts nahezu irreversibel zu sperren. So gesehen ist es ein Pluspunkt, dass der Schutz durch das ATA-Passwort nicht unüberwindbar ist...

Hersteller sollten daraus lernen, Anwendern konfigurierbare Sicherheitsfunktionen nur zugänglich zu machen, wenn diese bekannt und einfach konfigurierbar sind – sonst droht Missbrauch durch Angreifer.

1.6 Wegmarke bei ISIS-MTT

Am 14.04.2005 wurde im Rahmen einer Präsentation beim Bundeswirtschaftsministerium (BMWA) das im Jahr 2001 als „Public-Private-Partnership" gestartete Projekt ISIS-MTT in die „Obhut" der Wirtschaft übergeben.

Das mit einem Auftrag des BMWA an TeleTrusT e.V. in Kooperation mit T7 e.V. im Jahr 2001 gestartete Projekt zielte auf eine bessere Interoperabilität von PKI-Anwendungen. Seitdem wurden – unter Mitwirkung von Secorvo – die ISIS-MTT-Spezifikation weiter entwickelt, ein Testbed auf Open-Source-Basis konzipiert und realisiert sowie für inzwischen sechs Produkte ISIS-MTT Siegel vergeben, deren Standard-Konformität vom anerkannten ISIS-MTT-Prüflabor bei Secorvo bestätigt wurde.

1.7 WinZIP-Verschlüsselung

Immer wieder wird die im Kompressionsprogramm WinZIP integrierte Verschlüsselungsfunktion als Alternative zu einem Dateiverschlüsselungsprogramm eingesetzt. Früher war das riskant: Der PKZIP-kompatible Verschlüsselungsalgorithmus war 1994 von Biham und Kocher, 2001 mit einem verbesserten Verfahren von Stay erfolgreich attackiert worden.

Mit der Anfang 2004 publizierten Version 9 wurde die Verschlüsselung auf AES umgestellt (128 bzw. 256 bit Schlüssellänge) und HMAC-SHA-1 zur Integritätssicherung eingeführt. Seither gilt die Verschlüsselung als

kryptographisch stark. Dennoch ist Vorsicht geboten, wie Tadayoshi Kohno in einer Analyse vom 08.05.2004 zeigt: Er identifizierte zahlreiche Sicherheitsmängel der Implementierung (unverschlüsselte Dateiinformationen, Mischung verschlüsselter und offener Dateien, fehlerhafte Ableitung des AES-Keys von der Passphrase), die spezielle Angriffe ermöglichen.

2 Secorvo News

2.1 Secorvo College aktuell

Speziell für Administratoren haben wir zwei neue Seminare entwickelt, die sich dem Thema „Sichere IT-Administration“ widmen. Im Wechsel von Theorie, Workshop und Übung werden technische Anleitungen zur sicheren IT-Administration gegeben:

IT-Sicherheit für Admins (Windows) am **07.-08.06.2005**

IT-Sicherheit für Admins (Unix) am **09.-10.06.2005**

http://www.secorvo.de/college

2.2 Security Awareness Symposium 2005

Zum dritten Mal veranstaltet Secorvo am **21. und 22.06.2005** das “Security Awareness Symposium”. Es hat sich in den vergangenen Jahren zur Plattform für den Erfahrungsaustausch entwickelt. Security-Awareness-Aktivitäten leben von guten Ideen – und damit auch von einem aktiven Ideenaustausch. An den Symposien 2003 und 2004 wirkten u.a. BMW, die Münchener Rück, SAP, RWE Systems, Finanz-IT, die schweizerische Armee, BASF und T-Systems mit Erfahrungsberichten mit. Auch in diesem Jahr werden wieder mehrere deutsche Unternehmen mit einem Erfahrungsbericht vertreten sein; das Programm ist derzeit in Abstimmung. Das vorläufige Programm und ein Anmeldeformular finden Sie unter

http://www.security-awareness-symposium.de

3 Veranstaltungshinweise

April 2005	
26.-28.04.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.04.	Live Hacking Spezial (Secorvo College, Karlsruhe)
Mai 2005	
10.-11.05.	Datenschutzkongress 2005 (Euroforum, München)
10.-12.05.	IT-Sicherheitskongress 2005 (BSI, Bonn)
22.-26.05.	Eurocrypt 2005 (IACR, Aarhus/DK)
23.-25.05.	Spurensuche im Web (Secorvo College, Karlsruhe)
31.05. -02.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juni 2005	
01.-02.06.	Einführung in die Praxis des DSB (Euroforum, Wiesbaden)
06.-07.06.	IT-Risk Management 2005 (COMPUTAS, Karlsruhe)
13.- 14./17.06.	Information Security Management (Secorvo College, Karlsruhe)
21.-22.06.	Security Awareness Symposium (Secorvo, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Mai 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 5, 4. Jhrg. 2005
Stand 25. Mai 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial:
Spieglein, Spieglein ...

1 Security News

1.1 RSA-200 faktorisiert

1.2 Cross-Zertifikats-Report

1.3 BSI-Antispam-Leitfaden

1.4 Phishing exposed

1.5 Hash-Workshop

1.6 PIV-Standards

1.7 LAND unter

1.8 „Roo“ v1.0 erschienen

1.9 Firefox strikes back

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Toll Collect auf Midvision

2.3 Security Awareness Symposium 2005

3 Veranstaltungshinweise

Impressum

Editorial: Spieglein, Spieglein ...

Der Traum von biometrischen Identifikationssystemen, die uns von der Not befreien, unser Gedächtnis mit Myriaden ständig wechselnder User-IDs, Passwörter und PINs zu quälen, ist viel älter, als so manche Science Fiction-Verfilmung uns glauben machen will. Schon unter den von den Gebrüdern Grimm tradierten klassischen Märchen findet sie sich: „Schneewittchen und die sieben Zwerge“ kommt zwar ohne Elektrizität und fließendes Wasser aus, wäre aber ohne Biometrie nicht denkbar.

In der Gestalt des Spiegels der Königin erwacht sie zum vollen Leistungsumfang. Nicht nur erkennt der seine Herrin eindeutig an Stimme und Gesicht, sondern er gibt auch bereitwillig Auskunft über biometrische Merkmale Dritter – wie der Schönheit Schneewittchens. Mehr noch: Selbst den Aufenthaltsort Schneewittchens kennt er (dank RFID?) und gibt ihn Preis, er weiß sogar um ihren aktuellen Gesundheitszustand. Ganz zu schweigen von der fortschrittlichen natürlichsprachlichen Benutzerschnittstelle...

Vielleicht ist es Zeit, Schneewittchen neu zu interpretieren. Denn das Märchen zeigt in drastischer Klarheit, was durch die Vernetzung biometrischer und personenbezogener Daten möglich ist. Der Zauberspiegel, der zweifellos eine sehr effektive Durchführung von Schönheitswettbewerben ermöglichen würde, wird in der Hand der Königin zum Mordwerkzeug. Wir erinnern uns: Jede Technik öffnet auch dem Missbrauch Tür und Tor – nicht nur in Herrscherhand.

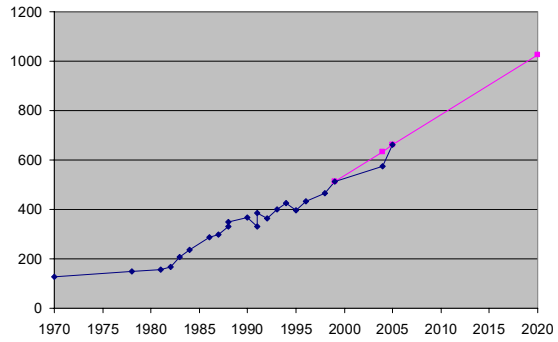
Dabei lassen sich biometrische und andere Identifikationssysteme auch so gestalten, dass eine Erfassung und Auswertung biometrischer Daten sowie der Aufenthaltsinformation nicht oder nur in kontrolliertem Umfang möglich ist. Dazu gehören die Einhaltung von Löschfristen, eine bedachte Technikgestaltung – vor allem aber der politische Wille, die Freiheit nicht um ihrer selbst Willen abzuschaffen.

„Spieglein, Spieglein an der Wand, wie lebenswert ist die Zukunft in diesem Land?“

1 Security News

1.1 RSA-200 faktorisiert

Am 09.05.2005 meldete die Bonner Forschungsgruppe von Prof. Jens Franke die erfolgreiche Faktorisierung der RSA-Challenge „RSA-200“ (Modullänge: 663 bit). Knapp 17 Monate hatte die Faktorisierung durch die Gruppe um Bahr, Böhm, Franke, Kleinjung, Montgomery und te Riele gedauert; der Rechenaufwand lag bei umgerechnet etwa 120.000 MIPS-Jahren. Für die Faktorisierung der Challenge „RSA-576“ Ende 2003, die auch auf das Konto dieser Forschergruppe ging, hatte sie „nur“ ca. 13.200 MIPS-Jahre benötigt (SSN 5/2004).



Grafik: Faktorisierungsprognose [BoFT_02]

Diese jüngste Faktorisierung entspricht fast exakt der Secorvo-Vorhersage aus dem Jahr 2001 – damals haben wir für 2005 die Faktorisierung eines 660 bit langen Moduls prognostiziert. Hält die Prognose, dann ist die Faktorisierung eines RSA-Moduls der Länge 1.024 bit in 15 Jahren zu erwarten.

1.2 Cross-Zertifikats-Report

Die Verknüpfung von Public-Key-Infrastrukturen (PKI) über Cross-Zertifikate oder Bridge-CAs ist in der Praxis noch immer nicht zufrieden stellend gelöst. Insbesondere Standard-Anwendungen wie Browser und E-Mail-Clients zeigen beim Umgang mit den entsprechenden Zertifikaten auch heute noch ein eher „holpriges“ Verhalten.

Diesem Problem sind die DFN-CERT Services GmbH und SURFnet in der Studie “PKI-Linking-Report: Connecting Public-Key-Infrastructures” nachgegangen, die am 26.04.2005 veröffentlicht wurde. Darin ist dokumentiert, wie unterschiedliche PKI-Anwendungen mit Cross-Zertifikaten etc. in der Praxis umgehen – und wo sie scheitern. Untersucht wurden Outlook Express, Outlook, Mozilla, Thunderbird, KMail, Internet Explorer, Mozilla, Firefox, Opera und Konqueror.

1.3 BSI-Antispam-Leitfaden

Spam ist schon lange nicht mehr nur eine Belästigung: Durch den Missbrauch zur Verbreitung von Phishing-Mails und Schadprogrammen ist Spam auch ein Sicherheitsproblem. Am 12.05.2005 stellte das BSI eine „Antispam-Strategien – Unerwünschte E-Mails erkennen und abwehren“ betitelte Studie zu diesem Thema vor. Die Untersuchung widmet sich dem Thema in großer Ausführlichkeit: Neben technischen Problemen und Lösungsvorschlägen werden auch die (vor allem finanziellen) Hintergründe organisierter Spammer diskutiert.

1.4 Phishing exposed

Phishing-Angriffe, in denen über Massen-E-Mails, die vorgeblich z. B. von Ebay oder einer Bank stammen, versucht wird, die Empfänger auf eine gefälschte Webseite zu locken und zur Eingabe vertraulicher Daten wie Passwörter, PINs oder TANs zu verleiten, nehmen nicht nur bedenklich zu, sondern werden auch immer perfider.

Dem Honeynet-Projekt ist es jetzt gelungen, hinter die virtuellen Kulissen einiger Phishing-Angriffe zu schauen. So konnten „Phisher“ dazu gebracht werden, Köder-Rechner (Honeypots) zu hacken und von dort ihre Angriffe (Aufsetzen gefälschter Webseiten, Verschicken von Massen-E-Mails, etc.) durchzuführen. Die Phisher wurden dabei mehrere Monate lang beobachtet. Dabei konnten drei generelle Angriffsmuster identifiziert werden. Ein am 16.05.2005 veröffentlichtes White Paper beschreibt die Details dieser Live-Analyse: Vieles weist darauf hin, dass zunächst automatisierte Angriffs-Tools verwendet

werden, um Hintertüren in einem System zu installieren. Über diese werden anschließend die Phishing-Attacken initiiert. Offenbar sind die Angreifer dabei sehr gut organisiert: So wurden Phishing-Archive mit gefälschten Webseiten vieler großer Online-Anbieter entdeckt. Erschreckend ist die Beobachtung, dass sehr viele Privatnutzer den Phishern auf den Leim gehen und auf deren gefälschte Webseiten zugreifen.

1.5 Hash-Workshop

Als Reaktion auf die jüngsten kryptoanalytischen Erfolge beim SHA-1 (SSN 02/2005) hat die Computer Security Division des NIST am 28.04.2005 einen Workshop zu kryptographischen Hashfunktionen ausgeschrieben (31.10.-01.11.2005). Interessierte sind aufgefordert, bis zum 15.07.2005 Vorschläge für Präsentationen einzureichen. Nähere Informationen finden sich auf der Workshop-Webseite.

1.6 PIV-Standards

Zur Umsetzung der Homeland Security Presidential Directive 12 vom 27.08.2004 wurde am 25.02.2005 vom NIST mit FIPS 201 ein Standard für eine einheitliche Personal Identity Verification (PIV) von Federal Employees und Contractors verabschiedet. Darin sind sowohl die grundsätzlichen Anforderungen an Identity-Cards als auch – sehr detailliert – die physisch-technischen Merkmale festgelegt, darunter die Abmessungen, Mechanismen (Foto, Barcode, Chip, Unterschriftsfeld, Magnetstreifen, Bedruckung) und Daten (z. B. biometrische Merkmale).

Der am 25.04.2005 publizierte NIST Special Report SP 800-78 enthält die Spezifikation der für PIV-Karten gemäß FIPS 201 zugelassenen kryptographischen Algorithmen und Schlüssellängen, vergleichbar der Algorithmenempfehlung des BSI für qualifizierte digitale Signaturen. Empfohlen werden darin bis Ende 2008/2010 RSA (ab 1024 bit), ECDSA (Kurven nach FIPS 186-3, ab 224 bit), TripleDES und AES (ab 128 bit) und als Hashfunktion SHA-1, SHA-224 oder SHA-256.

1.7 LAND unter

Am 17.05.2005 wurde auf der Bugtraq-Mailingliste die Anfälligkeit aktueller Windows-Systeme für LAND-Attacken gemeldet. Dieser Denial-of-Service Angriff wurde 1997 erstmalig veröffentlicht und eine entsprechende Schwachstelle bei Windows 95 geschlossen. Anfang 2005 wurde bei aktuellen Windows-Systemen erneut eine LAND-Anfälligkeit festgestellt. Die von Microsoft veröffentlichten Sicherheitspatches vom April sollten sie beheben; offenbar wirkt der Patch aber nicht bei Einsatz von IPv6. Wenn aber selbst die Patches vor Verbreitung nicht besser getestet werden als die Originalsoftware – was bleibt dann noch?

1.8 „Roo“ v1.0 erschienen

Am 17.05.2005 veröffentlichte das Honeynet-Projekt die Version 1.0 der kostenlosen Software „Honeywall CDROM Roo“. Dabei handelt es sich um eine auf Fedora basierende, sehr mächtige Tool-Sammlung, die es erlaubt, ein Honeynet der neuesten Generation sehr leicht aufzusetzen und zu administrieren, sowie potentielle Angriffsversuche auf das Honeynet effizient zu analysieren.

Stefan Kelm von Secorvo war während der mehrwöchigen Beta-Testphase intensiv an der Honeywall-Entwicklung beteiligt: Eine entsprechende Testumgebung wurde mehrere Wochen betrieben und Angriffe beobachtet. Die Ergebnisse dieser Testphase werden in Bälde als Secorvo White Paper veröffentlicht.

1.9 Firefox strikes back

Brian Livingston berichtet in seinem Newsletter vom 12.05.2005 von einem neuen Sicherheitsvergleich zwischen Internet Explorer und Firefox. Darin wurde nicht einfach die Anzahl der schwer wiegenden Schwachstellen verglichen, sondern die Zahl der Tage im Jahr 2004, an denen ein Browser mindestens eine ungepatchte, schwere Schwachstelle aufwies. Danach besaß die jeweils aktuelle Version des IE im Jahr 2004 an nur sieben Tagen keine

bekannten Schwachstellen. An 200 Tagen kursierten bereits Exploits (Angriffscode), ohne dass ein geeigneter Patch für den IE verfügbar war – bei Firefox kam dies nicht ein einziges Mal vor. Damit hat die Open-Source Community eindrucksvoll ihre hohe Reaktionsgeschwindigkeit bewiesen.

2 Secorvo News

2.1 Secorvo College aktuell

Wie sorge ich systematisch für Informationssicherheit im Unternehmen? Welche „Best Practices" gibt es, und was fordern die wichtigsten Standards? Antworten auf diese Schlüsselfragen gibt das zwei- bis fünftägige Seminar „Information Security Management von A(udit) bis Z(ertifizierung)" am **13.-14./17.06.2005**.

2.2 Toll Collect auf Midvision

Anlässlich der IT-Mittelstandsmesse „Midvision 2005" (Neue Messe Karlsruhe, 08.-09.06.2005) wird die Karlsruher IT-Sicherheitsinitiative am Abend des **08.06.2005** gemeinsam mit CAS und Cyberforum ein besonderes Event gestalten, in dessen Rahmen der Datenschutzbeauftragte von Toll Collect, Herr Reinhard Fraenkel, über Entwicklung und Umsetzung des Datenschutzkonzepts bei Toll Collect berichten wird. Programm und Anmeldung zu diesem Event mit anschließendem Buffet finden Sie auf der Webseite der KA-IT-Si.

2.3 Security Awareness Symposium 2005

Auf dem diesjährigen dritten „Security Awareness Symposium" am **21.-22.06.2005** in Karlsruhe, das sich in den beiden vergangenen Jahren als Plattform für den Erfahrungsaustausch über Sensibilisierungsmaßnahmen etabliert hat, werden unter anderem die Kampagnen von Bosch, DAK, Novartis und SAP präsentiert. Das aktuelle Programm und ein Anmeldeformular finden sich unter http://www.security-awareness-symposium.de/.

3 Veranstaltungshinweise

Mai 2005	
31.05. -02.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juni 2005	
01.-02.06.	Einführung in die Praxis des DSB (Euroforum, Wiesbaden)
06.-07.06.	IT-Risk Management 2005 (COMPUTAS, Karlsruhe)
08.06.	Datenschutz bei Toll Collect (KA-IT-SI/Midvision, Karlsruhe)
13.-14.06.	IT-Security Management (Secorvo College, Karlsruhe)
13.-17.06.	Information Security Management (Secorvo College, Karlsruhe)
14.-15.06.	Einführung in die Praxis des DSB (Euroforum, Berlin)
21.-22.06.	Security Awareness Symposium (Secorvo, Karlsruhe)
26.06.- 01.07.	17th Annual Computer Security Incident Handling Conference (FIRST, Singapore)
Juli 2005	
05.-07.07	Western European Workshop on Research in Cryptography (WEWoRC, Leuven-Heverlee)
27.-28.07.	Black Hat Briefings (Black Hat USA, Las Vegas)
29.-31.07.	Defcon 13 (Defcon, Las Vegas)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Abonnement des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Juni 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 6, 4. Jhrg. 2005
Stand 01. Juli 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Es wird ernst

1 Security News

1.1 Malcode Analysetools

1.2 Remote Desktop Attacke

1.3 VoIP-Scanning

1.4 Bluetooth-Angriff

1.5 Phisher-Test

1.6 SHA-Angriff publiziert

1.7 Win Security Monitoring

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Suchen in Security News

2.3 Thitz gestaltet Plakat

2.4 Security Awareness 2005

2.5 Forensische Analysen

3 Veranstaltungshinweise

Impressum

Editorial: Es wird ernst

Seit Jahren registrieren wir steigende Vorfallszahlen – jährlich eine Verdreifachung der Anzahl neuer Viren, Würmer und Trojaner, eine Verdoppelung der vom CERT registrierten Angriffsarten und einen rapiden Anstieg der in verbreiteter Software gefundenen kritischen Sicherheitslücken.

Allerdings: Der Anstieg der veröffentlichten – und nach unserer Beobachtung auch der der tatsächlichen – Schadensfälle entwickelte sich bislang moderat. Als Ursache dafür werden häufig wachsende Sensibilität der Verantwortlichen und die Etablierung wirksamer Schutzmaßnahmen vermutet.

Eine genaue Analyse der Angriffe und Schadensfälle zeigt jedoch, dass dies nicht die Hauptursache ist. Denn das vergleichsweise geringe Schadensniveau verdanken wir im Kern der Harmlosigkeit der Attacken:

- Die Entwickler von Viren und Würmern konzentrierten sich bisher auf Verbreitungs- und Tarnfunktionen; die Schadensroutinen waren oft primitiv und meist wirkungslos.
- Die Verbreitungsmechanismen waren ungezielt und nur auf große öffentliche Sichtbarkeit ausgelegt.
- Schäden wurden meist durch Programmierfehler verursacht; finanziell profitierten die Angreifer nicht.

Das ändert sich jedoch derzeit. Vermehrt lassen sich gezielte Angriffe beobachten, hinter denen wirtschaftlich interessante Geschäftsmodelle erkennbar werden: Im Auftrag entwickelte Trojaner, die Unternehmen aushorchen, ausgeklügelte Phishing-Attacken und Verschlüsselungs-Trojaner, die erst nach Lösegeldzahlung das Passwort preisgeben.

Daher wird es dringlich, die unseren Schutzmaßnahmen zu Grunde liegenden Annahmen zu überprüfen – denn gezielt geplante und professionell umgesetzte kriminelle Angriffe schaffen eine grundsätzlich neue Situation.

Die „Zeit der Spiele“ ist vorbei – es wird ernst.

1 Security News

1.1 Malcode Analysetools

David Zimmer vom Sicherheitsdienstleister iDefense hat am 07.06.2005 unter dem Namen Malcode Analyst Pack sieben Tools zur Analyse von Windows-Schadsoftware veröffentlicht. Darunter findet sich auch ein kleiner DNS-Server, der alle Anfragen an die IP-Adresse eines Forensikers lenkt. Die ebenfalls enthaltene Shell Extension zur Anzeige von Datei-Hashsummen im Explorer verwendet zwar noch den MD5 als Hashfunktion; da die Sammlung unter GPL Lizenz veröffentlicht wurde, steht einer Ersetzung durch den SHA nichts im Wege.

Dem wollte das BSI offenbar nicht nachstehen: Es veröffentlichte am 17.06.05 unter dem Namen BOSS (BSI OSS Security Suite) eine Knoppix CD mit Open Source Security Tools, darunter einer grafisch bedienbaren Version des Nessus Scanners. Dem beliebten Security Scanner wurde eine deutsche Oberfläche verpasst, die für versierte Nessus-User allerdings etwas gewöhnungsbedürftig ist. Da die Ergebnisse weiterhin in Englisch dargestellt werden und eine Übersetzung der inzwischen über 7.000 Nessus-Plugins recht aufwändig sein dürfte, sind Zweifel am Sinn dieser Eindeutschung angebracht. Auch wenn einige weitere Tools wie beispielsweise NMap mitgeliefert werden, besitzen spezialisierte Knoppix-Versionen wie Knoppix-STD deutlich umfangreichere Möglichkeiten.

Schließlich erschien am 22.06.2005 eine aktualisierte Fassung der Auditor Security Collection CD, eine der mächtigsten Sammlungen aktueller Versionen wichtiger Tools zur Durchführung von Sicherheitsanalysen.

1.2 Remote Desktop Attacke

Mit der am 10.06.05 erschienenen Version 2.7.3 des Auditwerkzeugs Cain&Abel ist es möglich – einen geeigneten Netzzugang vorausgesetzt – die Schutzmechanismen einer Remote Desktop Protocol Sitzung im Rahmen einer Man-in-the-Middle Attacke zu unterlaufen und die Tastatureingaben aufzuzeichnen. Betroffen von dieser Möglichkeit sind alle aktuellen Windows Releases (WXP SP2 / W2K3 SP1), auf denen die Terminal Services eingesetzt werden. Der Angriff funktioniert dank der integrierten ARP Poison Routing-Technolgie auch in geswitchten Netzwerkinfrastrukturen.

Ermöglicht wird dieser Angriff durch ein grob fehlerhaftes Design der initialen Public-Key Authentifikation bei Microsoft: Der generierte Public-Key des Terminal Servers, der bei der Initialisierung der Terminal-Session verwendet wird, wird mit einem Private Key signiert, der fest kodiert im Betriebssystem vorhanden und damit für jedermann auslesbar ist (mstlsapi.dll).

Zum Schutz vor diesem Angriff bleibt für eine sichere Remote Administration von Windows Systemen (XP/2003) auf Basis von RDP nur der konsequente Einsatz der Virtual Private Network Funktionalität.

1.3 VoIP-Scanning

Viele Hacker- und Analyse-Tools werden in den aktuellen Versionen mit Funktionen zum Mitschneiden von VoIP-Datenströmen ausgeliefert, mit denen Telefonate als wav-Datei gespeichert werden können.

Mit diesen Analysetools lassen sich sehr eindrucksvolle Demonstrationen gestalten – z. B. durch die Aufnahme eines via ARP-Poisoning umgelenkten Telefonats im internen Netz. Aber Vorsicht: Das Belauschen und Mitschneiden eines Telefongesprächs, selbst die „näheren Umstände“ (Zeitpunkt, Teilnehmer) auch eines erfolglosen Verbindungsversuchs ohne Wissen der Kommunikationspartner ist ein strafbewehrter Verstoß gegen § 88 TKG, der das in Artikel 10 Grundgesetz garantierte Fernmeldegeheimnis schützt – unabhängig vom Motiv des Abhörvorgangs und unabhängig davon, ob der Betreiber der Anlage geeignete Schutzmaßnahmen getroffen hat.

Für WLAN-Verbindungen gelten verschärfte Bedingungen: § 89 TKG enthält ein explizites Abhörverbot für Funkanlagen, das nicht nur Telefonverbindungen umfasst,

sondern alle Nachrichten, die für die Funkanlage nicht bestimmt sind. Erfolgt ein unbeabsichtigter Empfang, unterliegen die Daten der Geheimhaltung und dürfen nicht an Dritte weitergegeben werden.

1.4 Bluetooth-Angriff

Zwei israelische Forscher präsentierten am 06.06.05 einen Bericht, in welchem sie den erfolgreichen Angriff auf einen zentralen Sicherheitsmechanismus von Bluetooth – die PIN beim Pairing von Geräten – darstellen. Durch ein Belauschen des Pairing-Prozesses kann eine kurze PIN (4 Zeichen) selbst auf veralteten PCs (Pentium III, 450 MHz) in weniger als einer Sekunde (0,3 sec) bestimmt werden.

Zusätzliche Relevanz erlangt der Angriff dadurch, dass die Autoren auch beschreiben, wie ein Angreifer per Funk zwei bereits „gepaarte" Bluetooth-Geräte zum erneuten Pairing veranlassen kann – um auch deren PIN zu gewinnen.

1.5 Phisher-Test

Phishing-Angriffe nehmen nicht nur in ihrer Anzahl stetig zu – die verschickten E-Mails sind auch immer schwieriger von „echten" E-Mails zu unterscheiden. Wer mag, kann sein diesbezügliches Urteilsvermögen beim (zweiten) „Phishing IQ Test" der Firma MailFrontier auf die Probe stellen: Für zehn Beispiele (eBay, Amazon, Bank of America etc.) ist zu entscheiden, ob es sich um eine Phishing-Mail handelt.

Der Test schärft nicht nur die eigene Urteilsfähigkeit, sondern bietet dank ausführlicher Erläuterungen auch eine gute Hilfestellung bei der Gestaltung eigener Online-Dienstleistungen. Am ersten Test haben sich angeblich mehr als 225.000 Personen beteiligt.

1.6 SHA-Angriff publiziert

Für Kryptologen interessant: Die Autoren des SHA-Angriffs (siehe SSN 02/2005), die Forschungsgruppe um Wang, haben am 17.06.2005 ihre für die Crypto 2005 eingereichte Forschungsarbeit zu SHA-0 und SHA-1 öffentlich zugänglich gemacht.

1.7 Win Security Monitoring

Microsoft hat am 06.06.2005 einen Security Monitoring and Attack Detection Planning Guide veröffentlicht, der Hilfestellung bei der Konfiguration und Nutzung der Microsoft Windowxs Security Event Logs für ein wirksames Security Monitoring leistet. Im Anhang des 53seitigen Dokuments finden sich außerdem Empfehlungen für die Konfiguration der Audit Policy in den Group Policy Settings.

2 Secorvo News

2.1 Secorvo College aktuell

Nach einer Sommerpause in den Monaten Juli und August startet das College-Programm des zweiten Halbjahrs 2005 im September mit Seminaren zu Public Key Infrastrukturen (20.-21./22.09.2005) und Web-Application Security (27.-29.09.2005). Wir freuen uns, wenn wir Sie im Herbst auf einem unserer Seminare begrüßen dürfen.

http://www.secorvo.de/college

2.2 Suchen in Security News

Viele Leser schätzen die seit Juli 2002 monatlich erscheinenden Secorvo Security News wegen der zahlreichen Links auf wertvolle Originaldokumente. Bisher war die Suche nach älteren Links jedoch mühsam: Es gelang bestenfalls mit einer Volltextsuche in den pdf-Dateien des Jahrgangsarchivs, und gelegentlich hatte sich die gesuchte URL inzwischen verändert.

Daher finden sich inzwischen alle in den Secorvo Security News zitierten Dokumente vollständig im Security Finder und ermöglichen so eine thematische Recherche und eine regelmäßige Aktualisierung der Links. Mit dem Erscheinen der vorliegenden Juni-Ausgabe der SSN können jetzt auch SSN-Jahrgänge komplett im Security Finder durchsucht werden.

Zur Erinnerung: Bis 30.06.2005 gibt es den Security Finder noch zum Einstiegspreis.

2.3 Thitz gestaltet Plakat

Der Secorvo-Künstler Thitz hat für SWR3 das Plakat des diesjährigen New Pop Festival gestaltet – und folgt damit James Rizzie und Chales Kaufman, die 2003 und 2004 die Plakate entwarfen. Ein weiterer Meilenstein auf dem Weg zum Weltruhm – erst Ende 2004 hielt er mit einer Tüte zur Gründung Einzug in die „Sammlung Frieder Burda“ in Baden-Baden.

2.4 Security Awareness 2005

Die Materialien des diesjährigen dritten Security Awareness Symposium am 21. und 22.06.2005 sind jetzt – wie auch die der Vorjahresveranstaltungen – auf CD erhältlich – darunter die Präsentationen der Security Awareness Kampagnen von Bosch, Novartis und SAP, eine Vorstellung der Initiative „Deutschland sicher im Netz“ und ein Vortrag von Herrn Prof. Dr. Zerr zur Evaluation und Erfolgskontrolle von Awareness-Maßnahmen. Die CDs der beiden Vorjahresveranstaltungen enthalten Darstellungen der Kampagnen von BASF, BMW, Fiducia, Münchener Rück, RWE, der Schweizerischen Armee und T-Systems sowie weiterführende Materialien und eine Fotodokumentation der Ausstellung auf dem Symposium 2003.

2.5 Forensische Analysen

Die zunehmende Anzahl und „Qualität“ interner und externer Angriffe führt immer häufiger zu größeren Schadensfällen. In der Praxis treten damit verstärkt Fragestellungen nach dem Schadensumfang, der Zielsetzung des Angreifers und hinterlassenen Spuren für eine mögliche Strafverfolgung auf. Antworten auf diese und ähnliche Fragen kann eine Forensische Analyse liefern. Secorvo bietet diese Dienstleistung bereits seit einiger Zeit an – die wachsende Nachfrage hat uns nun dazu veranlasst, das entsprechende Leistungsangebot deutlich zu überarbeiten und zu konkretisieren.

3 Veranstaltungshinweise

Juli 2005	
05.-07.07	Western European Workshop on Research in Cryptography (WEWoRC, Leuven-Heverlee)
27.-28.07.	Black Hat Briefings (Black Hat USA, Las Vegas)
29.-31.07.	Defcon 13 (Defcon, Las Vegas)
August 2005	
01.-05.08.	14th USENIX Security Symposium (Usenix, Baltimore/US)
14.-18.08.	Crypto 2005 (IACR, Santa Barbara/US)
September 2005	
20.-21.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
22.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
27.-29.09.	Web-Application Security (Secorvo College, Karlsruhe)
Oktober 2005	
04.10.	Datenschutz kompakt (Secorvo College, Karlsruhe)
05.-06.10.	Inside Windows Security (Secorvo College, Karlsruhe)
11.-13.10.	IT-Sicherheit heute (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Juli 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 7, 4. Jhrg. 2005
Stand 29. Juli 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Wilder Westen

1 Security News

1.1 MBSA 2.0 verfügbar

1.2 Anwendungs-Bugs

1.3 Exploits mit Trojaner

1.4 CSI/FBI-Studie 2005

1.5 Vorsorgeüberwachung

1.6 Security-Checklisten

1.7 Postraub anno 2005

1.8 PKI-Token-Evaluierung

2 Secorvo News

2.1 Secorvo College aktuell

2.2 eco-AK “Sicherheit”

3 Veranstaltungshinweise

Impressum

Editorial: Wilder Westen

Als ich nach Bloody Corner kam, sah ich von weitem her:
Die Summe unter meinem Namen hatte zwei Stellen mehr.
Ein Prämienjäger sagte: Pfeifer, ich wart' schon auf dich!
Ich fuhr herum, pfiff einen Ton –
dann sprach mein Colt für mich.

Bald zwei Jahre ist es her: Am 05.11.2003 setzte Microsoft im Rahmen des Antivirus Reward Program Kopfgelder in Höhe von insgesamt 5 Mio. US$ für Hinweise aus, die zur Identifikation und Ergreifung der Entwickler von Blaster, Sobig, MyDoom et. al. führen (SSN 11/2003). Mit der Verurteilung des Deutschen Sven Jaschan, Autor des Sasser-Wurms, am 08.07.2005 zu 21 Monaten Haft auf Bewährung kommt nun das erste Kopfgeld zur Auszahlung: Die beiden Whistleblower aus der „Szene“, die die entscheidenden Hinweise auf Jaschan gaben, erhalten 250.000 US$.

Zweifellos schreien die ausufernde Verbreitung von Viren und Würmern und die irrsinnigen Schadenssummen geradezu nach unkonventionellen Maßnahmen, um einer Entwicklung Einhalt zu gebieten, die die Informationstechnik als Ganzes existentiell zu bedrohen beginnt.

Dennoch drängt sich die Frage auf, ob diese medienwirksam in Szene gesetzten Kopfgelder noch angemessen sind. Der Maßnahme haftet nicht nur ein Hauch Selbstjustiz an, sondern sie verzerrt auch die Verhältnisse: Die Belohnungen deutscher Behörden für Hinweise auf Geiselnehmer, Mörder und Raubmörder bewegen sich zwischen 1.000 und 5.000 €. Ist daraus nun zu schließen, dass die Ergreifung eines Virenprogrammierers so begrüßenswert ist wie die Verhaftung von 50 bis 250 Kapitalverbrechern?

Bleibt zu hoffen, dass diese auf die Verursacher nahezu spurenloser Straftaten ausgesetzten monströsen Kopfgelder wenigstens zur Selbstanzeige motivieren...

Jetzt sitz’ ich hinter Gittern, von Zweifeln angenagt.
Vielleicht war doch des Denkers Plan
so gut nicht wie er sagt.
Er sagte: Es bringt Dir 10.000 Dollar, wenn Du's wagst
zum Sheriff ins Büro zu geh'n,
Dich vorstellst und ihm sagst:
Grüß Gott, ich bin der Pfeifer, ich komm' selber wie ihr seht,
um die Belohnung zu kassier'n, die auf meinen Kopf steht!
Reinhard Mey, Die Ballade vom Pfeifer

1 Security News

1.1 MBSA 2.0 verfügbar

Seit dem 01.07.2005 ist der Microsoft Baseline Security Analyser (MBSA) in der Version 2.0 verfügbar – ein seit Dezember 2002 angebotenes Tool (SSN 1/2003), das die Duchführung lokaler und Remote-Scans von Windows-Systemen auf Sicherheitsschwächen ermöglicht und detaillierte Vorschläge für Abhilfemaßnahmen liefert. Neu hinzugekommen sind neben einer verbesserten Bewertung der festgestellten Schwachstellen und fehlenden Patches umfangreiche Hilfefunktionen sowie die Unterstützung von Office XP und 64 bit Windows-Versionen. MBSA 2.0 ist kostenfrei und zu Microsofts Windows Server Update Services kompatibel.

1.2 Anwendungs-Bugs

Beim Thema Patch Management darf man die Anwendungen nicht vernachlässigen – auch diese können Schwachstellen aufweisen, die eine Übernahme des Systems mit dem Rechteprofil des Benutzers erlauben.

Das beweist eine am 05.07.2005 veröffentlichte Schwachstelle in Adobes Acrobat Reader 5.0.9 und 5.0.10 unter UNIX und Linux, die es einem Angreifer ermöglichen kann, durch Zusendung eines geeignet konstruierten PDF-Dokuments beliebigen Code auf dem Empfängersystem auszuführen. Ein Update auf die aktuelle Version des Readers wird empfohlen.

Eine ähnliche Schwachstelle wurde am 12.07.2005 in Microsoft Word 2000 und Word 2002 entdeckt: Ein Buffer Overflow erlaubt die Ausführung von Angriffscode über ein Word-Dokument. Passende Updates sind inzwischen verfügbar.

1.3 Exploits mit Trojaner

So genannte Exploits, das sind über das Internet verbreitete Quellcode-„Häppchen“, die neue sicherheitsrelevante Lücken in Betriebssystemen oder Anwendungen vorführen, verwenden häufig einen Codeabschnitt, der bei Ausführung des Programmcodes eine Kommandozeilen-Shell auf dem befallenen System startet.

Am 26.07.2005 wurde bekannt, dass zahlreiche der im Internet kursierenden Exploits versteckte Trojaner, Rootkits oder Schadensroutinen enthalten – dort wurde jeweils der Shellcode ersetzt. Jeder, der diesen manipulierten Code ausprobiert oder ihn sogar unverändert in ein Analysetool integriert, installiert beim ersten Starten einen Trojaner oder ein Rootkit auf seinem System – oder wird von einer rekursiven Löschfunktion („`rm -rf /*`“) überrascht.

1.4 CSI/FBI-Studie 2005

Seit dem 18.07.2005 ist der zehnte jährlich von CSI und FBI publizierte Computer Crime and Security Survey 2005 verfügbar, der aufgrund der regelmäßigen Durchführung und der rund 700 Befragten ein sehr repräsentatives Bild der Entwicklung der IT-Security in den USA zeichnet (siehe auch Studien-Überblick in SSN 4/2002).

Die Ergebnisse sind immer wieder erhellend: So liegen die durchschnlittlichen jährlichen Ausgaben für IT-Sicherheit bei 200-300 US$ je Mitarbeiter, hat der Missbrauch von WLANs erheblich zugenommen und verschlüsseln schon 68% der Unternehmen ihre Daten während der Übertragung.

1.5 Vorsorgeüberwachung

Mit seiner Entscheidung vom 27.07.2005 (1 BvR 668/04) hat das Bundesverfassungsgericht die Regelung des niedersächsischen „Gesetzes über die öffentliche Sicherheit und Ordnung“ (SOG) über die Zulässigkeit einer Telefonüberwachung zur „Vorsorge für die Verfolgung oder die Verhütung dieser Straftaten“ (§ 33a) als mit dem Grundgesetz nicht vereinbar und daher nichtig erklärt.

Ein wichtiges Urteil, denn es setzt erstmals seit den New Yorker Terroranschlägen vom 11.09.2001 den ausufernden Begehrlichkeiten und Kompetenzerweiterungen deutscher Strafverfolgungs- und Sicherheitsbe-

hörden eine verfassungsrechtliche Grenze. Bleibt zu hoffen, dass auch der Bundesinnenminister die Begründung liest.

1.6 Security-Checklisten

Mit dem Cyber Security Research and Development Act des Jahres 2002 wurde das amerikanische NIST verpflichtet, Checklisten zu entwickeln, die es erlauben, das für Hard- und Software bestehende und mit deren Nutzung einher gehende Risiko in US-Bundesbehörden zu minimieren. Das NIST startete daraufhin das „Security Configuration Checklists Program for IT Products“ und veröffentlichte am 26.05.2005 die gleichnamige NIST Special Publication SP 800-70 und das NIST Beta Checklists Repository.

Die Checklisten im Repository sind derzeit nach elf Kategorien sortiert, die mit sicherheitsrelevanten Checklisten anderer Regierungsorganisationen (u.a. NSA, DISA, CIS) und von Herstellern befüllt werden. Inzwischen finden sich darin insgesamt schon mehr als 50. Ziel ist, auf der Basis standardisierter Checklisten und des Austauschs von Erfahrungen die Voraussetzungen für ein vereinheitlichtes „Basis-Sicherheitsniveau“ zu entwickeln. Die eingereichten Checklisten werden daher vom NIST mit 32 formalen Rahmenparametern charakterisiert.

Das NIST plant, für Checklisten, die von Herstellern eingereicht werden, ein SP 800-70-Konformitätssiegel zu vergeben. Im Fall eines Siegelerhalts verpflichten sich die teilnehmenden Hersteller, die Garantie der Herstellerserviceverträge auf die Anwendung dieser Checklisten auszudehnen. Noch gibt es weder eine einheitliche Struktur noch das geplante Siegel, daher wurde das Repository auch als „Beta“ eingestuft. Einen Vorgeschmack auf mögliche zukünftige standardisierte Checklisten gibt die Spezifikation des Extensible Configuration Checklist Description Format (XCCDF). Allerdings warten auch die NIST-eigenen Dokumente noch auf die Umsetzung in XCCDF.

1.7 Postraub anno 2005

Am 07.06.2005 musste die Citybank öffentlich den Verlust eines Backup-Bands mit ca. 4 Mio. Kundendatensätzen während eines Transports durch United Parcel Service (UPS) einräumen. Die vermissten Datensätze enthalten u.a. auch die Social Security Numbers – und bilden damit die Grundlage für zukünftige Identitätsdiebstähle. Kein Einzelfall: Ameritrade vermisst seit Jahresanfang ein Band mit 200.000 Kundendaten, Time Warner verlor ein Tape mit Daten von 600.000 Kunden, und der Bank of America fehlen seit Mai 2005 100.000 Kundendatensätze.

Die Sicherheitslücke scheint systematisch zu sein: Offenbar umfass(t)en die Sicherheitskonzepte zwar die Erstellung von Backups, nicht aber den Umgang mit dieser höchst sensiblen Konzentration kritischer Daten. So waren die Daten auf den Bändern weder verschlüsselt, noch erfolgte der Versand unter besonderen Sicherheitsauflagen, wie z.B. dem Rückgriff auf einen besonders vertrauenswürdigen und sicherheitsüberprüften Kurier.

1.8 PKI-Token-Evaluierung

Immer häufiger kommen – nicht nur in PKI-Umgebungen – Hardware-Token wie USB-Sticks oder Smartcards zum Einsatz, um vor allem kryptographisches Schlüsselmaterial geeignet vor Missbrauch zu schützen. Jedoch funktionieren diese Token nicht immer mit der gewünschten Anwendung, bzw. bestimmte Anforderungen an die Sicherheit werden entgegen den Herstellerangaben nicht erfüllt.

Die DFN-CERT Services GmbH hat daher gemeinsam mit SURFnet mehrere dieser Hardware-Tokens intensiven Tests unterzogen. Die Autoren des Reports prüften die Verwendbarkeit von USB-Token zur PKI-Unterstützung in verschiedenen Standard-Anwendungen (u.a. Internet Explorer, Outlook, Mozilla, Acrobat) unter Windows und Linux. Mangels Teststellungen durch die Hersteller konnten von ursprünglich 20 ausgewählten nur acht Token getestet werden, von denen nur sechs aktiv Private-

Key Operationen im Token durchführen. Von diesen wiederum ist nur ein einziges in der Lage, Operationen mit asymmetrischen Schlüsseln durchzuführen, die länger sind als 1024 bit.

Das Ergebnis der Untersuchung ist wenig überraschend: Microsoft-Anwendungen und aktuelle Windows-Versionen werden allgemein gut unterstützt, auch wenn dem Benutzer einiges Mitdenken abgefordert wird. Bei Windows-Anwendungen, die über die PKCS#11-Schnittstelle bedient werden, traten bei verschiedenen Token Fehler auf. Auch decken sich Herstellerangaben nicht immer mit der Realität. Die Unterstützung für Linux bleibt vergleichsweise rudimentär.

2 Secorvo News

2.1 Secorvo College aktuell

Am 20.09.2005 startet das Programm des zweiten Halbjahrs 2005. In den bis dahin verbleibenden beiden Monaten werden alle Seminare einem gründlichen „Lifting“ und alle Vorträge – wie in jeder Seminarpause – einer systematischen Aktualisierung und Überarbeitung unterzogen.

Mehr noch: Unser Seminarangebot 2006 wird um neue Seminare zu aktuellen und spannenden Themen der IT-Sicherheit erweitert – mehr dazu im September. Auf ein Wiedersehen in Karlsruhe!

http://www.secorvo.de/college

2.2 eco-AK “Sicherheit”

Nach dem großen Zuspruch, den die Sitzung des von Dirk Fox geleiteten Arbeitskreises „Sicherheit“ des eco e.V. zum Thema „Zertifizierte Sicherheit“ am 08.04.2005 fand, wird die nächste Sitzung des Arbeitskreises am 16.09.2005 das Thema „Forensik“ vertiefen – wieder in den Räumen der Karlsruher Secorvo Security Consulting GmbH. Programm und Anmeldung sind in Bälde auf der Webseite des eco-Arbeitskreises verfügbar. Interessierte können sich in den E-Mail-Verteiler des Arbeitskreises aufnehmen lassen.

3 Veranstaltungshinweise

Juli 2005	
29.-31.07.	Defcon 13 (Defcon, Las Vegas)
August 2005	
01.-05.08.	14th USENIX Security Symposium (Usenix, Baltimore/US)
14.-18.08.	Crypto 2005 (IACR, Santa Barbara/US)
September 2005	
05.-09.09.	Computer Network Forensics Workshop 2005 (IEEE/Create-Net, Athen/GR)
16.09.	Forensik (AK „Sicherheit“ des eco e.V.)
20.-21.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
22.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
27.-29.09.	Web-Application Security (Secorvo College, Karlsruhe)
Oktober 2005	
04.10.	Datenschutz kompakt (Secorvo College, Karlsruhe)
05.-06.10.	Inside Windows Security (Secorvo College, Karlsruhe)
11.-13.10.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
25.-27.10.	Spurensuche im Web (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
August 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 8, 4. Jhrg. 2005
Stand 29. August 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Der Phisher und die 7 Geißlein

1 Security News

1.1 Web Password Hashing

1.2 iTAN

1.3 XP-Client-Honeypots

1.4 Anonym ins Web

1.5 Lage der IT-Sicherheit

1.6 Bluetooth-Kfz-Attacken

1.7 Infosec Dictionary

1.8 Wettlauf mit der Zeit

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Mehr Datenschutz

2.3 IT-Forensik

2.4 Neues Video verfügbar

3 Veranstaltungshinweise

Impressum

Editorial: Der Phisher und die 7 Geißlein

„Liebe Kinder, sperrt die Türe gut zu und nehmt euch in acht vor dem Wolf! (...) Der Bösewicht verstellt sich oft, aber an seiner rauen Stimme und an seinen schwarzen Füßen werdet ihr ihn gleich erkennen.“
Gebrüder Grimm, Der Wolf und die sieben Geißlein

Fast gleichlautend lesen sich die Mahnungen der deutschen Banken. Letztere leiden unter der zunehmenden Flut von Phishing-Angriffen: Im Mai 2005 zählte Messagelabs über 9 Mio. Phishing-E-Mails, ein trauriger Rekord. Die Anti-Phishing Working Group erhielt im Juli 2005 über 14.000 Phishing-Reports, im Juli 2004 waren es erst 2.000.

Bisher ließen sich deutsche Phishing-E-Mails leicht an der „rauen Stimme“ erkennen: Das Deutsch war holprig, die Geschichte unglaubwürdig. Aber der Wolf hat Kreide gefressen – neue Phishing-E-Mails sind sprachlich einwandfrei und klingen plausibel. Und auch die Pfote ist nicht mehr verräterisch schwarz – die gefälschten Webseiten der Phisher sind perfekt nachgebildet, verwenden originale Frames, Grafiken, Schriften und Texte.

Einige Banken unterstützen die Phisher, indem sie E-Mails an ihre Kunden senden, oft im HTML-Format, manchmal sogar mit verborgenen Links. Häufig werden zudem Domains für das Online-Banking verwendet, die auch einem Phisher gehören könnten, oder SSL-Zertifikate, die nicht zweifelsfrei die Bank als Anbieter erkennen lassen.

Wenn zugleich E-Commerce-Anbieter aus falscher Sparsamkeit selbst signierte SSL-Zertifikate nutzen, der Support bei abgelaufenem Zertifikat empfiehlt, die Sicherheitseinstellungen des Browsers herab zu setzen oder die Warnung vor einer unverschlüsselten Passwortübertragung zu deaktivieren, muss man sich nicht wundern, wenn die Geißlein keine Chance haben.

Irgendwann passt auch das Märchen nicht mehr. Zumal es bei grenzüberschreitendem Phishing ohnehin schwierig ist, dem Wolf den Bauch aufzuschneiden und die Geißlein lebendig herauszuholen. Passender wird dann vom „Tapferen Phisherlein“ zu berichten sein: Sieben auf einen Streich.

1 Security News

1.1 Web Password Hashing

Von einem Forschungsteam der Stanford University wurde auf dem USENIX Security Symposium Anfang August ein interessantes Verfahren zur Individualisierung von Internet-Passworten vorgestellt. Das Tool und Verfahren Pwd-Hash erfordert keine Änderungen an den Systemen und ist für die Benutzer weitgehend transparent.

Die – oft identischen – Passworte der Benutzer werden mit einem Browser-Plugin (derzeit verfügbar für Mozilla und Internet Explorer) durch ein für jede Zieldomäne individuelles Passwort ersetzt. Hierbei dienen die Ziel-Website, das ursprüngliche Passwort und bei Bedarf ein „salt" auf dem Clientsystem als Eingangsgrößen. Eine Pseudozufallsfunktion berechnet daraus dann ein neues Passwort. Fällt einem Angreifer auf einem schlecht geschützten System eine Passwortdatei in die Hände, kann er nicht mehr einfach mit derselben User-/Passwortkombination auf weitere sensiblere Systeme zugreifen.

Hierdurch wird implizit in vielen Fällen auch ein Schutz vor Phishing-Angriffen geboten, da die Plugins gefälschte Zielsysteme anhand des Domänennamens vom Originalsystem unterscheiden können.

1.2 iTAN

Auf Phishing-Angriffe reagieren jetzt auch die deutschen Banken mit zusätzlichen Sicherheitsmerkmalen. Die Postbank meldete am 07.08.2005, dass sie ihr PIN-TAN-Verfahren um ein iTAN genanntes Merkmal ergänzt: Zukünftig sind die TAN auf der Liste indexiert. Bei jeder Transaktion schickt der Bankserver den Index, und nur die passende TAN ist gültig. Dieser einfache Challenge-Response-Mechanismus entwertet abge-„phishte" TAN, denn die Wahrscheinlichkeit, dass eine solche passt, sinkt auf 1/(Anzahl TAN je Bogen). Die iTAN schützt nicht vor allen Angriffen, erhöht aber die Sicherheit des Online-Bankings deutlich.

1.3 XP-Client-Honeypots

Honeypots werden immer beliebter (SSN 5/2005). Während diese jedoch üblicherweise als Server implementiert werden, der darauf wartet, von Angreifern oder Würmern kompromittiert zu werden, verfolgen Forscher von Microsoft Research einen anderen interessanten Ansatz: Im Rahmen des Projekts „Strider HoneyMonkey" surfen Windows-XP-Clients ständig durch das World Wide Web und identifizieren dabei Webseiten, die insbesondere auf Grund von Schwachstellen im Internet Explorer geeignet sind, einen XP-Rechner zu kompromittieren. Die Rechner verwenden dabei unterschiedliche Patch-Stände – von einem völlig ungepatchten XP-System bis hin zu einem mit den aktuellen Updates ausgestatteten Rechner. Da die Clients innerhalb von virtuellen Maschinen laufen, können sie nach „erfolgreicher" Kompromittierung sofort und automatisiert in den Ursprungszustand gebracht werden.

Auf dem am 05.08.2005 in Baltimore zu Ende gegangenen USENIX Security Symposium stellte Microsoft im Rahmen eines Kurzvortrags erste Zwischenergebnisse vor. So gelang es den Forschern beispielsweise, innerhalb weniger Wochen 752 URLs zu identifizieren, nach deren Besuch ein ungepatchtes XP-System kompromittiert würde. Interessant ist ferner die Tatsache, dass viele dieser URLs von denselben Betreibern gehostet werden und zudem untereinander stark verlinkt sind.

Ob Microsoft die Informationen der HoneyMonkeys zu Gunsten von besser gepatchten eigenen Produkten nutzen wird, ist fraglich: Der Report enthält im Ausblick lediglich Statistiken und „legal actions" gegen die Betreiber solcher Webseiten.

1.4 Anonym ins Web

Das Projekt AN.ON (TU Dresden) hat am 14.08.2005 eine neue Version des kostenlosen Anonymisierungsproxies zum Download bereit gestellt. Wie die vorhergehenden Versionen macht die Version 0.05.022 einen stabilen Eindruck – auch wenn sie offiziell als Testversion bezeichnet wird.

Durch JAP erfolgt der Zugriff beim Surfen verschlüsselt über einen extern gehosteten Proxy, der das MIX-Protokoll zur Anonymisierung verwendet. Da dieser in der Regel von mehreren Tausend Benutzern verwendet wird, kann eine Verbindung keinem bestimmten User zugeordnet werden. Wenn man die Protokollierungsfunktionen des Servers nicht berücksichtigt, ist so eine anonyme Internetnutzung möglich. Das einfache Updateverfahren, die umfangreiche Auswahl an Servern inklusive Aktualisierungsmöglichkeit und die Beschränkung der netzseitigen Zugriffsmöglichkeit auf die lokale Clientkomponente machen einen sehr guten Eindruck.

Allerdings werden hierdurch Content-Filter-Mechanismen von Unternehmensnetzen ausgehebelt, sofern ein Zugriff auf die Anonymisierungsdienste über HTTPS zugelassen ist. Auch Angriffe auf HTTP-Ebene können über den Proxy ausgeführt und somit nicht zurückverfolgt werden. Aus Sicherheitssicht ein Nachteil, aus Datenschutzsicht ein Gewinn.

1.5 Lage der IT-Sicherheit

Vom BSI wurde am 19.08.2005 ein Lagebericht zur IT-Sicherheit in Deutschland veröffentlicht – zur aktuellen Situation, Bedrohungen und Trends. Die Ergebnisse überraschen nicht: Der Stellenwert von IT-Sicherheit wird insbesondere angesichts der gewachsenen Abhängigkeit von einer funktionierenden IT nach wie vor unterschätzt. Auch wenn das Bewusstsein um die Bedrohungslage zugenommen hat, stellen nur 39% der Unternehmen ein höheres Budget zur Verfügung. Auch im öffentlichen Bereich fehlen finanzielle Mittel. Recht gut werden neuere Bedrohungen wie Phishing und Bot-Netze zusammengefasst.

1.6 Bluetooth-Kfz-Attacken

In den SSN 11/2003 und 8/2004 berichteten wir von Angriffsmöglichkeiten über Bluetooth. Die Wirklichkeit hat uns inzwischen eingeholt: Eine der Methoden, bei denen ein Angreifer Audiodaten in die integrierte Freisprechanlage eines Fahrzeugs einspielt, wird seit dem 02.08.2005 als Tool im Internet verbreitet. Opfer des Angriffs sind Bluetooth-Geräte mit fest voreingestellter zu einfacher PIN (z.B. 0000, 1234).

Mit dem Tool kann ein Angreifer nicht nur Musik wiedergeben, sondern auch ein lautstarkes „Bremsen!“ über die Lautsprecher erklingen lassen – kein Spaß bei hoher Geschwindigkeit. Liebe (Bluetooth-) Hersteller: Es gibt bessere Verfahren als feste PINs. Riskiert nicht die Gesundheit Eurer Kunden zu Gunsten eines vermeintlichen Bequemlichkeitsgewinns.

1.7 Infosec Dictionary

In der August-Ausgabe des CSO-Magazins erschien The Devil's Infosec Dictionary – ein unterhaltsames, leider z.T. sehr wahres Glossar zentraler Begriffe der Informationssicherheit.

1.8 Wettlauf mit der Zeit

Das Zeitfenster zwischen Fehlerentdeckung und Ausnutzung durch ein Angriffsprogramm schrumpft: Am 17.08.2005 meldete das Online-Magazin WindowsITpro, dass derzeit mindestens sieben Internet-Würmer (u.a. Zotop und RBOT) Systeme befallen, die den erst am 09.08.2005 veröffentlichten Microsoft-Patch MS05-39 nicht installiert haben. Betroffen sind Windows 2000, Windows XP und auch Windows 2003. Ein Testen und Einspielen der Patches wird dringend empfohlen.

2 Secorvo News

2.1 Secorvo College aktuell

Angesichts der wachsenden Herausforderungen, vor die sich Sicherheitsbeauftragte durch neue Kommunikationstechniken gestellt sehen, haben wir diesem Thema ein eigenes, neues Seminar gewidmet. Im Zentrum der dreitätigen Veranstaltung stehen sowohl die Bedrohungen und Risiken von E-Mail, WLANs, Bluetooth, Laptops, PDAs und Voice over IP als auch konkrete Schutzmöglichkeiten, von Verschlüsselung

über die SPAM-Abwehr bis zur Content-Filterung. Dabei stellen sich nicht nur technische Fragen; auch zahlreiche rechtliche Anforderungen sind bei der Umsetzung zu berücksichtigen. Das Seminar wird erstmals am **08.-10.11.2005** durchgeführt.

Alle Termine und Seminarangebote des zweiten Halbjahrs 2005 finden Sie unter

http://www.secorvo.de/college

2.2 Mehr Datenschutz

Seit dem 15.08.2005 gehört Karin Schuler zum Secorvo Team. Sie bringt mehr als 15 Jahre Erfahrung in IT-Sicherheit und Datenschutz mit und verstärkt vor allem unsere Expertise in Datenschutzfragen.

2.3 IT-Forensik

Forensische Fragestellungen treten immer öfter auf. Eine vertiefte Einführung bietet Secorvo College mit dem Seminar Spurensuche im Web (**25.-27.10.2005**). Auch die nächste Sitzung des eco-Arbeitskreises Sicherheit am **16.09.2005** ist dem Thema Forensik gewidmet.

2.4 Neues Video verfügbar

Zum Ende des vergangenen Jahres hatten wir es angekündigt – jetzt ist es endlich verfügbar: unser neues Lehrvideo „Passwort-Sicherheit“ zur Sensibilisierung von Mitarbeitern und Kollegen.

Das ca. zehnminütige Flash-Video nimmt sich dieses schon seit Jahren diskutierten Themas an und zeigt, was ein gutes Passwort ausmacht, wie leistungsfähig heutzutage die Tools und Methoden potenzieller Angreifer sind und was im Umgang mit Passworten beachtet werden sollte, um Angreifer auf Distanz zu halten. Einen kurzen Ausschnitt aus dem Video finden Sie in Kürze als Demo auf unseren Webseiten.

Das Video ist in deutscher Sprache als Einzel- und Intranet-Lizenz verfügbar, als Intranet-Lizenz auch in englischer Sprache. Weitere Sprachversionen erstellen wir auf Anfrage; nehmen Sie diesbezüglich gerne Kontakt mit uns auf.

3 Veranstaltungshinweise

September 2005	
05.-09.09.	Computer Network Forensics Workshop 2005 (IEEE/Create-Net, Athen/GR)
16.09.	Forensik (AK „Sicherheit“ des eco e.V.)
20.-21.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
21.09.	1. IT-Grundschutz Tag 2005 (BSI, Bonn)
22.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
27.-29.09.	ISSE 2005 (Teletrust, Budapest/H)
27.-29.09.	Web-Application Security (Secorvo College, Karlsruhe)
Oktober 2005	
04.10.	Datenschutz kompakt (Secorvo College, Karlsruhe)
05.-06.10.	Inside Windows Security (Secorvo College, Karlsruhe)
11.-13.10.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-15.10.	hack.lu 2005 (CSRRT-LU, Kirchberg/L)
19.10.	2. IT-Grundschutztag 2005 (BSI,Fraunhofer SIT, St. Augustin)
25.-27.10.	Spurensuche im Web (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
September 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 9, 4. Jhrg. 2005
Stand 05. Oktober 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Das Gegenteil von gut ist ... gut gemeint

1 Security News

1.1 To Patch Or Not To Patch

1.2 BDSG-Korrektur?

1.3 Multi-Plattform-Virus

1.4 DropMySecurity

1.5 Es geht auch „ohne“ (II)

1.6 Big Brother Awards

2 Secorvo News

2.1 Secorvo College aktuell

2.2 PhonoNet zertifiziert

2.3 Sicher ist nicht genug

2.4 IsSec/ZertiFA 2005

2.5 Team-Verstärkung

3 Veranstaltungshinweise

Impressum

Editorial: Das Gegenteil von gut ist ... gut gemeint

Die Komplexität von Software wächst ungebremst: Kam Windows 3.1 (1990) mit 2,5 Mio. Programmzeilen aus, benötigte XP (2002) schon 40 Mio. – vier Mal so viel wie die Software des Space Shuttle. Zugleich wächst die Programmvielfalt und mit beidem die Zahl sicherheitskritischer Fehler. Deren schiere Menge relativiert bisher jede Qualitätsverbesserung im Softwareentwicklungsprozess. Das zeigt nicht zuletzt der exponentielle Anstieg der gefundenen Bugs: Von 171, die das CERT/CC 1995 zählte, auf mehr als 2.800 allein im ersten Halbjahr 2005.

Immerhin werden zunehmend Sicherheitsmechanismen in Softwareprodukte integriert. Das ist grundsätzlich eine begrüßenswerte Entwicklung. Problematisch sind jedoch die handwerklichen und konzeptionellen Fehler, die sich dabei immer wieder beobachten lassen. Das beginnt mit Offensichtlichem wie der Klartextübermittlung von Passwörtern beim Login, geht weiter mit fehlerhaften Authentifikationsprotokollen, bei denen sich nicht der Client gegenüber dem Server sondern umgekehrt der Server gegenüber dem Client authentifiziert, über die „versteckte“ Klartext-Übermittlung eines Verschlüsselungsschlüssels oder die Ableitung eines 256-bit-Schlüssels aus einer sechsstelligen numerischen PIN (Schlüsselraum: 2^{20} bit) bis hin zur „raffinierten“ Beschleunigung des Verschlüsselungsalgorithmus durch das Weglassen einer rechenintensiven Operation.

Diese Fehler zeugen von mangelhaftem Verständnis der, zugegeben oft komplexen, relevanten Zusammenhänge – und haben zudem die fatale Folge, dass der Nutzer der Anwendung sich auch noch bestens geschützt wähnt. Damit gewinnt „Security Engineering“ an Bedeutung, erstmals systematisch behandelt von Ross Anderson in seinem einschlägigen Kompendium. Jüngst trugen SAP und Microsoft dieser Entwicklung mit der Veröffentlichung einer Fibel Sicheres Programmieren Rechnung – vielleicht wichtigstes Ergebnis der Initiative „Deutschland sicher im Netz“.

1 Security News

1.1 To Patch Or Not To Patch

Jeder, der für das Patch-Management verantwortlich ist – und das sollten in der Regel nicht dieselben Mitarbeiter sein, die das Patch-Management ausführen – kennt das Dilemma: Aus Sicherheitssicht sollte ein Patch installiert, zur Gewährleistung der Produktivität laufender Systeme jedoch möglichst nicht verändert werden.

Daher sind – auch in den Fachabteilungen – Ressourcen zum Testen und zusätzliche „Wartungsfenster" zur Durchführung der Updates erforderlich. Doch was tun im Fall der Fälle? Wie reagiert man beispielsweise als Dienstleister, wenn für die betriebenen Webserver Updates gegen vermutete Schwachstellen verfügbar, sie in der jeweiligen Distribution aber noch nicht als „stabil" gekennzeichnet sind?

Dieses Dilemma wird zunehmend durch die normative Kraft des Faktischen entschieden: Die schnelle Verbreitung von Exploits verkürzt die verfügbare Reaktionszeit inzwischen so stark, dass beispielsweise seit 09.09.2005 von Debian auch für die Testing-Version Patches bereit gestellt werden.

1.2 BDSG-Korrektur?

Der Bundesrat hat in seiner 814. Sitzung am 23.09.2005 auf Antrag der Länder Hessen und Niedersachsen einen Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) beschlossen: Danach soll das Quorum, ab dem die Bestellung eines betrieblichen Datenschutzbeauftragten und die Meldung automatisierter Verarbeitungen für nicht-öffentliche Stellen verpflichtend sind, von derzeit fünf auf 20 Mitarbeiter, die mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschäftigt sind, angehoben werden.

Mit dem derzeit innenpolitisch zugkräftigen Argument der Entbürokratisierung und Entlastung kleiner Unternehmen würden damit, falls der Bundestag dem Entwurf zustimmt, mehr als 95% aller Unternehmen von der Pflicht zur Bestellung eines Datenschutzbeauftragten befreit. Zwar würde so zweifellos zunächst ein faktisches Vollzugsdefizit des BDSG legalisiert – angesichts der zunehmenden automatisierten Verarbeitung personenbezogener Daten jedoch ein Pyrrhussieg. Denn betriebliche Datenschutzbeauftragte sind nicht zuletzt in kleinen Unternehmen die wesentliche Triebfeder bei der Umsetzung des datenschutzrechtlichen Persönlichkeitsschutzes.

1.3 Multi-Plattform-Virus

Viren und Würmer, die sich plattformunabhängig verbreiten und Schaden stiften können, sind nicht neu: Bereits der allererste, von Robert Morris Jr. programmierte Internet-Wurm sprang am 02.11.1988 von DEC- auf SUN-3-Systeme über und umgekehrt. Allerdings sind heutige Plattformen zugegebenermaßen ein wenig komplexer.

Laut Trendmicro wurde am 21.09.2005 erstmals ein plattformunabhängiger Handy-Virus gesichtet. Cardtrp.A setzt hinterlistige Methoden ein – hat er ein mit SymbianOS Series 60 betriebenes SmartPhone infiziert, nutzt er die Routinen von Cabir.A zur Weiterverbreitung via Bluetooth. Zusätzlich kopiert er Windows-Schadsoftware auf die Speicherkarte des Handys. Wird die infizierte Speicherkarte in einen PC-Kartenleser eingelegt, droht dort eine Infektion mit der Backdoor Berbew.A und dem Wurm Wukill.B.

1.4 DropMySecurity

Microsoft bietet seit dem 15.11.2004 mit dem auch als Source-Code verfügbaren Tool DropMyRights von Michael Howard ein Hilfsmittel, um Anwendungen aus dem Administratorkontext heraus mit eingeschränkten Berechtigungen zu starten.

Dass Microsoft damit den Spagat versucht, die potenziellen Schadensauswirkungen bekannter „Sicherheitsproblem-Magneten" trotz schlecht programmierte Anwendungen, die Administrator-Rechte erfordern, zu begrenzen, ist zunächst löblich. Dennoch setzt der Ansatz die falschen Zeichen: Anstatt das Übel an der Wurzel zu bekäm-

pfen und die Ursachen der Sicherheitsprobleme zu eliminieren, wird an den Symptomen herumgedoktert: Benutzern wird ermöglicht, weiterhin mit administrativen Berechtigungen zu arbeiten, und nur für bestimmte, besonders risikobehaftete Anwendungen wie E-Mail und Browser werden reduzierte Rechte gewährt.

Zudem kann es gefährlich sein, sich auf Tools wie DropMyRights zu verlassen: Am 01.09.2005 wurden Schwachstellen publiziert, über die sich die vollen Rechte wieder herstellen lassen.

Die Verantwortung ist allerdings auch auf Seiten der Anwender zu suchen, die auch heute noch Anwendungen einsetzen, die einfachste Sicherheitsmechanismen missachten. Bei der Beschaffung von Softwarelösungen sollten Sicherheitsanforderungen nie im Kriterienkatalog fehlen.

1.5 Es geht auch „ohne“ (II)

Dass man es auch besser machen kann als mit DropMyRights zeigt Microsoft in einer Sonderbeilage zum Thema Sicherheit, unter anderem in der aktuellen Ausgabe der c’t. Neben strategischen Themen wie dem Risikomanagement werden auch technische Architekturen wie Trustworthy Computing vorgestellt.

Eines der wichtigsten Themen (siehe SSN 9/2004) wird unter dem Titel „Least Privileges! Es geht auch ohne Administratorrechte!“ behandelt. Darin werden Lösungswege für die tägliche Praxis aufgezeigt: Wie findet man heraus, warum eine Anwendung Administratorrechte benötigt, und wie kann man das System so umkonfigurieren, dass der Benutzer die Anwendung auch „ohne“ nutzen kann? Dazu werden hilfreiche Tools wie der Application Verifier und das Application Compatibility Toolkit vorgestellt.

Aus technischer Sicht kann der Artikel sehr empfohlen werden, ein „Danke“ für die gute Hilfestellung seitens der Redaktion. Nur auf einen wichtigen Punkt weist der Text lediglich am Rande hin: die Aufwände zum Recherchieren der Problemursachen und zum Testen geeigneter Lösungen und Einstellungen binden wertvolle Ressourcen.

Ein weiterer Beitrag beschäftigt sich mit der Entwicklung sicherer Software. Zum selben wichtigen Thema arbeitet Microsoft mit SAP in der Initiative Deutschland sicher im Netz zusammen. In diesem Rahmen präsentieren die beiden Unternehmen ihre Erfahrungen und Richtlinien für die Berücksichtigung von Sicherheitsaspekten bei der Softwareentwicklung: Im Rahmen von drei offenen Veranstaltungen an Universitäten zwischen dem 16.09. und 13.10.2005 und in Gestalt einer von SAP entwickelten 74-seitigen Fibel Sicheres Programmieren, die nicht nur für Programmierer, sondern für alle am Entwicklungszyklus Beteiligten einen Blick wert ist – auch wenn bei der Schlussredaktion der eine oder andere kleine Fehler durchgerutscht ist.

1.6 Big Brother Awards

Die diesjährige Verleihung der deutschen Big Brother Awards, die seit dem Jahr 2000 von FoeBuD e.V. organisiert wird, findet am Freitag, 28.10.2005 im historischen Saal der Ravensberger Spinnerei in Bielefeld statt. Der Preis wird jährlich in mehreren Kategorien für besondere Verdienste um die Überwachung in Deutschland vergeben. Die Auszeichnungen der vergangenen Jahre finden sich inklusive Laudatio auf der Webseite des FoeBuD e.V.

2 Secorvo News

2.1 Secorvo College aktuell

Die Seminare von Secorvo College in Oktober und November spiegeln die vielen Facetten der IT-Sicherheit: IT-Sicherheit heute (11.-13.10.) liefert die Grundlagen und einen aktuellen Überblick über das ständig wachsende Gebiet, Spurensuche im Web (25.-27.10.) erläutert die Möglichkeiten der Forensik mit zahlreichen Beispielen und vielen erkenntnisreichen praktischen Übungen, und schließlich vertieft das Seminar Kommunikationsschutz und Datensicherheit (08.-10.11.) Risiken und Sicherheitsmechanismen der unterschiedlichen elektronischen Kommunikationsmedien und -techniken.

Weitere Seminarangebote und Termine von Secorvo College finden Sie unter http://www.secorvo.de/college

2.2 PhonoNet zertifiziert

Jörg Völker, Autor des mit über 25.000 Downloads derzeit meist gelesenen Secorvo-Whitepapers „BS 7799 – Von Best Practice zum Standard" und seit November 2004 lizensierter BS 7799-Lead Auditor, hat die BS 7799-Zertifizierung der PhonoNet GmbH erfolgreich begleitet: Am 16.09. 2005 wurde das Zertifikat auf der PopKomm 2005 in Berlin offiziell überreicht.

2.3 Sicher ist nicht genug

Auf dem kommenden Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 20.10. 2005 (18 Uhr) wird Herr Christoph Machner (WebQuake) von seinen Erfahrungen mit dem Aufbau eines Hochsicherheitsrechenzentrums in einem ehemaligen Stollen in Österreich berichten. Anschließend: Net(t)working. Anmeldung und weitere Informationen unter http://www.ka-it-si.de/.

2.4 IsSec/ZertiFA 2005

Das Programm der diesjährigen Computas-„Doppelkonferenz" IsSec und ZertiFA am 05.-06.12.2005 steht. Unter anderem stehen die Sicherheitsaspekte von VoIP, Outsourcing, ITIL, Phishing und Identity-Management sowie Erfahrungsberichte über Datenschutz-Standardisierung, Videoüberwachung und BS 7799-Zertifizierung auf der Agenda, die wie immer mit kompetenten Referenten glänzt.

2.5 Team-Verstärkung

Am 01.10.2005 erhält das Secorvo-Team erneut Verstärkung: Zum Beratungsteam stößt Kai Jendrian hinzu. Er bringt mehrjährige Erfahrung aus der Umsetzung von IT-Sicherheitslösungen in mittelständischen Unternehmen und als IT-Leiter mit. Besonders in den Bereichen Sicherheit von Datenbanken und Web-Applikationen wird er unser Leistungsangebot ergänzen.

3 Veranstaltungshinweise

Oktober 2005	
11.-13.10.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
20.10.	Sicher ist nicht genug (KA-IT-Si, Karlsruhe)
25.-27.10.	Spurensuche im Web (Secorvo College, Karlsruhe)
November 2005	
02.-04.11.	Lotus Notes Security (Secorvo College, Karlsruhe)
08.-11.11.	Kommunikationsschutz und Datensicherheit (Secorvo College, Karlsruhe)
14.-18.11.	Information Security Management (Secorvo College, Karlsruhe)
15.-16.11.	Einführung in die Praxis des DSB (Euroforum, Berlin)
22.-25.11.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.-30.11.	IT-Sicherheit für Windows-Admins (Secorvo College, Karlsruhe)
Dezember 2005	
01.-02.12.	Einführung in die Praxis des DSB (Euroforum, Düsseldorf)
05.-06.12.	IsSec/Zertifa 2005 (COMPUTAS, Berlin)
06.-07.12.	Prüfung zum Certified IT Security Professional (CISP) (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Oktober 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 10, 4. Jhrg. 2005
Stand 28. Oktober 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial:
Das Enigma-Trauma

1 Security News

1.1 Open Source und zurück

1.2 ISO 27001 + Grundschutz

1.3 No-NX

1.4 Pünktchen und Xerox

1.5 Where Do You Want to Surf Today?

1.6 Langzeitarchivierung

1.7 Überlistete Scanner

2 Secorvo News

2.1 Secorvo College aktuell

2.2 IsSec/ZertiFA 2005

2.3 Secorvo White Paper ISM

3 Veranstaltungshinweise

Impressum

Editorial: Das Enigma-Trauma

Mit der Veröffentlichung in der Wirtschaftswoche platzte am 05.10.2005 die Bombe: In einer internen Studie vom 20.09.2005 bescheinigt das BSI dem auch liebevoll Tamagotchi für Manager genannten Blackberry des kanadischen Herstellers RIM, er sei „auf Grund der unsicheren Architektur (...) für den Einsatz in der öffentlichen Verwaltung und spionagegefährdeten Unternehmen nicht geeignet“ – ein Verdikt, dass die Wogen hoch schlagen ließ. Die Angst: Der britische Geheimdienst könnte trotz Verschlüsselung über das in Egham bei London gelegene RIM-Rechenzentrum auf Verbindungs- und Inhaltsdaten zugreifen.

Ob hier ein Enigma-Trauma nachwirkt? Lange glaubte man bei den Nachrichtendiensten, auch dem BSI-Vorläufer ZfCh, an die Sicherheit der von der Wehrmacht eingesetzten Verschlüsselungsmaschine, bis Ende der 60er Jahre bekannt wurde, dass der britische Geheimdienst seit Anfang der 40er Jahre in Bletchley Park deutsche Funksprüche entschlüsselte.

Damit sich die Geschichte nicht wiederhole, informierte Lutz Diwell, Staatssekretär im BMI, bereits am 16.09.2005 alle Bundesministerien und bat „nachdrücklich, keine weiteren Investitionen in Blackberry-Geräte zu tätigen“. Statt dessen empfahl er, sich an einer in den Informationsverbund Berlin-Bonn (IVBB) integrierten Alternativlösung zu beteiligen, die „aufgrund der hohen Bedarfslage in der Bundesverwaltung“ von BMI, BMF und BSI „mit Hochdruck“ entwickelt werde und sich bereits im Pilotbetrieb befinde.

Nach RIM-Managerin Eggberry beruhen die BSI-Schlussfolgerungen „auf einem kompletten Mangel an Kenntnis von RIMs Sicherheitsarchitektur und –infrastruktur“. Für RIM und die Mobilfunkbetreiber steht viel auf dem Spiel: Schon über 3,65 Millionen Manager lassen sich ihre E-Mails direkt auf Blackberry oder Handy liefern.

Zur Versachlichung der Diskussion plant Secorvo für den 30.11.2005 eine Veranstaltung mit einem Vertreter von RIM und dem BSI in Karlsruhe – Näheres in Kürze.

1 Security News

1.1 Open Source und zurück

Kürzlich wurde das Unternehmen Sourcefire, maßgeblich an der Entwicklung des Open Source IDS-Systems snort beteiligt, durch Checkpoint übernommenen. Nun soll auch die nächste Nessus Version 3 zwar kostenfrei bleiben, aber vom maßgeblich am Nessus-Projekt beteiligten Unternehmen Tenable (siehe SSN 2/2005) als closed source weiterentwickelt werden.

Die Begründung des Tenable-Geschäftsführers Ron Gula, dieser Schritt sei auf zunehmende Kundenanfragen zurück zu führen, die OpenSource nicht einsetzen möchten oder können, klingt vorgeschoben. Auch anderen scheint es so zu gehen: So wurden bereits Nessus-Ableger wie die Projekte Porz-Wahn und GNessUs gegründet, die Nessus als Open Source unter GPL weiterentwickeln möchten.

1.2 ISO 27001 + Grundschutz

Seit dem 14.10.2005 ist die ISO 27001 nun offiziell publiziert und kann für 124 CHF unter http://www.iso.ch bezogen werden.

Mit der ISO 27001 wurde der britische Standard BS7799-2:2002 in einen internationalen Standard überführt. Die Änderungen zu BS7799-2:2002 sind eher gering. Es gibt einige wenige zusätzliche Detailanforderungen, eine leichte Umstrukturierung der Gliederung (das Kapitel 6.4 "Internal ISMS audits" aus BS7799 ist nun als eigenes Kapitel 6 geführt) und der normative Annex A (control objectives and controls) verweist jetzt auf die ISO/IEC 17799:2005 statt der 2000er Version.

Bestehende bzw. laufende Zertifizierungen nach BS7799-2:2002 sollten eigentlich nach ISO 27001 überführt werden können. Die für Deutschland zuständige Akkreditierungsstelle (Trägergemeinschaft für Akkreditierung GmbH) müsste hierzu ein entsprechendes „certification transition statement“ veröffentlichen; bislang scheint es ein solches aber nicht zu geben.

Das BSI hat das Sicherheitsmanagement beim IT-Grundschutz maßgeblich an den neuen ISO-Standard 27001 angepasst. Der BS 7799-2 Nachfolger ist ab 2006 auch Bestandteil der Zertifizierung nach IT-Grundschutz. Daher wurde zum 01.10.2005 auch das Lizenzierungsschema für IT-Grundschutzauditoren geändert: Die Anforderungen der internationalen Norm EA 07/03 müssen zukünftig erfüllt werden. Für bereits lizenzierte Auditoren werden entsprechende Kompaktkurse angeboten.

1.3 No-NX

Seit 2004 verfügen moderne x86-Prozessoren über ein „No Execute“ (NX) genanntes Sicherheits-Feature. Dieses Feature realisiert die schon seit vielen Jahren (zumindest in der Theorie) bekannte strikte Trennung zwischen Daten- und Codesegmenten, die vor allem dem Missbrauch der weit verbreiteten Buffer Overflow Bugs ein Ende setzen sollen. AMD bezeichnet diese neue Funktionalität gar als „Enhanced Virus Protection“; führt sie doch dazu, dass nicht mehr beliebiger Code im Stack oder Heap des Prozessors ausgeführt werden kann.

Noch bevor dieses Feature von allen Betriebssystemen unterstützt wird, gibt es bereits erste erfolgreiche Angriffe dagegen: am 04.10.2005 veröffentlichte Suse-Mitarbeiter Sebastian Krahmer einen technischen Artikel, in dem er zeigt, wie entsprechende Prozessorregister trotz gesetztem NX-Bit mit beliebigen Werten vorbelegt werden können. Dabei handelt es sich nicht um ausführbaren Code, sondern um beliebige Einsprungadressen, an denen Angreifer dann z. B. eigenen Code platzieren könnten. Und obwohl dieser Angriff nicht trivial ist, veröffentlichte der Autor zeitgleich einen unter Linux laufenden Proof-of-concept.

Fazit: Leider ein weiteres Beispiel für „gut gedacht, schlecht gemacht“...

1.4 Pünktchen und Xerox

Schon länger wird gemunkelt, dass hochwertige Farblaserdrucker und –kopierer auf jedem Ausdruck für das bloße Auge

unsichtbare Markierungen anbringen. Hauptziel solcher individueller Wasserzeichen ist es, leichter die Herkunft gefälschter Banknoten oder anderer „Wert"-Papiere aufspüren zu können.

Missbrauchsmöglichkeiten dieses Überwachungsmechanismus liegen aber genau so auf der Hand. Daher hatte die Electronic Frontier Foundation (EFF) dazu aufgerufen, Testseiten möglichst vieler verschiedener Druckertypen für Vergleichstests einzuschicken. Am 13.10.2005 wurde nun als Ergebnis dieser Bemühungen die Analyse des von Xerox verwendeten Markierungscodes aus winzigen gelben Punkten veröffentlicht.

Ein grundsätzliches Problem von derlei Wasserzeichen ist es, korrekt auseinander zu halten, wenn mehrere davon nacheinander angebracht wurden. Es ist daher wohl nur eine Frage der Zeit, bis die erste Software bereit steht, die es erlaubt, beim Ausdruck einer Seite „eigene" Xerox-Pünktchen anzubringen – unabhängig vom Hersteller des Druckers.

1.5 Where Do You Want to Surf Today?

Gleich auf mehreren Wegen versucht man im Moment, der Phishing-Plage Herr zu werden. So hat der Gouvernator von Kalifornien am 30.09.2005 einen Anti-Phishing Act of 2005 in Kraft gesetzt, der bei Strafandrohung von mindestens US$ 2.500 pro Fall (zuzüglich US-üblich hohen Schadensersatzforderungen) Phishing verbietet. Ob dieses Gesetz mehr Wirkung zeigt als Verbote anderer Straftaten, bleibt abzuwarten.

Technisch statt legislativ versucht es Microsoft: Bereits am 29.08.2005 wurde unter dem sperrigen Namen Microsoft® Phishing Filter Add-in for MSN® Search Toolbar (Beta) ein Zusatzmodul für den Internet Explorer 6 veröffentlicht, das eine Funktion der Version 7 vorweg nimmt. URLs bzw. Webserver, die nicht in einer lokalen Whitelist aufgeführt sind, werden von einem zentralen, von Microsoft betriebenen Server geprüft. Ist einer davon als Phishing-Server bekannt, wird der Anwender gewarnt.

Gegen Pharming, bei dem eine gültige URL mit DNS-Tricks auf den falschen Server „verbogen" wird, hilft dieser Ansatz alleine jedoch nicht viel. Und ob der erzielbare Sicherheitsgewinn gegen Phisher es aufwiegt, Microsoft direkt über (fast) alle aufgerufenen URLs zu informieren, darf auch bezweifelt werden.

1.6 Langzeitarchivierung

Die Universität Kassel führt im Auftrag des Bundesministeriums für Wirtschaft und Arbeit (BMWA) eine Studie über Anforderungen und Trends zur Langzeitaufbewahrung elektronisch signierter Dokumente unter der Leitung von Prof. Dr. Roßnagel durch. Dazu sollen Anwender aus Verwaltung und Wirtschaft sowie Hersteller von Aufbewahrungssystemen befragt werden.

Auf der Webseite des Projekts können der Fragebogen und weitere Informationen zur Studie abgerufen werden. Die Universität Kassel freut sich über eine rege Beteiligung bis zum 11.11.2005. Die Ergebnisse der Studie werden Mitte Dezember publiziert.

1.7 Überlistete Scanner

Zentrale oder dezentrale Virenscanner gehören schon seit vielen Jahren zu den Standard-Anwendungen jeder IT-Infrastruktur: Immer mehr verlässt man sich auf hohe Erkennungsraten sowie einwandfreie Funktionalität zum Schutz lokaler Netze.

Um so schlimmer, wenn systematische Schwachstellen in diesen Scannern gefunden werden, wie im Oktober gleich doppelt geschehen: Am 05.10.2005 veröffentlichten Mitarbeiter der SecuBox Labs ein Advisory, in dem sie beschreiben, wie bestimmte Archive so manipuliert werden können, dass Virenscanner nicht mehr in der Lage sind, diese auszupacken und nach Viren zu suchen. Und am 25.10.2005 beschrieb Andrey Bayora in einem weiteren Advisory, dass viele Scanner beim Erkennen von Dateitypen überlistet werden können, in dem wenige Bytes einer Datei verändert

werden, die jedoch weiterhin ausführbar bleibt – interessanterweise ist auf ein ähnliches Problem bereits im Jahr 2000 hingewiesen worden.

Von beiden Schwachstellen sind nahezu alle gängigen Produkte betroffen; viele Hersteller haben jedoch kurzfristig mit entsprechenden Patches ihrer Scanner reagiert. Fazit: nicht nur die Viren-Datenbanken müssen oft und regelmäßig aktualisiert werden, auch die Programme selbst bedürfen ständiger Updates.

2 Secorvo News

2.1 Secorvo College aktuell

Angesichts der aktuellen Entwicklungen beim IT-Grundschutz und dem ISO-Standard 27001 (siehe oben) haben wir unser Seminar „Information Security Management“ entsprechend aktualisiert. Am 14.-16.11. bzw. 14.-18.11.2005 erhalten Sie einen aktuellen Einblick in Best Practices, Standards und Zertifizierungserfahrungen.

Weitere Seminarangebote und Termine von Secorvo College finden Sie unter http://www.secorvo.de/college

2.2 IsSec/ZertiFA 2005

Am 05.-06.12.2005 lädt COMPUTAS nach Berlin zu der von Dirk Fox und Stefan Kelm inhaltlich mitgestalteten Doppelkonferenz IsSec/ZertiFA 2005. Das Programm lässt eine spannende Tagung erwarten.

2.3 Secorvo White Paper ISM

Das von Jörg Völker im November 2003 veröffentlichte Secorvo White Paper zum Sicherheitsmanagement nach BS 7799 hat sich mit seitdem mehr als 25.000 Downloads zum meistgelesenen White Paper von Secorvo entwickelt.

Inzwischen hat die Veröffentlichung des ISO 17799:2005 eine Überarbeitung erforderlich gemacht. Die Neufassung des White Papers steht inzwischen auf den Secorvo-Webseiten zum Download bereit.

3 Veranstaltungshinweise

November 2005	
08.-11.11.	Kommunikationsschutz und Datensicherheit (Secorvo College, Karlsruhe)
14.-18.11.	Information Security Management (Secorvo College, Karlsruhe)
15.-16.11.	Einführung in die Praxis des DSB (Euroforum, Berlin)
22.-25.11.	Live Hacking Lab (Secorvo College, Karlsruhe)
Dezember 2005	
01.-02.12.	Einführung in die Praxis des DSB (Euroforum, Düsseldorf)
05.-06.12.	IsSec/Zertifa 2005 (COMPUTAS, Berlin)
06.-07.12.	Prüfung zum Certified IT Security Professional (CISP) (Secorvo College, Karlsruhe)
27.-30.12.	22nd Chaos Communication Congress (CCC, Berlin)
Januar 2006	
24.-26.01.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
30.-31.01.	Net-ID 2006 (COMPUTAS, Berlin)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
November 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 11, 4. Jhrg. 2005
Stand 01. Dezember 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Getrübter Blick

1 Security News

1.1 Codebreaker im Plan

1.2 BlackBerry Symposium

1.3 High-speed spoofing

1.4 Literaturpreis für Sober

1.5 Standards-Workshop

1.6 (w)Or(m)acle

1.7 Dunkle Seite der Macht

1.8 Neue Top 20-Liste

2 Secorvo News

2.1 Secorvo College aktuell

2.2 White Paper: BlackBerry

2.3 DuD 2006 – 27.-28. März

3 Veranstaltungshinweise

Impressum

Editorial: Getrübter Blick

Stellen wir uns vor, wir seien Politiker. Einflussreich, gerne gesehener Gast im Fernsehen und bei öffentlichen Veranstaltungen. Jovial, eloquent, erfolgreich. Und täglich Seite an Seite mit unserem Bodyguard unterwegs. Gepanzerter Dienstwagen, Fahrer mit wachsamem Auge und Fluchttraining. Schusssicheres Glas in Büro und Wohnzimmer, Personenkontrollen für jeden, der sich auf Wurfweite nähert, überwachter Schulweg für unsere Kinder. Aus einer solchen Perspektive nimmt sich Freiheit anders aus. Ertrüge man diese Randbedingungen über Jahre, erscheint es unvorstellbar, dass sie unser Urteil unbeeinflusst ließen – vor allem bei Fragen der inneren Sicherheit.

Das war schon so in den Hochzeiten des Terrorismus in Deutschland. Obwohl sich die Zahl der Opfer der menschenverachtenden Ideologie der RAF zum Glück zahlenmäßig in Grenzen hielt, wurde ihr eine polizeiliche Aufmerksamkeit zu Teil, die kein anderer Mörder je fürchten müsste – dabei war die Identität der Täter bekannt. Die Folgen des Perspektivwechsels ließen sich bei niemandem so ausgeprägt beobachten wie bei Bundesinnenminister Schily, der als ehemaliger RAF-Anwalt nach den Attentaten des 11.09.2001 die Befugnisse der Strafverfolgung fast geräuschlos ausweitete wie kein Minister zuvor.

Kaum hat die Große Koalition mit der Opposition im Bundesrat die letzte Bastion des Widerstandes geschliffen, wachsen die Begehrlichkeiten weiter: Die Vorratsdatenspeicherung von Telekommunikationsdaten und die Umwandlung des LKW-Maut-Systems in ein PKW-Verfolgungs-System stehen jetzt auf der Tagesordnung. Dabei bleiben die Strafverfolgungsbehörden bis heute den Nachweis schuldig, dass Großer Lauschangriff, Telefonüberwachung oder Rasterfahndung auch nur einen einzigen Täter überführt oder wenigstens abgeschreckt hätten. Aus der Perspektive des Kaninchens, das auf den Fuchs starrt, ist der mit wachsender Überwachung einher gehende Verlust an Lebensqualität jedoch offenbar kein gewichtiges Argument.

1 Security News

1.1 Codebreaker im Plan

Am 02.11.2005 konnte die auf dem Gebiet der angewandten Faktorisierung führende Arbeitsgruppe der Universität Bonn die beiden Primfaktoren der Zahl RSA-640 benennen und den von RSA Security Inc. ausgelobten Preis von $ 20.000 einstreichen.

Kein Grund zur Panik für Anwender des RSA-Verfahrens – es liegt alles im Plan: Weder ist dies ein neuer Weltrekord (bereits am 09.05.2005 hatte die selbe Gruppe die 663-Bit-Zahl RSA-200 gebrochen, siehe SSN 05/05), noch wurde ein radikal neuer Algorithmus angewandt. Das Resultat bestätigt lediglich die in den Jahren 2001 (Lenstra) und 2002 (Secorvo) aufgestellten Prognosen über den Fortschritt der Faktorisierung unter Berücksichtigung der Entwicklung der Rechenleistung.

Vielleicht gelingt der nächste große Durchbruch ja den Nachwuchs-Codebreakern, die die NSA derzeit mit ihrer CryptoKids™ Kampagne sucht.

1.2 BlackBerry Symposium

Die Diskussion um die bislang unveröffentlichte BSI-Studie vom 20.09.2005, die dem Push-Mail-System „BlackBerry“ der Firma RIM die Eignung für sicherheitskritische Bereiche abspricht, dauert an. Zum Glück hat sie wieder die Sachebene erreicht.

Zwei Veranstaltungen sind in den kommenden Tagen dieser Fragestellung gewidmet: Das von Secorvo veranstaltete „BlackBerry Security Symposium“ am 30.11.2005 in Karlsruhe und das Simedia-Tagesseminar „Sicherheit von E-Mail-Push-Diensten“ am 08.12.2005 in Bonn. Wer am 30.11.2005 verhindert ist, kann die Teilnehmerunterlagen auf CD online ordern.[1]

[1] Security Finder-Abonnenten finden Materialien zum Thema unter *Mobile Security*. Eine Darstellung des BlackBerry-Sicherheitskonzepts erschien in der DuD 11/05.

1.3 High-speed spoofing

Dass IP- sowie MAC-Adressen leicht gefälscht werden können, ist seit langem bekannt. Inzwischen existieren zahlreiche frei verfügbare Tools, mit denen ein Angreifer – ohne eigenes Know-how zu besitzen – derartige Spoofing-Angriffe durchführen kann. Dennoch wird vor allem die Kombination aus IP- und MAC-Adresse noch immer in vielen Netzbereichen zur Authentisierung verwendet.

Am 03.11.2005 nun veröffentlichte Paweł Pokrywka ein im Rahmen seines Master of Science-Studiengangs erstelltes Angriffsprogramm namens multispoof. Dieses Tool unterscheidet sich in zwei wesentlichen Punkten von bisher verfügbaren Spoofing-Programmen: zum einen kann es mehrere IP-/MAC-Adresskombinationen gleichzeitig fälschen (was den Datendurchsatz deutlich erhöhen kann), zum anderen fälscht multispoof nur inaktive Adressen, so dass es nicht zu Konflikten mit legitimen Benutzern kommt – was das Entdecken solcher Angriffe erheblich erschwert.

Will man diese Funktionalität nutzen, wird multispoof zunächst in einer Art „Lernmodus“ betrieben: Das Tool protokolliert dazu über einen bestimmten Zeitraum alle gültigen Adressen eines Netzes in einer eigenen Datenbank; anschließend nutzt es diese Informationen, um inaktive Adressen zu missbrauchen.

Wer noch immer auf IP- und MAC-Adressen als Authentisierungsmechanismus vertraut, den wird ein Probelauf von multispoof eines Besseren belehren...

1.4 Literaturpreis für Sober

Seit dem 19.11.2005 grassiert eine neue Variante des altbekannten E-Mail-Wurms Sober, die mancherorts sogar das Aufkommen an Spam-Mails in den Schatten stellt. Die hohe Verbreitung verursacht nicht etwa eine neue Verbreitungstechnik – sie ist einzig auf die bessere „literarische Qualität“ der Social-Egineering Komponente, vulgo E-Mail-Betreff und -Text, zurück zu führen: Unzählige Empfänger starten das komprimierte anhängende Schadprogramm.

Bleibt nur zu hoffen, dass die Versender von Phishing-Mails und Anwerbeversuchen für Geldwäscher noch eine Weile brauchen, bis sie mit ihren bislang meist sehr holprigen Texten diese Verführungsqualität erreichen.

1.5 Standards-Workshop

Für den 05.12.2005 lädt der ISO/IEC SC27 „Security Techniques" des DIN zu einem eintägigen internationalen Workshop nach Berlin. Das Programm der Veranstaltung ist viel versprechend; eine Anmeldung zu dieser unentgeltlichen Veranstaltung ist auch online möglich.

1.6 (w)Or(m)acle

Der Ablauf war schulbuchartig: Erst sprach man darüber (2002), dann wurde fachlich präzisiert (Q3/2005) – die praktische Umsetzung stellte sich dann von selbst ein. Am 31.10.2005 wurde der „Voyager Beta Worm" für Oracle anonym auf der Mailingliste Full-Disclosure veröffentlicht. Am 05. 11.2005 folgte eine Warnung von Oracle an alle Kunden.

Käme nun noch eine erfolgreiche Freisetzung des „Proof of Concept", müsste sich der Hersteller Oracle mit seinen 22 Sicherheitszertifizierungen wohl zu den Themen Compliance, SOX, Haftungs- und Schadensersatzansprüche neu positionieren. Die Checkliste anlässlich des aktuellen Vorfalls könnte sich dafür als unzureichend erweisen.

1.7 Dunkle Seite der Macht

Das durch das vielfältige Medienecho seit der ersten Meldung am 31.10.2005 zur Affäre gewordene Kopierschutz-„Rootkit" auf CDs von Sony BMG hat eine Welle der Empörung ausgelöst. Es lehrt zweierlei:

- Erstens sollte insbesondere derjenige, der bestrebt ist, sein eigenes geistiges Eigentum zu schützen, dasjenige von anderen peinlich genau beachten.

Denn sollte die eingesetzte Kopierschutz-Software tatsächlich die Open-Source Lizenzen GPL und LGPL verletzen, dann muss dies Konsequenzen für den Lieferanten der Software haben.

- Zweitens ist die Grenze zwischen unerwünschter Malicious Software und nützlichen System-Tools mindestens so durchlässig wie die zwischen den beiden Seiten der StarWars Macht.

Denn die Eigenschaften „gut" und „böse" lassen sich nicht aus technischer Funktionalität ableiten, sondern einzig aus der jeweiligen Nutzung. Und die ist oft nicht eindeutig, wie die Wandlung von NetBus vom Saulus (Trojaner) zum Paulus (Administrations-Tool) eindrucksvoll demonstriert.

Auch für Sony BMGs Kopierschutz, der in der öffentlichen Wahrnehmung ein Schritt auf die „dunkle Seite" war, haben findige Online-Spieler schon eine neue Anwendung ausgemacht: Sie verstecken damit ihre kleinen „Schummel"-Programme.

1.8 Neue Top 20-Liste

Zum fünften Mal veröffentlichte SANS am 20.11.2005 seine Liste der 20 kritischsten IT-Sicherheitslücken. Teilten sich diese bis 2004 nur zwei Klassen, nämlich Windows und Unix, wurde die Liste 2005 deutlich erweitert: Neben den Betriebssystemen Windows und Unix werden Sicherheitslücken in systemübergreifenden Programmen (wie Backup, DNS, PHP und Datenbanken) und in Netzkomponenten (wie Cisco) unterschieden.

Auch hat sich das Gewicht verschoben: Nur noch sieben der 20 Sicherheitslücken betreffen Microsoft (5) oder Unix (2). Die Liste ist auch nicht mehr „kumulativ", d.h. Sicherheitslücken, die 2005 in der Top 20-Liste vermerkt waren, werden 2006 nicht mehr aufgenommen.

Die in der – als Hilfestellung für Unternehmen gedachten – Aufstellung gelisteten Top-Sicherheitsmängel sollten schnellstmöglich durch das Einspielen der entsprechenden Patches beseitigt werden.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminarangebot von Secorvo College wartet im Jahr 2006 mit zahlreichen neuen Themen auf, darunter die sichere Gestaltung von IT-Outsourcing, die Praxis von IT-Sicherheitsaudits und das kürzlich erstmalig durchgeführte Seminar Kommunikationsschutz und Datensicherheit, das eine besonders gute Seminarbewertung erhielt.

Auf vielfachen Wunsch hat endlich auch der E-Commerce bei College Einzug gehalten: Mit dem Programm 2006 ist nun auch eine Online-Seminaranmeldung möglich – natürlich SSL-gesichert.

Weitere Seminarthemen und Termine von Secorvo College finden Sie unter http://www.secorvo.de/college

2.2 White Paper: BlackBerry

Die Sicherheit des BlackBerry-Push-Mail-Systems ist seit Bekanntwerden der internen BSI-Studie Gegenstand zahlreicher Diskussionen. Das am 23.11.2005 publizierte 12. Secorvo White Paper „BlackBerry Security“ stellt das Sicherheitskonzept des Push-Dienstes vor und bewertet die von RIM verwendeten Schutzmechanismen.

2.3 DuD 2006 – 27.-28. März

Das Programm der achten jährlichen Fachkonferenz „Datenschutz und Datensicherheit – DuD 2006“ am 27.-28.03.2006, seit 1999 von COMPUTAS in Zusammenarbeit mit den Herausgebern der Zeitschrift DuD konzipiert und durchgeführt, wird in Kürze verfügbar sein.

Das etablierte Treffen führender Datenschützer und IT-Sicherheitsverantwortlicher in Deutschland wird sich aktuellen Themen wie Phishing, Spam, Pharming, BlackBerry Security, Kundenkarten, Scoring und Honeynets widmen. Schon jetzt ist eine Voranmeldung möglich.

3 Veranstaltungshinweise

November 2005	
30.11.	BlackBerry Security Symposium (Secorvo, Karlsruhe)
Dezember 2005	
01.-02.12.	Der bDSB in der Praxis (Euroforum, Düsseldorf)
05.-06.12.	IsSec/Zertifa 2005 (COMPUTAS, Berlin)
06.-07.12.	Prüfung zum Certified IT Security Professional (CISP) (Secorvo College, Karlsruhe)
08.12.	Sicherheit von E-Mail-Push-Diensten (Simedia, Bonn)
27.-30.12.	22nd Chaos Communication Congress (CCC, Berlin)
Januar 2006	
24.-26.01.	IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College, Karlsruhe)
30.-31.01.	Net-ID 2006 - Identity, Trust, Privacy & Security (COMPUTAS, Berlin)
Februar 2006	
07.-10.02.	PKI (Secorvo College, Karlsruhe)
14.-15.02.	Inside Windows Security (Secorvo College, Karlsruhe)
März 2006	
27.-28.03.	DuD 2006 (COMPUTAS, Berlin)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Dezember 2005

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch, Kai Jendrian

Secorvo Security Consulting GmbH

Nr. 12, 4. Jhrg. 2005
Stand 23. Dezember 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial:
War es Prometheus?

1 Security News

1.1 ETSI on the Road

1.2 Schwachstellenauktion

1.3 Generationenproblem?

1.4 OpenCA goes OpenXPKI

1.5 Happy New Year, Sober!

1.6 W2K3 SP1 CC EAL4+

1.7 Softies und Saboteure

1.8 Sandkastensicherheit

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Externer DSB

3 Veranstaltungshinweise

Impressum

Editorial: War es Prometheus?

Genug, ich traue den Geschenken nicht,
Die mir von solchen Freunden kommen!
Auf ein Kamin zu stellen, nun, dazu
Ist diese Büchse schön genug; gib immer her!
Christoph Martin Wieland, „Pandora“ (1779)

Vor über 200 Jahren geschrieben, und doch merkwürdig aktuell: Dies könnte das einleitende Zitat in der umstrittenen BlackBerry-Studie des BSI sein. Pandoras Büchse als Symbol für das unbekannte Gerät, die „Closed Source“-Software, die, einmal geöffnet, Übles über die Welt bringt.

Tatsächlich lässt sich das Bild auf praktisch jedes IT-System anwenden, das wir heute einsetzen. Kennen wir die Software? Wissen wir wirklich, was Prozessor und Hardwarekomponenten tun? Schließlich gibt es zahlreiche Möglichkeiten, ein Sicherheitssystem unbemerkt zu penetrieren: Manipulation der Schlüsselgenerierung, Erweiterungen des Kommunikationsprotokolls, oder, ganz perfide, verdeckte Informationskanäle wie vermeintliches „Padding“ zum Auffüllen der Datenpakete in Normlänge.

Erwiesenermaßen lässt sich nicht beweisen, dass ein IT-System nicht mehr als das Gewünschte leistet. Wir sind daher angewiesen auf Audits, im besten Fall eine Zertifizierung nach international anerkannten Standards wie den Common Criteria. Nur: Auch eine solche Zertifizierung zeigt lediglich, dass es in einer konkreten Version keine Hintertür gab – mit jedem Versionswechsel, ja mit jeder Neuübersetzung des Codes kann sich das ändern, bei Vorsatz ohnehin. Lernen wir also von Hesiod:

Erstens: Es ist gar nicht ausgemacht, dass Pandora die Büchse geöffnet hat – womöglich war es ihr Schwager Prometheus oder Epimetheus, ihr Gatte. Mit Verdächtigungen sollte man also vorsichtig sein.

Zweitens: Inzwischen gilt als erwiesen, dass es gar keine Büchse war, sondern ein Krug – ein Übersetzungsfehler. Dem geschriebenen Wort sollte man demnach lieber nicht automatisch trauen.

Und drittens: Dem Krug ist auch *Ελπίς*, die Hoffnung, entwichen. Immerhin bleibt uns die.

1 Security News

1.1 ETSI on the Road

Vom 16.01. bis 19.01.2006 macht das European Telecommunications Standards Institute (ETSI) im Rahmen einer ICT-Roadshow durch mehrere europäische Länder in Deutschland Station und bietet vier Informationsveranstaltungen zu seinen Standardisierungsaktivitäten im Bereich Informations- und Kommunikationstechnik an.

Hochrangige deutsche ETSI-Vertreter werden über die Gremienarbeit referieren und die Vorteile von Standards für beteiligte Unternehmen beleuchten. Ziel der Roadshow ist es – neben der Präsentation aktueller Entwicklungen – vor allem, neue Mitglieder und aktive Teilnehmer für die ETSI-Gremien zu gewinnen – also eine gute Gelegenheit zur Kontaktaufnahme für alle, die ETSI-Standards nutzen, z. B. im Mobilfunk oder bei elektronischen Signaturen.

1.2 Schwachstellenauktion

Anfang Dezember versuchte ein Anbieter Informationen zu einer noch nicht veröffentlichten Excel-Schwachstelle via eBay zu versteigern. Die Auktion wurde angeblich auf Betreiben von Microsoft vorzeitig abgebrochen. Offensichtlich wollte der Anbieter die teilweise langwierige Behebung von Schwachstellen bei Microsoft kritisieren. Microsoft-Mitarbeitern wollte er bei Nennung des Rabatt-Codes „LINUXRULZ“ Vergünstigungen einräumen...

Tatsächlich hätte uns diese Auktion eine Vorstellung vom (Markt-) Wert einer Sicherheitslücke in einer verbreiteten Software liefern können – nicht uninteressant.

Dennoch: Schwachstellen sollten immer unmittelbar und zuerst, vor allem auch bedingungslos dem betroffenen Hersteller zur Verfügung gestellt werden. Über Probleme hierbei berichteten wir allerdings bereits in den SSN 9/2004.

1.3 Generationenproblem?

Am 08.11.2005 veröffentlichte eine Gruppe um den u.a. durch seine Angriffe auf den Clipper-Abhörchip bekannten Sicherheitsexperten Matt Blaze eine Sicherheitsanalyse von in den USA verwendeten Abhörgeräten für analoge Telefongespräche. Grundlage der Analyse waren ausschließlich öffentlich zugängliche Informationen und auf dem freien Markt erworbene Geräte.

Ergebnis: Verdächtige, die befürchten, abgehört zu werden, können durch das Senden von Signalisierungstönen die Aufzeichnungen über von ihnen geführte Telefongespräche manipulieren, teilweise sogar die Aufzeichnung vorzeitig abschalten. Das alles erinnert fatal an das Blue-Boxing, mit dem Captain Crunch vor mehr als 30 Jahren die Abrechnung von Gesprächen über AT&T deaktivieren konnte.

Die Frage drängt sich auf: Wie kann man heutigen Systemdesignern genug über Angriffe und Konzepte der Vergangenheit beibringen, damit sie nicht ständig altbekannte Schwachstellen in neuer Form wiederbeleben?

1.4 OpenCA goes OpenXPKI

Viele Jahre gab es bei der Frage nach geeigneter Software für den Betrieb einer eigenen PKI nur die Auswahl zwischen sehr teuren kommerziellen Produkten, der ins Microsoft Betriebssystem integrierten, teilweise rudimentären PKI und sehr aufwändigen „Bastellösungen“, bestehend aus frei verfügbaren OpenSource-Paketen und selbst entwickelten Skripten. Bereits 1998 versuchte deshalb das OpenCA-Projekt durch den Aufbau einer OpenSource-Toolbox samt graphischer Oberfläche dieses Problem zu adressieren. Mangels Ressourcen konnte sich OpenCA dennoch nie zu einer produktionsreifen Lösung entwickeln.

In den vergangenen beiden Jahren jedoch wurde OpenCA an vielen Stellen erheblich weiterentwickelt. Seit dem 09.12.2005 wird die Toolbox nun unter dem Namen OpenXPKI neu entworfen und fortgeführt. Open-

XPKI ist – vor allem im universitären Umfeld – bereits in vielen Organisationen im Einsatz: Beispielweise basieren auch die neuen Dienste der DFN-PKI auf OpenXPKI, wie am 18.10.2005 vorgestellt.

Fazit: Wieder einmal schafft es die „Open-Source-Szene“, eine ernst zu nehmende Alternative zu kommerziellen Produkten zu entwickeln.

1.5 Happy New Year, Sober!

Es gibt wenig, worauf man sich heutzutage noch verlassen kann. Aber ein Bekannter bleibt uns zumindest auch noch im neuen Jahr erhalten: der Sober-Wurm. Mitarbeitern des Herstellers F-Secure ist es gelungen, den Update-Mechanismus des Wurms zu entschlüsseln. Dabei entdeckten sie, dass ab 05.01.2006 mit einer neuen Sober-Angriffswelle zu rechnen ist.

1.6 W2K3 SP1 CC EAL4+

Was in der Überschrift aussieht wie ein Geekcode, bedeutet: Am 14.12.2005 gab Microsoft bekannt, dass Windows 2003 und XP in verschiedenen Versionen – jeweils mit Service Pack 1 bzw. 2 und ganz bestimmten Kombinationen von Hotfixes – sowie die Certificate Services von Windows 2003 nach Common Criteria (CC) mit Evaluation Assurance Level (EAL) 4+ zertifiziert wurden.

Neben der Angabe der Prüftiefe mit dem Marketing-wirksamen EAL-Wert ist bei einer CC-Evaluierung stets zu beachten, welcher Funktionsumfang denn geprüft wurde (siehe SSN 2/2005). Und hier steckt – wie bei vergleichbaren Evaluierungen anderer Betriebssysteme (u.a. Solaris, SuSE Linux, AIX) auch – der Pferdefuß: Einmal mehr wurde das Controlled Access Protection Profile (CAPP) angewandt, das keine besonderen Anforderungen an die Netzwerksicherheit stellt. Wörtlich heißt es da: „Any other systems [...] are assumed to be under the same management control”. Mit anderen Worten: Schon ein Internet-Anschluss verstößt gegen die der Zertifizierung zu Grunde liegenden Annahmen.

An zwei Stellen geht Microsoft löblicherweise über CAPP/EAL4 hinaus: Zum einen wurde neben den Grundanforderungen der CC auch der Umgang mit Schwachstellen (Flaw Remediation) mit geprüft. Zum anderen wurden die Certificate Services nach dem vom NIST speziell für PKI entwickelten Protection Profile CIMC evaluiert.

1.7 Softies und Saboteure

Eine am 21.12.2005 auf Deutsch veröffentlichte Studie wertet in sechs verschiedenen europäischen Ländern erstellte Umfragen zur Gefährdung der IT-Sicherheit durch interne Mitarbeiter aus. Die Studie wurde im Auftrag von McAfee erstellt, was angesichts eines Produktportfolios, das sich besonders dem Schutz gegen „Gefahren von innen“ widmet, wenig verwundert.

Die Zahlen werden aber auch all denen eine Hilfe sein, die Maßnahmen in den Bereichen Security Awareness oder interne Sicherheit begründen müssen und sich dabei nicht auf hinter vorgehaltener Hand gemunkelte Beispiele und Mutmaßungen verlassen wollen.

Bei der Klassifikation der internen Gefahren waren die Autoren humorvoll-kreativ: es wird nach fahrlässigen „Sicherheits-Softies“, verspielten „Gadget-Freaks“, Umnutzung durch „Illegale“ (im englischen Original der Studie: „Squatter“ – Systembesetzer) und vorsätzlichen „Saboteuren“ unterschieden.

1.8 Sandkastensicherheit

Auch in einem Sandkasten kann hin und wieder etwas passieren, was von den Erbauern so nicht vorhergesehen wurde. Das ist mit Kindern auf dem Spielplatz im realen Leben ähnlich wie bei Software in einer virtuellen Maschine.

Am 21.12.2005 wurde auf [Full-Disclosure] von Tim Shelton auf eine Schwachstelle in den meisten VMWare-Versionen (außer ESX-Server) hingewiesen. Durch einen Fehler in der NAT Implementierung wird ein Nutzer des Gastsystems in die Lage

versetzt, Kommandos auf dem Wirtssystem auszuführen.

Das Konzept der virtuellen Maschinen ist nicht nur aus Verfügbarkeitsgründen ein wertvoller Schritt in Richtung erhöhter Sicherheit. Auch wenn dies der erste nachgewiesene Einbruch in das Hostsystem ist, darf man sich allerdings nicht in der trügerischen Sicherheit wähnen, dass diese Maschinen in allen Fällen wasserdicht sind. Sehr kritische Systeme sind daher nach wie vor auf einer eigenen (Hardware-) Plattform besser aufgehoben. Bei der Mehrzahl der Systeme dürften die Vorteile der Virtualisierung die Risiken aber überwiegen.

2 Secorvo News

2.1 Secorvo College aktuell

Für den „Jahrgang 2006“ wurde das bewährte Seminar Public Key Infrastrukturen um einen (optional buchbaren) vierten Tag erweitert, an dem die an den vorangegangenen Tagen vermittelten Grundlagen und Erfahrungen aus zahlreichen PKI-Projekten in Workshop-Form in die Praxis umgesetzt werden können. Es findet erstmals vom 07.-10.02.2006 statt.

Der Workshop-Tag kann auch separat oder zusammen mit dem dritten Seminartag, der fortgeschrittene PKI-Fragestellungen adressiert, gebucht werden.

Weitere Seminarthemen und Termine von Secorvo College finden Sie unter http://www.secorvo.de/college

2.2 Externer DSB

Für mehrere Unternehmen hat Secorvo bereits die Funktion des externen Datenschutzbeauftragten übernommen. Mit Karin Schuler, Volker Hammer und Dirk Fox stehen jetzt drei erfahrene Datenschutzexperten für diese Aufgabenstellung zur Verfügung. Eine detaillierte Leistungsbeschreibung kann unter info@secorvo.de angefordert werden.

3 Veranstaltungshinweise

Dezember 2005	
24.12.	Heiligabend
Januar 2006	
16.-19.01.	ETSI ICT Roadshow (Vier Veranstaltungen in Bonn, Mainz, Ulm, München)
24.-26.01.	IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College, Karlsruhe)
30.-31.01.	Net-ID 2006 – Identity, Trust, Privacy & Security (COMPUTAS, Berlin)
Februar 2006	
07.-10.02.	PKI (Secorvo College, Karlsruhe)
14.-15.02.	Inside Windows Security (Secorvo College, Karlsruhe)
20.-21.02.	IT-Governance (COMPUTAS, Berlin)
20.-23.02.	Sicherheit 2006 (Gesellschaft für Informatik, Magdeburg)
28.02.-03.03.	Black Hat Europe 2006 (Black Hat, Amsterdam)
März 2006	
01.-02.03.	DFN-CERT-Workshop (DFN-CERT, Hamburg)
27.-28.03.	DuD 2006 (COMPUTAS, Berlin)
28.-29.03.	D-A-CH Security 2006 (Universität Klagenfurt)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Januar 2006

Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 42, 5. Jhrg. 2006
Stand 27. Januar 2006

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: 42

1 Security News

1.1 Pikanter Patch

1.2 GSHB heiratet BS 7799-2

1.3 WAF-Auswahlhilfe

1.4 Experimentierkasten

1.5 CERT/CC Statistik

1.6 Wendung zum Besseren

1.7 BlackBerry Bugs

2 Secorvo News

2.1 Secorvo College aktuell

2.2 ISO 27001-AaBvITG

2.3 KA-IT-Si wird fünf

2.4 „DuD 2006" – 27.-28.03.

3 Veranstaltungshinweise

Impressum

Editorial: 42

"I think, to be quite honest with you, is that you've never actually known what the question is."
Douglas Adams (Hitchhiker's Guide to the Galaxy)

Die Antwort von *Deep Thought* auf die „Frage nach dem Leben, dem Universum und dem ganzen Rest" ist Kult – und weckt Assoziationen. Denn mit simplen Antworten, die in keinem nachvollziehbaren Zusammenhang mit der gestellten Frage zu stehen scheinen, werden wir nicht nur in Politikerinterviews beglückt. Sie sind vielmehr zu einer unserer häufigsten Informationsquellen geworden.

Nur ein Beispiel: „Über 70% aller Angriffe kommen von innen" – eine beliebte Aussage zahlreicher Studien, begeistert aufgegriffen von Journalisten und gerne als Argument für die Durchsetzung verschiedenster Sicherheitsmaßnahmen genutzt.

Einmal abgesehen von Defiziten bei der handwerklichen Gestaltung und Auswertung der zugehörigen Studien, irritiert bei genauer Betrachtung mindestens zweierlei:

- Gefragt wurden die für IT-Sicherheit in Unternehmen Verantwortlichen – nicht etwa die Täter oder eine Fallstatistik.
- Unter „Angriff" wird meist inflationär jeder Sicherheitsvorfall (bis zum vergessenen Passwort) subsummiert.

Liest man die den Studien zu Grunde liegenden Fragebögen, kann man sich des Eindrucks nicht erwehren, dass hier die Branche begeistert ihre eigene Wichtigkeit feiert. Nicht, dass die Aussagen unwahr sind – allerdings: Wir wissen es nicht. Gerade bei Aussagen zur tatsächlichen Bedrohung, den Schäden und Täterarten wären aber belastbare Erkenntnisse sehr wichtig – und stünde mehr diesbezügliche Seriosität uns allen gut zu Gesicht.

Bleibt zu fragen, warum Douglas Adams in seinem Kult-Roman die Erde als Computer zur Formulierung der richtigen Frage bauen lässt. Ob er tatsächlich angenommen hat, dass sich diese Kompetenz hier entwickelt? Dass er die Erde vor Ablauf des Programms sprengt, lässt auf eine realistischere Sicht der Dinge schließen...

1 Security News

1.1 Pikanter Patch

Zum Jahresausklang wurde nach bereits zweiwöchiger „Verbreitung“ des zugehörigen Remote-Exploit-Codes ein Designfehler im Windows Meta File-Format (WMF) auf Bugtraq einer breiteren Öffentlichkeit zugänglich gemacht. Fatalerweise genügt bereits das Anklicken oder Anschauen einer Grafikdatei, beispielsweise auf einer Webseite, um beliebigen Code zur Ausführung zu bringen. Eine gute Demonstration findet sich beim Heise Verlag. Betroffen sind nicht nur Microsoft-Betriebssysteme, sondern auch WMF-Metadaten verarbeitende Anwendungen (u.a. Lotus Notes und Debian Linux). Auch der Wine Windows API-Emulator bildet diesen Designfehler unter Linux „ordnungsgemäß“ nach.

Obwohl für diese sehr kritische Schwachstelle bereits Software zur Ausnutzung im Umlauf war, wurde der offizielle Patch MS06-001 von Microsoft erst zwei Wochen später zur Verfügung gestellt.

Pikantes Detail: Offenbar war zunächst vorgesehen, den Patch erst zum regulären Patch-Day Mitte Januar auszuliefern. Nutzer hatten daher zur Selbsthilfe gegriffen und inoffizielle Patches (u. a. von Ilfak Guilfanov) sowie Anleitungen zur Verhinderung der Schwachstelle veröffentlicht.

Wichtig: Microsoft bietet keinen Patch für Systeme wie WindowsNT oder Win2000 SP3 an, deren „Extended Security Support“ abgelaufen ist. Ein Update auf ein aktuelleres Betriebssystem ist unvermeidlich.

1.2 GSHB heiratet BS 7799-2

Am 16.01.2006 hat das BSI in einer Pressemitteilung die Veröffentlichung der neuen Version des Grundschutzhandbuchs angekündigt. Bei dieser Version handelt es sich um eine grundlegende Überarbeitung des Handbuchs. Die wichtigste Änderung ist die Anpassung an den ISO Standard 27001 (internationaler Nachfolger des BS 7799-2).

Ebenfalls neu ist die Abspaltung von ehemaligen Bestandteilen des GSHB in eine neue Schriftenreihe, die BSI-Standards 100-1 bis 100-3. Die Standards beschreiben vorrangig Prozesse und Vorgehensweisen, während die Bausteine, Gefährdungen und Maßnahmen weiterhin in den so bezeichneten Grundschutz-Katalogen enthalten sind.

Mit der Überarbeitung und Anpassung an ISO 27001 hat das BSI ein bereits gutes Hilfsmittel weiter verbessert und die Attraktivität einer Zertifizierung erhöht. Derzeit ist die neue Version nur in gedruckter Form über den Bundesanzeiger-Verlag oder den Buchhandel erhältlich. Eine Online-Version soll in Kürze über die Webseite des BSI zur Verfügung gestellt werden.

1.3 WAF-Auswahlhilfe

Am 14.01.2006 hat das Web Application Security Consortium (WASC), ein im Januar 2004 gegründetes internationales Expertengremium, Version 1.0 der „Web Application Firewall Evaluation Criteria“ vorgelegt. Dabei handelt es sich um eines der ersten Dokumente, in welchem Entscheidern und Firewall-Architekten ein ausführlicher Katalog wichtiger Anforderungen an eine Web-Application-Firewall (WAF) zur Verfügung gestellt wird. Diese Anforderungsliste erleichtert den Vergleich, die Bewertung und die Auswahl geeigneter WAF-Lösungsansätze und verfügbarer Produkte.

1.4 Experimentierkasten

Das bekannte, von der TU Darmstadt, der Universität Siegen und der Deutschen Bank entwickelte Lernwerkzeug Cryptool ist seit Ende 2005 als Beta-Release in der Version 1.4 verfügbar – ein schöner praktischer Einstieg in die Kryptographie.

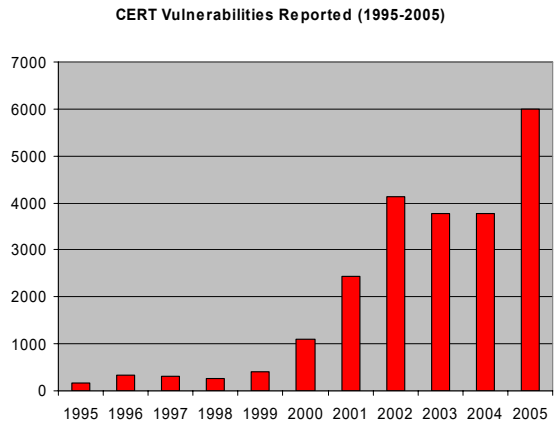
In der Roadmap sind die durchgeführten und geplanten Änderungen beschrieben. Besonders interessant sind eine Demo von Authentifizierungsmöglichkeiten im Netz, verschiedene aktuelle Angriffsdemonstrationen (u.a. Seitenkanal-Attacken und spezielle Angriffe gegen RSA) sowie neue Visualisierungsfunktionen (u.a. animierte

Veranschaulichungen von Algorithmen und 3D-Visualisierung großer Mengen von Zufallszahlen).

Vor der Publikation der Endfassung freuen sich die Autoren über kritische Beta-Tester.

1.5 CERT/CC Statistik

Das CERT Coordination Center an der Carnegie Mellon University (CERT/CC) führt eine Statistik der jährlich entdeckten (und gemeldeten) Sicherheitsschwachstellen (Vulnerabilities). Beunruhigend sind die Zahlen aus 2005:



Nach einem explosionsartigen Anstieg Anfang des Jahrtausends hatten sich die Softwarefehler 2002-2004 bei rund 4.000 eingependelt. 2005 ist die Zahl trotz der verstärkten Bemühungen vieler Hersteller um sichere Softwareentwicklung um fast 60% angestiegen.

1.6 Wendung zum Besseren

Seit dem 22.12.2005 ist das von ISACA entwickelte und erstmals 1996 veröffentlichte CobiT-Framework in der Version 4.0 verfügbar. CobiT (Control Objectives for Information and Related Technology) ist ein internationales Modell von Kontrollzielen speziell für IT-Prozesse.

In der neuen Version wurden Redundanzen zwischen allgemeinen und spezifischen Kontrollen beseitigt, so dass die Anzahl der Control Objectives von 318 auf 215 reduziert werden konnte. Weiter wurde der zentrale Fokus der IT Governance innerhalb einer Corporate Governance vertieft. Im Rahmen der inhaltlichen Ergänzung der „Detailed Control Objectives“ wurden im Bereich „Plan & Organise“ insgesamt 16 Control Objectives ergänzt, im Bereich „Aquire & Implement“ sind es sechs und im Bereich „Delivery & Support“ acht. Schließlich wurde auch der Bereich „Monitor & Evaluate“ überarbeitet.

Bei eingehender Lektüre lässt sich feststellen, dass die Homogenität des CobiT-Ansatzes verbessert wurde und die praktische Arbeit mit dem Framework deutlich leichter fällt.

1.7 BlackBerry Bugs

Auf dem 22. Chaos Communication Congress des CCC (22C3) am 27.-30.12.2005 wurden von FX (Phenoelit) mehrere BlackBerry-Bugs vorgestellt. Die meisten der gefundenen Schwächen (u.a. Buffer Overflow bei JAD-Files, fehlerhafte TIFF-Anhänge) betreffen die Endgeräte und sind klassische Programmierfehler, wie sie fast täglich für zahlreiche Smartphones und PDAs gemeldet werden. Da ist es ein Qualitätsmerkmal, dass für BlackBerry-Handhelds bislang nur sehr wenige Bugs dieser Art entdeckt wurden.

Unschön könnten die von FX erwähnten Protokollfehler sein – leider gibt es bislang keine publizierten Unterlagen oder valide CERT-Meldungen dazu.

Alle anderen Schwachstellen betreffen ausschließlich die Funktionsfähigkeit von Spezialdiensten und sind schlimmstenfalls lästig, keiner davon aber sicherheitskritisch. Kein Grund zur Beunruhigung also – zumal man sich durch Software-Updates oder Sperrung dieser Dienste leicht vor solchen Angriffen schützen kann.

2 Secorvo News

2.1 Secorvo College aktuell

Die Bosch Sicherheitssysteme GmbH ist nach SAP, T-Systems und dem BSI seit dem 18.01.2006 neuer Ausbildungspartner.

Die nächste Gelegenheit zum Besuch eines Secorvo-College-Seminars bietet sich am 07.-10.02.2006 – vier Tage Intensivkurs rund um Public Key Infrastrukturen.

http://www.secorvo.de/college

2.2 ISO 27001-AaBvITG

Seit dem 19.01.2006 ist Stefan Gora vom BSI lizenzierter ISO 27001-Auditor auf Basis von IT-Grundschutz (AaBvITG).

2.3 KA-IT-Si wird fünf

Vor fast exakt fünf Jahren wurde die „Karlsruher IT-Sicherheitsinitiative“ von den Karlsruher Versicherungen und Secorvo aus der Taufe gehoben. Das Ziel: Verbesserung der IT- und Informationssicherheit vor allem mittelständischer Unternehmen der TechnologieRegion Karlsruhe. Seitdem hat die Initiative, die von zahlreichen Unternehmen gefördert wird, darunter Amec Spie, Junctim, Lampertz, L-Bank, neef it solutions, SAP, Sparkassen Informatik, Vogon und Würth Phönix, 17 Veranstaltungen mit über 400 Teilnehmern zu Themen der IT-Sicherheit durchgeführt.

Die Initiative hat sich nicht nur etabliert, sondern lockt immer wieder Interessierte aus ganz Deutschland nach Karlsruhe. Den fünften Geburtstag wird die KA-IT-Si mit einer Veranstaltung am 21.03.2006 feiern.

2.4 „DuD 2006” – 27.-28.03.

Der Klassiker – zum achten Mal treffen sich am 27.-28.03.2006 Autoren und Leser, Koryphäen und Verantwortliche auf der Jahrestagung der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“ in Berlin. Auch in diesem Jahr stehen spannende Themen auf dem Programm – von Blackberry Security über Honeynets, die Privacy-Initiative von Microsoft bis hin zu Whistleblower-Systemen. COMPUTAS wird wieder für ein angemessenes Ambiente Sorge tragen.

3 Veranstaltungshinweise

Januar 2006	
30.-31.01.	Net-ID 2006 (COMPUTAS, Berlin)
Februar 2006	
07.-10.02.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
14.-15.02.	Inside Windows Security (Secorvo College, Karlsruhe)
20.-21.02.	IT Governance 2006 (COMPUTAS, Köln)
20.-22.02.	Sicherheit 2006 – Schutz und Zuverlässigkeit (GI, Magdeburg)
28.02. - 03.03.	Black Hat Europe 2006 (Black Hat, Amsterdam/NL)
März 2006	
01.-02.03.	DFN-CERT Workshop (DFN-CERT, Hamburg)
09.-15.03.	CeBIT 2006 (Deutsche Messe AG, Hannover)
21.03.	KA-IT-Si-Geburtstagsfeier (KA-IT-Si, Karlsruhe)
27.-28.03.	Datenschutz und Datensicherheit – DuD 2006 (COMPUTAS, Berlin)
27.-31.03.	Information Security Management (Secorvo College, Karlsruhe)
28.-29.03.	D*A*CH Security 2006 (GI/Bitkom/TeleTrusT, Düsseldorf)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Februar 2006

Dirk Fox, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 2, 5. Jhrg. 2006
Stand 06. März 2006

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial:
The Show must go on

1 Security News

1.1 Frischzellenkur

1.2 Zertifikatsbedarf

1.3 13. DFN-CERT Workshop

1.4 Neue Malware-Allianz

1.5 Jäger und Sammler

1.6 GnuPG Bug

1.7 NIST Neuigkeiten

1.8 Anonym, aber langsam

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Awareness Symposium

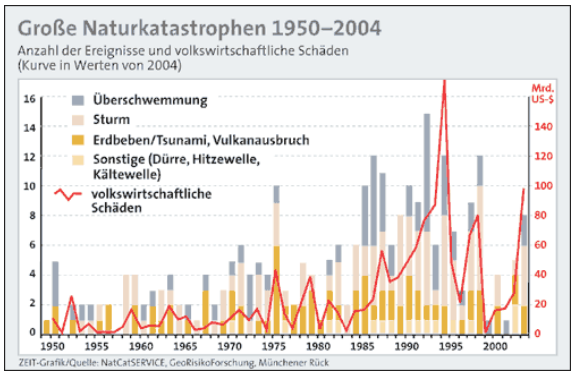
2.3 security-finder.de

3 Veranstaltungshinweise

Impressum

Editorial: The Show must go on

Ganz oben auf der CIO-Wunschliste steht derzeit die Notfallplanung: „Business Continuity“, gefordert von zahlreichen gesetzlichen Bestimmungen zur Risikovorsorge, ist zum Top-Thema avanciert. Nach den Ursachen dieser Entwicklung muss man nicht lange suchen: Schadenshöhe und Eintrittswahrscheinlichkeit von menschen- und naturverursachten Störfällen nehmen seit 20 Jahren drastisch zu (s. Abb.).



(Quelle: DIE ZEIT/Münchener Rück)

Ein Trend, der nicht nur Versicherungen zum Handeln zwingt. Da zahlreiche Schäden nicht versicherbar sind, steigt der Druck auf das IT-Management, auch bei bislang für unwahrscheinlich gehaltenen Störfällen wie längerem Stromausfall oder Wasser- und Sturmschäden eine Betriebsfortsetzung zu ermöglichen.

Das aber ist leichter gesagt als getan. Denn selten liegt eine aktuelle Übersicht maximal tolerierbarer Ausfallzeiten vor – oft ist nicht einmal verlässlich dokumentiert, welche IT-Anwendungen und -Systeme die Geschäftsprozesse tatsächlich benötigen. Und selbst da, wo Disaster Recovery-Maßnahmen getroffen wurden, existiert meist kein erprobtes Konzept für den Notbetrieb. Was aber hilft es, wenn bei Stromausfall die Kommunikationssysteme durch Handys ersetzt werden – alle wichtigen Telefonnummern aber im CRM gespeichert sind?

Nicht zuletzt müssen die Kosten der Maßnahmen im Rahmen bleiben, denn schon *Jean-Baptiste Molière* (1622-1673) wusste:

Die meisten Menschen sterben nicht an ihren Krankheiten, sondern an ihren Medikamenten.

1 Security News

1.1 Frischzellenkur

Am 31.01.2006 erschien Version 4.0 des populären Netzwerkscanners nmap – zwei Jahre nach Veröffentlichung der Vorgängerversion 3.50. Die neue Fassung enthält mehr als 230 Änderungen. Als Highlights stechen die Neuentwicklung der Port-Scanning-Engine und des Mechanismus zum Senden von Raw-Ethernet-Frames hervor. Dabei wurden Perfomance und Portabilität verbessert; insbesondere ist nmap nicht mehr auf die Socket-Implementierung des benutzten Betriebssystems angewiesen. Zusätzlich wurde die Datenbank zur Erkennung von Zielsystemen stark erweitert.

Erste Tests hinterlassen einen guten Eindruck. So wird die Einarbeitung in die neuen Features zur Entdeckungsreise – dabei ist die überarbeitete Dokumentation sehr hilfreich.

1.2 Zertifikatsbedarf

Dieser Winter verläuft unruhig für Zertifikatsanbieter auf dem deutschsprachigen Markt. Nachdem die deutsche TC Trustcenter GmbH am 14.09.2005 Insolvenz angemeldet hat, ist sie am 18.01.2006 von dem globalen Anbieter GeoTrust übernommen worden. Damit bleibt ein nach dem deutschen Signaturgesetz akkreditierter Zertifizierungsdiensteanbieter erhalten.

Dank einer Finanzspritze der österreichischen Großbanken gibt es auch für den Dienstanbieter a.trust GmbH nach dem Ausstieg von Telekom Austria und ÖNB wieder eine Perspektive. Beide Unternehmen kämpfen mit mangelnder Nachfrage nach qualifizierten Zertifikaten, deren Mehrwert einem Großteil der möglichen Nutzer noch nicht nahe zu bringen ist. Einen Bedarf für günstige Zertifikate scheint es hingegen zu geben, wie die Statistik der gemeinnützigen Organisation CAcert zeigt: Dort wurden seit 2004 knapp 100.000 kostenlose Zertifikate basierend auf einem Web of Trust ausgestellt.

1.3 13. DFN-CERT Workshop

Dass die Zahl 13 auch positiv belegt sein kann, zeigt die 13. Ausgabe des DFN-CERT Workshops „Sicherheit in vernetzten Systemen“, der am 01. und 02.03.2006 wie gewohnt in Hamburg stattfinden wird. Auch 2006 werden wieder über 300 Teilnehmer aus Forschung, Unternehmen und Behörden die interessanten Vorträge auf sehr hohem Niveau verfolgen.

Als eingeladener Sprecher wird diesmal Bill Cheswick vortragen – Titel seines Vortrags: „My Dad's Computer, Microsoft and the future of Internet Security“. Neben weiteren interessanten Themen wird Stefan Kelm von Secorvo Erfahrungen mit „Honeypots und Honeywall in der Praxis“ vorstellen.

1.4 Neue Malware-Allianz

In jüngster Vergangenheit wurden zahlreiche neue, immer leistungsfähigere Tools für Honeypots veröffentlicht (SSN 5/2005, SSN 8/2005). Ein prominentes Beispiel ist das Tool mwcollect. Dabei handelt es sich um ein kleines, auf Linux- und BSD-Systemen laufendes Tool, das Windows-Schwachstellen simuliert und somit Viren, Würmer und andere elektronische Ferkeleien („Malware“) sammeln kann. mwcollect öffnet bestimmte, oft von Malware verwendete Ports (zum Beispiel den TCP-Port 2745, einen der „Bagle“-Ports), simuliert dort bestimmte Dienste, nimmt Netzwerkverbindungen auf diesen Ports an und zeichnet sämtliche ankommenden Pakete auf. Die protokollierten Daten können anschließend detailliert ausgewertet werden.

Am 03.02.2006 wurde nun die Gründung der „mwcollect Alliance“ angekündigt. Mitglieder dieser Gruppe, vor allem Antivirus- und Schwachstellenforscher, sammeln mit mwcollect Schadsoftware und stellen diese einander für Analysen zur Verfügung. Deren Ergebnisse helfen, das Schadenspotenzial neuer Viren und Würmer besser einzuschätzen und entsprechende Sicherheitsmaßnahmen zu treffen. An der Allianz beteiligen kann sich jeder, der bereits ist, die selbst protokollierten Daten allen anderen Mitgliedern zur Verfügung zu stellen.

1.5 Jäger und Sammler

Die Sammler haben einen Dämpfer bekommen: Am 25.01.2006 stellte das Landgericht Darmstadt in der Berufung letztinstanzlich klar, dass T-Online bei Flatrate-Kunden die IP-Adressen unmittelbar nach Beendigung einer Verbindung löschen muss – und das jeweils übertragene Datenvolumen nicht einmal erheben darf. Für Zuwiderhandlungen wurde ein Ordnungsgeld von € 100.000 festgesetzt.

Ein Sieg des Datenschutzes auf ganzer Linie, könnte man meinen. Wenn da nicht die Jäger wären: Am 21.02.2006 setzte der EU-Rat die vom Europäischen Parlament im Dezember 2005 verabschiedete EU-Richtlinie zur Vorratsdatenspeicherung von Verbindungsdaten in Kraft. Damit sind deutsche Internet-Provider in spätestens drei Jahren zur sechs- bis 24-monatigen Speicherung anfallender Verbindungsdaten verpflichtet.

1.6 GnuPG Bug

Bei einer automatisierten Signaturprüfung akzeptiert die freie, PGP-kompatible Open-Source-Implementierung GnuPG unter Umständen eine ungültige Signatur, wie am 15.02.2006 auf der GnuPG-Mailingliste bekannt gemacht wurde: Findet der Prüfalgorithmus die Signatur nicht, liefert er den Wert „0“ zurück, der ohne Kontextauswertung als „success“ interpretiert werden kann. Betroffen sind alle Versionen bis 1.4.2; ein Update (1.4.2.1) wird empfohlen.

1.7 NIST Neuigkeiten

An dieser Stelle sei auf die zahlreichen Publikationen der Computer Security Division des amerikanischen National Institute of Standards and Technology (NIST) hingewiesen. Im ITL Bulletin für Februar 2006 wurde eine erheblich überarbeitete Version der „NIST Special Publication 800-40, Creating a Patch and Vulnerability Management Program“ vorgestellt, die eine systematische Vorgehensweise für die Etablierung eines regelmäßigen und zuverlässigen Patch-Managements empfiehlt. Im Anhang finden sich umfangreiche Tabellen mit Links zu Anbietern von Patch Management Software und Patch-Quellen der verbreitetsten Betriebssysteme, Client- und Server-Applikationen.

Zu vielen weiteren aktuellen Themen der IT-Sicherheit finden sich in der Publikationsübersicht hilfreiche Dokumente, von denen einige in der letzten Zeit aktualisiert worden sind. Die wichtigsten sind auch über den security-finder erreichbar.

1.8 Anonym, aber langsam

Neben dem (in den SSN 08/2005 vorgestellten) Projekt AN.ON, das wegen des Auslaufens der Fördermittel in Bälde kostenpflichtig werden wird, gibt es seit der Konferenz Shmoocon 2006 ein weiteres Anonymitätsprojekt: Das Privacy Operating System "Anonym.OS".

Diese Distribution, die als Live-CD verfügbar und in jedem Standard-PC bootfähig ist, basiert auf dem Sicherheitsbetriebssystem OpenBSD 3.8 und ist auf die Anonymisierung und Verschlüsselung von Netzverbindungen spezialisiert. Sie verwendet Tor als Gateway für das anonymisierte Internet. Gegenüber dem Netzumfeld tarnt sich Anonym.OS als "Windows XP Service Pack 2". Damit ist erstmals eine Anonymizer-Lösung verfügbar, die es Laien mit sehr geringen technischen Grundkenntnissen ermöglicht, sich einer Anonymisierungsinfrastruktur anzuschließen.

Allein die Performance des Tor-Netzwerkes trübt die Anwendbarkeit: Man fühlt sich spontan in die Zeiten der 1200-9600 Baud-Modemanbindungen zurückversetzt. Zur Verbesserung der Anonymitäts-Bandbreite hilft nur eines: Baut Tor-Server!

2 Secorvo News

2.1 Secorvo College aktuell

Über die Winterpause wurden alle „Bestseller“-Seminare von Secorvo gründlich über-

arbeitet. Das Ziel: Eine deutliche Ausweitung des Praxisanteils.

Das erste Seminar hat die Premiere nun hinter sich: Die Neufassung des PKI-Seminars Anfang Februar erreichte mit einer Gesamtnote von 1,4 eine sehr gute Bewertung. Insbesondere die Mischung aus Theorie und Praxis mit Demonstrationen, Workshops und der praxisnahen Aufbereitung der Themen in den einzelnen Vorträgen kam sehr gut an.

Ähnlich „frisch" präsentiert sich das Seminar „Information Security Management – von A(udit) bis Z(ertifizierung)" vom 03. bis 07.04.2006. Gleiches gilt für das vollständig neu konzipierte Seminar Kommunikationsschutz und Datensicherheit – intern, extern, mobil am 25. bis 27.04.2006.

Programme und Anmeldung (auch online): http://www.secorvo.de/college

2.2 Awareness Symposium

Vom 02. bis 03.05.2006 findet das inzwischen schon vierte „Security Awareness Symposium" in Karlsruhe statt. Wie in den Vorjahren werden zahlreiche Unternehmen ihre Aktivitäten zur Sensibilisierung der Mitarbeiter für Informationssicherheit vorstellen. Das Programm ist derzeit in Abstimmung – es sind wieder ideenreiche und anregende Präsentationen und Diskussionen zu erwarten. Schon jetzt können Sie sich die Teilnahme an diesem Event durch frühzeitige Anmeldung sichern.

2.3 security-finder.de

Die vor knapp einem Jahr freigeschaltete virtuelle Online-Bibliothek security-finder.de wächst und gedeiht: Knapp 600 Dokumente zu IT-Sicherheit und Datenschutz sind darin inzwischen zu finden, kategorisiert und versehen mit einer aussagekräftigen Zusammenfassung und Bewertung.

Für Interessierte gibt es nun einen kostenfreien „Schnupperzugang" (Benutzer: gast, Passwort: gast), über den Struktur und Aufbau des security-finders und etwa 60 ausgewählte Dokumente zugänglich sind.

3 Veranstaltungshinweise

Februar 2006	
28.02. - 03.03.	Black Hat Europe 2006 (Black Hat, Amsterdam/NL)
März 2006	
01.-02.03.	DFN-CERT Workschop (DFN-CERT, Hamburg)
09.-15.03.	CeBIT 2006 (Deutsche Messe AG, Hannover)
27.-28.03.	Datenschutz und Datensicherheit – DuD 2006 (COMPUTAS, Berlin)
28.-29.03.	D*A*CH Security 2006 (GI/Bitkom/TeleTrusT, Düsseldorf)
April 2006	
03.-07.04.	Information Security Management (Secorvo College, Karlsruhe)
25.-27.04.	Kommunikationsschutz und Datensicherheit (Secorvo College)
Mai 2006	
02.-03.05.	Security Awareness Symposium 2006 (Secorvo, Karlsruhe)
09.-10.05.	IT-Sicherheitsaudits (Secorvo College, Karlsruhe)
10.-11.05.	Datenschutzkongress 2006 (Euroforum, München)
11.05.	IT-Outsourcing sicher gestalten (Secorvo College, Karlsruhe)
16.-18.05.	Forensic Lab (Secorvo College, Karlsruhe)
28.05. - 01.06.	Eurocrypt 2006 (IACR, St. Petersburg/RU)

Aktuelle Veranstaltungsübersicht: http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")
Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
März 2006

Dirk Fox, Stefan Gora, Kai Jendrian, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 3, 5. Jhrg. 2006
Stand 28. März 2006

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Der Grüffelo

1 Security News

1.1 Symantec Threat-Report

1.2 Neues BSI-GSHB online

1.3 Virenverseuchte Katzen?

1.4 Bürger-CERT

1.5 déjà-vu: Punkt im Pfad

1.6 Berechtigungseskalation

1.7 „Setzen, Sechs!“

1.8 Datenbüchsen öffnen

1.9 Open Source Inspektion

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Wem die Stunde schlägt

2.3 “DuD” im security-finder

3 Veranstaltungshinweise

Impressum

Editorial: Der Grüffelo

„Zum Grüffelo? Sag, was ist das für ein Tier?“
„Den kennst Du nicht? Dann beschreib ich ihn Dir...“
Axel Scheffler, Julia Donaldson

Wie alt sind Ihre Kinder? Zwischen vier und zwölf? Dann kennen Sie zweifellos das wunderschöne Kinderbuch „Der Grüffelo“. Allen anderen sei die Geschichte schnell erzählt: Auf dem Weg durch den Wald begegnet die Maus ihren ärgsten Feinden – dem Fuchs, der Eule und der Schlange. Listig schlägt sie alle drei mit der Behauptung in die Flucht, sie sei mit dem Grüffelo verabredet – einem schrecklichen Tier, das sich bevorzugt von Fuchsspieß, gezuckerter Eule und Schlangenpüree ernähre.

Überrascht muss die Maus jedoch feststellen, dass es den Grüffelo tatsächlich gibt – und er genau so aussieht, wie sie ihn den Tieren in schillernden Worten beschrieben hat. In höchster Not behauptet sie, alle Tiere im Wald hätten Angst vor ihr – und beweist es, indem sie mit ihm Schlange, Eule und Fuchs aufsucht. Die nehmen sofort Reißaus, der Grüffelo aber ist tief beeindruckt – und ergreift selbst die Flucht, als die Maus erklärt, sie verspüre plötzlich Appetit auf eine Portion Grüffelogrütze ...

Die Erfolgsstrategie der Maus ist so einfach wie entwaffnend – der japanischen Kampfkunst Aikido ähnlich, die die Kraft des Angreifers nicht blockt, sondern umlenkt. Eine Technik, der sich auch die Scam Baiter bedienen, die die Versender von Betrugs-E-Mails der „Nigeria-Connection“ in Korrespondenzen verstricken und zur Versendung eigener Fotos verleiten. Möglicherweise ist dies eine Erfolgsstrategie im rechtsvollzugsarmen Cyberspace. Man stelle sich vor: Empfänger von Phishing-Mails, die die Betrüger mit falschen TANs auf präparierte Konten locken, als vorgebliche Geldboten Polizeikonten zur Überweisung anbieten oder mit Honeypots Hackern einen Crack vortäuschen – und beim Datendownload den Sound „Hab’ mich beim Hacken erwischen lassen“ installieren.

Keine Selbstjustiz – aber ein bisserl Sand im sich gerade organisierenden kriminellen Online-Getriebe könnte reinigend wirken.

1 Security News

1.1 Symantec Threat-Report

Am 07.03.2006 veröffentlichte Symantec die Ergebnisse ihres Sicherheitsreports für die zweite Jahreshälfte 2005. Danach ist ein deutlicher Anstieg der Internetkriminalität festzustellen, die vor allem professioneller und profitorientierter geworden ist. Insbesondere die Gefährdungen durch Bot-Netze und Schwachstellen in Webanwendungen haben deutlich zugenommen. Phishing bleibt eine ernst zu nehmende Bedrohung. Erschreckend: Die Entwicklung der Zahl neu entdeckter Viren und Würmer.

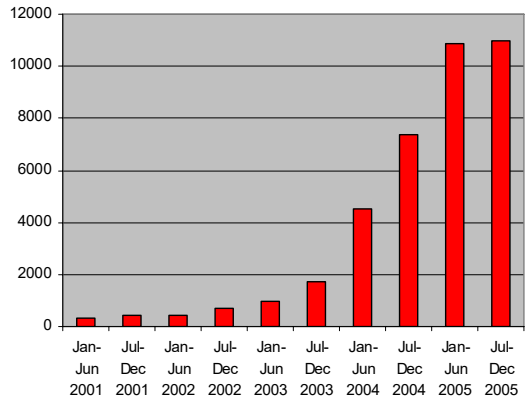


Abb.: Neue Viren und Würmer [Symantec]

1.2 Neues BSI-GSHB online

Die in den SSN 01/2006 vorgestellte aktualisierte Version des IT-Grundschutzhandbuches mit Unterteilung in IT-Grundschutz-Standards (BSI-Standard 100-1: Managementsysteme für Informationssicherheit, BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz) und IT-Grundschutzkataloge ist seit Anfang März online als PDF-Version verfügbar. Das Information Security Management basiert nun auf dem internationalen Standard ISO 27001; weite Teile des bisherigen IT-GSHB sind neu sortiert in den Katalogen zu finden. Die Änderungen wurden am 14.03.2006 auf der CeBIT vorgestellt.

1.3 Virenverseuchte Katzen?

Ja, Sie lesen richtig – mit Vogelgrippe hat dieser Beitrag allerdings rein gar nichts zu tun. Auf der diesjährigen Percom (IEEE International Conference on Pervasive Computing and Communications, 13.-17.03. 2006) wurde das Paper „Is your cat infected with a Computer Virus?" von Andrew Tanenbaum et al. zum Thema RFID-Viren mit dem Best Paper Award ausgezeichnet. Als proof-of-concept wurde ein Virus entwickelt, der sich in den 127 Zeichen fassenden Transponderspeicher eines Chips einschleusen lässt und die RFID-Middleware von Oracle infiziert.

1.4 Bürger-CERT

In seinem Newsletter vom 03.03.2006 stellt das BSI das gemeinsam mit Mcert gestartete Projekt Bürger-CERT vor. Ziel ist es, Bürger und kleine Unternehmen vor aktuellen Gefährdungen der IT-Sicherheit zu warnen und zu informieren. Die kostenlos herausgegebenen technischen Warnungen unterscheiden sich bislang jedoch kaum von anderen ebenfalls kostenfreien Diensten wie beispielsweise den DFN-CERT Advisories.

1.5 déjà-vu: Punkt im Pfad

Am 10.03.2006 berichtete Heise über eine von Reed Arvin entdeckte Möglichkeit, Berechtigungen durch ein installiertes ActiveState Perl zu eskalieren. ActiveState Perl stellt bei der Installation das Verzeichnis mit den Binaries an den Beginn des Systemsuchpfades und räumt dort allen Benutzern Schreibrechte ein. Dadurch kann ein nicht-privilegierter Benutzer einem Administrator beliebige Programme oder sogar DLLs unterschieben, die dann im Kontext des Administrators ausgeführt werden.

Dieses Verhalten ist unschön – aber alles andere als neu. Schon am 18.03.1993 wurde in der Unix-FAQ 2.13 davor gewarnt, den ´.´ (d. h. das aktuelle Verzeichnis, in dem sich beliebige Benutzeranwendungen befinden können) im Pfad zu führen. Auch 13 Jahre danach ist bei allen Betriebssys-

temen angeraten, den Pfad und darüber mögliche Kompromittierungsmöglichkeiten genau im Auge zu behalten.

1.6 Berechtigungseskalation

Ein weiteres Beispiel von Eskalations-Berechtigungen wurde von Ramon Kukla bei der Antivirensoftware Antivir von Avira (ehemals H+B EDV) festgestellt und am 11.03.2006 in full-disclosure veröffentlicht.

Die Fehlerursache liegt hier im Dienst „AntiVir PersonalEdition Classic Planer“, einem zum Virenschutz gehörenden Zeitplanungsdienst, der im System-Kontext läuft. Bei Updates wird über diesen Dienst ein Report erzeugt, der mit der Windows-Anwendung Notepad angezeigt wird – auch mit Systemberechtigungen, versteht sich. Ein Benutzer kann mit diesem Notepad System- und Konfigurationsdateien öffnen und ändern, obwohl er dazu gar keine Berechtigung besitzt. Auch die kostenpflichtige Premium-Variante der Lösung soll betroffen sein; eine Aktualisierung wird daher dringend empfohlen.

1.7 „Setzen, Sechs!“

Man könnte es für eine Satire halten: Die Washington Post berichtete am 15.03.2006 über die Ergebnisse der jährlichen Analyse der Sicherheit staatlicher Stellen in den USA. Eine der am schlechtesten bewerteten Behörden ist das Department for Homeland Security: Sie erhielt ein glattes „F“ für „failed“ – im dritten Jahr in Folge. Pikanterweise ist diese Behörde unter anderem für Terrorbekämpfung und „cyber security“ zuständig.

1.8 Datenbüchsen öffnen

Bereits im Oktober 2005 wurde der NIST Interagency Report 7250 Cell Phone Forensic Tools: An Overview and Analysis veröffentlicht. Dieser Bericht ist angesichts der am 27.02.2006 gemeldeten Handy-Trojaner brandaktuell: Er führt auf über 180 Seiten in guter und sehr detaillierter Form in die für forensische Analysen von mobilen Geräten verfügbare Software ein.

Insgesamt wurden 12 Toolkits evaluiert. Die im Dokument betrachteten Telefonie-Geräte haben teilweise einen engen Bezug zu Personal Digital Assistants (PDA), was auch durch die ihnen zu Grunde liegenden Betriebssysteme deutlich wird (Windows Mobile, Palm OS, RIM OS und Symbian).

Speziell für Manager und technische Entscheider, aber auch für Angreifer liest sich das Dokument zwischen den Zeilen wie eine Offenbarung hinsichtlich der Machbarkeit von Angriffen auf sensitive Daten in Mobiltelefonen. Bleibt zu ergänzen, dass ein starker Trend zu beobachten ist, Login/ Passwort-Kombinationen, PINs, TANs etc. auf solchen Geräten zu speichern. Zweifellos zur großen Freude derjenigen, die ein solch gut gefülltes Osterei „finden“.

1.9 Open Source Inspektion

Die ersten Ergebnissen der Open Source-Analyse der US-Regierung lesen sich auf den ersten Blick wie eine weitere Metrik, die die Welt nicht braucht. Die Ergebnisse liegen in einer Tabelle online vor und geben die Zahl der festgestellte Bugs pro 1.000 Zeilen Code an.

Die Messbarkeit im Bereich Sicherheit ist ein wichtiges, aber schwieriges Feld. Erfolgreiche Metriken erlauben konkrete Aussagen über betrachtete Entitäten. Auf den ersten Blick scheint die Metrik Fehler/ kLoC (1.000 Lines of Code) diesbezüglich wenig aussagekräftig. Sie ermöglicht zwar eine grobe Einschätzung, lässt aber keine Vergleichbarkeit zwischen den Projekten zu. Beispielsweise kann ein schwerer Fehler im Betriebssystem fataler sein als zehn leichte Bugs im Browser.

Der Ansatz der Autoren von Coverity geht jedoch über die reine Generierung von Metriken hinaus und nimmt mit den Verantwortlichen der betroffenen Projekte Kontakt auf, erläutert die festgestellten Schwachstellen und trägt so ein gutes Stück zur Verbesserung der Qualität von Open Source bei. Detailliertere Reports können auf Anfrage und nach erfolgter Registrierung bei Coverity heruntergeladen werden.

2 Secorvo News

2.1 Secorvo College aktuell

Der persönliche Kontakt zu den Referenten und die Möglichkeit, individuelle Fragestellungen in die Vorträge einfließen zu lassen, werden von unseren Seminarteilnehmern sehr geschätzt. Ein Mehrwert, dem wir mit unserem neuen Angebot Individuelles Coaching zukünftig noch mehr Gewicht verleihen. Sie erhalten im Seminarverlauf zusätzlich die Möglichkeit, individuelle Fragestellungen im „Vier-Augen-Gespräch“ mit einem ausgewählten Secorvo Security Consultant zu diskutieren.

www.secorvo.de/college

2.2 Wem die Stunde schlägt

Die Geschichte der Hans Unsicher GmbH, Ein (IT-)Drama, wie das Leben es schreibt. Sie erzählt vom Umgang des Mittelstands mit doch nicht ganz so unwahrscheinlichen Risiken („Uns wird schon nichts passieren“), vom Leichtsinn in Raten, versteckt in kleinen, alltäglichen Unternehmensentscheidungen: Ein etwas anderes Theaterstück über die ganz normalen Risiken des Unternehmerdaseins.

Uraufführung am 23.05.2006 in Rust (Anmeldung und nähere Informationen).

2.3 „DuD” im security-finder

Die von Secorvo entwickelte virtuelle Bibliothek zu IT-Sicherheit und Datenschutz erhält exklusive Inhalte: Ab dem 01.04.2006 werden Abonnenten des security-finder.de ausgewählte Beiträge aus früheren Jahrgängen der im Vieweg-Verlag erscheinenden Fachzeitschrift „Datenschutz und Datensicherheit“ (DuD) digital zugänglich gemacht – eine starke Bereicherung der inzwischen auf über 600 sorgfältig ausgewählten und kommentierten Publikationen angewachsenen elektronischen Fachbibliothek.

3 Veranstaltungshinweise

März 2006	
27.-28.03.	Datenschutz und Datensicherheit – DuD 2006 (COMPUTAS, Berlin)
28.-29.03.	D*A*CH Security 2006 (GI/Bitkom/TeleTrusT, Düsseldorf)
April 2006	
03.-07.04.	Information Security Management (Secorvo College, Karlsruhe)
25.-27.04.	Kommunikationsschutz und Datensicherheit (Secorvo College)
29.04. - 02.05.	15th EICAR Annual Conference (Eicar, Hamburg)
Mai 2006	
02.-03.05.	Security Awareness Symposium 2006 (Secorvo, Karlsruhe)
09.-10.05.	IT-Sicherheitsaudits (Secorvo College, Karlsruhe)
10.-11.05.	Datenschutzkongress 2006 (Euroforum, München)
11.05.	IT-Outsourcing sicher gestalten (Secorvo College, Karlsruhe)
16.-18.05.	Forensic Lab (Secorvo College, Karlsruhe)
23.05.	„Wem die Stunde schlägt“ (amec spie/Lampertz, Rust)
28.05. - 01.06.	Eurocrypt 2006 (IACR, St. Petersburg/RU)
30.05. - 01.06.	Web-Application Security (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)
Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
April 2006

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 4, 5. Jhrg. 2006
Stand 27. April 2006

ISSN 1613-4311

http://www.secorvo-security-news.de/

Inhalt

Editorial: Small World!

1 Security News

1.1 GnuPG legt nach

1.2 ... und keiner merkt's

1.3 IPv6-Werkzeugkasten

1.4 VM Based Rootkits

1.5 Selbsthilfe-Ecke

1.6 Kapitulation

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Security Awareness

2.3 Honeypots betreiben

2.4 Veranstaltungshinweise

Impressum

Editorial: Small World!

Wir kennen uns alle. Wenn nicht direkt, so über maximal sechs Ecken: Die These der „six degrees of separation" aus der 1929 erschienenen Kurzgeschichte *Chains* des ungarischen Schriftstellers Frigyes Karinthy (1887-1938) erlangte 38 Jahre später durch den Psychologen Stanley Milgram (1933-84) Berühmtheit, der dafür den Begriff Kleine-Welt-Phänomen prägte. Seitdem beschäftigt sie nicht nur Forscher wie Duncan J. Watts, die Karinthys These per Modell zu bestätigen versuchen, sondern wurde erfolgreich in Geschäftsmodelle (wie z. B. Online-Kontaktnetzwerke) umgesetzt.

Bewiesen ist Karinthys These bisher nicht, widerlegt werden konnte sie allerdings auch nicht. Selbst in OpenBC, mit einer Million Benutzern eine der erfolgreichsten Online-Kontaktbörsen, lässt sich auch zu Neu-Usern keine Kontaktkette finden, die länger ist als sechs.

Auch Vertrauensnetze wie das „Web of Trust" von PGP profitieren von kurzen Vertrauensketten – je kürzer, desto größer das Vertrauen in die Identität eines fremden Schlüsselinhabers. Voraussetzung für diese enge Vermaschung ist dabei die Verknüpfung der Beziehungsdaten: Aus mehr Beziehungen resultiert eine kürzere Kette – und damit mehr Vertrauen.

Sollten wir also mehr Beziehungswissen preisgeben, um mehr Vertrauen zu erreichen? Das zu glauben wäre ein typischer Naturalistischer Fehlschluss – ein unzulässiges Ableiten von Soll- aus Ist-Zuständen. Denn je enger wir „zusammenrücken", desto wichtiger wird der Schutz der Privatsphäre – sofern wir eine erhalten wollen.

Auch in der Online-Enzyklopädie Wikipedia wirkt das Small-World-Phänomen („Six degrees of Wikipedia"): „Kleine-Welt-Phänomen" und „Naturalistischer Fehlschluss" sind über fünf Links verbunden (Soziale Netzwerke – Soziologie – Philosophie – Sprachphilosophie – G. E. Moore). Bis zum „Datenschutz" ist die Kette allerdings einen Klick länger (Soziale Netzwerke – Herrschaft – Gesetze – Grundgesetz – Grundrechte – Informationelle Selbstbestimmung).

1 Security News

1.1 GnuPG legt nach

Am 03.04.2006 ist eine neue Version der freien Krypto-Software GnuPG erschienen. Während frühere Versionen in erster Linie Sicherheitslücken bereinigten, enthält Version 1.4.3 etliche interessante neue Features: Neben dem deutlich verbesserten Management von GPG-Schlüsseln unterstützt GnuPG nun einige der DNSSEC-Erweiterungen direkt. Dabei geht es in erster Linie darum, kryptographisches Schlüsselmaterial sowie Zertifikate im DNS speichern und von dort abrufen zu können.

GnuPG kann jetzt auf diese Erweiterungen zugreifen. Interessant ist dies deshalb, weil DNSSEC zwar schon seit Jahren „kurz vor der Einführung steht“ (vgl. SSN 05/2004, SSN 04/2005), bis heute aber nur wenig bis gar kein Gebrauch davon gemacht wird – ein Grund dafür war die mangelnde DNSSEC-Unterstützung in den Anwendungen.

1.2 ... und keiner merkt's

Wie erst am 31.03.2006 in einem Report veröffentlicht, waren die Root-Nameserver im Februar dieses Jahres wieder einmal Ziel einer großflächigen Denial-of-Service-Attacke. Die Angreifer setzten Bot-Netze ein, um die DNS-Server mit übergroßen Paketen zu beschäftigen.

Pikanterweise versuchten die Angreifer eine recht neue Erweiterung des DNS-Protokolls auszunutzen: EDNS0 wurde erst im Rahmen der DNSSEC-Aktivitäten spezifiziert und implementiert, um die ehemals geltende Größenbeschränkung von 512 Bytes pro DNS-Paket aufzuheben, damit beispielsweise kryptographische Schlüssel via DNS transportiert werden können (s.o.).

Wie schon bei früheren Angriffen wirkte die Attacke nur bei schlecht konfigurierten Nameservern. Geholfen hätte auch diesmal die korrekte Konfiguration der Nameserver gemäß längst bekannten Best-Practice-Methoden – nicht besondere Schutzmechanismen à la DNSSEC. Interessanterweise hat jedoch auch diesen Angriff kaum ein Endbenutzer wahrgenommen...

1.3 IPv6-Werkzeugkasten

Seit der cansecwest/core06 ist das dort Anfang April 2006 vorgestellte „IPv6 Attack Toolkit“ von THC/VH auch für die Allgemeinheit zur praktischen Verwendung verfügbar. Die darin enthaltenen 12 Spezialwerkzeuge und die zu Grunde liegende „IPv6 packet factory library“ demonstrieren u. a. Schwachstellen in IPv6, die auf Angriffsstrategien wie Denial-of-Service und Man-in-the-Middle beruhen. Die Packet Library selbst sowie der verfügbare Sourcecode (derzeit noch auf Linux beschränkt) ermöglichen sowohl die einfache Erstellung weiterer „Werkzeuge“, als auch die Änderung der Paketsignaturen, um Intrusion Detection Systemen zu entwischen.

Mit diesem Werkzeugkoffer existiert erstmals eine abgestimmte Tool-Sammlung für Netzwerksicherheitsanalysen von IPv4 mit parallel zugelassenem IPv6.

1.4 VM Based Rootkits

Eine neue Variante von Rootkits wurde von Forschern der Michigan University und Microsoft Research vorgestellt: Durch die Kombination von Rootkits mit der Technik virtueller Maschinen entstehen perfide aber auch technisch anspruchsvolle Angriffsmöglichkeiten. Die im Rahmen des Projekts „SubVirt“ auf Basis von VirtualPC und VMware entwickelten Tools übernehmen dabei komplett die angegriffenen Systeme unter Windows XP oder Linux und emulieren das ursprüngliche Betriebssystem innerhalb einer virtuellen Maschine. Eine zweite virtuelle Maschine kann für beliebige Angriffszwecke wie beispielsweise den Betrieb eines Phishing Webservers verwendet werden.

Das Fatale an dieser Technik ist, dass die Übernahme für den Benutzer nicht erkennbar ist: Da die Benutzermaschine durch die VM-Umgebung kontrolliert wird, fanden die Forscher in ihren Untersuchungen lediglich den deutlich verlängerten Bootvorgang und

eine verminderte 3D-Leistung als Indizien. Da solche Virtual Machine Based Rootkits (VMBRs) sogar Shutdown-Prozesse emulieren und das System in standby versetzen, ist selbst ein Neustart des Benutzersystems unter Kontrolle des Rootkits. Nur wenn das System wirklich „aus“ ist, kann von einem alternativen Medium gebootet und das Rootkit festgestellt werden.

Die Ergebnisse der Forschungen und weitere Schutzmaßnahmen sind im Paper „SubVirt: Implementing malware with virtual machines" zusammengefasst, welches für das diesjährige IEEE Symposium on Security and Privacy eingereicht wurde.

1.5 Selbsthilfe-Ecke

Gegen Spam gibt es eine Reihe von technischen Gegenmaßnamen wie Spamfilter und Greylisting. Eine der wirksamsten Methoden ist aber immer noch, Vorsicht bei der Preisgabe oder Weitergabe seiner E-Mail-Adresse walten zu lassen.

Aber was tun, wenn man sich Informationen zusenden lassen oder auf einer Website registrieren will? Ein Weg ist die Nutzung von Einmal- oder Wegwerf-E-Mail-Adressen, vorgeschlagen von Stefan Kelm auf dem Anti-Spam-Symposium 2003. Dabei helfen Angebote wie Spamgourmet: Dort können temporäre E-Mail-Adressen eingerichtet werden, die eingehende E-Mails an die „echte“ eigene E-Mail-Adresse weiterleiten. Nach einer zuvor festgelegten Zahl eingegangener E-Mails wird die Adresse vom Anbieter automatisch gelöscht. Dem Anbieter muss man allerdings vertrauen, dass er die echten Adressen keinem Dritten preisgibt.

1.6 Kapitulation

Das Bundeskabinett hat am 25.04.2006 einen Gesetzentwurf aus 16 Einzelmaßnahmen zum „Abbau bürokratischer Hemmnisse insbesondere der mittelständischen Wirtschaft“ verabschiedet. Darunter: Die Anhebung des Schwellwerts für die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten. Die soll zukünftig nur noch bestehen, wenn mindestens 10 (und nicht wie bisher fünf) Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind. Schon am 22.07. 2005 hatten die Länder Hessen und Niedersachsen einen Gesetzentwurf im Bundesrat eingebracht, der das Quorum auf mindestens 20 Arbeitnehmer anheben will; am 23.09.2005 winkte der Bundesrat diesen Entwurf durch. Die Festlegung des Kabinetts auf ein Quorum von 10 riecht verdächtig nach Formelkompromiss – eine inhaltliche Begründung gibt es nicht.

Tatsächlich wirkt die vermeintliche Entbürokratisierungsmaßnahme wie eine Kapitulation vor dem faktischen Vollzugsdefizit in kleinen und Kleinstunternehmen: Die wenigsten kommen bisher der seit 1978 bestehenden Pflicht zur Berufung eines betrieblichen Datenschutzbeauftragten nach, und selbst das oft nur pro forma.

Allerdings war es noch nie ein Ausdruck besonderer Weisheit, bedauernswerte Ist-Zustände zu Soll-Zuständen zu erheben (siehe Editorial). Zwar würden durch diese Regelung über 90 % der deutschen Unternehmen von der Verpflichtung befreit – so viele der insgesamt knapp drei Millionen Betriebe beschäftigen maximal 10 Mitarbeiter. Bestehen bleiben jedoch alle anderen Verpflichtungen: die Auskunftspflichten gegenüber den Betroffenen, die Festlegung und Einhaltung von Löschfristen, die Prüfung der Rechtmäßigkeit und Ordnungsmäßigkeit der Verarbeitung, die Schulung und Verpflichtung der Mitarbeiter auf das Datengeheimnis sowie eine gesetzmäßige Vertragsgestaltung bei Auftragsdatenverarbeitung und Übermittlung in Drittländer. Wer aber wird zukünftig in diesen Unternehmen die Sachkunde besitzen, für die Einhaltung des BDSG zu sorgen?

Bedenklich ist, dass hier mit dem Argument der Entbürokratisierung der Schutz des zentralen Grundrechts der freien Entfaltung der Persönlichkeit geschwächt wird. Denn außer Frage steht, dass die Konstruktion des betrieblichen Datenschutzbeauftragten in Deutschland erheblich zum international vergleichsweise hohen Schutz personenbezogener Daten beiträgt.

2 Secorvo News

2.1 Secorvo College aktuell

Gleich zwei neue Seminare stehen im Mai auf der Agenda von Secorvo College:

- IT-Sicherheitsaudits in der Praxis führt am **09.-10.05.2006** in die Grundlagen aussagefähiger Sicherheitsanalysen ein – von der Planung über die technische und organisatorische Prüfung bis zu Tools, rechtlichen Rahmenbedingungen und Praxiserfahrungen.
- IT-Outsourcing sicher gestalten trägt der wachsenden Bedeutung von Sicherheitsfragen bei der Auslagerung von IT-Prozessen Rechnung. Rechtsfragen, die Gestaltung von SLAs und die Einbindung in das Sicherheitsmanagement stehen im Zentrum des eintägigen Seminars am **11.05.2006**.

Programme und Online-Anmeldung:
www.secorvo.de/college

2.2 Security Awareness

Am 02.-03.05.2006 findet das inzwischen vierte „Security Awareness Symposium“ statt – mit Praxisberichten von Areva NP, DAK, SwissRe und T-Systems und einem intensiven Erfahrungsaustausch. Für Kurzentschlossene empfehlen wir die Online-Anmeldung – es gibt nur noch wenige freie Plätze.

2.3 Honeypots betreiben

Honeypots und Honeynets sind bereits seit einiger Zeit als effektive Sicherheitskomponente bekannt; dennoch waren viele Unternehmen sehr zurückhaltend, wenn es um den Aufbau entsprechender Honeypot-Umgebungen innerhalb der eigenen Infrastruktur ging. Dies scheint sich jetzt zu ändern: immer mehr Nachfragen haben uns veranlasst, die von Secorvo bereits seit einiger Zeit angebotenen Dienstleistungen in diesem Bereich in einem Leistungsangebot zusammen zu stellen und zu veröffentlichen.

2.4 Veranstaltungshinweise

Mai 2006	
02.-03.05.	Security Awareness Symposium 2006 (Secorvo, Karlsruhe)
09.-10.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
10.-11.05.	Datenschutzkongress 2006 (Euroforum, München)
11.05.	IT-Outsourcing sicher gestalten (Secorvo College, Karlsruhe)
23.05.	„Wem die Stunde schlägt“ (amec spie/Lampertz, Rust)
28.05. - 01.06.	Eurocrypt 2006 (IACR, St. Petersburg/RU)
30.05. - 01.06.	Web-Application Security (Secorvo College, Karlsruhe)
Juni 2006	
06.-09.06.	ETRICS 2006 (Univ. Freiburg)
20.-22.06.	Live Hacking Lab (Secorvo College, Karlsruhe)
21.-22.06.	Midvision 2006 (Karlsruher Messe)
25.-30.06.	Annual FIRST Conference 2006 (FIRST, Baltimore/US)
27.-28.06.	Lotus Notes Security (Secorvo College, Karlsruhe)
29.06.	Lotus Notes Security – advanced (Secorvo College, Karlsruhe)
Juli 2006	
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/CA)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de/

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)
Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Mai 2006

Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 5, 5. Jhrg. 2006
Stand 23. Mai 2006

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Zauberlehrlinge

1 Security News

1.1 Sicherheitsstudie 2006

1.2 DoD-Sicherheitslücken

1.3 IT-Grundschutz News

1.4 Codename Secure Blue

1.5 GPG-Schutz für E-Mails

1.6 Behörden-Desktop

1.7 Hase und Igel Reloaded

1.8 Zukunftsblick

2 Secorvo News

2.1 Secorvo College aktuell

2.2 SAS 2006 – Nachlese

2.3 Wer haftet?

3 Veranstaltungshinweise

Impressum

Editorial: Zauberlehrlinge

Seine Wort und Werke merkt ich und den Brauch
und mit Geistesstärke, tu ich Wunder auch.

Sie erinnern sich – es war einmal... Nein, nicht Ihre Deutschstunde, sondern die Diskussion der Entwürfe des deutschen Signaturgesetzes. Zehn Jahre ist es her, dass sich die Hoffnungen des deutschen eCommerce auf die vertrauensbildende Wirkung des 10-seitigen Gesetzestextes richteten. Noch im Evaluierungsbericht schrieb die Bundesregierung dem Signaturgesetz „eine Lokomotivfunktion für den Einsatz und die Verbreitung digitaler Signaturen“ zu.

In der Erwartung von Millionen Signaturzertifikaten wurden seitdem erhebliche Summen in Trust Center investiert, die „elektronische Form“ im BGB verankert und eine eigene Aufsichtsbehörde geschaffen.

Immer neue Güsse bringt er schnell herein,
Ach! und hundert Flüsse stürzen auf mich ein.

Allein: Der erhoffte Durchbruch blieb aus – die Lokomotive zog nicht. Darauf reagierte der Bund mit konfusen neuen Signatur-Kreationen (SSN 02/2003), verstärktem Aktionismus wie dem Signaturbündnis und der Erfindung vermeintlicher Killer-Applikationen wie der elektronischen Steuererklärung Elster (tatsächlich mit SSL realisiert) oder der Konzeptidee Jobcard – ohne Erfolg.

Ein verruchter Besen, der nicht hören will!
Stock, der du gewesen, steh doch wieder still!

Sieben akkreditierte Zertifizierungsdiensteanbieter existierten zu Hochzeiten. Nun stoppte auch die Datev die Ausgabe qualifizierter Zertifikate: Der Nutzen war „schwer zu vermitteln“, die wenigen ausgestellten Zertifikate rechtfertigten die Kosten nicht.

Herr, die Not ist groß!
Die ich rief, die Geister werd ich nun nicht los.

Die Reaktion des Marktes ist unzweideutig: Fortgeschrittene Signaturen genügen in der Praxis fast immer, das Restrisiko wiegt die erforderliche Mehrinvestition in qualifizierte meist nicht auf. Zeit zur Einsicht und zum Umsteuern: Regulatives Beharren wird den Erfolg nicht herbeizwingen – und ist in einer Marktwirtschaft nie eine gute Idee.

"In die Ecke, Besen, Besen! Seids gewesen.“

1 Security News

1.1 Sicherheitsstudie 2006

Seit 1991 wird – gesponsert durch das Department of Trade and Industry (DTI) – alle zwei Jahre eine Studie zu Sicherheitsvorfällen in Großbritannien erstellt (SSN 04/2002). Diese Studien dienen Unternehmen als Informationsquelle und zur Einschätzung des unternehmensrelevanten Risikos.

Der aktuelle, von PwC erstellte „Information Security Breaches Survey 2006" wurde Ende April veröffentlicht. Obwohl die Zahl betroffener Firmen gegenüber dem Vorjahr gesunken ist, stiegen die Anzahl der insgesamt gemeldeten Sicherheitsvorfälle und der Mittelwert der Schäden (um 20 % auf 12.000 £). Bei „worst-case incidents", insbesondere in Konzernen, lag der Mittelwert sogar bei 90.000 £. 68 % der befragten Unternehmen erwarten eine Zunahme der Sicherheitsvorfälle.

1.2 DoD-Sicherheitslücken

Wie das Pentagon am 28.04.2006 in einer Stellungnahme einräumte, wurde in ein öffentliches System der vom Militär genutzten Krankenversicherungsanwendung TRICARE eingebrochen. Dabei konnten zahlreiche, auch personenbezogene Daten abgezogen werden. Alle potentiell betroffenen Personen wurden informiert und über die Gefahr aufgeklärt, möglicherweise Opfer eines Identitätsdiebstahls zu werden.

Eine erneute Peinlichkeit, nachdem das Department for Homeland Security im März für ihr Sicherheitsniveau das dritte „failed" in Folge kassiert hatte (SSN 03/2006). Immerhin kündigte das Department of Defense (DoD) an, weiterte Schutzmaßnahmen zu ergreifen.

1.3 IT-Grundschutz News

Nach den aktuellen BSI-Standards (SSN 01/2006) wurden im April auch die Grundschutzkataloge (Bausteine, Maßnahmen, Gefährdungen) auf den Webseiten des BSI im HTML-Format online gestellt. Die vollständigen Grundschutzkataloge können jetzt auch als ZIP-Datei geladen werden.

Zur Erleichterung der Zuordnung von ISO 27001 und IT-Grundschutz publizierte das BSI Ende April eine tabellarische Gegenüberstellung (19.04.2006). Die umfassende Tabelle stellt zum Einen dar, wie die neue Struktur des IT-Grundschutzhandbuchs die Inhalte der ISO 27001 abdeckt. Zum Anderen erleichtert die Tabelle das Auffinden der jeweils zugehörigen Bausteine und Maßnahmen.

1.4 Codename Secure Blue

Am 10.04.2006 gab IBM die Entwicklung einer „Secure Blue" genannten Sicherheitsarchitektur bekannt, die die ressourcenaufwändige Ver- und Entschlüsselung von Daten direkt im Prozessor durchführen soll. Ein weiterer konsequenter Baustein des „Trusted Computing", das das Ziel verfolgt, mehr Sicherheitsfunktionen in manipulationsichere Hardware zu verlagern, um bösartigem Code die Angriffsfläche zu entziehen.

Mit der Ankündigung, „die Sicherheit von Daten in Elektronikprodukten wie Konsumer-Elektronik, Medizintechnik und Digital-Media-Produkten" zu verbessern, wurde jedoch auch die seit Jahren andauernde Kritik am Trusted Computing wieder lauter, die spekuliert, dass es dabei nur um die Durchsetzung kommerzieller Kopierschutzinteressen im Unterhaltungssektor geht (SSN 02/2003, SSN 04/2003).

Die Qualität von „Secure Blue" wird sich sicher an dem komplexeren Schlüsselmanagement und der noch immer erforderlichen Entschlüsselung der Daten vor der Nutzung durch den Anwender erweisen.

1.5 GPG-Schutz für E-Mails

Das Open-Source-Projekt GnuPG hat Zuwachs bekommen: Pünktlich zum Linux-Tag wurde vom BSI am 26.04.2006 Version 1.0.1 des Gnu Privacy Guard for Windows (gpg4win) veröffentlicht. Es umfasst

neben Schlüsselmanagement-Tools ein Plugin für Outlook. Die Lösung setzt dabei allerdings auf die Mitwirkung des Anwenders – ein „Auslaufmodell“, denn unsere Erfahrungen haben gezeigt, dass Plugins in Punkto Benutzerakzeptanz weit hinter transparenten Gateway-Lösungen liegen.

Eine attraktive „Mischlösung“ bietet GPG-relay (aktuell Version 0.959): Es sorgt anhand eines konfigurierbaren Regelsatzes als lokaler POP3/IMAP-Proxy zuverlässig für eine transparente Ver- und Entschlüsselung aller ein- und ausgehenden E-Mails – unabhängig vom E-Mail-Client.

1.6 Behörden-Desktop

Im Rahmen des BSI-Projekts ERPOSS – Erprobung des Einsatzes von Open Source Software – wurde von der credativ GmbH ein Desktop auf Basis von Debian GNU/Linux 3.1 (sarge) und KDE 3.3 entwickelt. Seit dem 28.04.2006 steht er zum Download bereit. Der Desktop bietet eine Verschlüsselung des Dateisystems, eine vorkonfigurierte Personal Firewall, einen E-Mail-Client mit Virenschutz und Spamfilter und unterstützt die vom BSI entwickelte Verschlüsselungslösung Ägypten.

1.7 Hase und Igel Reloaded

Nach der iTAN – die inzwischen von zahlreichen Banken zum Schutz des Online-Banking vor Phishing eingeführt wurde – bietet die Postbank ihren Kunden als erste Bank bundesweit die mTAN an. Dafür wirbt sie seit dem 18.04.2006 mit einem TÜV-Gütesiegel, dessen proprietäre Prüfgrundlagen dem Zertifikat zu entnehmen sind.

Beim mTAN-Verfahren erhält der Kunde zu jeder beauftragten Transaktion eine SMS mit einer einmalig gültigen, transaktionsspezifischen TAN. Zusätzlich werden Zielkontonummer und Betrag in der SMS mitgeschickt. Die Sicherheit des Verfahrens ist hoch, wenn die hinterlegte Mobilfunknummer vor Phishing-Tricks gefeit ist.

Während viele Banken die Bedrohung durch Phishing schrittweise reduzieren, spielen die Phisher Hase und Igel und erfinden ständig neue Angriffsmethoden: Inzwischen versuchen sie, Kunden die Telefon-Banking PIN zu entlocken, z.B. über die Aufforderung zur Eingabe der Telefon-PIN auf gefälschten Webseiten.

Auch der Wechsel des Kommunikationsmediums wird zum Ausspähen der persönlichen Informationen genutzt. So gibt es Angriffe, die dazu auffordern, Rufnummern anzurufen, hinter denen sich ein fingiertes Phone-Banking System verbirgt.

Den besten Schutz vor derartigen Angriffen bietet – Technik hin, Technik her – immer noch die Aufmerksamkeit der Nutzer. Denn Banken fordern Kunden grundsätzlich nicht per E-Mail zur Preisgabe vertraulicher Informationen auf. Auch sollte bei E-Mails der Absender überprüft werden – die Postbank versucht dies durch das Signieren von E-Mails zu vereinfachen.

Realistische Hoffnung auf eine Verschnaufpause für Banken und Kunden besteht allerdings nur, wenn es den Banken gelingt, Mechanismen zu etablieren, durch die der Aufwand für Phisher so ansteigt, dass er den Nutzen des Betrugs überwiegt, z.B. aufgrund einer niedrigen Erfolgsquote.

1.8 Zukunftsblick

Am 06.-09.06.2006 wagt die Konferenz „ETRICS 2006“ an der Universität Freiburg einen Blick in die Zukunft der Informations- und Kommunikationssicherheit. Allein 19 international renommierte Keynote-Speaker lassen spannende und erkenntnisreiche Tage erwarten: Professor Acquisti (Carnegie Mellon University) beleuchtet, was der Datenschutz von der Verhaltensökonomie lernen kann, David Gavrock (Intel) gibt Insider-Einblicke in Trusted Computing und Professor Kemmerer (University of California) zieht Lehren aus 30 Jahren Computer Security.

Das gesamte Programm umfasst 70 Vorträge, zahlreiche Workshops, Tutorien und ein attraktives Begleitprogramm – für einen Teilnahmebeitrag von 150 € (Studenten) bis 350 €. Noch sind Anmeldungen möglich.

2 Secorvo News

2.1 Secorvo College aktuell

Dem Hacker über die Schulter schauen – und dann sogar selbst Hand anlegen und live Systeme attackieren: völlig legal und ohne schlechtes Gewissen. Das bietet Ihnen das „Live Hacking Lab“ am **20.-22.06.2006**: Drei Tage, in denen wir Sie in die aktuellen Hacking-Technologien einweihen. Schließlich sollten Sie wissen, was Ihre Gegner können, wenn Sie Ihre IT-Infrastruktur schützen wollen.

Wenn du weder den Feind noch dich selbst kennst,
wirst du in jeder Schlacht unterliegen.
Sunzi, Die Kunst des Krieges (ca. 500 v. Chr.)

2.2 SAS 2006 – Nachlese

Dass Security Awareness bei vielen Unternehmen hoch im Kurs steht, belegt die steigende Teilnehmerzahl des von Secorvo veranstalteten „Security Awareness Symposium“, das in diesem Jahr schon zum vierten Mal die Plattform für einen intensiven Erfahrungsaustausch bot. Die engagierten Praxisberichte lieferten zahlreiche Anregungen, Denkanstöße – und sicherlich auch den einen oder anderen Motivationsschub. Die Unterlagen aller Awareness-Symposien (2003 bis 2006) sind für Interessierte auch auf CD erhältlich.

2.3 Wer haftet?

In Kooperation mit der Neuen Messe Karlsruhe findet das nächste Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am Abend des ersten Messetags der Midvision 2006 statt: Am 21.06.2006 wird Professor Dr. Michael Bartsch von der renommierten (Kanzlei des Jahres 2003/2004 in Baden-Württemberg) und im IT-Recht besonders ausgewiesenen Kanzlei Bartsch und Partner zum Thema „Risiken, Pannen, Schäden – und wer haftet?“ vortragen. Beginn 18 Uhr, anschließend Networking am Büfett (bei Live-Übertragung der Spiele Niederlande-Argentinien und Elfenbeinküste-Serbien/Montenegro auf Großleinwand). Um Anmeldung wird gebeten.

3 Veranstaltungshinweise

Mai 2006	
28.05. - 01.06.	Eurocrypt 2006 (IACR, St. Petersburg/RU)
29.05.	Linux-Sicherheit (eco AK Sicherheit, Frankfurt)
Juni 2006	
06.-09.06.	ETRICS 2006 (GI, Freiburg)
20.-22.06.	Live Hacking Lab (Secorvo College, Karlsruhe)
21.06.	Risiken, Pannen, Schäden (KA-IT-Si, Karlsruher Messe)
21.-22.06.	Midvision 2006 (Karlsruher Messe)
25.-30.06.	18th Annual FIRST Conference (FIRST, Baltimore/USA)
27.-28.06.	Lotus Notes Security (Secorvo College, Karlsruhe)
29.06.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
Juli 2006	
13.-14.07.	DIMVA 2006 (GI, Berlin)
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/USA)
August 2006	
02.-03.08.	Black Hat USA 2006 (Black Hat, Las Vegas/USA)
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/USA)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Juni 2006

Dirk Fox, Stefan Gora, Kai Jendrian,
Stefan Kelm, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 6, 5. Jhrg. 2006
Stand 20. Juni 2006

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Weltmeister

1 Security News

1.1 Admin – nein danke!

1.2 Un-SSL-Zertifikate?

1.3 Security Focus: Apple

1.4 Datenklau bei US-Armee

1.5 Office im Visier

1.6 ... back to the Future

1.7 Big Brother Awards

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Gemalte Städte

2.3 KA-IT-Si @ Midvision

3 Veranstaltungshinweise

Impressum

Editorial: Weltmeister

Bei der wichtigsten Nebensache der Welt zählt Deutschland auch 2006 allen Unkenrufen zum Trotz zu den Favoriten. Nicht nur da: Im internationalen Vergleich liegen wir bei Telefonüberwachungen (Abhöranordnungen je Bürger) auf Rang vier, hinter Italien, den Niederlanden und der Schweiz.

Durch das mit der Verbreitung von Handys geänderte Nutzerverhalten sind auch immer mehr Kontaktpersonen von Abhörmaßnahmen betroffen. Die Wahrscheinlichkeit einer Gesprächsüberwachung ist hier inzwischen 30 mal so hoch wie in den USA.

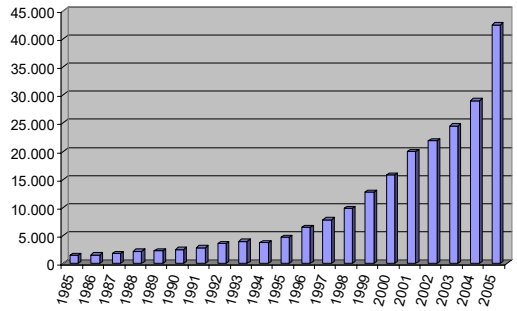


Bild: *Telefonüberwachungsanordnungen*

Erschreckend sind die durch Studien belegten Seiteneffekte dieser Entwicklung: Die schiere Zahl der Anordnungen macht die Durchbrechung des grundrechtlich geschützten Fernmeldegeheimnisses zur Formsache: Von 300 untersuchten richterlichen Beschlüssen entsprachen drei Viertel nicht den gesetzlichen Vorgaben, die Hälfte der Richter unterschrieb einfach den Beschlussentwurf des Staatsanwalts.

„Weder Staatsanwälte noch Richter mochten sich die Ansicht zu eigen machen, dass der Richtervorbehalt als eine besondere Form des Grundrechtsschutzes für die Betroffenen anzusehen sei“ (Backes et.al.). Die vorgeschriebene Benachrichtigung der Betroffenen erfolgte entweder gar nicht (66 %, Albrecht et.al.) oder beschränkte sich auf die Beschuldigten – „es fehlte jede Sensibilität dafür, dass es sich hierbei um Grundrechtseingriffe handelt.“

Dann doch lieber ein Weltmeistertitel für eine Leistung, auf die man stolz sein darf.

1 Security News

1.1 Admin – nein danke!

Hatte Microsoft noch im April 2004 berichtet, dass ca. 95 % aller Angestellten lokale Administrator-Rechte besitzen, so deuten aktuelle Bemerkungen darauf hin, dass sich dieses Verhältnis jetzt umkehren könnte. Das würde die Aussagen Microsofts in einem aktuellen White-Paper zur Information Security bei Microsoft bestätigen – dort wird unter „Lessons Learned and Best Practices“ gefordert: „consolidate local administrator accounts“.

Derzeit verursacht ein Verzicht auf lokale Administrationsrechte häufig Probleme. Für deren Analyse und Behebung hat Microsoft am 23.05.2006 den „Microsoft Standard User Analyzer“ zur Verfügung gestellt.

Der Trend, Administrator-Rechte nicht als Statussymbol, sondern als Sicherheitsrisiko zu betrachten, ist positiv zu bewerten. Halbherzige Work-Arounds sollte man dabei allerdings tunlichst vermeiden (siehe SSN 09/2005). Ein konsequenter Entzug von Admin-Rechten bei Microsoft könnte die Beseitigung von Problemen in diesem Zusammenhang deutlich beschleunigen: „Go, Microsoft, go!“

1.2 Un-SSL-Zertifikate?

Für ein wenig Aufregung sorgte die Meldung vom 03.06.2006, zukünftige Versionen der populären Mozilla-Browser würden Root-Zertifikate der israelischen StartCom-CA beinhalten. Diese waren Anfang 2006 ins Gerede gekommen, nachdem bekannt wurde, dass man bei StartCom Zertifikate ohne Identitätsprüfung beantragen konnte.

Die Aufregung erscheint unangemessen: Einerseits erlauben die Listen der vorinstallierten Root-Zertifikate *sämtlicher* Browser seit jeher keinerlei Rückschlüsse auf die Qualität der ausgestellten Zertifikate. Und andererseits haben auch andere CAs wie Verisign schon 1996 Zertifikate für E-Mail-Adressen wie root@localhost ausgestellt.

Auch den Mozilla-Entwicklern ist die Problematik längst bekannt, wie interne Diskussionen zeigen. Schon jetzt enthält beispielsweise Firefox (v1.5.0.4) Root-Zertifikate von gut drei Dutzend Firmen, denen man mit der Installation des Browsers automatisch vertraut. Um die Zertifikate bewerten zu können, hilft also nur ein Blick in die Zertifizierungsrichtlinien der jeweiligen CA.

Da kein Anwender sämtliche CA-Policies kennen dürfte, erscheint die Aufregung über die StartCom-Zertifikate ungerechtfertigt. Oder wissen Sie, wie „NetLock Halozatbiztonsagi Kft.“ und „The Go Daddy Group, Inc.“ die Identifikationsprüfung durchführen?

Besonders vorsichtige Zeitgenossen empfehlen daher das Löschen aller vorinstallierten Root-Zertifikate. Dies führt allerdings unter Windows 2000 dazu, dass das komplette System instabil wird:



1.3 Security Focus: Apple

Seit dem 31.05.2006 gibt es nun auch eine Mailingsliste zur Diskussion von Sicherheitsfragestellungen zu Apple’s Hard- und Software. Durch eine E-Mail an focus-apple-subscribe@securityfocus.com kann die Aufnahme in den Verteiler initiiert werden. Sicherheitsschwachstellen werden weiterhin über Bugtraq gemeldet.

1.4 Datenklau bei US-Armee

Am 22.05.2006 hat das US-amerikanische Department of Veterans Affairs (zuständig für die medizinische und finanzielle Versorgung von Veteranen) die Serie peinlicher und brisanter Sicherheitsvorfälle in amerikanischen Bundesbehörden (siehe SSN 05/2006) um ein weiteres Highlight ergänzt.

Danach wurde einem Mitarbeiter zu Hause ein Laptop mit über 26 Millionen unge-

schützten Datensätzen von Militärangehörigen (9 % der US-Bevölkerung, davon ca. 2,2 Millionen Aktive) entwendet. Die Daten umfassen Name, Social Security Number und Geburtsdatum – alles, was in den USA zum Identitätsmissbrauch benötigt wird.

Die private Aufbewahrung des Laptop verstieß gegen die Security Policy. Daher wurden nach diesem Vorfall alle Mitarbeiter per Direktive zu einem jährlichen Privacy and Security Training verpflichtet. Denn neben geeigneten technischen und organisatorischen Maßnahmen ist auch ein hohes Sicherheitsbewusstsein im Umgang mit sensiblen Daten unverzichtbar.

1.5 Office im Visier

Am 10.05.2006 meldete Microsoft eine MS-Word Schwachstelle im Microsoft Security Advisory (919637). Sie ermöglicht einem Angreifer, der sein Opfer zum Öffnen präparierter Word-Dokumente verleiten kann, beliebigen Code mit den Berechtigungen des Opfers zur Ausführung zu bringen. Das ist an sich nichts grundsätzlich Neues – allerdings dauerte es über einen Monat, bis Microsoft am 13.06.2006 mit einem Patch im Microsoft Security Bulletin MS06-027 eine zielgruppengerechte Lösung veröffentlichte. Alle zuvor publizierten Workarounds von Trendmicro, Microsoft, US-CERT u. a. setzen zu viel Detailwissen voraus oder sind für den Arbeitsalltag nicht geeignet (Einsatz von WordViewer). Microsoft bewertete die Schwachstelle als „nicht kritisch“; erst im aktuellen Bulletin wurde die Bewertung auf „kritisch“ korrigiert.

Es ist dringend angeraten, den Patch einzuspielen und sich nicht nur auf den aktuellen Virenschutz zu verlassen.

Übrigens: Nicht nur Microsofts Office-Suite steht im Fokus. Am 31.05.2006 hat Kaspersky einen Proof-of-Concept Virus für StarOffice/OpenOffice veröffentlicht. In einer Stellungnahme relativierte das OpenOffice-Team am 02.06.2006 die Bedrohung durch diesen Virus.

1.6 ... back to the Future

BackTrack 1.0, eine Live-Linux-Distribution auf einer bootfähigen CD (oder einem USB-Stick) enthält eine umfassende Sammlung von Netzwerksicherheits- sowie Penetration-Testing-Tools und Exploits. Die neue, am 26.05.2006 freigegebene Distribution enthält sehr aktuelle Programmversionen dieser Werkzeuge (z. B. Metasploit 2.6). Darin laufen die Entwicklungslinien von Auditor Security Linux und WHAX (davor Whoppix) zusammen. Erstmals wurde auch ein eigener Bereich für Datenbankscanner integriert. Ob die Distribution auch die bewährte Robustheit und Funktionsfähigkeit ihrer Vorgänger erreicht, muss sich noch in der Praxis erweisen.

1.7 Big Brother Awards

Ganz ohne Fernsehen und Container werden seit 1998 in inzwischen 17 Ländern jährlich die Big Brother Awards für besondere Verdienste um Datenschutz feindliche Techniken und Datenerhebungen verliehen. In Deutschland organisiert seit dem Jahr 2000 der FoeBuD e. V. in Bielefeld die Nominierung der Preisträger und die Verleihung der „Oscars für Datenkraken“.



Die Nominierung von Preisverdächtigen ist noch bis zum 31.07.2006 möglich. Die diesjährige Verleihung der Awards erfolgt am 20.10.2006 im historischen Saal der Ravensberger Spinnerei im Zentrum von Bielefeld.

2 Secorvo News

2.1 Secorvo College aktuell

Nach der Sommerpause startet Secorvo College im September mit

- dem aktuellen Grundlagenseminar IT-Sicherheit heute (**19.-21.09.2006**) und
- einem Intensivseminar zu Public Key Infrastrukturen (PKI) (**26.-29.09.2006**).

Programme, weitere Seminarangebote, Preise und Online-Anmeldung unter http://www.secorvo.de/college

2.2 Gemalte Städte

Der Künstler Thitz, einigen von Ihnen durch Secorvo-Weihnachtskarten oder einem Besuch in Karlsruhe bekannt, zeigt seine „Gemalten Städte“ noch bis zum 29.10. 2006 in der Staatlichen Kunsthalle Karlsruhe.

2.3 KA-IT-Si @ Midvision

Die Karlsruher IT-Sicherheitsinitiative ist auf der Midvision 2006 am 21. und 22.06.2006 in der Messe Karlsruhe mit einem eigenen Stand vertreten. Auch die KA-IT-Si-Partner AMEC SPIE System Integration und Lampertz sind dabei und zeigen aktuelle Sicherheitslösungen.

Am **21.06.2006** wird um 18:30 Uhr Herr Professor Dr. Bartsch von der renommierten, auf IT-Recht spezialisierten Karlsruher Kanzlei Bartsch und Partner im Foyer der Messe über „Risiken, Pannen, Schäden – und wer haftet?“ sprechen. Anmeldung zu diesem KA-IT-Si-Event bitte über die Webseite (Anfahrtskizze).

Zum Vormerken: Ihren fünften Geburtstag wird Deutschlands älteste IT-Sicherheitsinitiative am **18.10.2006** im Saal Baden der IHK Karlsruhe angemessen feiern. Die Key Note wird Herr Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) halten.

3 Veranstaltungshinweise

Juni 2006	
21.06.	"Risiken, Pannen, Schäden – und wer haftet?" (KA-IT-Si, Messe Karlsruhe)
21.-22.06.	Midvision 2006 (Messe Karlsruhe)
25.-30.06.	18th Annual FIRST Conference (FIRST, Baltimore/USA)
Juli 2006	
13.-14.07.	DIMVA 2006 (GI, Berlin)
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/CA)
August 2006	
02.-03.08.	Black Hat USA 2006 (Black Hat, Las Vegas/USA)
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/US)
September 2006	
19.-21.09.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
26.-29.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2006	
18.10.	KA-IT-Si-Jubiläumsfeier (KA-IT-Si, IHK Karlsruhe)
23.-27.10.	Systems 2006 (Messe München, München)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Juli 2006

Dirk Fox, Stefan Gora, Kai Jendrian,
Stefan Kelm, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 7, 5. Jhrg. 2006
Stand 20. Juli 2006

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: FlieWaTüüt

1 Security News

1.1 BCM-Standard

1.2 Security Tool Hitparade

1.3 Operational Risk Survey

1.4 Mehr Glück als Verstand

1.5 SSL Revisited

1.6 SAP-Baustein IT-GSHB

1.7 bDSB-Handreichung

1.8 PIN-Reset bei O2 (UK)

1.9 Spyware by Microsoft

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Business Continuity

2.3 5 Jahre KA-IT-Si

3 Veranstaltungshinweise

Impressum

Editorial: FlieWaTüüt

Eine Lieblingsgeschichte meiner Kindheit, „Robbi, Tobbi und das FlieWaTüüt“ von Boy Lornsen, hat wahrscheinlich den Ingenieur in mir geweckt. Die phantastischen Abenteuer des kleinen Erfinders Tobbi mit einem Roboterjungen und seinem selbst entworfenen „FlieWaTüüt“, einer Kreuzung aus Mini-Wasserhubschrauber und dreirädriger Piaggio-APE, waren für mich der Jules Verne des 20. Jahrhunderts. (Die spektakuläre WDR-Verfilmung von 1972 gibt es übrigens seit 2005 auf DVD.)

Begeistert hat mich die Vision eines Fahrzeugs, das alle wesentlichen Funktionen vereint. Heute gibt es ein Wort dafür: Konvergenz – das Zusammenwachsen unterschiedlichster technischer Lösungen. Standardisierte anwendungsneutrale Basistechnologien wie PC, Internet und digitale Ton- und Bilddaten ermöglichen heute verschiedenste Funktionen auf einem Gerät.

So mutiert das mobile Telefon mit Fotoapparat, Radio, Armbanduhr, MP3-Player, Spielekonsole und mobilem Fernseher zum „TelMusKlick“. Als Smartphone enthält es Adressbuch, Taschenrechner, Terminkalender, E-Mailer, Notizblock und Internet-Browser, erlaubt es die Bearbeitung von Office-Dokumenten, schickt Präsentationen an einen Beamer und navigiert durch unbekannte Städte. Es ist Informationsdienst und Online-Auskunft, Vorleser, Fremdenführer und Dolmetscher in einem.

Bald sucht es sich automatisch die günstigsten Netze (UMTS, WLAN oder Bluetooth), synchronisiert seine Daten mit zentralen Adress- und Datenservern über das Internet, ersetzt Privatbibliothek, Tageszeitung und Musiksammlung. Es öffnet und verschließt Türen und Fahrzeuge und steuert Jalousien und Haushaltsgeräte.

Ein Alleskönner für die Hosentasche – und ein gefundenes Fressen für Angreifer. Firewall-freie Kommunikationsverbindungen und sensibelste Daten mit komplexer (ergo fehleranfälliger) Softwarekonzentration in den Händen unkundiger Nutzer – hätte Jules Verne das geahnt, wäre daraus ein spannender Science Fiction geworden.

1 Security News

1.1 BCM-Standard

Am 03.07.2006 hat das British Standards Institute (BSI) eine Vorabversion des Standards BS 25999-1 *Guide of Practice for Business Continuity Management (BCM)* zur Kommentierung bis zum 31.08.2006 und zur Diskussion veröffentlicht.

In der Tradition des BS 7799 gibt das BSI mit diesem Standard auf Best Practices beruhende Richtlinien und Empfehlungen heraus. Das Dokument liefert eine gute Einführung in BCM-Begriffe und Vorgehensweisen. Für BCM-Interessierte ist daher schon die Vorabversion des Standards eine Lektüre wert.

1.2 Security Tool Hitparade

Von Fyodor, dem Entwickler des bekannten Port-Scanners nmap wurde am 21.06. 2006 das Ergebnis seiner Umfrage zum Thema Security Tools auf der Mailing-Liste Nmap Hackers veröffentlicht. Aus den 3243 Antworten wurde eine repräsentative Rangliste von Security Tools erstellt und unter SecTools.Org publiziert. Die Liste ist eine wahre Fundgrube und gibt Auskunft über die Popularität eines Tools, den kommerziellen Status, das Abschneiden im Vergleich zur letzten Umfrage 2003 und die unterstützten Betriebssysteme. Sie enthält eine kurze Zusammenfassung der Funktionsweise und einen Link auf das Tool.

1.3 Operational Risk Survey

Am Henley Management College wird derzeit eine anonyme Online-Befragung über den Zusammenhang zwischen operationellen Risiken und Informationssicherheit in der Praxis durchgeführt. Zur Teilnahme sind Sicherheitsexperten mit Praxiserfahrung aufgerufen. Der Fragebogen umfasst 44 Multiple-Choice-Fragen und Statements und lässt sich in wenigen Minuten beantworten. Auf Wunsch erhalten Teilnehmer das Summary der Studie zugesandt.

1.4 Mehr Glück als Verstand

... könnte das Fazit des Datendiebstahl-Vorfalls bei der US-Armee sein, über den wir in den SSN 06/2006 berichtet haben: Am 29.06.2006 wurden der Laptop und die betroffene externe Festplatte sichergestellt; Untersuchungen des FBI ergaben, dass ein Zugriff auf die betroffenen Daten mit hoher Wahrscheinlichkeit ausgeschlossen werden kann.

Erwähnenswert ist der offizielle Bericht des Office of Inspector General der betroffenen Behörde. Das Dokument ist lesenswert für jeden Sicherheitsverantwortlichen, da hier auf über 40 Seiten ein GAU beim Umgang mit einem Sicherheitsvorfall schonungslos dokumentiert wird.

1.5 SSL Revisited

„Trau, schau, wem!“ war das Fazit des Artikels „Un-SSL-Zertifikate?“ aus den SSN 06/2006. Die negativen Erfahrungen mit dem Entfernen aller CA-Zertifikate unter Windows 2000 veranlassten uns zu untersuchen, welche Zertifikate gefahrlos aus dem Zertifikatsspeicher gängiger Browser entfernt werden können, um sie auf eine individuell vertrauenswürdige Sammlung zu reduzieren. Dazu wurden die gängigen Versionen von Internet Explorer, Firefox und Opera unter Windows 2000 untersucht. Als Ergebnis lässt sich festhalten, dass Windows 2000 nur die sechs von Microsoft zwingend vorgeschriebenen CA-Zertifikate benötigt. Bemerkenswerterweise sind von diesen bereits vier abgelaufen. Ein Windows XP System startete auch ohne diese sechs CA-Zertifikate fehlerfrei; zumindest für den Bootvorgang ist Microsofts Vorgabe an Minimalzertifikaten unter Windows XP demnach nicht erforderlich. Aus den Browsern Firefox und Opera ließen sich alle lokalen CA-Zertifikate ohne funktionale Einschränkung entfernen.

„Trau, schau, wem!“ bleibt also auch nach den Tests die Botschaft im Umgang mit SSL-Zertifikaten. Wer daher nicht blind jeder SSL-Verbindung trauen mag, sollte alle CA-Zertifikate löschen, deren Vertrauenswürdigkeit ihm nicht gesichert erscheint.

1.6 SAP-Baustein IT-GSHB

Auf den Webseiten des BSI wurde am 20.06.2006 eine Vorabversion des neuen Bausteins „B 5.13 SAP System“ für das IT-Grundschutzhandbuch bereit gestellt. Der recht umfassende Baustein (133 Seiten) gibt einen Überblick der potentiellen Gefährdungen sowie der relevanten Maßnahmen auf Basis von IT-Grundschtz. Die Maßnahmen sind recht gut beschrieben und wurden durch Kontrollfragen ergänzt. Somit wird nun mit SAP eine weitere wesentliche Anwendung und Plattform abgedeckt.

1.7 bDSB-Handreichung

Für den betrieblichen Datenschutzbeauftragten hat der Arbeitskreis Datenschutz des BITKOM am 21.04.2006 zwei wertvolle Handreichungen veröffentlicht: Einen Praxisleitfaden zum Verfahrensverzeichnis nach BDSG, der neben einigen wichtigen Klarstellungen, konkreten Beispielen und Formblättern für die Datenerhebung auch eine tabellarische Gegenüberstellung von Tools zur Gestaltung des Verfahrensregisters enthält. Eine wertvolle Hilfestellung zur Umsetzung des BDSG in der Praxis.

Das zweite Dokument zur Datenschutzproblematik bei grenzüberschreitender Datenübermittlung macht die nicht ganz einfache Rechtslage transparent und gibt konkrete Empfehlungen für die Praxis.

1.8 PIN-Reset bei O2 (UK)

Im aktuellen Cryptogram vom 15.07.2006 stellt Bruce Schneier das vereinfachte PIN-Reset-Verfahren von O2 in Großbritannien zur Diskussion. Danach kann nach einer Sperrung der SIM-Karte ein PUK (Personal Unlocking Key) ohne weiter gehende Authentifizierung allein mit Angabe der Handynummer beantragt werden.

In Ermangelung eines britischen Kartenvertrags konnten wir dies nicht verifizieren; nach den Angaben von Bruce Schneier wurde aber von O2 zu den Risiken des Verfahrens wie folgt Stellung genommen:

- Ist das gestohlene Handy ausgeschaltet, kann die Telefonnummer nicht in Erfahrung gebracht und so auch keine PUK beantragt werden.
- Ist das Handy eingeschaltet, kann ein Dieb auch ohne PIN/PUK telefonieren.

Das Risiko wird von O2 daher als gering eingestuft, da in beiden Fällen der Provider ohnehin umgehend über den Verlust informiert und die SIM-Karte sperren würde.

Von O2 wurden jedoch nicht alle denkbaren Fälle bedacht. Uns sind mindestens drei Denkfehler aufgefallen. Ihnen auch? Dann senden Sie Ihre Überlegungen bis 15.08.2006 an sommerquiz@secorvo.de. Unter allen Einsendern verlosen wir einen kostenlosen Zugang zum security-finder für ein Jahr. Die kreativsten Angriffsideen werden in den nächsten SSN veröffentlicht.

1.9 Spyware by Microsoft

Die aus Microsofts „Windows Genuine Advantage“ (WGA) Programm hervorgegangene Lizenz-Validation wurde am 27.06. 2006 zu einer WGA-Notification erweitert, die sich nach der Installation wie Spyware verhält: wiederholte Starts (bei jedem Windows Logon und alle 24 Stunden), Untersuchung von Hard- und Software (MAC-Adresse, IP-Adresse, Informationen zum Benutzerkontext), unaufgeforderte Anzeige von Informationen (Popups), Übermittlung von Daten ohne Autorisierung und Wissen des Endbenutzers an externe Microsoft-Server.

Das Unterschieben der erweiterten Funktionalität als sicherheitskritisches Update im Rahmen des (ggf. automatischen) Windows-Update Services führte insbesondere auf Privatsystemen zu einer starken Verbreitung. Allerdings handelt es sich bei diesem Update inhaltlich nicht um System-Sicherheit, sondern um Lizenzkontrolle. Für ein ähnliches Verhalten wurden Spyware-Anbieter unlängst rechtkräftig verurteilt (Smartbot.Net und Odysseus).

Auch wenn die bisherigen Stellungnahmen von Microsoft eine Identifizierung der Endbenutzer verneinen, bleibt eine negativer

Beigeschmack, da das Tool Informationen in der Privatsphäre des Nutzers erhebt und an Microsoft sendet.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminar IT-Sicherheitsaudits in der Praxis wurde auf Anregung zahlreicher Teilnehmer zu einem dreitägigen Seminar ausgebaut. Das Vortragsprogramm wird nun ergänzt durch drei Workshop-Teile; für das Thema „Rechtliche Rahmenbedingungen und Datenschutz“ ist mehr Raum vorgesehen.

2.2 Business Continuity

In Folge der insbesondere im Kontext von KontraG, SOX und Basel II verstärkten Bemühungen aller Unternehmen um Compliance, d.h. die Übereinstimmung der Form der Geschäftsausübung mit gesetzlichen Anforderungen aller Art, rückt neben dem Datenschutz auch die Beschäftigung mit denkbaren Notfällen in den Fokus der Informationssicherheit.

Aus mehreren Projektarbeiten ist nun eine ausführliche Darstellung unseres Leistungsangebots im Gebiet Business Continuity und Disaster Recovery entstanden.

2.3 5 Jahre KA-IT-Si

In diesem Jahr jährt sich die Gründung der Karlsruher IT-Sicherheitsinitiative zum fünften Mal. Dieses Jubiläum wird die KA-IT-Si am **18.10.2006** feiern – im **Saal Baden der IHK Karlsruhe**, dem Ort, an dem am 25.01.2001 die KA-IT-Si aus der Taufe gehoben wurde. Die Key Note wird Herr Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) halten, flankiert von anschaulichen Praxisberichten zur „Herausforderung IT-Sicherheit im Mittelstand“, einer Ausstellung der Sicherheitslösungen der KA-IT-Si-Partner und einem anschließenden „Net(t)-working-Büfett“. Online-Anmeldung unter www.ka-it-si.de.

3 Veranstaltungshinweise

Juli 2006	
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/CA)
August 2006	
02.-03.08.	Black Hat USA 2006 (Black Hat, Las Vegas/USA)
04.-06.08.	DEFCON 14 (Defcon, Las Vegas/USA)
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/USA)
September 2006	
19.-21.09.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
26.-29.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2006	
04.-05.10.	Inside Windows Security (Secorvo College, Karlsruhe)
10.-12.10.	ISSE 2006 (TeleTrusT/EEMA, Rom/IT)
16.-20.10.	Information Security Management (Secorvo College, Karlsruhe)
17.-18.10.	DACH Mobility 2006 (GI/ÖCG/BITKOM/SI, München)
18.10.	KA-IT-Si-Jubiläumsfeier (KA-IT-Si, IHK Karlsruhe)
23.-27.10.	Systems 2006 (Messe München, München)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
August 2006

Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Natalie Mareth, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 8, 5. Jhrg. 2006
Stand 17. August 2006

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Feine Freunde

1 Security News

1.1 Offene Fenster

1.2 Compliance

1.3 Rootkits auf der Blackhat

1.4 Defcon Rocks

1.5 PhishPharming

1.6 CrypTool v1.4

1.7 Standard-Kompass

1.8 Auswertung Sommerquiz

1.9 Ruf' mich an, Kleines

2 Secorvo News

2.1 Secorvo College aktuell

2.2 TISP @ Secorvo College

3 Veranstaltungshinweise

Impressum

Editorial: Feine Freunde

Das Wettrüsten zwischen den Entwicklern von Sicherheitstechnologien und den Erfindern von Penetrations- oder Umgehungsmöglichkeiten, gemeinhin „Hacker" genannt, durchzieht die Geschichte der IT-Sicherheit wie ein roter Faden.

Zwar stimuliert Wettbewerb bekanntlich die Qualität eines Produkts, und zweifellos wären ohne ein solches Stimulans weder Firewalls noch Hackingtools, weder Virenscanner noch Trojaner so leistungsstark und bedienungsfreundlich. Dennoch ist die Wirkung dieses Wettrüstens eher destruktiv und verursacht Kosten und Schäden.

Konnte man dem Wettkampf früher wenigstens in Ansätzen noch etwas Sportliches abgewinnen, da Viren und Würmer in der Regel keine komplexen Schadfunktionen enthielten und eher den Charakter eines „proof of concept" besaßen, haben kriminelle Interessen aus dem Wettkampf inzwischen eine Schlacht gemacht. Mit Spammern, Bot-Netzen, Warez-Servern und Phishing lässt sich Geld verdienen – oder zumindest waschen.

Aber nicht nur der Kampf ist härter geworden. Auch die Fronten verschwimmen. So verbreiten Softwarehersteller Copyright-Schutzmechanismen, die sich mit Stealth-Techniken im System verstecken oder wie Spyware verhalten (SSN 7/2006). Banken verwenden eigenartige Domain-Namen und führen wenig intuitive „Sicherheitsmerkmale" für ihr Online-Banking ein, die ein wechselndes und befremdliches Erscheinungsbild hervorrufen – und sich kaum mehr von einer Phishing-Seite unterscheiden lassen. Marketiers verschicken HTML-E-Mails mit versteckten URLs (um Empfängerreaktionen zu analysieren). Und Entwickler von Peer-to-Peer-Anwendungen wie Skype „perforieren" Firewalls trickreich mit dem verbindungslosen UDP-Protokoll – und etablieren so Kommunikationsverbindungen, die komplett an der Filterung vorbeilaufen.

Damit werden Hacking-Techniken zu Produkt-Features. Wer solche Freunde hat, braucht keine Feinde mehr.

1 Security News

1.1 Offene Fenster

Zum Patchday am 08.08.2006 wurden von Microsoft zwölf Sicherheits-Hotfixes veröffentlicht, von denen besonders die Sicherheitslücke im Server-Service und die so genannten RemoteExecution Schwachstellen erhebliche „Nachwirkungen“ haben dürften. Fatal ist, dass diese Lücken in fast allen Versionen der Windows-Familien 2000 / XP / 2003 inklusive Service Packs existieren – alle installierten Windows-Systeme, bei denen dieser Dienst ungeschützt aktiv ist, können derzeit automatisiert übernommen werden.

Die auf der Mailingliste Full Disclosure publizierte Schwachstelle im /proc-Filesystem, die lokalen Benutzern mit shell-Zugriff eine Privilegieneskalation bis auf root-Ebene erlaubt, erscheint dagegen fast als „harmloser“ Sonderfall.

Trotz Microsofts Paradigmenwechsel von der „Featuritis“ zur Softwaresicherheit als erster Priorität nimmt die Anzahl kritischer Schwachstellen nicht ab. Ohne sauber konfigurierte (Personal) Firewalls und ein konsequentes Patch-Management ist ein ausfallfreier IT-Betrieb inzwischen völlig undenkbar geworden.

1.2 Compliance

Am 07.07.2006 hat Microsoft seine zahlreichen Dokumente zu verschiedenen Themen der IT-Sicherheit um den Regulatory Compliance Planning Guide ergänzt. Darin werden auf 71 Seiten Maßnahmen zur Umsetzung der organisatorischen und technischen Anforderungen von Gesetzen und Standards mit Microsoft-Technologien und -Produkten dargestellt.

Vorgestellt und berücksichtigt werden Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), EG-Datenschutzrichtlinie sowie die ISO 17799 (2005). Zwar ist das Dokument mit „Microsoft-Brille“ geschrieben, enthält aber wertvolle Hinweise und Beispiele.

Es steht in engem Kontext anderer lesenswerter Microsoft-Dokumente zum Thema IT-Security wie dem Security Risk Management Guide, dem Security Monitoring and Attack Detection Planning Guide und dem etwas technischeren Windows Server 2003 Security Guide.

1.3 Rootkits auf der Blackhat

Auf der diesjährigen Blackhat vom 29.07.-03.08.2006 in Las Vegas wurden von Dino Dai Zovi und Joanna Rutkowska Rootkits für die neuen Intel- und AMD-Prozessoren präsentiert, die deren Virtualisierungstechniken nutzen. Bisherige Hardware Based Rootkits (SSN 04/2006) benötigten eine komplette virtuelle Maschine wie VMWare oder VirtualPC; die neue Generation führt die Virtualisierung im laufenden Betrieb durch und ist nicht einmal mehr an vermeintlichen Änderungen der Hardware erkennbar.

Schutz bietet derzeit nur die Deaktivierung der Virtualisierungsfunktionen im BIOS – sofern sie nicht benötigt werden.

1.4 Defcon Rocks

Die 14. Defcon vom 04.-06.08.2006, ebenfalls in Las Vegas, war etwas chaotischer organisiert als die Blackhat und begann mit zwei Stunden Verspätung. Die gebotenen Inhalte und das wohl "most hostile network on earth" machten diesen Mangel jedoch wett. Neben den verschiedenen Hacking-Events waren einige der „0-day attacks“ sehr spannend.

Unter anderem wurde vorgestellt, wie Systeme über Schwachstellen im WLAN-Treiber übernommen (Johnny Cache) und wie bei verbreiteten SmartPhones unter Windows CE 4.2 über Multi-Media Messages (MMS) beliebige Programmcodes zur Ausführung gebracht werden können (Collin Mulliner). Auch das Thema Blackberry-Security, insbesondere die Architektur, wurde von FX (Phenoelit) ausführlich beleuchtet.

1.5 PhishPharming

Deloitte veröffentlichte am 15.06.2006 den Global Security Survey 2006, Ergebnis einer Befragung von Datenschutz- und Sicherheitsbeauftragten weltweit tätiger Finanzinstitute über Art und Anzahl von Sicherheitsattacken. Eine wesentliche Beobachtung ist, dass systematische Angriffe, die auf finanziellen Gewinn abzielen, offenbar stark zunehmen. Mehr als die Hälfte der externen Angriffe (51 %) beruhten auf Phishing oder Pharming. Auch für das laufende Jahr zählen Identitätsdiebstahl und Betrug mit gefälschten Zugangsdaten zu den größten erwarteten Bedrohungen. Bei 58 % der Befragten rangieren Schutzmaßnahmen gegen diese Risiken unter den wichtigsten fünf Sicherheitsaktivitäten.

1.6 CrypTool v1.4

Die inzwischen unter Open-Source-Lizenz verbreitete Kryptografie-Lernsoftware CrypTool steht seit dem 31.07.2006 in der Version 1.4 zur Verfügung. CrypTool ermöglicht dem Nutzer einen anschaulichen Zugang zum Verständnis von kryptografischen Verfahren und deren Grenzen. Es wurde vor allem für die Mitarbeiter-Sensibilisierung und zu Ausbildungszwecken entwickelt (zur Historie siehe SSN 3/2002).

Neu sind neben Parametererweiterungen (längere Schlüssel, größere Dateien) und neu implementierten Verfahren und Angriffen unter anderem auch sehr verständliche Java-Animationen, die Schritt für Schritt die Funktionsweise der Verschlüsselung mit Caesar, Vigenère, Nihilist oder DES demonstrieren. Außerdem gibt es das Lernspiel „Der Zahlenhai“, das den Umgang mit Teilern und Primfaktoren veranschaulicht.

1.7 Standard-Kompass

Am 28.06.2006 hat der AK Sicherheitsmanagement des Bitkom Version 2.0 des „Kompass der IT-Sicherheitsstandards“ herausgegeben. Aktualisierung und Überarbeitung durch viele kompetente Autoren haben zu einem sehr informativen, 90seitigen „Standard-Werk“ beigetragen.

1.8 Auswertung Sommerquiz

Zahlreiche Zuschriften haben uns zu unserem Sommerquiz (SSN 07/2006) erreicht. Der kreativste Input kam von Hanno Langeweg aus Gjøvik in Norwegen – für seine Überlegungen bedanken wir uns mit einem Jahresabo für den Security-Finder.

Die meisten Kommentare bezogen sich auf die Annahme, dass bei ausgeschaltetem Telefon die Telefonnummer nicht in Erfahrung gebracht werden könne. Wird ein Mobiltelefon gezielt gestohlen, greift diese Annahme nicht: Die Telefonnummer des Opfers ist entweder bekannt oder kann leicht ermittelt werden. Häufig ist auch die eigene Nummer im Handy (nicht auf der SIM) gespeichert oder in Unterlagen notiert, die zusammen mit dem Handy entwendet werden (Handtasche o.ä.). Erwischt der Dieb ein eingeschaltetem Handy, kann er die Telefonnummer leicht ermitteln und sich damit die PUK besorgen.

Fazit: Die eigene Telefonnummer ist ein sehr schwaches alleiniges Authentisierungsmerkmal; O2 (und jedem anderen Helpdesk) empfehlen wir einen ausgefeilteren Authentisierungsprozess.

1.9 Ruf’ mich an, Kleines

In einem Fachvortrag setzte sich Doug Mohney am 02.08.2006 auf der Blackhat mit dem Thema Stimmanalyse in Callcentern und Großunternehmen kritisch auseinander. Als Schutz vor Social Engineering Angriffen erfreuen sich Stimmanalysesysteme mit Filtermechanismen (Whitelists, Blacklists, Word Spotting) und statistischer Stimm- und Stressanalyse derzeit großer Nachfrage. Tatsächlich stellen diese Systeme nicht nur ein attraktives Ziel für Identitätsdiebe dar, wie die zunehmende Anzahl von Angriffen auf Call-Center-Infrastrukturen zeigt, sondern sind auch datenschutzrechtlich problematisch: Sie erlauben die Erstellung von „Stimmprofilen“. Von da ist es nicht mehr weit bis zu „Stimmenspuren“, die wir im Netz hinterlassen – beispielsweise via Google Voice Search – und die systematisch recherchiert und missbraucht werden können.

2 Secorvo News

2.1 Secorvo College aktuell

In den Herbst startet Secorvo College mit zwei Anfang 2006 komplett renovierten „Klassikern“: dem Grundlagenseminar „IT-Sicherheit heute“ am 19.-21.09.2006 und dem Intensivseminar „PKI – Public Key Infrastrukturen“ vom 26.-29.09.2006.

Beide Seminare sind eine ausgewogene Mischung aus Theorie (Grundlagen, Hintergründe, Zusammenhänge) und Praxis (Vorführungen, Beispiele, Best Practices). Der Bewertung eines Teilnehmers des PKI-Seminars im Frühjahr 2006 haben wir nichts hinzuzufügen: *„Sehr gut strukturiertes Seminar für alle, die im Kontext PKI auf ‚Ballhöhe’ kommen wollen, aber auch für die, die es bereits sind.“*

Programm und Online-Anmeldung unter http://www.secorvo.de/college

2.2 TISP @ Secorvo College

Vor drei Jahren entwickelte TeleTrusT ein europäisches Expertenzertifikat für den Bereich Informationssicherheit – den „TeleTrusT Information Security Professional“, kurz TISP. Dieses Zertifikat wurde im Unterschied zu den zahlreichen internationalen Zertifikaten auf die spezifischen deutschen und europäischen Anforderungen zugeschnitten. In 18 Themenmodule sind die Inhalte gegliedert; Ausbildung und Prüfung erfolgen in deutscher Sprache.

Seit 2004 haben mehr als 100 Security-Experten die TISP-Ausbildung und –Zertifizierung absolviert. Drei Jahre Berufserfahrung und eine erfolgreiche Prüfung mit vorausgehender fünftägiger Intensivschulung sind dafür Voraussetzung.

Secorvo, selbst seit 1998 aktives Mitglied bei TeleTrusT, hat nun die Anerkennung als „TISP-Schulungsanbieter" beantragt und wird, vorbehaltlich der endgültigen Akkreditierung, am 20.-25.11.2006 die erste TISP-Schulung mit anschließender Prüfung durchführen.

3 Veranstaltungshinweise

August 2006	
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/US)
September 2006	
19.-21.09.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
26.-29.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2006	
04.-05.10.	Inside Windows Security (Secorvo College, Karlsruhe)
10.-12.10.	ISSE 2006 (TeleTrusT/EEMA, Rom/IT)
16.-20.10.	Information Security Management (Secorvo College, Karlsruhe)
17.-18.10.	DACH Mobility 2006 (GI/ÖCG/BITKOM/SI, München)
18.10.	KA-IT-Si-Jubiläumsfeier (KA-IT-Si, IHK Karlsruhe)
23.-27.10.	Systems 2006 (Messe München, München)
November 2006	
06.-07.11.	IT-Risk Management 2006 (COMPUTAS, Karlsruhe)
20.-25.11.	TISP-Schulung (Secorvo College, Karlsruhe)
26.11.	TISP-Prüfung (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

September 2006



Editorial: 5-50-I000

Jubiläen sind bekanntlich ebenso wichtig wie willkürlich. Wichtig, weil sie die Wurzeln in Erinnerung rufen, zugleich etwas Vollbrachtes vor Augen führen, und sowohl Ermutigung als auch Ansporn sein können. Willkürlich, weil der Termin eines Jubiläums weniger vom objektiven Zeitablauf als vom gewählten Maßsystem abhängt, wie jeder Informatiker weiß. Denn auch wenn die natürliche Beschaffenheit unseres Körpers die Nutzung des Dezimalsystems nahe legt (zehn Finger), versteht sich dies keineswegs von selbst, wie nicht zuletzt die Rechenwerke unserer elektronischen Gehilfen belegen.

Gleich drei Jubiläen feiern wir in diesem Frühherbst:

- Am 18.10.2006 begehen wir das fünfjährige Jubiläum der Karlsruher IT-Sicherheitsinitiative – mit einer halbtägigen Veranstaltung in der IHK Karlsruhe und einer Key Note des BSI-Präsidenten, zu der wir Sie sehr herzlich einladen (Anmeldung).
- Vor Ihnen liegt die 50. Ausgabe der „Secorvo Security News" – und hinter uns 50 Monate, in denen wir Nachrichten recherchiert, gefiltert, bewertet und für Sie aufbereitet haben. Ausgedruckt ein ansehnliches Büchlein von 200 Seiten.
- Am 01.09.2006 konnten wir ein besonderes Ereignis begehen: Vor I000 Jahren wurde Secorvo gegründet – in der Schnelllebigkeit des dot-com-Zeitalters ein gar „biblisches" Alter, dem die Verwendung des Dualsystems angemessen Rechnung trägt.

Das Jubiläum unserer kleinen News, deren Leserzahl ständig wächst, haben wir zum Anlass genommen, die Gestaltung einer gründlichen Überarbeitung zu unterziehen. Dabei wollten wir insbesondere den einzigen Kritikpunkt, der aus Ihren Reihen gelegentlich geäußert wurde, ausräumen: das durch die Spaltenformatierung erforderliche Vor- und Zurückblättern innerhalb einer Seite.

Und auch der security-finder hat ein neues Gesicht bekommen – schauen Sie einmal hinein. Wir freuen uns auf Ihre Rückmeldungen.



Inhalt

Editorial: 5-50-I000

Security News

Krypto-Bug in OpenSSL

ISO 27001-Zertifikat für SAP SI

BDSG 2006 in Kraft

.dd -> .vmdk

Besser zweimal messen ...

Awareness @ ENISA

Dynamische Malware-Analyse

Wer AN.ONymisiert, wird beschlagnahmt

Secorvo News

Secorvo College aktuell

White Paper Security Management Praxis

Veranstaltungshinweise

Fundsachen

secorvo
security consulting

Security News

Krypto-Bug in OpenSSL

Auf der legendären „Rump Session" der diesjährigen Weltkonferenz der Kryptologen, der Crypto 2006 in Santa Barbara, präsentierte Daniel Bleichenbacher am 22.08.2006 eine Möglichkeit zur Fälschung von RSA-Signaturen, die den öffentlichen Exponenten „3" verwenden. So überprüfen die betroffenen OpenSSL-Implementierungen (bis v0.9.7j und v0.9.8b) die Füllbytes („padding") nicht korrekt. Ein Angreifer kann diese Schwachstelle relativ einfach nutzen, um eine dritte Wurzel als gültige Signatur in den überschüssigen Bytes zu verstecken. Forscher der TU Darmstadt haben einen Exploit entwickelt.

Ein am 05.09.2006 veröffentlichtes Advisory empfiehlt ein Update auf neuere OpenSSL-Versionen. Produkte, die direkt auf OpenSSL aufsetzen (z.B. BIND in Verbindung mit DNSSEC-Signaturen) sind ebenfalls betroffen, genauso die Browser Firefox (bis v1.5.0.6), SeaMonkey (bis v1.0.4), Opera (bis v9.01) sowie alle Netscape-Browser. Lachende Dritte sind diesmal der nicht betroffene Internet-Explorer (v6) und Apples Safari. Eine Alternative zu einem Upgrade ist das Entfernen von Root-Zertifikaten mit dem öffentlichen Exponenten „3" aus dem Zertifikatsspeicher des Browsers – die leider nach wie vor verwendet werden, obwohl deren Anfälligkeit für Angriffe seit mehr als 10 Jahren bekannt ist.

ISO 27001-Zertifikat für SAP SI

Den hochverfügbaren Serverzentren des Geschäftsbereichs Hosting der SAP Systems Integration AG am Standort Dresden wurde am 31.07.2006 vom BSI ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz verliehen. Diesem Beispiel werden in Kürze zweifellos weitere Unternehmen folgen, die in den beiden vergangenen Jahren eine IT-Grundschutz-Zertifizierung erfolgreich absolviert haben, da die Umstellung auf ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz mit moderatem Aufwand möglich ist.

BDSG 2006 in Kraft

Am 25.08.2006 wurde das „Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft" veröffentlicht. Es trat am 26.08.2006 in Kraft. Artikel 1 ändert das Bundesdatenschutzgesetz (BDSG): So wurde das Quorum, bis zu dem kein betrieblicher Datenschutzbeauftragter zu bestellen ist, von „höchstens vier Arbeitnehmer" in „höchstens neun Personen" geändert. Damit stellt der Gesetzgeber klar, dass es um die Zahl der Personen unabhängig von ihrem arbeitsrechtlichen Status geht – Geschäftsführer, Praktikanten, Auszubildende und externe Hilfskräfte zählen nun unstreitig dazu. Unternehmen, die unterhalb des Quorums liegen, werden damit jedoch nicht von den Pflichten des betrieblichen Datenschutzbeauftragten befreit. Die Neufassung des § 4g legt für diesen Fall fest, dass „der Leiter der Stelle die Erfüllung der Aufgaben (...) in anderer Weise sicher zu stellen" hat.

.dd -> .vmdk

Der erste Schritt in fast jeder forensischen Analyse ist das Erstellen einer Bit-genauen Kopie (Image) des zu untersuchenden Datenbestands, um die Analyse anschließend auf dieser Kopie durchführen zu können, ohne Originaldaten zu verändern. Oft kommt dabei das in der Unix-Welt verbreitete Tool „dd" zum Einsatz. Die so erstellten Images können dann einer statischen oder dynamischen Analyse unterzogen werden. Nachteil der dynamischen Analyse ist, dass dabei das Image grundsätzlich verändert wird – der Forensiker wird daher mehrere Images des Originals erstellen, damit er immer wieder auf den Ausgangszustand der Daten zurückgreifen kann.

Am 25.08.2006 wurde Live View vorgestellt, ein neuartiges Tool, das es erlaubt, dd-Images in virtuelle Maschinen zu konvertieren. Diese können anschließend mit der Software VMware analysiert werden, um beispielsweise Details über laufende Prozesse oder offene Netzwerkverbindungen auf dem zu untersuchenden Rechner zu erhalten.

Das Tool wurde im CERT-Umfeld entwickelt und setzt Java voraus. Es befindet sich noch in einem sehr frühen Entwicklungsstadium, läuft jedoch bereits recht stabil.

Besser zweimal messen ...

... als einmal vergessen. Getreu diesem Motto fand am 01.08.2006 im Rahmen des 15th Usenix Security Symposium in Vancouver der Workshop Metricon 1.0 engagierter Experten der securitymetrics.org-Community statt. Die 44 Teilnehmer diskutierten intensiv über den Sinn von Metriken, Software-Security-Metriken, Governance und insbesondere Case-Studies. Die Zusammenfassung und einzelnen Vortragsunterlagen geben einen guten Überblick über die aktuellen Entwicklungen. Dan Geer, Initiator von securitymetrics.org, hielt auf dem Symposium ein Tutorial zum Thema Measuring Security. Darin gab er einen umfassender Überblick über das Thema Metriken im Allgemein und in Bezug auf Sicherheit im Besonderen. Ein begrüßenswerter Trend zu mehr Mess- und Vergleichbarkeit in der IT-Sicherheit.

Awareness @ ENISA

Dass die Sensibilisierung von Mitarbeitern und Benutzern – neudeutsch auch „Security Awareness“ genannt – ein wichtiger Bestandteil eines übergreifenden Sicherheitskonzepts sein sollte, ist längst bekannt. Dennoch sind Konzeption und Umsetzung von erfolgreichen Awareness-Maßnahmen ein anspruchsvolles Unterfangen, wie Erfahrungsberichte auf Symposien oder in E-Books zeigen.

Diesem Umstand hat sich jetzt auch die noch relativ junge europäische Sicherheitsbehörde ENISA angenommen und am 10.08.2006 den Leitfaden “A Users' Guide: How to Raise Information Security Awareness“ veröffentlicht. Der Leitfaden enthält zahlreiche Tipps und Hilfestellungen für die Umsetzung eigener Awareness-Kampagnen und richtet sich auch an KMUs, deren Budget für derartige Projekte meist sehr begrenzt ist.

Dynamische Malware-Analyse

Kostenlose Web-Dienste zur Analyse von Viren und anderen verdächtigen Dateien existieren bereits seit einiger Zeit. Viele Antiviren-Hersteller bieten auf Ihren Webseiten entsprechende Online-Schnittstellen an (z.B. norman, virustotal oder jotti). Die Ergebnisse beschränken sich jedoch im Wesentlichen auf die Information, ob die untersuchte Datei mit einem bekannten Virus oder Wurm infiziert ist.

Einen Schritt weiter geht der am 20.09.2006 öffentlich angekündigte Dienst CWsandbox: Entstanden aus einer Diplomarbeit an der Uni Mannheim wurde eine Web-Schnittstelle zum Hochladen verdächtiger Dateien entwickelt. CWsandbox unterzieht diese Datei anschließend einer dynamischen Analyse; die Datei wird in einer kontrollierten Umgebung ausgeführt und beobachtet. CWsandbox dokumentiert für den untersuchten Prozess z.B. die nachgeladenen Systembibliotheken (DLLs), das Starten und Beenden weiterer Prozesse, Verändern oder Lesen von Registry-Einträgen, das Installieren oder Starten von Diensten sowie aktive Netzwerkverbindungen. Das Ergebnis wird dem Benutzer anschließend in Form einer XML-Datei per E-Mail übermittelt – ein echter Mehrwert bei der Analyse verdächtiger Anwendungen.

Wer AN.ONymisiert, wird beschlagnahmt

Im Rahmen aktueller Vorermittlungen der Staatsanwaltschaft Konstanz gegen die Verbreitung von Kinderpornografie wurden Anfang September ca. ein Dutzend IT-Systeme beschlagnahmt, unter denen sich auch Exit-Nodes und Kaskadensysteme der Anonymisierungsdienste TOR und AN.ON befanden, darunter auch ein System des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD). Ein déjà vu – AN.ON wurde am 03.07.2003 schon einmal per Gerichtsbeschluss verpflichtet, Protokollierungsdaten an Strafverfolgungsbehörden herauszugeben, mit längerem Nachspiel.

Der Informationsgewinn über die anonymisierten Dienstnutzer dürfte gering ausfallen, da in Mix-Netzen die Kommunikationsbeziehung nur dann rekonstruiert werden kann, wenn alle Systeme eines vollständigen „Kommunikationspfads“ vorliegen. Inwieweit die Professionalisierung zukünftiger Ermittlungen auch die Recherche bereits verfügbarer Informationen umfassen wird, bleibt abzuwarten.

Als sicher dagegen kann gelten, dass die Fahndungszielgruppe einfach auf ausländische Serverknoten solcher Anonymisierungsnetzwerke ausweichen wird, und dass sicherlich auch keine Backbonerouter von großen ISPs beschlagnahmt werden, die illegalen Inhalt transportieren (genauer: durchleiten und nicht speichern). Die nächste Generation von autonomen Anonymisierungsnetzwerken wird sich wohl ohnehin über Wurm-Mechanismen automatisch verbreiten, sodass der direkte Bezug zwischen Infrastruktur und Betreiber wegfällt – wie aber beschlagnahmt man einen Wurm?

Secorvo News

Secorvo College aktuell

Der Herbst steht bei Secorvo College im Zeichen des Sicherheitsmanagements: Einen umfassenden Einstieg bietet das bewährte Seminar „Information Security Management von A(udit) bis Z(ertifizierung)“ vom 17.-18./20.10.2006. Im November folgt ein ganz besonderes Seminar: Über 3,5 Tage werden vom 06.-09.11.2006 die „Erfolgsfaktoren für IT-Security Management“ beleuchtet. Darin werden die besonderen Anforderungen an Kommunikation, Präsentation, Gruppenmanagement und Führung vertieft und geübt, denen sich IT Security Verantwortliche stellen müssen. Das Seminar wird im Januar fortgesetzt.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

White Paper Security Management Praxis

Nach dem großen Erfolg seines Secorvo White Papers “BS 7799 – von Best Practice zum Standard“ (über 30.000 Downloads) hat Jörg Völker seine Einführung in das Sicherheitsmanagement nun um eine Case Study ergänzt, in der er an einem konkreten Fall seine Erfahrungen mit dem Aufbau zertifizierter Information Security Management-Systeme dokumentiert. Es ist als Secorvo White Paper Nr. 13 seit dem 24.09.2006 online.

Veranstaltungshinweise

Auszug aus www.veranstaltungen-it-sicherheit.de

Oktober 2006	
10.-12.10.	ISSE 2006 (TeleTrusT/EEMA, Rom/IT)
16.-20.10.	Information Security Management (Secorvo College, Karlsruhe)
17.-18.10.	DACH Mobility 2006 (GI/ÖCG/BITKOM/SI, München)
18.10.	KA-IT-Si-Jubiläumsfeier (KA-IT-Si, IHK Karlsruhe)
23.-27.10.	Systems 2006 (Messe München, München)
November 2006	
06.-09.11.	Erfolgsfaktoren für IT-Security Management (Secorvo College, Karlsruhe)
07.11.	IT Risk Management 2006 (COMPUTAS, Berlin)
14.-16.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
20.-25.11.	TISP-Schulung (Secorvo College, Karlsruhe)
26.11.	TISP-Prüfung (Secorvo College, Karlsruhe)
28.-30.11.	Kommunikationsschutz und Datensicherheit (Secorvo College, Karlsruhe)

Fundsachen

Auszug aus www.security-finder.de

Introducing a Free New Self-Service Tool That Runs Comprehensive Security Checks in Minutes, Not Days. Vorstellung des SAP-Tools "Security Optimization Self-Service", das mit dem SAP Solution Manager (ab Version 3.1) kostenfrei mitgeliefert wird. Es erleichtert Überprüfungen der Berechtigungen in einer SAP-Systemlandschaft.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Oktober 2006



Editorial: Verboten

Je mehr Verbote, desto ärmer das Volk.
Laotse, Dao-de-dsching

Verbote besitzen einen unbestreitbaren Vorteil: Mit ihnen wird zielgerichtetes Handeln des Gesetzgebers demonstriert – und diese Klarheit kommt an beim Publikum. Die Wirklichkeit dagegen besitzt einen hässlichen Nachteil: Sie ist komplex – und das häufig in größerem Maße, als es der Mensch mit seiner zur Vereinfachung neigenden Wahrnehmung zu erfassen vermag. Das dürfte die tiefere Ursache dafür sein, dass klare Verbote einerseits so beliebt sind – und mit ihnen andererseits oft nicht nur nicht das angestrebte Ziel, sondern sogar dessen Gegenteil erreicht wird.

Beispielhaft lässt sich dies bei der geplanten Änderung des Strafgesetzbuches beobachten. Mit dem neuen § 202c sollen Vorbereitungshandlungen des Ausspähens und Zugänglichmachens von Daten unter Strafe gestellt werden – darunter auch die Herstellung, Verschaffung und Verbreitung von Computerprogrammen, „deren Zweck die Begehung einer solchen Tat ist". An wenigstens drei grundsätzlichen Fehlverständnissen krankt dieses Vorhaben:

1. *Ein Hacker-Tool ist von einem Sicherheits-Tool oft nicht unterscheidbar*. So wird der ehemalige Trojaner Netbus heute als Tool für die Remote-Wartung vertrieben, und Cain & Abel wird zur Wiedergewinnung verlorener Passwörter empfohlen. Eine „objektive Zweckbestimmung" ist da schwer auszumachen.
2. *Die öffentliche Verbreitung von Angriffs-Tools ist ein Sicherheitsgarant*. Nur wenn Hacker nicht im Verborgenen wirken, wissen wir, was sie wirklich können. Dies ist wesentliche Vorbedingung für das Ergreifen angemessener Sicherheitsmaßnahmen.
3. *Die Nutzung von Hacker-Tools steigert die Sicherheit von IT-Infrastrukturen* – das fordert auch das BSI und verbreitet Nessus seit dem 17.06.2005 (SSN 06/2005) über ihre BOSS-CD. Vielleicht hört die Justizministerin wenigstens auf das Bundesamt?



Inhalt

Editorial: Verboten

Security News

Schach den Wahlmaschinen

Internet Security Threat Report

iPod spielt „Trojanisches Pferd"

USB Dumper

Panzerung publik

Überblick SAP-Ports

Manipulation des Vista Kernel

Security Awareness Monitor

Secorvo News

Secorvo College aktuell

T.I.S.P. @ Secorvo College

Erfolgreiches KA-IT-Si-Jubiläum

Veranstaltungshinweise

Fundsachen

secorvo
security consulting

Security News

Schach den Wahlmaschinen

Seit einigen Jahren werden zur Vereinfachung des Auszählungsverfahrens bei Wahlen Maschinen der niederländischen Firma Nedap für die Stimmabgabe eingesetzt. Das Modell ESD1 besitzt eine Zulassung des Bundesinnenministeriums; mehr als 15 Mio. Stimmabgaben erfolgten bisher bei Kommunal-, Landtags- und Bundestagswahlen auf solchen Geräten. Geschäftsführer Jan Groenendaal preist seine Geräte als „Dedicated Special Purpose" Maschinen: „Dass man mit unserer Wahlmaschine auch Schach spielen kann, würde ich gerne vorgeführt bekommen."

Der Spott dürfte ihm am 04.10.2006 im Halse stecken geblieben sein: In einem Bericht des niederländischen Fernsehens demonstrierte eine Aktivistengruppe ihren „Nedap Schachcomputer" – der Austausch des EPROMs beim (in 90 % der Wahllokale in den Niederlanden eingesetzten und mit ESD1 weitgehend baugleichen) Wahlcomputer ES3B dauerte keine fünf Minuten, die Anbringung des Schachbretts auf der schrägen Bedienfläche war etwas aufwändiger.

Am 05.10.2006 publizierte die Gruppe eine umfangreiche Sicherheitsanalyse und schob am 10.10.2006 auf YouTube ein Video nach, das zeigt, dass die Stimmabgabe noch aus 25 m Entfernung abgehört werden kann. Tatsächlich lassen sich Manipulationen an Wahlmaschinen nur durch Geräteprüfungen verbunden mit signiertem Programmcode und versiegelten Maschinen nachweisen – eine sehr aufwändige Prozedur, die allerdings nicht vor Manipulationscode im Original-EPROM schützt.

Internet Security Threat Report

Am 25.10.2006 veröffentlichte Symantec ihren 10. Internet Security Threat Report. Darin werden auf gut 100 Seiten die von Symantec im Zeitraum vom 01.01. bis 30.06.2006 mit über 40.000 Sensoren weltweit beobachteten Bedrohungen zusammengefasst. Gegenüber früheren Reports ist bei Angriffen eine Verlagerung der Ziele von der Infrastruktur hin zu Endbenutzer-PCs und Web-Applikationen zu beobachten. Ursächlich dürfte dies auf eine Verschiebung der Interessen von Angreifern zurück zu führen sein – weg von „traditionellen" Motiven wie Geltungssucht hin zu kriminellen Interessen.

Etwa 69 % aller gefundenen Schwachstellen betreffen Web-Applikationen. Hier besteht seitens der Software-Entwickler erheblicher Handlungsbedarf – vor allem, weil diese Schwachstellen 78 % aller leicht nutzbaren ausmachen. Meist handelt es sich um längst bekannte Probleme wie SQL-Injection und Cross-Site-Skripting. Ebenfalls bemerkenswert ist der starke Anstieg von Phishing-Attacken, die im Beobachtungszeitraum um 81 % auf über 157.000 unterschiedliche Nachrichten anstiegen. Als Top-Herausforderungen sieht der Report die Entwicklungen um Web 2.0 (AJAX) und Windows Vista.

iPod spielt „Trojanisches Pferd"

Am 18.10.2006 gab Apple bekannt, dass Video-iPods mit dem Windows RavMonE.exe-Virus ausgeliefert worden waren. Erst am 13.10.2006 hatte die japanische McDonalds-Zentrale vor 10.000 im Rahmen eines Gewinnspiels verteilten, mit dem Trojaner QQPass verseuchten MP3-Playern gewarnt. Zwei Beispiele für Bedrohungen, die in Geräten aus vermeintlich vertrauenswürdiger Quelle lauern können – Trojanische Pferde im ursprünglichen Sinn.

USB Dumper

Dass *mit* USB-Sticks Viren übertragen oder unerlaubt Daten ausgetauscht werden können, ist bekannt. Die Bedrohung *von* USB-Sticks wird jedoch meist nicht gesehen: Steckt man den eigenen USB-Stick in ein fremdes System, auf dem ein Tool wie „USB-Dumper" installiert ist, so werden unbemerkt sämtliche Inhalte des Sticks auf das System kopiert. Ebenso ist es möglich, ein komplettes Image des USB-Sticks zu erstellen, mit dem selbst gelöschte Dateien wieder hergestellt werden können.

Daher ist grundsätzlich der Einsatz von Verschlüsselungslösungen für sensible Daten auf USB-Sticks, mindestens aber eines Tools zum sicheren Löschen (wie beispielsweise „Eraser") zu empfehlen.

Panzerung publik

Am 10.10.2006 berichtete die Financial Times Deutschland über einen bereits am 21.09.2006 erfolgten Diebstahl von Laptops und Flachbildschirmen aus einem VW- und Audi-Vertriebszentrum in Teltow. Das ermittelnde LKA hat den Fall als brisant eingestuft, da auf den entwendeten Systemen auch Informationen über die Sicherheitseigenschaften und -ausstattungen sowie den Aufbau der Dienstfahrzeuge hochrangiger Spitzenpolitiker gespeichert sein sollen. Die Meldung gelangte trotz Nachrichtensperre während der noch andauernden Ermittlungen in die Öffentlichkeit.

Bleibt zu hoffen, dass der Vorfall nicht nur den betroffenen Unternehmen zu denken gibt, sondern allen, die noch immer über keinen durchgängigen Schutz sensibler Daten insbesondere auf mobilen Systemen verfügen – selbst wenn es sich herausstellen sollte, dass es sich in diesem Fall um keinen gezielten Informationsdiebstahl gehandelt hat.

Überblick SAP-Ports

SAP veröffentlichte am 13.10.2006 im NetWeaver Security Knowledge Center eine Neufassung der praktischen und umfassenden Übersicht der von den unterschiedlichen SAP-Anwendungen genutzten TCP- und UDP-Ports. Allein die Zahl der Kommunikationsmöglichkeiten verdeutlicht, wie wichtig es ist, beim Einsatz von SAP-Anwendungen ein ausgereiftes Netzsicherheitskonzept umzusetzen – mit jeder Schwachstelle in der Software droht sonst ein Einfallstor.

Begrüßenswert wäre es allerdings, wenn SAP sich hinsichtlich der genutzten und publizierten Ports mit den Protocol Number Assignment Services der global anerkannten Portliste von IANA abstimmen würde.

Manipulation des Vista Kernel

Einen perfiden Angriff auf den Vista Kernel demonstrierte Joanna Rutkowska auf der diesjährigen Blackhat: Es gelang ihr, durch direkte Zugriffe auf die Festplatte das Swapfile so zu manipulieren, dass dem Vista Kernel unsignierter Code untergeschoben wurde – was die Architektur des Kernels eigentlich durch die Verwendung von Codesignaturen verhindern sollte.

Abhilfe könnte eine Verschlüsselung des Swapfiles schaffen; damit wäre der für diesen Angriff erforderliche direkte Plattenzugriff nicht mehr möglich. Alternativ könnte man auch – ausreichend physikalischen Speicher vorausgesetzt – das Swapfile komplett deaktivieren. Denn das Konzept der „Auslagerung von RAM auf Festplatte" stammt aus Zeiten, in denen Speicherbausteine noch sehr teuer waren.

Security Awareness Monitor

Das Steinbeis-Beratungszentrum Karlsruhe hat auf der Grundlage wissenschaftlicher Methoden der Marktforschung ein Tool entwickelt, mit dem die Sensibilität (Awareness) der Mitarbeiter für Belange der IT-Sicherheit gemessen werden kann – den Security Awareness Monitor (SAM). Der Monitor wurde bereits erfolgreich zur Erfolgsmessung in einer Awareness-Kampagne der T-Systems eingesetzt. Die Ergebnisse dieser Messungen hatte Professor Dr. Konrad Zerr, Leiter des Beratungszentrums, auf dem diesjährigen Karlsruher Security Awareness Symposium vorgestellt.

Secorvo News

Secorvo College aktuell

Neben der Zertifizierung zum T.I.S.P. vom **20. bis 25.11.2006** (siehe unten) gibt es in diesem Jahr noch zwei weitere Gelegenheiten, vom Wissenstransfer eines Secorvo College-Seminars zu profitieren:

- Vom **14. bis 16.11.2006** vermittelt das Seminar „IT-Sicherheitsaudits in der Praxis" unsere Best Practices aus acht Jahren Sicherheitsaudits.
- Vom **28. bis 30.11.2006** folgt ein echter Klassiker: die aktuelle Fassung eines des erfolgreichsten College-Seminare: Kommunikationsschutz und Datensicherheit – intern, extern, mobil.

Programm, Preise und Online-Anmeldung unter

http://www.secorvo.de/college

T.I.S.P. @ Secorvo College

In fünf Tagen zum zertifizierten Information Security Professional: Mit mehr als 100 Absolventen hat sich der „TeleTrusT Information Security Professional" (T.I.S.P.) in weniger als drei Jahren zu einem der verbreitetsten Security-Zertifikate „gemausert".

Dieser Entwicklung trägt Secorvo College durch das Angebot eines T.I.S.P.-„Steilkurses" Rechnung – erstmalig vom **20. bis 25.11.2006** inklusive zugehöriger Prüfung. Für diese Erstveranstaltung zahlen alle Teilnehmer den Frühbucherpreis.

Erfolgreiches KA-IT-Si-Jubiläum

Am 18.10. feierte die auf Initiative von Secorvo und den Karlsruher Versicherungen Anfang 2001 gegründete Karlsruher IT-Sicherheitsinitiative (kurz: KA-IT-Si) ihr fünfjähriges Bestehen – mit weit über 100 Teilnehmern, einer Key Note des Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik, BSI (vertreten durch den Abteilungspräsidenten Bernd Kowalski) und Vorträge und Demonstrationen rund um ein ganzheitliches Verständnis der IT-Sicherheit.

Pünktlich zum Geburtstag stießen zwei neue Partner zur Initiative: die Karlsruher ptv AG und die CONNECT Karlsruhe Computer und Netzwerktechnik GmbH.

Die Unterlagen der Veranstaltung können von der Webseite der Sicherheitsinitiative heruntergeladen werden.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2006	
23.-27.10.	Systems 2006 (Messe München, München)
November 2006	
07.11.	IT Risk Management 2006 (COMPUTAS, Berlin)
14.-16.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
20.-24.11.	TISP-Schulung (Secorvo College, Karlsruhe)
25.11.	TISP-Prüfung (Secorvo College, Karlsruhe)
28.-30.11.	Kommunikationsschutz und Datensicherheit (Secorvo College, Karlsruhe)
Dezember 2006	
04.-05.12.	IsSec / ZertiFA 2006 (COMPUTAS, Berlin)
27.-30.12.	23. Chaos Communication Congress (CCC, Berlin)

Fundsachen

Auszug aus www.security-finder.de

Security Engineering –
A Guide to Building Dependable Distributed Systems
Das wegweisende Standardwerk von Ross Anderson ist nun auch online verfügbar. Obwohl fünf Jahre auf dem Markt, hat es nichts an Aktualität eingebüßt, sondern thematisiert alle für die Entwicklung von IT-Systemen relevanten Sicherheitsaspekte, von Passwörtern über Protokolle, Tamper Resistance und Telekommunikationssicherheit bis Monitoring und Management. Ein Muss für alle, die mit Design, Entwicklung oder Implementierung sicherer Systeme befasst sind.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

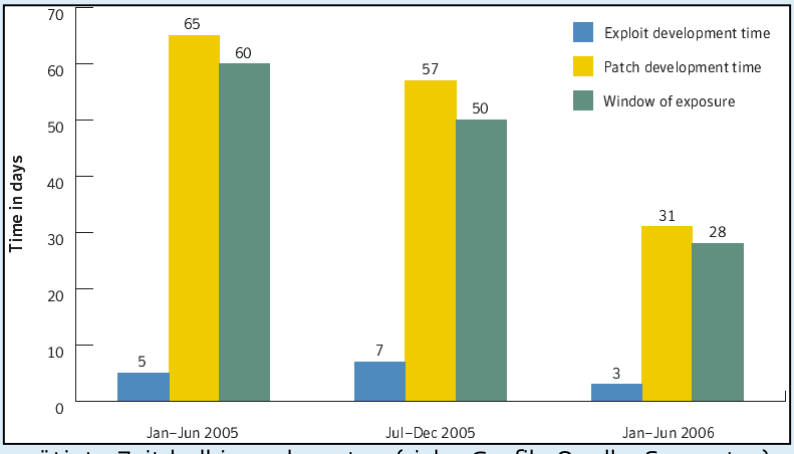
Secorvo Security News

November 2006



Editorial: Mo*Bing

Die Zahl gefundener sicherheitskritischer Programmfehler steigt – allen Bemühungen um sichere Software zum Trotz. Jetzt nehmen Cracker die Hersteller gar in den Schwitzkasten: Während noch diskutiert wird, ob die Veröffentlichung eines sicherheitskritischen Bugs ohne Vorabinformation des Herstellers und ohne „Anstandsfrist“ vertretbar ist, haben einige Cracker offenbar die letzten Hemmungen abgelegt: Mit der Veröffentlichung von „Zero-Day“-Bugs zwingen sie Herstellern einen Wettlauf mit den Entwicklern von Exploit-Code auf. Eine Entwicklungsabteilung, die jeden Patch für heterogene Umgebungen testen muss, bevor sie ihn ausrollen kann, hat gegen Tausende Ehrgeiz getriebene Cracker keine faire Chance – auch wenn die Hersteller die zur Patchentwicklung



benötigte Zeit halbieren konnten (siehe Grafik; Quelle: Symantec).

Nun folgt gezieltes „Mo*Bing“: Nach dem Monat der Browser-Bugs (MoBB, 6/2006) und dem der Kernel-Bugs (MoKB, 11/2006) wurde für Anfang Dezember die Woche der Oracle Database Bugs angekündigt (WoODB). Gezielte Attacken mit Ansage auf selbstgerecht



Inhalt

Editorial: Mo*Bing

Security News

Datensammeln im Vorbeigehen

Bugs mit Ansage

Preisgekrönte Verlierer

Top 20 Internet Security Targets

Sysinternals reloaded

Unabhängigkeitsverluste

Phrowsers Phisherschutz phisht phrischer

Core Wars

Secorvo News

Secorvo College aktuell

Video “Social Engineering”

Veranstaltungshinweise

Fundsachen

secorvo
security consulting

Security News

Datensammeln im Vorbeigehen

Die am 23.10.2006 veröffentliche Entwurfsfassung der RFID-Studie "Vulnerabilities in first-generation RFID-enabled credit cards" belegt, dass aus mit RFID-Chips ausgestatteten Kreditkarten (Anteil: ca. 6 % des US-amerikanischen Kreditkartenmarkts) führender Anbieter die Kartendaten (Name, Kartennummer und Ablaufdatum) unbemerkt ausgelesen werden können. Den Autoren gelang es sogar, mit den abgegriffenen Daten RFID-Chips zu „klonen", sofern keine kryptografischen Komponenten integriert waren.

Angesichts zahlreicher Projekte zur Einführung RFID-basierter Ausweispapiere verdichtet sich der Eindruck, dass teilweise bewährte Sicherheitstechnologien leichtsinnig abgelöst werden. Die Möglichkeit zum spurenlosen und unbemerkten Auslesen von Ausweiskarten birgt zudem die Gefahr der „informationellen Aushorchung".

Bugs mit Ansage

Am 01.11.2006 startete die Kampagne „Month of Kernel Bugs". War der „Month of Browser Bugs" im Juli 2006 eher zum „Warmlaufen", steht jetzt das Allerheiligste der Betriebssysteme im Fokus. Jeden Tag im November wird auf der Webseite der Kampagne ein neuer Kernel-Bug publiziert. Der Initiator mit dem Pseudonym „LMH", einer der Forscher des Metasploit-Projekts, wird einen großen Teil davon aus seiner Sammlung bisher unveröffentlichter Bugs beitragen. Gefunden hat er sie mit Hilfe einer Technik aus dem Jahr 1989: Fuzzing, dem Füttern von Anwendungen mit automatisch erzeugten, pseudo-zufälligen Eingaben.

Dass bei dieser Art des Black-Box-Testings überhaupt Fehler in Betriebssystemen gefunden werden, ist ernüchternd – zeigt es doch, dass viele Softwarehersteller nach wie vor erheblichen Nachholbedarf in Sachen Softwarequalität haben. Dabei findet man mit Fuzzing nur vergleichsweise triviale Fehler. Wie mag es da erst um das Security-Engineering dieser Anwendungen bestellt sein?

Preisgekrönte Verlierer

Zum siebten Mal wurden am 20.10.2006 Institutionen, Organisationen und Einzelpersonen mit den Big Brother Awards 2006 prämiert – Auszeichnungen, zu deren Verleihung die Preisträger in der Regel nicht erscheinen. Einen Award erhält, wer in den Augen der Jury zu den Zeitgenossen zählt, die auf besonders kritikwürdige Weise mit personenbezogenen Daten umgehen. Dies kann, muss aber nicht automatisch ein Gesetzesverstoß sein.

Die jährlich wachsende Zahl der Vorschläge, aus denen die Jury die Preisträger auswählt, spricht für sich: In diesem Jahr mussten Unterlagen zu 350 potenziellen Preisträgern gesichtet und beurteilt werden, darunter zunehmend Meldungen verärgerter und enttäuschter Verbraucher, die sich über datenschutzfeindliche Praktiken zahlreicher Unternehmen beschweren.

Der Gesamtverband der deutschen Versicherungswirtschaft stand ganz oben in der Publikumsgunst für den intransparenten Betrieb seiner inhaltlich fragwürdigen Warn- und Hinweisdateien. Leicht abgeschlagen folgte die Kultusministerkonferenz für ihre Bemühungen, ohne die Berücksichtigung von Zweckbindung und anderen datenschutzrechtlichen Erfordernissen eine lebenslang gültige Schüler-ID einzuführen. Weitere Preisträger waren SWIFT (für die Durchbrechung des Bankgeheimnisses durch die Übermittlung von Überweisungsdaten an US-Behörden), die Philips GmbH (für die Vorgabe, dass CD-Brenner ihre eindeutige Seriennummer auf den Rohling schreiben und damit eine Rückverfolgbarkeit von Datenträgern zum Brenner ermöglichen), der Landtag von Mecklenburg-Vorpommern (für die Erlaubnis zum Abhören und zur Tonaufzeichnung an öffentlichen Plätzen, in öffentlichen Gebäuden und in öffentlichen Verkehrsmitteln) und die Innenministerkonferenz (für den Beschluss zur Einrichtung einer Anti-Terror-Datei).

Top 20 Internet Security Targets

SANS hat am 15.11.2006 die sechste jährliche Liste der 20 „Spitzenreiter" kritischer Security-Bedrohungen publiziert. Die Aufzählung fehlerhafter Cross-Plattform-Anwendungen führen diesmal die Web-Applikationen an. Erstmals berücksichtigt die Liste nicht nur Software, sondern enthält auch eine Rubrik „Security Policy and Personnel", in der nicht genehmigte Devices (wie USB Flash Drives), extensive Nutzerrechte, Phishing und unautorisierte Software vier der 20 Spitzenplätze belegen. Als Sonderrubrik wurden „Zero-Day"-Exploits aufgenommen, da sich hier ein bedenklicher Trend abzeichnet: Die Rubrik verzeichnet 20 Patches für verbreitete Betriebssysteme und Office-Programme, zu denen vor Veröffentlichung des Patches Exploits kursierten. Auch VoIP Server und Telefone haben die Aufnahme in die Top 20 geschafft.

Hilfreich ist die Liste, an deren Erstellung mehr als 50 Security-Experten und -Institutionen mitwirkten, nicht nur für die Priorisierung von Überprüfungen der eigenen Infrastruktur. Sie enthält auch Links auf alle Updates und Patches der gelisteten kritischen Systeme, die im Laufe des vergangenen Jahres veröffentlicht wurden.

Sysinternals reloaded

Das am 09.11.2006 publizierte neue Microsoft-Tool Process Monitor (v1.01, 913 kB) – nicht zu verwechseln mit dem Werkzeug „Process Explorer“ – zeigt nicht nur, wie der Name vermuten lässt, laufende Prozesse an, sondern kombiniert auch die Eigenschaften der beiden Monitoring-Tools Filemon und Regmon in einer Oberfläche. Process Monitor kann sowohl helfen, Systemproblemen auf die Spur zu kommen, als auch bei forensischen Echtzeit-Analysen komplexe Vorgänge abbilden. Gegenüber den bereits vorhandenen Tools verbesserte Microsoft insbesondere Filter- und Export-Möglichkeiten.

Unabhängigkeitsverluste

Im September und Oktober vollzogen sich einige wesentliche Änderungen der Security-Landschaft. Am 25.09.2006 gab die kalifornische Firma Breach Security Inc. die Akquisition von Thinking Stone Ltd. bekannt, dem Hersteller von modsecurity (Apache Modul und Basis vieler Web Application Firewall-Architekturen). Der Innovationsbereitschaft scheint das zunächst keinen Abbruch getan zu haben: Am 16.10.2006 erschienen neue Major-Releases von modsecurity: für Apache (2.0.4), Core Rules (2.0) und Console (1.0.0).

Knapp einen Monat später, am 20.10.2006, hatte IBM die am 23.08.2006 angekündigte Übernahme des in Atlanta ansässigen Sicherheitsspezialisten Internet Security Systems abgeschlossen. Und wenige Tage danach gab die 1999 von Bruce Schneier gegründete Counterpane Internet Security Inc. am 25.10.2006 ihre Unabhängigkeit auf – das Unternehmen gehört nun zu British Telecom (BT).

Wie schon die Übernahme von RSA durch EMC² sind dies deutliche Anzeichen für eine beginnende Konsolidierung des (amerikanischen) Sicherheitsmarkts, bei der selbst erfolgreiche Spezialisten unter die Fittiche großer Unternehmen schlüpfen – für den Preis der Aufgabe ihrer Unabhängigkeit.

Phrowsers Phisherschutz phisht phrischer

Der seit 01.11.2006 verfügbare Internet Explorer 7 arbeitet zur Abwehr von Phishing mit einer lokalen Whitelist von mehreren tausend seriösen Websites, parallel führt Microsoft eine zentrale Blacklist. Demgegenüber verwendet die seit dem 25.10.2006 erhältliche Firefox 2-Version eine lokale Blacklist von gemeldeten Phishing-Websites.

Entscheidend für die Filterung von Phishing-Websites ist die Aktualität der verwendeten Blacklist. Da hat das Modell der zentralen Blacklist, die wie beim IE 7 online angefragt wird, klare Vorteile gegenüber einer lokalen Blacklist (Firefox 2.0), die in regelmäßigen Zeitabständen aktualisiert wird.

Phishing-Blacklists haben bekanntermaßen (ähnlich Blacklists von Mailservern, die E-Mail-Adressen und Domänen von Spammern enthalten) das Problem, dass Firmen und Organisationen, die irrtümlich oder durch Denunzierung auf die Liste gerieten, nur schwer wieder gelöscht werden. Welche Prüfungen Microsoft oder Mozilla (via Google) durchführen, bevor eine Website auf eine solche Blacklist von Phishing-Websites gelangt, ist nicht bekannt. Nicht bekannt ist weiter, wie sorgfältig die Überprüfung der gemeldeten Websites überhaupt durchgeführt werden kann, sobald das System allgemein genutzt wird, da eine Phishing-Website im Schnitt nur eine „Lebenserwartung“ von vier bis sechs Tagen hat.

Derzeit dürfte das Vertrauen in eine von Google geführte Blacklist vermutlich höher sein als die Akzeptanz einer von Microsoft verwalteten Liste.

Core Wars

Die am 18.10.2006 von SecureWorks vorgestellte und am 13.11.2006 ergänzte Analyse lässt das Entstehen eines darwinistischen Überlebenskampfes unter Trojanern um ihren Lebensraum befürchten. Offenbar setzen Trojaner gezielt Sicherheitssoftware zur Löschung konkurrierender Malware und zur Verhinderung einer erneuten Reinfektion ein. So wird der Trojaners SpamThru (Botnetz und Spamgenerator) über seine Control Server mit einer Routine versorgt, die eine raubkopierte Antivirensoftware installiert. Der Kampf um die Kernel hat begonnen.

Secorvo News

Secorvo College aktuell

Im Januar startet das Seminarprogramm 2007 mit **Information Security Management** (23.-26.01.2007), gefolgt von den „Klassikern“ **PKI** (30.01.-02.02.2007) und **IT-Sicherheit heute** (06.-08.02.2007).

Die nächste Möglichkeit zur Zertifizierung Ihres Security-Know-Hows bietet Ihnen das **T.I.S.P.-Seminar** am 05.-09.03.2007 (Prüfung am 10.03.).

Programm, Preise und Online-Anmeldung unter

http://www.secorvo.de/college

Video “Social Engineering”

Der wachsenden Bedeutung von “Social Engineering” bei Wirtschaftsspionage und Hacking-Attacken tragen wir durch ein neues Sensibilisierungsvideo Rechnung. Das Video ist ab Mitte Dezember in deutscher und (als Netzlizenz) englischer Sprache erhältlich (www.secorvo.de/video).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2006	
28.-30.11.	Kommunikationsschutz und Datensicherheit (Secorvo College, Karlsruhe)
Dezember 2006	
04.-05.12.	IsSec / ZertiFA 2006 (COMPUTAS, Berlin)
27.-30.12.	23. Chaos Communication Congress (CCC, Berlin)
24.12.	Weihnachten (Weihnachtsmann, weltweit)
Januar 2007	
18.-19.01.	Tutorium "IT-Sicherheitskriterien im Vergleich" (DFN-CERT Services GmbH, Hamburg)
18.-19.01.	Tutorium "DFN-PKI in der Praxis" (DFN-CERT Services GmbH, Hamburg)
23.-26.01.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
30.01.-02.02.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)

Fundsachen

Auszug aus www.security-finder.de (Webanwendungen)

Sicherheit von Webanwendungen – Maßnahmenkatalog und Best Practices: Die aktuelle BSI-Studie (Stand 11.09.2006) enthält eine umfangreiche Zusammenstellung von Maßnahmen zur Sicherung von Webapplikationen und Best Practice Ansätzen sowie einen Leitfaden für die Erstellung sicherer Webanwendungen, der für Projektleiter, Entwickler und ggf. auch Auditoren interessant sein dürfte.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Petra Barzin, Dirk Fox, Stefan Gora, Kai Jendrian, Jochen Schlichting, Karin Schuler

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Dezember 2006



Editorial: Top five

Die Tyrannei der Listen, denen Nick Hornby 1995 in „High Fidelity“ ein Denkmal gesetzt hat, beschränkt sich längst nicht mehr auf die „Top Ten“ des Musikgeschäfts. Wer heute ein Buch sucht, kommt an den einschlägigen „Bestsellerlisten“ kaum vorbei, und jeder Online-Shop, der etwas auf sich hält, bietet auf Mausklick eine Übersicht der meistverkauften Produkte. Nun haftet diesen „Best of“ ein wenig der Ruch einer Aktienempfehlung an: Hat ein Produkt den Olymp einer Top-Liste erklommen, wird die Nennung zur „self fulfilling prophecy“ (Robert K. Merton). Dabei ist deren Zustandekommen oft nicht frei von Willkür: Erst kürzlich wurde ein Plattenproduzent überführt, große Bestände einer Neuerscheinung selbst aufgekauft zu haben, um mit dem Bestseller-Status die Verkäufe anzukurbeln. Eine probate Methode, um Ladenhüter in Saisonhits zu verwandeln.

Auch in der IT-Sicherheit geht der Trend zur Liste: SANS veröffentlicht seit sechs Jahren die „Top 20“ der Internet Security Attack Targets, OWASP pflegt seit 2003 die „OWASP Top Ten“ der kritischsten Fehler in Web-Anwendungen, und auf den Webseiten aller Anti-Viren-Hersteller findet man die „Viren des Monats“.

Bei so viel Orakel-Prominenz wollen wir uns nicht drücken – daher hier die Secorvo Top Five der Security-Trends 2007:

1. ***Sichere Softwareentwicklung***: Wenn die Software-Industrie hier nicht punktet, droht eine Regulierung der EU.
2. ***Awareness***: Angesichts zunehmender Mobilität und technischer Konvergenz wird das Nutzerverhalten zum Schlüsselfaktor.
3. ***Datenschutz***: Sensibilisierte Benutzer und gestärkte Aufsichtsbehörden reduzieren das verbreitete Vollzugsdefizit.
4. ***Best Practices***: Gestiegene (Haftungs-) Risiken lassen den Ruf nach Standards, Audits und Best Practices lauter werden.
5. ***Anti-Phishing***: Gelingt es nicht, den kriminellen Onlinekonten-Zugriff zu stoppen, kann das Vertrauen in das eBusiness kippen.



Inhalt

Editorial: Top five

Security News

BOSS reloaded

Zero-Day und Hexenjagd

Final BS 25999-1:2006

Fuzzing with JBroFuzz

DFN-PKI CA im Browser

Virtuelle Kriminalität

Honey-Clients

Privatsphäre mit Microsoft

Alle Jahre wieder...

Augen auf beim Weihnachtskauf

Secorvo News

Secorvo College aktuell

T.I.S.P.

Veranstaltungshinweise

Fundsachen

secorvo
security consulting

Security News

BOSS reloaded

Am 01.12.2006 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Verfügbarkeit der Version 2.0 seiner Sicherheits-CD BOSS (BSI OSS Security Suite) bekannt gegeben. Sie umfasst Version 2.2.8 von Nessus mit deutsch übersetzter Oberfläche; die Nessus-Meldungen erscheinen allerdings nur in englisch. Unter den weiteren Tools zur Sicherheitsanalyse findet sich überraschend Version 0.10.10 des bekannten Sniffers Ethereal vom 11.03.2005 (statt einer aktuellen Version des Nachfolgers Wireshark).

Auch wenn die BOSS-CD aus den inzwischen zahlreichen Tool-Suites nicht signifikant hervor sticht – die Veröffentlichung ist ein Signal, dass das BSI weiterhin auf die Rechtmäßigkeit des Besitzes und der Verbreitung von Hacking-Tools setzt.

Zero-Day und Hexenjagd

Seit Anfang Dezember gibt es einen öffentlichen und übersichtlichen Informationsdienst zu Echtzeitschwachstellen (Zero-Day Tracker). Darin werden erstmals alle Schwachstellen zusammengefasst, für die bereits technische Details zur Ausnutzbarkeit bekannt sind, der Hersteller aber noch keinen Patch veröffentlicht hat. Wichtig für IT-Sicherheitsmanager, die ihre Risiken aktiv steuern, sind die Angabe, wie lange eine ungepatchte Schwachstelle bereits bekannt ist (z.B. seit 393 Tagen) und wie zwischenzeitlich improvisiert werden kann. Ob zukünftig dort auch nicht behobene Fehler von Anwendungen, Datenbanken und Netzsoftware eingestellt werden, bleibt abzuwarten.

Von den Herstellern sollte das Angebot als Ansporn zur Verbesserung der Sicherheit in der Softwareentwicklung verstanden werden. Repressalien sind sicher die falsche Antwort, wie im Fall des Boarding Pass Generators "Create your own boarding pass" für Northwest Airlines versucht: Der PhD-Student Christopher Soghoian hatte darin ein seit über drei Jahren bekanntes organisatorisches Sicherheitsloch als Proof-of-Concept in Software umgesetzt.

Final BS 25999-1:2006

Ende November 2006 wurde vom British Standards Institute (BSI) die Endfassung des BS 25999-1:2006 veröffentlicht. Dieser „Code of Practice for Business Continuity Management" gibt Empfehlungen für Notfall- und Notfallvorsorgeplanung in Unternehmen. Ein zweiter Teil, der eine Zertifizierung analog BS 7799-2 ermöglichen wird, soll 2007 folgen. Der neue Standard löst PAS 56 ab und wird ergänzt durch die im August 2006 veröffentlichten Empfehlungen PAS 77:2006 „IT Service Continuity Management".

Eine Gelegenheit zum Erfahrungsaustausch bietet vom 01.-02.02.2007 die Konferenz „3rd Annual: BUSINESS CONTINUITY 2007" in London.

Fuzzing with JBroFuzz

Am 13.11.2006 wurde im OWASP-Projekt das Fuzzing-Tool JBroFuzz veröffentlicht. JBroFuzz ist ein „stateles network protocol fuzzer" zur Aufdeckung von Schwachstellen in Netzwerkprotokollen durch halbautomatisch generierte fehlerhafte Datenpakete. Die intuitive Oberfläche von JBroFuzz erlaubt auch Anfängern, die Funktionsweise von Fuzzing nachzuvollziehen und anzuwenden. Das in Java programmierte Tool steht plattformübergreifend zur Verfügung.

Die Architekturen von Web 2.0 stellen neue Anforderungen an die Sicherheit von Online-Anwendungen. Interessant, auch im Zusammenspiel mit JBroFuzz, ist das Mozilla-Plugin Firebug, mit dem sich die Sicherheit von Web-Applikationen schnell auf vielfältige Weise untersuchen lässt.

DFN-PKI CA im Browser

Die oberste Zertifizierungsstelle des Deutschen Forschungsnetzes, die DFN-PCA, feiert 2006 ihren 10. Geburtstag. Dass sie nicht zum alten Eisen zählt, beweisen etliche Neuigkeiten, über die am Nikolaustag informiert wurde. Die spektakulärste darunter ist, dass das Root-Zertifikat der DFN-PCA ab sofort über einen direkten Zertifizierungspfad in die wichtigsten Standard-Browser verfügt.

Um dies zu realisieren wählte man nicht den teuren und aufwändigen Weg der direkten Einbindung in die Browser – vielmehr hat eine Kooperation mit der in den Browsern bereits enthaltenen Deutsche Telekom Root CA dazu geführt, dass störende Warnmeldungen, z.B. beim Aufbau einer SSL-Verbindung, der Vergangenheit angehören. Von diesem im Forschungsumfeld bislang weltweit einmaligen Schritt profitieren sowohl Endanwender mit kostenlosem Webserver-Zertifikat als auch die vielen Forschungseinrichtungen, die den Betrieb ihrer CA an die DFN-PKI ausgelagert haben.

Virtuelle Kriminalität

Am 21.02.2005 veröffentlichte McAfee den ersten Bericht zum Thema virtuelle Kriminalität. Beschrieben wurde darin der Trend zum Missbrauch des Internet für Zwecke des organisierten Verbrechens.

Am 08.12.2006 wurde der zweite Bericht der Öffentlichkeit vorgestellt. Er enthält eine Reihe kon-

kreter Fallstudien und Zitate von Security-Experten zu virtueller Kriminalität. Zu den drei wesentlichen Erkenntnissen zählen (1) die Entstehung einer neuen Generation von Kriminellen, die das Internet für Straftaten nutzt, die bislang nicht oder nur schwer durchführbar waren; (2) die Entdeckung der Missbrauchsmöglichkeiten durch die organisierte Kriminalität, die insbesondere Großereignisse wie die Fußball-WM für virtuelle Straftaten ausnutzt; sowie (3) die noch immer unterschätzte Bedrohung durch Innentäter. Nur der Titel mag nicht passen – denn virtuell ist diese Kriminalität bei Weitem nicht.

Honey-Clients

Die Honeypot-Technologie wird in der Regel server- oder netzwerkseitig – beispielsweise in Form kompletter Honeynets – betrieben. Einen interessanten anderen Ansatz verfolgen Client-Honeypots: Sie suchen selbst aktiv nach Schad-Software auf Webseiten, mit denen ungepatchte Browser angegriffen werden können.

Bereits 2005 stellte Microsoft Research mit dem Projekt „Strider HoneyMonkey“ eine Realisierung von XP-basierten Client-Honeypots vor (SSN 8/05). In den vergangenen Tagen wurden drei weitere viel versprechende Ansätze veröffentlicht:

- Bei Capture handelt es sich um einen „High Interaction Client Honeypot”, der insbesondere Webseiten nach versteckten Viren, Würmern und Trojanern durchsucht und die Ergebnisse protokolliert. Capture läuft in einer virtuellen Umgebung, so dass das System nach einer Infizierung schnell „gesäubert“ werden kann.
- Wie Capture sucht auch Monkey Spider nach maliziösen Webseiten, hat eine deutlich weniger aufwändige Architektur und zählt eher zur Klasse der „Low Interaction Honeypots“. Es basiert unter anderem auf CWsandbox.
- Botspy schließlich geht einen Schritt weiter: Es beobachtet Bot-Netze, die häufig die Quelle für per E-Mail versandte Phishing- oder Viren-Nachrichten sind.

Fazit: Obwohl die Tools sich in einem frühen Entwicklungsstadium befinden, zeigen sie die Leistungsfähigkeit des Client-Honeypot-Ansatzes.

Privatsphäre mit Microsoft

Vom 16.10.2006 datieren die „Privacy Guidelines for Developing Software Products and Services“ von Microsoft (v2.1). Einige der darin postulierten Prinzipien decken sich mit dem europäischen Datenschutzrecht – wie Datensparsamkeit, Transparenz und Nutzerkontrolle. Insgesamt ist das Dokument jedoch stark „sicherheitslastig“ und betont Integrität und Zugriffsschutz, vergisst aber das Prinzip der Zweckbindung. Auch die Checklisten der gut gemeinten beispielhaften Szenarien lesen sich mit europäischen Augen eigenwillig: Für das „anonyme Monitoring“ durch einen Internet-Provider wird die „explizite Zustimmung des Nutzers“ gefordert.

Immerhin wurde die Bedeutung des Datenschutzes von Microsoft durch die Integration der Guidelines in den „Trustworthy Computing Security Development Lifecycle (SDL)“ unterstrichen.

Alle Jahre wieder...

...findet der DFN-CERT Workshop „Sicherheit in vernetzten Systemen“ in Hamburg statt – am 07.-08.02.2007 nun schon zum 14. Mal. Neben etlichen spannenden eingereichten Beiträgen bildet der eingeladene Vortrag zu „Stealth Malware – can good guys win?“ von Joanna Rutkowska ein Highlight.

Augen auf beim Weihnachtskauf

Die Warnung der bayrischen Polizei vom 24.04.2006 vor dem Kauf von Plüschtieren mit eingebauter Überwachungskamera ist laut Pressemitteilung vom 11.12.2006 von mindestens einem Käufer ignoriert worden. Diesem drohen jetzt rechtliche Konsequenzen, da nach § 90 Telekommunikationsgesetz (TKG) schon der Besitz von Sendeanlagen, „die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind“ verboten ist. Vorsicht beim Kauf Ihrer Weihnachtsgeschenke!

Secorvo News

Secorvo College aktuell

In das Jahr 2007 startet Secorvo College mit den aktualisierten Seminarklassikern ISM – Information Security Management (23.-26.01.2007), PKI (30.01.-02.02.2007) und IT-Sicherheit heute (06.-08.02.2007), gefolgt von dem komplett überarbeiteten Seminar Erfolgsfaktoren für IT-Sicherheitsmanagement (26.02.-01.03.2007).

Programm und Online-Anmeldung unter http://www.secorvo.de/college

T.I.S.P.

Auf seiner Sitzung am 07.12.2006 bei Secorvo hat sich das T.I.S.P.-Board darauf verständigt, 2007 eine Weiterentwicklung des erfolgreichen T.I.S.P. Zertifikats in Angriff zu nehmen. So ist geplant zusätzliche Spezialisten-Zertifikate zu entwickeln. Die zweite T.I.S.P.-Zertifikat-Schulung mit anschließender Prüfung wird Secorvo am 05.-09.03.2007 durchführen; mehrere Anmeldungen liegen bereits vor.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2006	
24.12.	Heiligabend
27.-30.12.	23. Chaos Communication Congress (CCC, Berlin)
Januar 2007	
18.-19.01.	Tutorium "IT-Sicherheitskriterien im Vergleich" (DFN-CERT Services GmbH, Hamburg)
23.-26.01.	Information Security Management – von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
30.01.-02.02.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
Februar 2007	
06.-08.02.	IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College, Karlsruhe)
07.-08.02.	DFN-CERT Workshop: Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
26.02.-01.03.	Erfolgsfaktoren für IT-Security Management (Secorvo College, Karlsruhe)
26.-27.02	Net-ID 2007 (Computas, Berlin)

Fundsachen

Auszug aus www.security-finder.de

Microsofts Security Risk Management Guide (v1.2) beschreibt einen vierphasigen Planungsprozess für ein effektives Security Risk Management System. Die Vorgehensweise basiert auf etablierten Industriestandards und Best Practices. Der Guide umfasst eine Sammlung von Excel-Tools.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Januar 2007



Editorial: Nichts zu verbergen

Betrug, Diebstahl, Erpressung – nun hat auch die „gewöhnliche" Kriminalität das Internet erobert. Die Hemmschwelle Technik hat die organisierte Kriminalität durch die Verpflichtung kompetenter Programmierer inzwischen vollständig eingeebnet. Die Möglichkeit nahezu spurenloser und grenzüberschreitender Nutzung macht das Netz der Netze zum boomenden Tummelplatz für Gangster. Anders als befürchtet erweist sich allerdings nicht allein mangelnde IT-Sicherheit als Achillesferse; vielmehr bildet der nachlässige Umgang mit personenbezogenen Daten den Nährboden für gänzlich neue kriminelle Geschäftsmodelle.

Suchmaschinen und Portale geben persönliche Details preis: Arbeitgeber und Ausbildung (Alumni-Portale), Berufs- und Privatkontakte sind dort für jedermann einsehbar; persönliche Webseiten vervollständigen das Bild mit Hobbys und Urlaubsfotos. Zugehörige Adressen, Familienstand und Geburtsdatum lassen sich auf anderem Weg leicht herausfinden (Telefonbuch, Sportverein, social engineering). Mit diesen Daten lässt sich, genügend Fantasie und kriminelle Energie vorausgesetzt, manch geld-werte Erkenntnis gewinnen.

Dass solche Befürchtungen nicht an den Haaren herbeigezogen sind, zeigte eine am 07.12.2006 veröffentlichte Warnung des amerikanischen FBI vor einer anonymen, via Spammer verbreiteten Morddrohung: Darin wurden die Empfänger zur Zahlung mehrerer tausend Dollar Lösegeld aufgefordert, um ihre Ermordung abzuwenden, die angeblich einer ihrer Freunde in Auftrag gegeben hatte.

Falls Sie noch immer überzeugt sind, dass Sie als unbescholtener Bürger nichts zu verbergen und daher auch nicht um Ihre Privatsphäre zu fürchten haben – dann sei Ihnen das jüngste Werk von John Katzenbach („Der Patient") ans Herz gelegt: „Wir haben Angst davor, getötet zu werden. Dabei ist es viel schlimmer, vernichtet zu werden. Das Schlimmste aber ist, innerhalb von wenigen Tagen seine Identität zu verlieren." Eine nicht nur höchst spannende, sondern auch erkenntnisreiche Lektüre für lange Winterabende.



Inhalt

Editorial: Nichts zu verbergen

Security News

Zero Day Bounty

Adobe anfällig

Gläserne Passagiere

23C3

Veteran streicht Segel

Zero Day Pranger

DuD 2007

Secorvo News

Secorvo College aktuell

"Social Engineering" – der Film

White Paper "Security Audits"

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Zero Day Bounty

So genannte „zero day exploits“ sind Werkzeuge zur Ausnutzung von gerade erst veröffentlichten Schwachstellen. Unabhängig von der andauernden Diskussion, ob eine Schwachstelle erst dem Hersteller gemeldet oder so früh wie möglich publiziert werden soll (z.B. in Bugtraq), ist klar, dass derartige Exploits in Ermangelung von Gegenmaßnahmen bei Angreifern besonders beliebt sind. Inzwischen gibt es einen regelrechten Markt für diese Exploits, bis hin zur (halb-) öffentlichen Versteigerung.

Eine legale Möglichkeit, mit solchen Schwachstellen Geld zu verdienen, bietet iDefense seit dem 08.01.2007. Das Unternehmen belohnt im Rahmen einer vierteljährlichen „Vulnerability Challenge“ aufgedeckte Schwachstellen in Windows Vista und IE 7 mit bis zu 12.000 US$. Auch das Snosoft Research Team hat am 17.01.2007 ein Exploit Aquisition Programm aufgelegt, und durch ein Teammitglied eine Diskussion zum Thema „Fair Exploit Price and Purchase“ auf full-disclosure angestoßen. Die finanziellen Anreize könnten die Motivation steigern, gefundene Schwachstellen zeitnah zu veröffentlichen, um die „Bounty“ einstreichen zu können.

Falls das Konzept aufgeht, dürfte die Zahl bekannt gewordener Schwachstellen weiter ansteigen.

Adobe anfällig

Am 03.01.2007 geriet der Adobe Reader wegen einiger Cross-Site-Skripting Schwachstellen in die Schlagzeilen. Neben einem Update gab Adobe in einem Security-Bulletin Hinweise zur Problemvermeidung. Kurz darauf wurde am 06.01.2007 im Rahmen des Month of Apple Bugs (MoAB) ein Fehler in der PDF-Spezifikation aufgedeckt: Fehlerhafte Einträge im Catalog Dictionary führen zu unvorhersehbarem Verhalten verschiedener PDF-Reader und können die Ausführung beliebigen Codes ermöglichen. Dies ist nicht auf den Adobe Reader oder ein bestimmtes Betriebssystem beschränkt.

Adobe empfiehlt in einem Security Bulletin vom 09.01.2007 dringend ein Update auf Version 8 des Acrobat Reader – dieser ist von der Schwachstelle nicht betroffen. Nutzer von KDE finden seit dem 15.01.2007 einen Fix für kpdf und KOffice. Anwender anderer Reader sollten sich möglichst bald nach Sicherheitsupdates umschauen – und bis dahin nur PDF-Dokumente aus vertrauenswürdiger Quelle öffnen.

Auch hier zeigt sich, dass ein über lange Zeit als sicher angenommenes Dokumentformat verborgene Schwachstellen besitzen kann. Die Faustregel der sicheren Softwareentwicklung, dass Fehler im Design schwer zu finden und nur teuer zu beheben sind, wurde wieder einmal bestätigt.

Gläserne Passagiere

Der Europäische Gerichtshof hatte am 30.05.2006 den Beschluss des EU-Rates vom 17.05.2004 über die Weitergabe von Fluggastdaten an die USA sowie die Entscheidung der EU-Kommission über die Angemessenheit des Schutzes dieser personenbezogenen Daten in den USA auf Antrag des EU-Parlaments für nichtig erklärt. Die Vereinbarung lief damit am 30.09.2006 aus. Am 06.10.2006 einigten sich die EU und die USA auf ein neues Abkommen, das nun bis 31.07.2007 gilt: Danach werden die bis zu 34 Einzelangaben umfassenden Datensätze aller Fluggäste von Transatlantik-Flügen nun auf Anfrage zahlreichen US-Behörden zugänglich gemacht.

Zu den übermittelten Daten zählen die Namen der Mitreisenden, Kreditkarten- oder Kontonummern, E-Mail-Adresse, Telefonnummern, Sonderwünsche wie vegetarisches Essen oder Sperrgepäck, ggf. Ausweisnummer, Geburtsdatum und Wohnort.

Wer vor dem Hintergrund dieser Entwicklung nicht auf USA-Reisen verzichten kann oder will, dem bleibt die schwache Hoffnung, dass die Zugriffsbefugnisse der US-Behörden auf diese Passagierdaten in der noch ausstehenden endgültigen Vereinbarung wirkungsvoll beschränkt werden.

23C3

Vom 27. bis 30.12.2006 fand der 23. Chaos Communication Congress in Berlin mit über 4.000 Teilnehmern statt. Im Verlauf von vier Tagen wurden in mehr als 120 Vorträgen, Workshops und Veranstaltungen unterschiedlichste Themenbereiche abgedeckt: Angefangen bei der Privatsphäre im Web 2.0 über ein mögliches Ende der Tor-Anonymität, verbesserte Bluetooth-Angriffe und Verkehrsüberwachung bis hin zur Suche nach Softwarefehlern in Binärcode. Weiter wurden innovative Ansätze zur Überwachung aus der Luft mit Microdrones vorgestellt – wehe dem Nachbarn, der Böses plant.

Aufschlussreich war auch der Bericht von Manfred Fink über Gästeüberwachung in Hotels durch professionelle Informationsbeschaffer – so Manches geht in der „analogen Welt“ viel einfacher. Aus der Welt der Pentester wurde Grundwissen über das Audit von Backbonerouten und die kreativen Möglichkeiten vermittelt, Paketflüsse zu steuern.

Wer diese inzwischen bei weitem größte deutsche Sicherheitskonferenz verpasst hat, kann sich anhand einiger Videostreams nachträglich ein Bild machen.

secorvo
security consulting

Veteran streicht Segel

Am 19.12.2006 hat die von dänischen Freiwilligen betriebene Open Relay Database (ORDB) ihre Dienste eingestellt. Seit dem 31.12.2006 ist auch die zugehörige ORDB-Webseite nicht mehr erreichbar.

Die ORDB-Betreiber reagierten damit auf die Veränderungen in der SPAM-Welt: Kam vor einigen Jahren noch mehr als 90% des SPAMs von offenen SMTP-Relays, wird der Löwenanteil heute über Drohnen in Botnetzen verschickt. Daher empfehlen die ORDB-Macher nicht, die ORDB-Verweise auf aktiven E-Mail-Servern durch alternative Real-Time-Blacklists (RBLs) wie Spamhaus oder Spamcop zu ersetzen, sondern auf eine Kombination aus Greylisting-Techniken und inhaltsbasierter Analyse, wie z. B. SPAM-Assassin umzustellen.

Die wirksamste Methode zur Abwehr von SPAM ist nach unserer Erfahrung die Kombination verschiedener Ansätze – einschließlich RBLs. Allerdings müssen diese Techniken weiterentwickelt werden und neue Ansätze auf den Tisch, damit sich auch zukünftig den rasanten Entwicklungen der Spammer etwas entgegensetzen lässt. Ereignisse wie die kurzfristige Reduzierung des SPAM-Aufkommens um ca. 30% in der Zeit des Jahreswechsels sind leider keine nachhaltigen Trends.

Zero Day Pranger

Auch von anderer Seite wächst der Druck auf die Hersteller: Symantec veröffentlicht schon seit längerem in seinem regelmäßigen Internet Security Threat Report die Größe des „Window of Exposure“ (vgl. SSN 11/2006). Noch plakativer werden die Hersteller vom Schwachstellen-Management-Anbieter Eeye an den Pranger gestellt (vgl. SSN 12/2006): In einem Zero Day Tracker wird die Zeit veröffentlicht, die Hersteller seit Bekanntwerden einer Schwachstelle verstreichen ließen, ohne diese zu schließen. Auch wenn der „virtuelle Pranger“ derzeit den Fokus auf einige wenige Hersteller legt, vermittelt er einen einfachen und aktuellen Schwachstellenüberblick. Die Historie der inzwischen behobenen Schwachstellen deckt auf, wie schnell oder wie langsam der jeweilige Hersteller reagiert hat.

Doch allein mit beschleunigter Fehlerbeseitigung lässt sich die Risk Exposure Time (RET) nicht minimieren. Denn auch wenn Patches deutlich schneller zur Verfügung gestellt würden, fielen die Zeiten für Tests und den Roll-Out der Patches zusätzlich an. Strategien zum Umgang mit Schwachstellen (Schwachstellen-Management) sollten daher unabhängig von Patch-Zyklen und der Verfügbarkeit von Bug-Fixes entwickelt und optimiert werden.

DuD 2007

Am 12.-13.03.2007 findet die diesjährige Fachtagung „DuD 2007“ in Berlin statt – zwei Tage voller spannender, prominent besetzter Vorträge rund um IT-Sicherheit und Datenschutz unter der Leitung der Herausgeber der Fachzeitschrift DuD – Dr. Johann Bizer und Dirk Fox. Thematische Schwerpunkte bilden die Gestaltung von Einwilligungserklärungen, die Sicherheit von Web-Applikationen und die ID-Strategie der Bundesregierung.

Secorvo News

Secorvo College aktuell

Die starke Nachfrage nach T.I.S.P.-Schulung und -Prüfung zeigt den großen Bedarf an einem unabhängigen Expertenzertifikat in der IT-Sicherheit. Die nächste T.I.S.P.-Schulung mit anschließender Prüfung findet am 05.-09.03.2007 statt. Das bereits veröffentlichte Seminarprogramm wird um das Seminar PKI – Grundlagen, Vertiefung, Realisierung am 26.-29.03.2007 erweitert.

Programm, Preise und Online-Anmeldung unter www.secorvo.de/college

“Social Engineering” – der Film

Das vierte Awareness-Video ist nun verfügbar – diesmal über „Social Engineering“. Es thematisiert eine Bedrohung, deren Bedeutung im Zuge von Globalisierung und verschärftem Wettbewerb spürbar zunimmt: Die Informationsbeschaffung mit überwiegend nichttechnischen Methoden. Tatsächlich ist es häufig weit einfacher als angenommen, gesuchte Informationen gezielt zu beschaffen, ohne dabei technische Sicherheitsmechanismen überwinden zu müssen. Falsch verstandene Höflichkeit, Gutgläubigkeit, Furcht vor Autoritäten und Vertrauensseligkeit sind dabei meist die heimlichen Komplizen der Angreifer. Ziel des Videos, das ab sofort bestellt werden kann, ist es, das typische Vorgehen eines „Informationsbeschaffers“ zu demonstrieren, um Mitarbeiter für Angriffsversuche dieser Art zu sensibilisieren.

White Paper “Security Audits”

Im aktuellen Secorvo White Paper vom 17.01.2007 fasst Stefan Gora die Erfahrungen von Secorvo mit der Konzeption und Durchführung von “Security Audits” zusammen. Nach einleitenden begrifflichen Klarstellungen stellt er die Vorgehensweise bei Black-Box- und White-Box-Analysen vor und beschreibt die Audit-Methodik in Anlehnung an die Standards ISO 17799, BS 7799-x, BSI 100-x und ISO 27001, an das IT-Grundschutzhandbuch sowie weitere Best Practice-Ansätze.

Veranstaltungshinweise

Auszug aus www.veranstaltungen-it-sicherheit.de

Februar 2007	
06.-08.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
07.-08.02.	DFN-CERT Workshop (DFN-CERT, Hamburg)
26.-27.02.	Net-ID 2007 (Computas, Berlin)
März 2007	
05.-09.03.	TISP-Schulung (Secorvo College, Karlsruhe)
10.03.	TISP-Prüfung (Secorvo College, Karlsruhe)
12.-13.03.	DuD 2007 (Computas, Berlin)
26.-28.03.	Fast Software Encryption 2007 (IACR, Luxembourg)
26.-29.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
27.-30.03.	Black Hat Europe 2007 (Black Hat, Amsterdam)
April 2007	
17.-19.04.	IT-Sicherheitsaudits in der Praxis (Secorvo, Karlsruhe)
24.-26.04.	Sichere Softwareentwicklung (Secorvo, Karlsruhe)

Fundsache

Auszug aus www.security-finder.de

Die BSI-Studie „Sicherheit von Web-Anwendungen“ vom 01.08.2006 enthält eine umfangreiche Zusammenstellung von Maßnahmen zur Sicherung von Web-Applikationen und Best-Practice-Ansätzen. Ergänzt wird der Maßnahmenkatalog um einen Leitfaden zur Erstellung sicherer Webanwendungen, der sowohl für Projektleiter und Entwickler als auch für Auditoren interessant sein dürfte.



Impressum

http://www.secorvo-security-news.de/

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Februar 2007



Editorial: Gedankenverbrechen

Vor allem drei Zukunftsvisionen haben in den vergangenen 100 Jahren die Gemüter bewegt: die „Schöne neue Welt“ von Aldous Huxley (1932), der Roman „1984“ von George Orwell (1948) und „Fahrenheit 451“ von Ray Bradbury (1953). Allen gemeinsam ist die düstere Prognose, dass eine autoritäre, anonyme und technokratische Herrschaftsform unter Nutzung modernster Technik die Menschen zu dumpfen, würdelosen Marionetten degradieren wird.

Der wesentliche Unterschied: Sah Huxley die Bedrohung in einer fortschreitenden Abstumpfung durch Amüsement, Drogenkonsum (Soma) und gezielte Embryonenmanipulation, zeichnet Orwell einen totalen Überwachungsstaat, der mittels Gedankenpolizei und Televisoren, die öffentliche Plätze und Wohnungen ausleuchten, keinen Raum für Privatsphäre lässt. In Bradburys Vision kommt beides zusammen: Bücher sind verboten und werden öffentlich verbrannt, das Volk schluckt Glückspillen und amüsiert sich vor Videowänden.

Es schien, als habe Huxley die Zukunft treffender prognostiziert: „Big Brother“ ist heute die Marke einer Fernsehshow, über die die Welt lacht. In „Wir amüsieren uns zu Tode“ beschrieb der Medienwissenschaftler Neil Postman 1985 Desinformation und Abstumpfung durch Fernsehkonsum. Dabei waren es 1988 „nur“ 2,5 Stunden; 2002 verbrachten die Deutschen durchschnittlich 3,5 Stunden pro Tag vor dem Fernseher – das sind 160 Acht-Stunden-Tage pro Jahr. Zugleich steigt die Analphabetenquote: 2004 galten 6,5-11% der Deutschen als „funktionale Analphabeten“ – das sind 4-7 Mio. Menschen.

Nun aber holt Orwell auf. Nach „großem Lauschangriff“, Vorratsdatenspeicherung und der Zunahme der Abhöranordnungen steht nun die „Online-Durchsuchung“ auf der Agenda. Neusprech vom Feinsten: Im Unterschied zur echten Durchsuchung erfolgt sie heimlich.

In „1984“ blieb Winston Smith eine Ausflucht: ein Tagebuch, in dem er in einer nicht einsehbaren Ecke seines Zimmers seine „Gedankenverbrechen“ notierte. 2007 dürfte er dafür keinen PC verwenden.



Inhalt

Editorial: Gedankenverbrechen

Security News

Anti-Spyware – Best Practices

Fast ausnahmslos betroffen

Globaler Überblick

FIPS-Validierung für OpenSSL

„Ist Fatalismus angebracht?“

Viel hilft viel – aber wem?

Machen 123 Mio. € sicherer?

DuD 2007

Secorvo News

Secorvo College aktuell

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Anti-Spyware – Best Practices

Die Anti-Spyware Coalition (ASC) ist eine Initiative von derzeit knapp 50 Mitgliedsunternehmen, die sich 2005 zur Bekämpfung von Spyware und anderer unerwünschter Software zusammengeschlossen haben.

Am 25.01.2007 veröffentlichte die ASC den Guide Best Practices: Factors for Use in the Evaluation of Potentially Unwanted Technologies. Darin werden Anti-Spyware-Herstellern Hinweise gegeben, nach welchen Kriterien Software als „unerwünscht" bewertet werden kann. Diese Hinweise sollten von allen Softwareherstellern als Orientierung genutzt werden, um Fehleinordnungen zu verhindern. Denn einer zentralen Grundforderung der ASC ist nichts hinzuzufügen: „Users should be in control of their computers at all times." (Benutzer sollen zu jeder Zeit wissen, was auf ihren Rechnern passiert.)

Fast ausnahmslos betroffen

Die am 31.01.2007 von der Information Systems Security Association (ISSA) und dem University College Dublin (UCD) veröffentlichte Studie „Irish Cybercrime Survey 2006" bringt ein erschreckendes Ergebnis zu Tage: 98% der befragten Firmen gaben an, von Sicherheitsvorfällen betroffen gewesen zu sein.

Auch wenn mit 42 Organisationen – von kleinen irischen Firmen über öffentliche Einrichtungen bis zu großen Konzernen – nur eine vergleichsweise kleine Stichprobe erhoben wurde, sind die Ergebnisse der Studie und die Aufschlüsselung der einzelnen Vorfälle sehr informativ.

Globaler Überblick

Seit dem 05.02.2007 ist das Active Threat Level Analysis System (ATLAS) von Arbor Networks auch für die breite Öffentlichkeit verfügbar und stellt damit als Expertensystem im Gegensatz zu anderen kommerziellen Diensten erstmals auch Privatpersonen statistisches und technisch detailliertes Datenmaterial zu aktuellen Angriffen kostenlos zur Verfügung.

Technisch basiert es auf einem Sensornetzwerk, das ca. 70% des Internet abdeckt. Die diesen Auswertungen zu Grunde liegenden Daten stammen u. a. aus Honeynetködern, eingefangener und analysierter Malware, Logs von Intrusion Detection Systemen und Netzwerkscans, Statistiken zu Denial-of-Service, ermittelten Daten zu Phishinginfrastrukturen und Botnet Command & Control sowie Nachrichten- und Schwachstellenmeldungen.

Damit wird ein komprimierter Echtzeitüberblick über die globalen Sicherheitsereignisse und -trends gegeben. So ist es möglich, auf einen Blick 24-Stunden-Zusammenfassungen sortiert nach aktuellen Angriffstypen oder regionalen Aktivitäten zu erhalten. Festgestellte automatisierte Scans werden u. a. nach Service/Port, Ausgangsland und Autonomous System Number aufgeschlüsselt.

Sehr aussagefähig ist auch der Risikoindex, der existierende technische Schwachstellen in Relation zu ihrer Ausnutzbarkeit und Verbreitung im Internet sowie den tatsächlich beobachteten Angriffen nach dem Common Vulnerability Scoring System bewertet. Dieses neue Informationsangebot ist hervorragend geeignet, kommerzielle Sicherheitsmeldungen zu verifizieren und die externen Bedrohungen, denen der eigene Arbeitsbereich ausgesetzt ist, objektiver zu bewerten.

FIPS-Validierung für OpenSSL

Am 06.02.2007 gab das Open Source Software Institute (OSSI) die erneute FIPS 140-2 Validierung des OpenSSL FIPS Object Modules bekannt. Die Validierung ist in den USA erforderlich, um Open Source Software für die Verarbeitung sensibler Daten bei US Behörden einsetzen zu dürfen.

Der Validierungsprozess dauerte statt der üblichen wenigen Monate mehr als fünf Jahre. Das lag zum Einen daran, dass kein Binärcode, sondern Source Code vom Computer Module Validation Program (CMVP), einem Joint Venture des US-amerikanischen National Institute of Standards and Technology (NIST) und des kanadischen Communications Security Establishment (CSE), geprüft werden musste – eine solche Prüfung hat es noch nie gegeben. Zum anderen wurde der Validierungsprozess von anderen kommerziellen Herstellern, die ähnliche Produkte vertreiben, durch zahlreiche Eingaben boykottiert. So musste die Validierung im Juli 2006 zunächst zurückgezogen werden, da Hersteller massive anonyme Beschwerden bei der CMVP eingereicht hatten.

Zwar wurde die Validierung letztlich erfolgreich abgeschlossen, aber die überprüfte Version ist mehr als drei Jahre alt. Dennoch enthält sie u. a. bereits die Hashfunktionen SHA-224, SHA-256, SHA-384 und SHA-512.

„Ist Fatalismus angebracht?"

Dies war eine der zahlreichen Fragen, die auf dem mittlerweile 14. DFN-CERT Workshop „Sicherheit in vernetzten Systemen" diskutiert wurden, der am 07. und 08.02.2007 stattfand – wie immer in Hamburg. Johannes Strümpfel stellte diese Frage in seinem sehr spannenden Abschlussvortrag „Werk-

zeuge der Industriespionage“ – und verneinte sie trotz etlicher beeindruckender Beispiele aus der Welt des „Cyber Crimes“.

Auch die anderen Vorträge der zweitägigen Veranstaltung präsentierten den auch in diesem Jahr über 300 Teilnehmern unterschiedliche Themen der System- und Netzwerksicherheit – von technischeren Aspekten (Joanna Rutkowska: „Fighting Stealth Malware – Towards Verifiable OSes“) über Fragen der sicheren Softwareentwicklung (Martin Johns: „CISAT: Integration von sicherheitszentrierter statischer Analyse in den Entwicklungsprozess“) bis zu sehr anschaulich vorgetragenen, aktuellen rechtlichen Fragestellungen (Heidi Schuster: „Wikis und Foren – Möglichkeiten eines rechtskonformen Betriebs“).

Fast alle Folien stehen zum Download bereit; in Kürze werden ferner die während des Workshops live im Internet übertragenen Vorträge als Aufzeichnungen verfügbar sein.

Viel hilft viel – aber wem?

Auf der am 09.02.2007 zu Ende gegangenen RSA Conference 2007 wurde ein Großangebot aus zahllosen Keynotes, 19 fachlichen Schwerpunktthemen und über 220 Einzelvorträgen zu allen erdenklichen Aspekten der IT-Sicherheit geboten. Die Kernbotschaft an die Teilnehmer nahm sich jedoch eher schlicht aus: die alten Probleme sind auch die neuen – Malware, Rootkits, Botnets vereint unter einer steuernden und kreativen Online-Kriminalität.

Ob PC, Handy, Spieleconsole oder zukünftig der Kühlschrank: Angreifer werden in allen Systemen Schwachstellen finden. Diese Entwicklung ist nach Aussagen führender Sicherheitsexperten wie Vint Cerf und Eugene Kaspersky unumkehrbar.

Dementsprechend war das Ausstellungsangebot eher auf technische als auf strategisch-organisatorische Schutzlösungen ausgerichtet.

Folgt aus solchen Aussagen der IT-Sicherheitsindustrie, dass IT-Sicherheit zukünftig nur noch von (großen) Herstellern "miteingekauft" werden kann? Da sollte man es wohl besser mit den Römern halten und sich fragen: Quis custodit custodes? (Wer überwacht die Wächter?). Die resignativen Tendenzen stimmen bedenklich – und sichere Softwareentwicklung ist bislang keine Stärke der Software-Anbieter.

Machen 123 Mio. € sicherer?

Am 24.01.2007 wurde durch den Beschluss des Bundeskabinetts im Forschungsbereich „Neue Technologien“ des BMBF das Rahmenprogramm „Sicherheitsforschung – Forschung für die zivile Sicherheit“ aufgelegt. Bis zum Jahr 2010 ist es mit rund 123 Mio. Euro budgetiert und verfolgt mit seinen zwei Programmlinien „Szenarienorientierte Sicherheitsforschung" und „Erforschung von Querschnittstechnologien in Technologieverbünden“ das Ziel, die zivile Sicherheit präventiv zu erhöhen, ohne dadurch die Freiheit der Bürgerinnen und Bürger einzuschränken. Erreicht werden soll dies durch innovative organisatorische Konzepte und Handlungsstrategien. Insbesondere den Quellen von Bedrohungen, dem Datenschutz und den Auswirkungen auf die Menschen- und Freiheitsrechte wird in der Zielsetzung ein hoher Rang eingeräumt.

Ob diese heren Ziele erreicht werden, bleibt abzuwarten. Denn wo viel Geld ist, ist auch viel Schatten: Die Verantwortlichen werden dazu in der Auseinandersetzung mit den um diese Forschungsgelder buhlenden Interessensgruppen sehr standhaft bleiben müssen.

DuD 2007

Knapp drei Wochen noch bis zur diesjährigen Fachtagung „DuD 2007“ am 12.-13.03.2007 in Berlin – zwei Tage mit spannenden, prominent besetzten Vorträgen rund um IT-Sicherheit und Datenschutz unter der Leitung der Herausgeber der Fachzeitschrift DuD, Dr. Johann Bizer und Dirk Fox. Thematische Schwerpunkte bilden in diesem Jahr die Sicherheit von Web-Applikationen und die ID-Strategie der Bundesregierung. Programm und Online-Anmeldung unter www.computas.de.

Secorvo News

Secorvo College aktuell

Der T.I.S.P.-Schulungstermin am **05.–09.03.2007** ist fast ausgebucht – es gibt nur noch zwei freie Plätze für Kurzentschlossene.

Aufgrund der großen Nachfrage nach dem T.I.S.P.-Zertifikat wird Secorvo eine zusätzliche T.I.S.P.-Schulung in der ersten Jahreshälfte anbieten. Der Termin wird in Kürze auf der Webseite von Secorvo College veröffentlicht. Wenden Sie sich bei Interesse bitte bis dahin an college@secorvo.de.

Programm, Preise und Online-Anmeldung für die Seminare

- PKI – Grundlagen, Vertiefung, Realisierung
  am **26.–29.03.2007**,
- IT-Sicherheitsaudits in der Praxis
  am **17.–19.04.2007** und
- Sichere Softwareentwicklung
  am **24.–26.04.2007**

finden Sie unter www.secorvo.de/college.

Veranstaltungshinweise

Auszug aus www.veranstaltungen-it-sicherheit.de

Februar 2007	
26.-27.02.	Net-ID 2007 (Computas, Berlin)
März 2007	
05.-09.03.	TISP-Schulung (Secorvo College, Karlsruhe)
10.03.	TISP-Prüfung (Secorvo College, Karlsruhe)
12.-13.03.	DuD 2007 (Computas, Berlin)
26.-28.03.	Fast Software Encryption 2007 (IACR, Luxembourg)
26.-29.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
27.-30.03.	Black Hat Europe 2007 (Black Hat, Amsterdam)
April 2007	
17.-19.04.	IT-Sicherheitsaudits in der Praxis (Secorvo, Karlsruhe)
24.-26.04.	Sichere Softwareentwicklung (Secorvo, Karlsruhe)
Mai 2007	
22.-24.05.	10. Deutscher IT-Sicherheitskongress (BSI, Bonn)

Fundsache

Auszug aus www.security-finder.de

Im Dokument „The Nepenthes Platform: An Efficient Approach to Collect Malware“ präsentieren die Autoren einen neuartigen Ansatz zur automatisierten Sammlung von Viren, Würmern und Trojanern: auf einem Server werden Netzwerk-Protokolle emuliert, die typischerweise von Schad-Software zur Verbreitung verwendet werden. Auf diese Weise kann Malware "gefangen" und anschließend analysiert werden.

Impressum

http://www.secorvo-security-news.de/

ISSN 1613-4311

Redaktion: Petra Barzin, Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

März 2007



Editorial: Wolf im Schafspelz?

Sie erinnern sich: Nicht einmal fünf Jahre ist es her, da erhielt Microsoft Deutschland bei der Verleihung der „Big Brother Awards 2002“ am 25.10.2002 in Bielefeld den Hauptpreis – in der Kategorie „Lifetime“. Prämiert wurden die Verdienste Microsofts um die „flächendeckende Einführung von Kontrolltechnologie für Urheberrechte“. In seiner Laudatio erinnerte Patrick Goltzsch an die automatische Online-Registrierung unter Windows 98, die seinerzeit die Wogen der Entrüstung hoch gehen ließ: Microsoft hatte die Hardware-Konfiguration der Client-Systeme analysiert und diese Daten zusammen mit einer eindeutigen Kennung „nach Hause telefoniert“.

Und nun das: Am 16.02.2007 wurde Microsoft Deutschland durch den Ministerpräsidenten von Schleswig Holstein das Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz (ULD) für den „Microsoft Update Service 6.0“ und den „Windows Server Update Service 2.0“ verliehen. Da reiben sich aufmerksame Beobachter die Augen: Wie ist das möglich? Wurde da ein Saulus zum Paulus?

Bei genauer Betrachtung löst sich der vermeintliche Widerspruch. Den Big Brother Award hatte der damalige Datenschutzbeauftragte von Microsoft Deutschland, Sascha Hanke, persönlich entgegengenommen – ein Novum in der Geschichte der Awards. Und er nahm ihn ernst: „Wir sind nicht erfreut über den Preis, akzeptieren aber das Urteil der Jury.“

Intern setzte er anschließend alle Hebel in Bewegung, um aus der „Vermarktungsbremse“ Datenschutz einen Wettbewerbsvorteil zu machen. Ein Ergebnis waren die „Privacy Guidelines“ für Softwareentwickler (SSN 12/2006). Sein Nachfolger konnte nun nach 18-monatiger Prüfung das Gütesiegel entgegennehmen. Auch wenn dies nur ein Anfang gewesen sein darf, soll die Mutation zum Lämmchen glaubwürdig bleiben, so drängt sich doch die Frage auf, warum erst ein *amerikanischer* Software-Konzern kommen muss, um in Deutschland Datenschutzgeschichte zu schreiben...



Inhalt

Editorial: Wolf im Schafspelz?

Security News

BKA-Forensik

Drive-by Pharming

Mcert schließt, DSIN lebt (noch)

27001 + 1 = 27006

Grundschutz extended

Month of PHP Bugs

Secorvo News

Secorvo College aktuell

Lizenz zum Prüfen

ITSF 2007

Virtuelle Sicherheit?

Security Awareness Symposium

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

BKA-Forensik

Für Wirbel sorgte ein kurzer Artikel in der Süddeutschen Zeitung vom 07.03.2007. Danach gelang es BKA-Forensikern, die Festplatte des Computers eines der beiden mutmaßlichen Bombenleger von Köln zu spiegeln und die vom Besitzer zuvor gelöschten Dateien zu rekonstruieren. Das Ergebnis der forensischen Analyse ist allerdings wenig spektakulär: Moderne Forensik-Tools, auch kostenlose OpenSource-Toolkits, konnten schon immer Dateien wiederherstellen, die nicht sicher gelöscht oder physisch zerstört waren. Der Aufwand hierfür ist überschaubar, was auch Secorvo in etlichen forensischen Analysen nachweisen konnte. Zudem hatte der Verdächtige zuvor gestanden, die später gefundenen Bombenbauanleitungen auf dem Rechner gespeichert zu haben.

Interessant wird die Nachricht jedoch im Zusammenhang mit einer Rede des BKA-Präsidenten Jörg Zierke anlässlich des 10. Europäischen Polizeikongresses in Berlin. Zierke nahm die „Kofferbomber" zum Anlass, um eingehend für die Notwendigkeit von Online-Durchsuchungen zu plädieren, „mit der ganz gezielt schwere Straftaten aufgedeckt werden sollen." Dass die Beispiel-Straftat freilich ohne jede Online-Durchsuchung aufgeklärt wurde und auch durch diese nicht hätte verhindert werden können, erwähnte Zierke indes nicht. „99,99% der Menschen in Deutschland werden davon niemals betroffen sein", wollte Jörg Zierke beruhigen. Dass diese Einschätzung noch gilt, wenn das Instrument erst eingeführt ist, darf angesichts wachsender Begehrlichkeiten der Strafverfolgungsbehörden bezweifelt werden. Ein stichhaltiges Argument für den Grundrechtseingriff ist Zierke jedenfalls schuldig geblieben.

Drive-by Pharming

Unter der Bezeichung „Drive-by Pharming" wurde am 15.02.2007 von Zulfikar Ramzan auf Bugtraq eine neue Angriffsmethode veröffentlicht: Auf einer Webseite hinterlegter bösartiger JavaScript-Code, der beim Betrachten der Seite ausgeführt wird, ändert die DNS-Einstellungen des (DSL-) Zugangsrouters so, dass der Netzwerkverkehr über das Angreifersystem umgeleitet wird. Das funktioniert, wenn die Standard-Kennwörter beibehalten wurden – Proof-of-Concepts für Router von Linksys, D-Link und Netgear sind verfügbar. Zweifellos funktioniert die Methode auch bei weiteren Herstellern.

Das Prinzip ist nicht neu, die Kombination aber kreativ. Schutz vor derartigen Angriffen bietet eine der einfachsten und ältesten Sicherheitsmaßnahmen: Das sofortige Ändern von Default-Passworten. Wer diesen Aufwand scheut, darf sich nicht wundern, wenn seine Kommunikationsinhalte in dunklen Kanälen landen.

Mcert schließt, DSIN lebt (noch)

Nach einem bisher unbestätigten, aber undementierten Bericht der Financial Times Deutschland vom 16.03.2007 stellt das Mcert im Juni seine Tätigkeit ein. Das vom BITKOM am 15.10.2002 ins Leben gerufene Mittelstands-CERT (SSN 05/2002) litt schon unter Startschwierigkeiten: Die operative Arbeit nahm es erst knapp 14 Monate später am 09.12.2003 auf (SSN 12/2003). Nachdem es offenbar nicht gelang, eine nennenswerte Zahl Kunden für das Dienstleistungsangebot zu gewinnen, wenden sich die Sponsoren nun Microsofts und SAPs Marketing-Initiative „Deutschland sicher im Netz" zu.

Aber auch diese am 31.01.2005 medienwirksam von Bill Gates gestartete Initiative schwächelt: Der im Juni 2005 initiierte monatliche Newsletter erlebte nur acht Ausgaben, vom „wöchentlichen Sicherheitstipp" gibt es nur noch ein Archiv und der Webauftritt wirkt unkoordiniert und strukturlos – zu viele Köche verderben bekanntlich den Brei.

Seit dem 31.12.2006 ist ein Verein Träger der Initiative; Bundesinnenminister Wolfgang Schäuble soll die Schirmherrschaft übernehmen. Vor welchen Marketing-Karren er da gespannt werden soll, entlarvt erst der Blick in die Details: Für einen PC-Neukauf werden die Modelle von Fujitsu-Siemens mit dem „Gütesiegel Sicherheitsempfehlung der Initiative Deutschland sicher im Netz" und zum Schutz vor Viren die „Virenschutzlösung eTrust EZ Antivirus 2005 (!)" des Partners CA empfohlen. Ein Schelm, wer Arges dabei denkt...

27001 + 1 = 27006

Am 01.03.2007 hat die International Organization for Standardization (ISO) mit dem Standard ISO/IEC 27006:2007(E) das zweite Werk aus der 27000er Reihe veröffentlicht. Der Standard mit dem sperrigen Titel "Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems" (ISMS) spezifiziert Anforderungen an Organisationen, die Audits und Zertifizierungen von Informationssicherheitssystemen nach ISO/IEC 27001:2005(E) durchführen.

Diese Anforderungen ergänzen die allgemeineren Erfordernisse aus den Standards ISO/IEC 17021:2006 und ISO/IEC 19011:2002. Zusätzlich werden Hinweise zur Vorbereitung und Durchführung von ISMS-Audits gegeben; damit ist der Standard auch für Organisationen interessant, die sich aktiv mit ISMS-Audits beschäftigen.

secorvo
security consulting

Grundschutz extended

Im Newsletter vom 09.03.2007 hat das BSI die Veröffentlichung der neuen Grundschutz-Bausteine „Sicherheit in SAP Systemen“, „Speichersysteme und Speichernetze“, „Windows Server 2003“, „Wireless LAN“ und „Voice over IP“ bekannt gegeben. Auch wurde der Baustein „Datenbanken“ grundlegend überarbeitet. Die Metadaten für das vom BSI entwickelte GSTOOL wurden entsprechend angepasst und stehen zum Download zur Verfügung. An den zahlreichen Erweiterungen lässt sich erkennen, dass der Grundschutz lebt. Die enge Verknüpfung mit dem Standard ISO/IEC 27001:2005(E) bei gleichzeitigem Ausbau der technisch orientierten Gefährdungs- und Maßnahmenkataloge macht den IT-Grundschutz zu einem mächtigen Werkzeug.

Month of PHP Bugs

Am 01.03.2007 begann der „Month of PHP Bugs“ (MoPB), ausgerufen vom „The Hardened-PHP Project“. Zielsetzung der Initiatoren ist es, auf bekannte Fehler im Kern von PHP aufmerksam zu machen. Der zu den bisher veröffentlichten 26 Fehlern verfügbare Patch-Status vom Februar 2007 wird ebenfalls aufgelistet. Aus Gründen der Übersichtlichkeit werden Fehler in PHP-Anwendungen nicht berücksichtigt; dazu finden sich genügend Schwachstellen auf einschlägigen Mailinglisten wie Bugtraq und Full Disclosure.

Amüsant sind die Zitate im Titel des jeweiligen Fehlers, die allein schon eine eigene Geschichte über sichere Softwareentwicklung erzählen: „Let's not break binary compatibility in PHP4 anymore“ oder „Hello, is this the end of the buffer?“ Nicht ohne Grund gibt es im PHP-Umfeld auch Sicherheitsprojekte, die sich speziell der Härtung von PHP (z.B. Suhosin) widmen.

Secorvo News

Secorvo College aktuell

Mit der T.I.S.P.-Schulung Anfang März haben inzwischen 12 Absolventen bei Secorvo College ein T.I.S.P.-Zertifikat erworben. Von den Absolventen wurden die gelungene Darstellung des Gesamtzusammenhangs und die Abstimmung der Vorträge aufeinander, der Praxisbezug und die Kompetenz der Referenten gelobt. Wegen der großen Nachfrage bietet Secorvo College vom 25.-30.06.2007 eine zusätzliche T.I.S.P.-Schulung mit Prüfung an. Weitere Seminare vor der Sommerpause:

- IT-Sicherheitsaudits in der Praxis (17.-19.04.)
- Sichere Softwareentwicklung (24.-26.04.)
- Kommunikationsschutz und Datensicherheit (08.-10.05.)

Programm, Preise und Online-Anmeldung unter www.secorvo.de/college

Lizenz zum Prüfen

Neben Stefan Gora wird nun auch Kai Jendrian vom BSI lizenzierter ISO-27001 Auditor auf der Basis von IT-Grundschutz. Beide haben sich außerdem 2006 als T.I.S.P. qualifiziert. Ende November 2006 erwarb Jörg Völker zu seiner Zertifizierung als BS 7799 Lead Auditor auch die Zertifizierung zum Lead Auditor nach ISO 27001.

ITSF 2007

Vom 07.-10.05.2007 findet das diesjährige IT-Sicherheits-Forum (ITSF) 2007 von ComConsult und GAI Netconsult in Königswinter statt, an dem auch diesmal wieder Referenten von Secorvo mitwirken .

Virtuelle Sicherheit?

„Wie virtuell ist Ihre Sicherheit?“ lautet der Titel des kommenden Events der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 29.03.2007 (Beginn: 18 Uhr im Schlosshotel Karlsruhe). Dr. Christian Riede und Stefan Kratzer von der Firma CONNECT werden die Herausforderungen von Virtualisierungskonzepten für die IT-Security beleuchten. Das verspricht nicht nur ein spannender Vortrag zu werden: die bis heute eingegangenen über 50 Anmeldungen lassen spannende Diskussionen und ein interessantes Net(t)working am Buffet erwarten. Online-Anmeldung unter www.ka-it-si.de.

Security Awareness Symposium

2007 jährt sich das „Security Awareness Symposium“ zum fünften Mal. Auch diesmal erwarten wir einen regen Erfahrungsaustausch von Verantwortlichen aus Unternehmen und Behörden, die Security Awareness-Kampagnen durchgeführt haben, planen oder derzeit umsetzen.

Nach Präsentationen von u. a. BASF, BMW, Bosch, DAK, Fiducia, FinanzIT, Münchener Rück, Novartis, SAP, Swiss Re und T-Systems in den Vorjahren werden in diesem Jahr Airbus, das BSI, Carl Zeiss, e.on, M. DuMont und RWE Systems ihre Kampagnen und „Lessons Learned“ vorstellen.

Wegen der wachsenden Teilnehmerzahlen wird das Symposium erstmals nicht in den Räumen von Secorvo, sondern in der Tagungsstätte Buhlsche Mühle in Ettlingen stattfinden (10 min. Fahrt vom Karlsruher Hbf). Termin: 12.-13.06.2007.

Eine Vorversion des Programms und ein Anmeldeformular finden Sie unter
www.security-awareness-symposium.de

Veranstaltungshinweise

Auszug aus www.veranstaltungen-it-sicherheit.de

März 2007	
26.-28.03.	Fast Software Encryption 2007 (IACR, Luxembourg)
26.-29.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
27.-30.03.	Black Hat Europe 2007 (Black Hat, Amsterdam)
29.03.	Wie virtuell ist Ihre Sicherheit? (KA-IT-Si, Karlsruhe)
April 2007	
10.-.13.04.	SecSE 2007 The First International Workshop on Secure Software Engineering (ENISA, Wien)
17.-19.04.	IT-Sicherheitsaudits in der Praxis (Secorvo, Karlsruhe)
24.-26.04.	Sichere Softwareentwicklung (Secorvo, Karlsruhe)
Mai 2007	
07.-10.05.	ITSF 2007 (ComConsult, Königswinter)
08.-10.05.	Kommunikationsschutz und Datensicherheit (Secorvo, Karlsruhe)
22.-24.05.	10. Deutscher IT-Sicherheitskongress (BSI, Bonn)

Fundsache

Auszug aus www.security-finder.de

Das über 30 Jahre alte Tutorial The Protection of Information in Computer Systems ist eine epochale Zusammenstellung der grundlegenden Entwurfsprinzipien und Mechanismen für sichere IT-Systeme aus der Sicht von Betriebssystemarchitekten. Eine historische Referenz, die belegt, wie lange einige der immer noch häufig angemahnten Prinzipien schon bekannt sein müssten.

Impressum

http://www.secorvo-security-news.de/

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

April 2007



Editorial: 1 x 1 > 2

Seit dem zweifelhaften „Siegeszug“ des Phishing ist die „Zwei-Faktor-Authentisierung“ als Ersatz für PINs, TANs und Passworte in aller Munde. Ein sicherheitstechnisches „Ei des Kolumbus“ ist der Ansatz allerdings nicht: Ein höheres Schutzniveau ist damit nicht automatisch verbunden. Wie so oft liegt der Teufel im Detail.

So gibt es zwei notwendige Eigenschaften, die ein „zweiter Faktor“ bei der Authentisierung erfüllen muss: er muss ein zusätzliches, vom ersten unabhängiges Merkmal sein (keine zweite PIN), und seine Gewinnung muss für einen Angreifer eine zusätzliche Hürde darstellen, sodass er beide Faktoren nicht „in einem Streich“ gewinnen kann. Beispielsweise erfordert ein Authentisierungstoken das physische Entwenden, das im Unterschied zu einer PIN bemerkt werden kann; gute biometrische Verfahren erfordern die körperliche Mitwirkung des „Opfers“. Häufig wird daher die Kombination von „Haben“ und „Wissen“ (z. B. eine Smartcard mit einer PIN), bei sehr hohen Sicherheitsanforderungen die von „Wissen“ und „Sein“ empfohlen (z. B. ein Fingerabdruck-Sensor mit einem Passwort).

Das allein aber genügt nicht, um einen Zugriffsschutz wirksam zu verbessern. Denn einen tatsächlichen Sicherheitsgewinn leistet eine solche Kombination nur, wenn beide Faktoren technisch gekoppelt sind: Nur eine Smartcard mit PIN-Schutz und Fehlbedienungszähler bietet ein höheres Schutzniveau, nicht aber eine Kartenprüfung mit unabhängiger PIN-Abfrage durch das System.

Schließlich muss die Authentisierung immer gegenüber dem Endsystem erfolgen – gibt es ein unsicheres „Zwischensystem“, so kann ein Angreifer den Mechanismus dort aushebeln. Daher sind Zwei-Faktor-Authentisierungen bei Client-Server-Anwendungen (wie Online-Banking) nur sicher, wenn die Authentisierung nicht am Client-PC endet, sondern das Authentisierungsprotokoll zwischen Token und Server abläuft – und der PC nur als „Übermittler“ auftritt. An einem Token mit eigener Recheneinheit führt da kein Weg vorbei.



Inhalt

Editorial: 1 x 1 > 2

Security News

Sargnagel für WEP

DNS Weakness

Vulnerabilities Reports

Vista Security Guide

Friendly Fire

Department of DNS Security?

TrueCrypt für Vista

„Two Factor“ – redefined

Secorvo News

Secorvo College aktuell

Tütenwelten

Online-Datensicherung

Security Awareness Symposium

Veranstaltungshinweise

secorvo
security consulting

Security News

Sargnagel für WEP

Wer noch immer hofft, sein Wireless LAN per WEP absichern zu können, muss sich endgültig eines Besseren belehren lassen. Drei Forscher der TU Darmstadt präsentieren in einem am 03.04.2007 veröffentlichten Papier ihre neuesten Ergebnisse zum Brechen von WEP in der Praxis. Durch Kombination von neuen theoretischen Optimierungen beim Angriff auf den RC4-Algorithmus mit bekannten Techniken zum Erlangen von Klartext/Chiffrat-Paaren wie z. B. ARP-Re-Injection ist es möglich, in Minutenschnelle auch 104 Bit WEP-Schlüssel (aus Marketing-Gründen gerne als „128 Bit WEP" bezeichnet) zu ermitteln. Eine Implementierung ihres Angriffs liefern die Forscher gleich mit. Die Attacke ist zwar probabilistischer Natur – allerdings lassen sich mit nur 85.000 Paketen, die innerhalb von etwa zwei Minuten aus dem Netz gefischt werden können, ganze 95% der Schlüssel knacken.

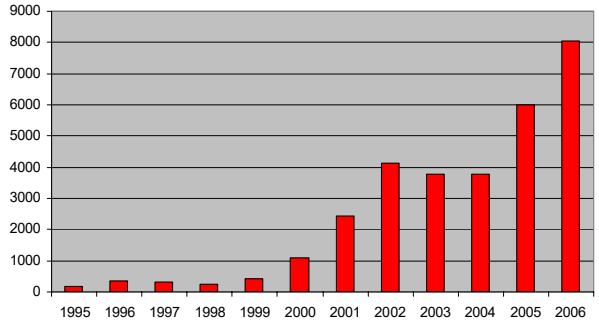
DNS Weakness

Die am 12.04.2007 publizierte Schwachstelle in Microsofts DNS-Dienst ist eine eigene Meldung wert. Nicht, weil sie eine Übernahme des Systems ermöglicht, Exploits zur Ausnutzung der Schwachstelle existieren und es noch keinen Patch gibt: Schwerer wiegt, dass auf ein wichtiges Betriebsrisiko nicht hingewiesen wird und die vorgeschlagenen Workarounds zumindest diskussionswürdig sind. So wird der DNS-Dienst oft auf Domänencontrollern betrieben; damit sind bei einer Übernahme das gesamte System und auch komplette Domänen kompromittiert – dadurch verschärft sich die Bedrohung in der Praxis.

Doch was tun ohne Patch? Einige der in Microsofts TechNet vorgeschlagenen Workarounds deaktivieren Funktionen wie das Remote Management des DNS-Dienstes. Andere wirken etwas hilflos, wie die vorgeschlagene Portfilterung der RPC-Verbindungen über eine Firewall – die sollten bei über das Internet erreichbaren Systemen ohnehin blockiert sein. Ein Seiteneffekt des Workarounds „Blocking port 445" verhindert SMB Connects – und wirkt wohl eher als Denial-of-Service. Besser wäre gewesen, auf Empfehlungen dieser Art zu verzichten – und die Energie in eine zügige Patch-Entwicklung zu stecken.

Vulnerabilities Reports

Jahr für Jahr veröffentlicht das Coordination Center des CERT an der Carnegie Mellon University eine Übersicht der von den weltweit verteilten CERTs berichteten sicherheitskritischen Software-Fehlern in verbreiteten Applikationen. Nach kurzer Stagnation (2002 bis 2004) steigt die Gesamtzahl der gefundenen kritischen Bugs seit zwei Jahren wieder kräftig an: Allein in 2006 wurden über 26 % aller seit 1995 entdeckten Bugs gefunden.



Grafik: CERT/CC-Statistik (Stand: 16.01.2007)

Auch wenn diese Entwicklung einem Gutteil der verbesserten und intensivierten Suche nach Sicherheitsfehlern zuzuschreiben sein könnte, ist diese Tendenz dennoch sehr beunruhigend – belegen die Zahlen doch, dass 2006 durchschnittlich 22 neue Sicherheitslücken täglich zu bewältigen waren, Wochenenden und Feiertage inklusive.

Vista Security Guide

Am 25.01.2007 hat Microsoft Version 1.2 des 107-seitigen Windows Vista Security Guide veröffentlicht. Der auf dem Windows XP Security Guide v2.2 vom 10.04.2006 basierende Leitfaden wurde in einer ersten Fassung schon am 08.11.2006 publiziert und anschließend mehrmals aktualisiert.

Der Guide beschreibt, mit welchen Einstellungen ein Grundschutz-Niveau („Basis-Sicherheit") auf einem Vista-Client erreicht werden kann, sowie die Konfiguration eines Hochsicherheits-Clients unter Inkaufnahme von Funktionseinschränkungen. Mitgeliefert wird ein Excel-Sheet mit Dutzenden von Group Policy Settings sowie dem Group Policy Objects (GPO) Accelerator Tool, das die Umsetzung der Sicherheitskonfiguration über vorgefertigte Templates erheblich erleichtert. Besonders hilfreich: Der tabellarische Vergleich der Default- mit der empfohlenen Grundschutz-Konfiguration von Vista.

Friendly Fire

Ein am 07.03.2007 vom Center for Strategic & International Studies (CSIS) veröffentlichter Bericht über „Foreign Influence on Software" beleuchtet Risiken, die sich aus der Verlagerung der Entwicklung von Software – besonders in kritischen Bereichen – ins Ausland ergeben. Bereits im Oktober 2005 wurde eine Task-Force des amerikanischen Verteidigungsministeriums mit der Erstellung einer

Studie zum „Mission Impact of Foreign Influence on DoD Software“ beauftragt. Der CSIS-Bericht kommt zu dem Schluss, dass die Entwicklungs- und Abnahmeprozesse für Software im Hinblick auf Sicherheit deutlich verbessert werden müssen, unabhängig davon, ob Software im Ausland oder Inland erstellt wird. Die Verurteilung eines Vertragspartners der U.S. Navy in Norfolk am 05.04.2007, der U-Boot-Computer sabotierte, unterstützt die These, dass nicht nur von unkontrolliertem Off-Shoring Gefahren ausgehen.

Department of DNS Security?

Auf einer Sitzung der Internet Corporation for Assigned Names and Numbers (ICANN) in Lissabon am 27.03.2007 berichtete der Chef der kanadischen Internet Registration Authority (CIRA), Bernard Turcotte, von einem internen Papier der US-Regierung, welches offenbar an einige Domainregistrare verteilt wurde: Das U.S. Department of Homeland Security (DHS) soll darin gefordert haben, die Kontrolle über den zur DNSSEC-Signierung der Root-Zone (.) notwendigen Root-Schlüssel zu erhalten. Sieht man einmal davon ab, dass DNSSEC (schon seit zu vielen Jahren) erst vor der Einführung steht (SSN 05/2004, 04/2006) und dieser Schlüssel daher noch gar nicht existiert, stellt sich doch die Frage, welchen Zweck das DHS mit dieser Forderung verfolgt. Denn weder könnte mit diesem Schlüssel etwas ver- oder entschlüsselt werden, noch würde er sich zum Spoofing von IP- oder DNS-Informationen eignen.

Theoretisch würde die Kontrolle des Root-Schlüssels erlauben, durch Fälschung von DNSSEC-Schlüsseln bestimmte (z. B. „unerwünschte“) Domains zu übernehmen. Die Domain boese-terroristen.org könnte dann bspw. vom DHS mit eigenen Inhalten betrieben werden. Dies würde jedoch relativ schnell bemerkt – vorausgesetzt, DNSSEC würde auch tatsächlich flächendeckend verwendet. Da drängt sich der Eindruck auf, dass die eigentliche Funktion der DNSSEC-Schlüssel vom DHS schlichtweg nicht verstanden wurde...

TrueCrypt für Vista

Am 19.03.2007 erschien Version 4.3 der freien Open Source-Implementierung TrueCrypt zur Verschlüsselung von Dateien und Festplattenpartitionen – jetzt auch für Windows Vista. TrueCrypt unterstützt mehrere Sprachen, zahlreiche Verschlüsselungsverfahren, ist leicht zu bedienen – und schnell.

„Two Factor“ – redefined

Zuerst verwirren sich die Worte, dann verwirren sich die Begriffe, und schließlich verwirren sich die Sachen (Konfuzius, 551-479 v. Chr.).

Am 11.04.2007 wurde in einer Pressemitteilung zu einem Sicherheitsvorfall bei der New Horizons Community Credit Union berichtet: „The computer was protected by two layers of security, a unique user-identifier and a multiple-character, alpha-numeric password.“ Vermutlich war die Erklärung irrtümlich zehn Tage zu spät veröffentlicht worden.

Secorvo News

Secorvo College aktuell

Lassen Sie sich Ihre Qualifikation zertifizieren: Die nächste Schulung und Prüfung zum Teletrust Information Security Professional (T.I.S.P.) findet am **25.-30.06.2007** statt. Programm und Online-Anmeldung unter http://www.secorvo.de/college

Tütenwelten

Was hat die Karlsruher IT-Sicherheitsinitiative mit Kunst zu tun? Das Geheimnis dieses Zusammenhangs wird von dem international renommierten Künstler Thitz auf der Vernissage der Neue Kunst Gallery (Karlsruhe) am 11.05.2007 ab 19 Uhr gelüftet. Wie immer mit Net(t)working und Erfahrungsaustausch. Eintritt frei, Anmeldung bis 10.05.2007.

Online-Datensicherung

Am 03.05.2007 lädt der von Dirk Fox geleitete Arbeitskreis Sicherheit des eco (Verband der deutschen Internetwirtschaft e. V.) zu einer halbtägigen Veranstaltung zum Thema Online-Datensicherung nach Frankfurt. Die Teilnahme ist unentgeltlich, eine Anmeldung ist bis 30.04.3007 erforderlich.

Security Awareness Symposium

Auf dem diesjährigen fünften „Security Awareness Symposium“ vom **12. bis 13.06.2007** werden u. a. das BSI, Carl Zeiss, e.on Ruhrgas, European Investment Bank, Fiducia und M. Dumont Schauberg ihre Konzepte und „Lessons Learned“ präsentieren – nach Kampagnenberichten von BASF, BMW, Bosch, DAK, FinanzIT, Münchener Rück, Novartis, RWE, SAP, Swiss Re und T-Systems in den Vorjahren.

Der jährliche Erfahrungsaustausch über wirksame Maßnahmen und Kampagnenideen zur Sensibilisierung der Mitarbeiter für Informationssicherheit findet wegen der wachsenden Teilnehmerzahlen in diesem Jahr in den stilvollen Räumlichkeiten der Buhlschen Mühle in Ettlingen statt (ca. 10 min. Fahrt vom Karlsruher Hauptbahnhof). Teilnahmegebühr: 490 Euro (zzgl. MwSt.). Programm, Online-Anmeldung und Anfahrtskizze:
http://www.security-awareness-symposium.de

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2007	
03.05.	Online-Datensicherung (eco AK Sicherheit, Frankfurt)
07.-08.05.	Datenschutzkongress (Euroforum, Berlin)
07.-10.05.	ITSF 2007 (ComConsult, Königswinter)
11.05.	Tütenwelten (KA-IT-Si, Karlsruhe)
15.-17.05.	6th OWASP Appsec Conference (Mailand)
20.-23.05.	2007 IEEE Symp. on Security and Privacy (Oakland)
20.-24.05.	Eurocrypt 2007 (IACR, Barcelona)
22.-24.05.	10. Deutscher IT-Sicherheitskongress (BSI, Bonn)
Juni 2007	
12.-13.06.	Security Awareness Symposium 2007 (Secorvo, Karlsruhe-Ettlingen)
25.-29.06.	T.I.S.P. Schulung (Secorvo, Karlsruhe)
30.06.	T.I.S.P. Zertifikatsprüfung (Secorvo, Karlsruhe)

Fundsachen

Auszug aus www.security-finder.de

Um ein Datenschutz-Zertifikat zur Bestätigung eines hohen Datenschutz-Niveaus erfolgreich zu etablieren, müssen die Rahmenbedingungen stimmen. Ausgehend vom Informationsbedarf möglicher Zielgruppen an ein solches Zertifikat begründet der Beitrag Cui bono? - Ziele und Inhalte eines Datenschutz-Zertifikats die Datenschutzorganisation als Prüfgegenstand und stellt die nach Ansicht der Autoren wichtigsten Inhalte der Prüfung vor.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim-Knobloch, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Mai 2007



Editorial: Die Bärenstrategie

Zwei Wanderer werden vom Bären verfolgt. Da stoppt der eine und zieht Laufschuhe an. Meint der andere: „Damit bist du auch nicht schneller als der Bär." Entgegnet der erste: „Ich muss ja nicht schneller sein als der Bär."

Zugegeben, eine etwas gewöhnungsbedürftige Perspektive und eine zweifellos wenig solidarische Haltung. Aber nicht nur auf der Flucht, sondern auch in der IT-Sicherheit ist diese Bärenstrategie ohne Zweifel ein Erfolgsrezept – mit einem sehr weiten Anwendungsbereich.

Denn in der Praxis genügt es in der Regel, ein etwas höheres Sicherheitsniveau zu bieten, um Phishern, Pharmern, Hackern und „Skript-Kiddies" zu entkommen. Einem Angreifer bieten die einfachsten Methoden das beste Kosten-Nutzen-Verhältnis – so wie ein Einbrecher auch das offene Balkonfenster einer verschlossenen Sicherheitstüre vorziehen wird. Der Effekt lässt sich derzeit gut bei Phishing-Attacken beobachten: Kaum führt ein Institut iTANs ein, konzentrieren sich die Angreifer auf einen Mitbewerber.

Auch bei der eigenen Prioritätensetzung hilft die Bärenstrategie: An der Stelle mit dem niedrigsten Sicherheitsniveau ist ein erfolgreicher Angriff am wahrscheinlichsten – daher verdient diese Stelle die größte Aufmerksamkeit. So sollte die konsequente Durchsetzung einer einheitlichen Mindest-Passwortqualität Vorrang vor einer Datenverschlüsselung genießen, die Reduktion überflüssiger (Administrator-) Privilegien wichtiger genommen werden als ein Intrusion Prevention System, und die Beschleunigung des Roll-Outs von Sicherheits-Patches der Einführung eines SmartCard-Logins vorgezogen werden. Nicht, dass Verschlüsselung, IPS oder SmartCards unwichtig oder gar unsinnig wären – allein: Siege werden auch in der IT-Sicherheit zuerst mit den handwerklichen „Basics" errungen.

Leider hat die Bärenstrategie einen Haken. Sie funktioniert, wenn beide Wanderer für den Bären gleich attraktiv sind. Ist der schnellere Happen der appetitlichere, retten auch die Laufschuhe nicht.



Inhalt

Editorial: Die Bärenstrategie

Security News

SAP im Fokus?

AHS und Ohs

Phishing-Windows-Aktivierung

Des Kaisers neue Kleider

Alte Erkenntnisse - neu belegt

Professionelles Social Engineering

Awareness-Grenzen

Secorvo News

Secorvo College aktuell

Innovationspreis für Video

Security Awareness Symposium

KA-IT-Si über sichere Software

Veranstaltungshinweise

Fundsachen

secorvo
security consulting

Security News

SAP im Fokus?

Im SAP Security Newsletter April 2007 reagiert SAP auf einen Vortrag bei der BlackHat Europe 2007 Konferenz vom 30.03.2007. Das Papier eines südamerikanischen Sicherheitsspezialisten beschäftigt sich mit dem in Hacker-Kreisen oft als „dunkler Kontinent" angesehenen Innenleben von SAP R/3 und analysiert das Remote Function Call (RFC) Interface. Im Rahmen dieser Analyse wurden mehrere, inzwischen von SAP behobene Sicherheitslücken aufgedeckt und mit sapyto ein Open-Source Tool für Penetrationstests von R/3-Systemen entwickelt. Dies könnte ein Indiz dafür sein, dass SAP mehr in den Fokus der Hacker-Gemeinde rückt, die dort ein weiteres Anwendungsfeld für „bewährte" Angriffstechniken vorfindet.

R/3-Anwender sollten das zum Anlass nehmen, spätestens jetzt den SAP RFC/ICF Security Guide zu beherzigen. Und wer die Einführung von SNC plant, dürfte in dem BlackHat-Beitrag ein weiteres Argument dafür finden.

AHS und Ohs

Getreu der chinesischen Weisheit, dass auch die längste Reise mit dem ersten Schritt beginnt, hat das NIST erste Aktivitäten in der bis 2012 angelegten Suche nach einer neuen sicheren Hashfunktion, dem Advanced Hash Standard (AHS) als Nachfolger für den angeschlagenen SHA-1 und die verwandte SHA-2-Familie, unternommen: Am 07.05.2007 wurden die Kommentare aus Wissenschaft und Industrie zu den im Januar vorgelegten Kriterien veröffentlicht, denen der AHS genügen soll.

Der Tenor vieler Kommentare ist, nicht nur die Sicherheit der Hashfunktion im engeren Sinne, sondern auch deren mittlerweile gebräuchliche weitere Einsatzbereiche wie z. B. als Pseudozufallsfunktion, zum symmetrischen Integritätsschutz als HMAC und zur Schlüsselherleitung für symmetrische Chiffren als Auswahlkriterium zu betrachten.

Das NIST lässt explizit offen, ob es nur einen oder mehrere unterschiedliche Hash-Algorithmen als Gewinner des AHS-Wettbewerbs geben wird – sofern genügend Vorschläge die Kriterien erfüllen.

Phishing-Windows-Aktivierung

Eine neue Phising-Variante erscheint uns eine Erwähnung wert: Wie am 27.04.2007 von Symantec berichtet ist derzeit eine Trojanerversion in Umlauf, die beim ersten Systemstart nach der Infektion eine Aktivierung der Windows-Installation mit Eingabe einer gültigen Kreditkartennummer fordert.

Da das System herunter gefahren wird, wenn man keine Nummer einträgt, und Nutzern von illegalen Betriebssystemkopien ein solcher Mechanismus glaubwürdig erscheinen könnte, wird sich wohl der eine oder andere Anwender zur Eingabe verleiten lassen. Die Kartennummern werden an Systeme in Russland übermittelt und beispielsweise über einschlägige Foren verkauft – ein weiteres Beispiel für die zunehmend kriminellen Motive hinter verbreiteter Schadsoftware.

Des Kaisers neue Kleider

Mit der seit dem 01.05.2007 verfügbaren Produktklasse „Forefront" bündelt Microsoft seine bis dato unterschiedlichen (selbst entwickelten und zugekauften) Lösungen für Sicherheitssoftware und präsentiert als Roadmap eine Client, Server und „Edge" umfassende Strategie. Damit entwickelt sich Microsoft zunehmend zum Anbieter von Sicherheitslösungen – zum Schutz vor hausgemachten Sicherheitsproblemen.

In der nun überarbeiteten Lösung „Forefront - Security für Exchange Server" (ehemals Antigen für Exchange) beispielsweise können von neun enthaltenden Antivirus-Engines bis zu fünf parallel für Prüfprozesse von E-Mail genutzt werden. Durch diesen integrativen Ansatz wirkt damit das Know How von AV-Mitbewerbern zusammen (darunter Kaspersky, Norman, CA).

Derzeit laufen Forefront-Services wie z.B. FSC-Controller, FSCMonitor, FSCStatisticsService, FSEIMC, FSEMailPickup auf Exchangeservern mit absoluten Systemprivilegien (LocalSystem) – ein schwieriger Kontext für ein nachvollziehbares Audit. Vielleicht sollte sich Microsoft auf seine bereits im Juni 2005 propagierte Sicherheitsphilosophie besinnen, Dienste mit möglichst geringen Privilegien laufen zu lassen.

Alte Erkenntnisse - neu belegt

Am 24.04.2007 hat McAfee eine in Zusammenarbeit mit Datamonitor erstellte Studie mit dem Titel „Datagate: The Next Inevitable Corporate Disaster?" veröffentlicht. Diese Studie beschäftigt sich mit Ursachen für und Folgen von Datenverlust insbesondere durch Entwendung. Es wurden über 1.400 Unternehmen mit mehr als 250 Mitarbeitern befragt, darunter 75% mit mehr als 1.000 Angestellten. Es überrascht nicht, dass über 60% der Unternehmen in den vergangenen zwölf Monaten Vorfälle zu verzeichnen hatten und gerade einmal 6% von sich behaupten, in den vergangenen beiden Jahren keine Probleme gehabt zu haben. Immerhin glaubt

ein Drittel aller Teilnehmer, dass sie einen größeren Vorfall nicht überleben würden.

Die Studie berichtet, dass 23% der Firmen angaben, beobachtete Vorfälle seien bösartiger und vorsätzlicher Natur gewesen. 32% haben grob fahrlässige Vorfälle verzeichnet (z. B. Kopien vertraulicher Daten auf ungeschützten USB-Sticks) und in 45% aller Fälle sind die Vorfälle fahrlässig herbeigeführt worden (z. B. Verlust eines Laptops mit unverschlüsselten Daten). Die geografische Lage eines Unternehmens spielt hingegen keine Rolle für die Risiken von Datenverlust: Die Untersuchungsergebnisse unterschieden sich in Australien, Frankreich, UK und den USA nicht signifikant.

Die Studie stellt einige wichtige Best-Practices zum Umgang mit sensiblen Daten vor. Dem Fazit der Studie können wir uns nur anschließen: „... we know that technology ist not always the answer."

Professionelles Social Engineering

Die schweizerische „Melde- und Analysestelle Informationssicherung" (MELANI) hat am 30.04.2007 ihren vierten Halbjahresbericht „Informationssicherung – Lage in der Schweiz und international" herausgegeben. Wieder einmal enthält der Bericht sehr interessante Informationen zu aktuellen Bedrohungen sowie Aussagen zu zukünftigen Trends der Informationssicherheit. Die MELANI-Studie zeichnet dabei aus, dass sie nicht nur die aktuelle Situation beschreibt, sondern konkrete Vorfälle – in der Schweiz sowie international – aufzeigt, welche die einzelnen Probleme noch einmal verdeutlichen.

MELANI führt als Angriffs-Schwerpunkte zunächst die „üblichen Verdächtigen" an: Spam, Daten- und Identitätsdiebstahl, sowie Malware und Angriffsvektoren. Interessanterweise wird das Social Engineering an erster Stelle genannt. So gehen die Autoren davon aus, dass „Social Engineering mit zunehmender (technischer) Sicherheit von Betriebssystemen und Applikationen weiter an Bedeutung gewinnen" wird. Sie empfehlen daher Prävention: „Regelmäßige, den aktuellsten Trends angepasste Schulungen und Tests helfen, die Angestellten zu sensibilisieren und mögliche Gefahren zu erkennen."

Awareness-Grenzen

Dass auch die beste Awareness ihre Grenzen hat, zeigen zwei aktuelle Beispiele. Der Belgier Didier Stevens berichtete am 07.05.2007 von einem „Social Engineering-Experiment": Er schaltete über mehrere Monate eine Google-Anzeige mit dem Text „Is your PC virus-free? Get it infected here!" und war erschrocken, dass tatsächlich 409 Menschen auf die (harmlose) URL geklickt hatten. Dass dieser Mechanismus bereits heute von professionellen Betrügern missbraucht wird, bestätigte am 26.04.2007 sogar Google selbst – Google-Anzeigen hatten auf maliziöse Webseiten geleitet.

Secorvo News

Secorvo College aktuell

Die Nachfrage nach einer Bestätigung der Qualifizierung im Gebiet IT-Sicherheit durch den Erwerb eines T.I.S.P.-Zertifikats ist ungebrochen. Für das zusätzliche T.I.S.P.-Seminar vom 25.-30.06.2007 gibt es nur noch wenige freie Plätze, und auch das Herbst-Seminar vom 05.-10.11.2007 füllt sich bereits. Wir freuen uns auf Ihre Anmeldung.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Innovationspreis für Video

Für das Sensibilisierungs-Video „Social Engineering" wurde Secorvo am 16.04.2007 von der Initiative Mittelstand in der Kategorie IT-Security mit dem Innovationspreis 2007 ausgezeichnet.

Security Awareness Symposium

Awareness ist „in" – das zeigen die vielen Anmeldungen zum fünften „Security Awareness Symposium" am **12. bis 13.06.2007**, auf dem u. a. das BSI, Carl Zeiss, e.on Ruhrgas, European Investment Bank, Fiducia und M. Dumont Schauberg ihre Kampagnen und Erfahrungen präsentieren.

Das Programm des diesjährigen Erfahrungsaustauschs in den Räumlichkeiten der Buhlschen Mühle in Karlsruhe-Ettlingen (ca. 10 min. vom Karlsruher Hauptbahnhof), eine Online-Anmeldung und Anfahrtskizze finden Sie unter:
http://www.security-awareness-symposium.de

KA-IT-Si über sichere Software

Kein Monat ohne Sicherheits-Patch, -Update oder -Bugfix: Das „Flicken" fehlerhafter Software ist zu einer Hauptdisziplin der IT-Sicherheit geworden. Am **28.06.2007** werden Dr. Boris Hemkemeier (Commerzbank AG) und Tom Schröer (SAP AG) die Ergebnisse des vom BMWi geförderten Projekts "Secologic" vorstellen, in dessen Rahmen u. a. „10 Goldene Regeln" für Auftraggeber entwickelt wurden, die helfen sollen, die Zahl sicherheitsrelevanter Fehler in Software systematisch zu reduzieren. Für ein angemessenes Net(t)working-Ambiente ist – wie immer – gesorgt. Online-Anmeldung über
http://www.ka-it-si.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2007	
12.-13.06.	5. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)
12.-13.06.	DACH Security 2007 (Klagenfurt/A)
25.-29.06.	T.I.S.P. Schulung (Secorvo, Karlsruhe)
28.06.	Software ist fehlerfrei. Und die Erde eine Scheibe. (KA-IT-Si, Karlsruhe)
30.06.	T.I.S.P. Zertifikatsprüfung (Secorvo, Karlsruhe)
Juli 2007	
12.-13.07.	DIMVA 2007 (GI, Luzern/CH)
28.07.-02.08.	Black Hat USA 2007 (Las Vegas/US)
August 2007	
03.-05.08.	Defcon 15 (Las Vegas/US)
06.-10.08.	USENIX Security Symposium (Boston/US)
19.-23.08.	Crypto 2007 (IACR, Santa Barbara/US)

Fundsachen

Auszug aus www.security-finder.de

Internet-Suchmaschinen werden bereits seit vielen Jahren auch von Angreifern verwendet, um sensitive Informationen (z. B. Passwort-Dateien, Login-Daten) zu recherchieren und anschließend zu missbrauchen. The Google Hacker's Guide beschreibt, wie die Suchmaschine Google zu diesem Zweck von Angreifern eingesetzt wird und wie man sich dagegen schützen kann.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim-Knobloch, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Juni 2007



Editorial: Zunehmendes Nichts

Wenn Du entdeckst, dass Du ein totes Pferd reitest, steig ab. (Weisheit der Dakota-Indianer)

Zehn Jahre ist es her, dass das deutsche Signaturgesetz im Rahmen des „Informations- und Kommunikationsdienste-Gesetzes“ das Licht der Welt erblickte. Seitdem flossen Steuergelder in mehrstelliger Millionenhöhe und erhebliche Investitionen der Industrie in gesetzeskonforme CA-Infrastrukturen und eGovernment-Anwendungen. Mit bitterem Ergebnis: Bis heute ist keine Massenanwendung in Sicht, die die Ausgaben rechtfertigen würde; sogar Elster kommt ohne qualifizierte Signaturen aus. Doch es wird methodisch weitergeritten:

Strategie 1: Richte eine unabhängige Behörde für das Hüten toter Pferde ein.

Die Bundesnetzagentur wurde 1997 mit dem Betrieb der Wurzel-CA und der Aufsicht über die Einhaltung des Gesetzes beauftragt.

Strategie 2: Schirre mehrere tote Pferde zusammen, damit sie schneller werden.

Am 13.12.1999 verabschiedete die EU eine „Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“, an die das deutsche Signaturgesetz am 16.05.2001 angepasst wurde.

Strategie 3: Bilde eine Task Force, um das tote Pferd wiederzubeleben.

Am 03.04.2003 gründeten „Staat und Wirtschaft“ auf Initiative von BMWi und BMI das „Bündnis für elektronische Signaturen“. (Die „SigBü“-ChipKarte gibt es bis heute nicht, und unter „Aktuelles“ findet man genau einen Eintrag - vom 28.03.2006.)

Strategie 4: Stelle Vergleiche unterschiedlicher toter Pferde an.

Derzeit lässt die EU die Anwendung elektronischer Signaturen in den Mitgliedsstaaten evaluieren. Erst im Oktober 2003 war eine Studie für die EU-Kommission zu ernüchternden Einsichten gelangt. Diesmal wurde ein anderes Autorenteam beauftragt...

Strategie 5: Wetten, dass das Vieh nur simuliert?!

Zum zehnten Geburtstag tröstet der Jahresbericht 2006 der Bundesnetzagentur optimistisch: „Damit steht auch dem (...) elektronischen Geschäftsverkehr zunehmend nichts mehr im Wege.“



Inhalt

Editorial: Zunehmendes Nichts

Security News

Unterschriften gegen SPAM

Baustein Datenschutz

Totgeglaubte leben länger

SSL-Zertifikate in XXL

Dicke Fische

Neue Richtlinien

Top Ten aktualisiert

Softwarehaftung

Secorvo News

Secorvo College aktuell

Whitepaper “PKI-Policy”

Security Awareness Symposium

Software ist sicher ...

Veranstaltungshinweise

secorvo
security consulting

Security News

Unterschriften gegen SPAM

Im Mai 2007 wurde von der IETF die RFC 4871 im Standards Track veröffentlicht. Hierbei handelt es sich um eine Spezifikation des DKIM-Ansatzes, an dessen Entwicklung Mitarbeiter namhafter Firmen wie Sendmail Inc., Yahoo, PGP und Cisco beteiligt waren. Die Motivation für DKIM wurde in RFC 4686 dokumentiert. Zur Sicherstellung der Identität von Absendern sollen E-Mails digital unterschrieben werden. Zur Überprüfung sind keine aufwändigen PKI-Infrastrukturen erforderlich, denn die öffentlichen Schlüssel werden über DNS-Mechanismen verteilt. Die Vorteile des Verfahrens liegen im geringen Aufwand für die Implementierung. Leider existieren zur Zeit nur wenige Lösungen, daher setzen bisher auch nur wenige Organisationen DKIM produktiv ein. Zur erfolgreichen Verbreitung von DKIM ist eine breite Akzeptanz erforderlich.

Derzeit ist noch nicht abzusehen, ob dieser Ansatz, auf den wir einige Hoffnung setzen, sich durchsetzen wird. Wir werden ihn weiterhin aktiv beobachten. Interessante Einblicke in aktuelle Anti-SPAM-Anätze bieten auch die Ergebnisse der ENISA.

Baustein Datenschutz

Seit dem 01.06.2007 gibt es einen neuen Baustein zum Datenschutz in den IT-Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Dieser Baustein wurde von den Datenschutzbeauftragten des Bundes und der Länder und den Aufsichtsbehörden der Länder für den nicht-öffentlichen Bereich unter Federführung von Claus Simon, Referatsleiter Technik beim Landesbeauftragten für Datenschutz und Informationsfreiheit des Saarlandes erarbeitet.

Insbesondere die tabellarische Zuordnung der Grundschutzmaßnahmen zu den technisch-organisatorischen Schutzzielen in der Anlage zum § 9 BDSG am Schluss des 65seitigen Dokuments sind höchst wertvoll für die Praxis. Nach entsprechender redaktioneller Überarbeitung wird er auch auf den Webseiten des BSI zum Abruf bereitgestellt.

Totgeglaubte leben länger

Auch wenn die Welt einige Zeit warten musste – die letzte Ausgabe von Phrack erschien am 16.01. 2004 – ist nun eine neue Ausgabe des wohl ältesten Online-Magazins der Hacker-Community erschienen: Phrack #64 ist seit dem 26.05.2007 online. Das neue Redaktionsteam, "The Circle of Lost Hackers", hat einige spannende Artikel beispielsweise zu Kernel Exploiting und aktuellen Möglichkeiten zum Blind TCP Hijacking zusammen gestellt.

SSL-Zertifikate in XXL

Zum Erhalt eines offiziellen SSL-Zertifikats der bekannten Trustcenter benötigt man nicht mehr als die E-Mail-Adresse, unter der die Internet-Domain des Webservers registriert wurde – und ca. 100 Euro für die Begleichung der Jahresgebühr. Um diesem Umstand abzuhelfen, der z. B. Phishern in die Hände spielt, wurden „Extended Validation" (EV) Zertifikate aus der Taufe gehoben, für die man amtliche Dokumente wie einen Handelsregisterauszug vorweisen muss. Ergänzend färbt Microsoft im neuesten Internet Explorer den Adressbalken grün, wenn der SSL-Server ein EV-Zertifikat vorweist.

Allerdings sind die etwa zehnfachen Kosten für ein EV-Zertifikat eine Investition in eine ungewisse Zukunft: So lange nicht (fast) alle anderen legitimen Webserver ebenfalls EV-Zertifikate verwenden oder gar – wie am 29.05.2007 auf der von Microsoft gesponserten „Sicher im Netz"-Seite geschehen – trotz EV-Zertifikat den Nutzern ein Zertifikatsfehler serviert wird, kann EV den Phishern herzlich egal sein. Zudem hat eine Usability-Studie von Microsoft und der Stanford University vom 15.02.2007 ergeben, dass untrainierte Anwender die grüne EV-Anzeige nicht einmal wahrnehmen – nach Lektüre der Hilfe-Seiten hingegen neigen sie dazu, ihren gesunden Menschenverstand abzuschalten und allen Webseiten zu vertrauen, vor denen nicht explizit gewarnt wird.

Dicke Fische

Vor der vietnamesischen Küste sind Dieben Ende März 2007 ziemlich dicke Fische ins Netz gegangen. Das staatliche e-Newspaper VietNamNet berichtete am 07.05.2007, dass Teile des optischen Kabels, über welches die Internet-Anbindung von Vietnam realisiert ist, von Unbekannten gestohlen wurden. Bis zur Reparatur des Schadens ist Vietnam jetzt nur noch über ein einziges Kabel erreichbar.

Das Beispiel zeigt, dass Risiko- und Bedrohungsanalysen regelmäßig aktualisiert werden müssen: War Diebstahl zum Zeitpunkt der Verlegung des Seekabels (1993-1995) kein realistisches Bedrohungsszenario, so haben sich seitdem (Schwarz-) Markt und technische Möglichkeiten der Angreifer erheblich entwickelt.

Neue Richtlinien

Im Juni sind gleich drei Entwurfsversionen interessanter Sonderveröffentlichungen des NIST erschienen. Alle drei Richtlinien können bis Juli kommentiert werden. Dabei handelt es sich um einen User's

Guide to Securing External Devices for Telework and Remote Access, die Guidelines on Securing Public Web Servers und einen Guide for Assessing the Security Controls in Federal Information Systems, die wertvolle Anregungen auch für Sicherheitsorganisationen außerhalb amerikanischer Regierungsinstitutionen enthalten.

Top Ten aktualisiert

Beim Lesen der aktuellen, gründlich überarbeiteten OWASP Top Ten Liste 2007, einer der wichtigsten aktuellen Übersichten über schwerwiegende Schwachstellen in Web-Applikationen, können sich durchaus unangenehme Gefühle einstellen. Mit der am 12.05.2007 veröffentlichten Zusammenstellung hat die OWASP-Gruppe das etablierte Referenzdokument an aktuelle Gegebenheiten angepasst und noch einmal deutlich verbessern können.

Softwarehaftung

Auf dem 10. Deutschen IT-Sicherheitskongress des Bundesamts für Sicherheit in der Informationstechnik (BSI) vom 22.-24.05.2007 wurde von Dr. Thomas Ramsauer (BSI) im Rahmen seines Vortrags „Verantwortungsverteilung und Anreizstruktur im Bereich der IT-Sicherheit“ die zwischenzeitlich erschienene Auftragsstudie mit dem Titel „Rechtsentwicklung in der IT-Sicherheit“ von Prof. Dr. Gerald Spindler angekündigt. Die Studie setzt sich auf über 300 Seiten mit der rechtspolitischen Frage auseinander, inwieweit das nationale Recht mit seinen Steuerungsinstrumenten in der Lage ist, den Risiken der Informationstechnik Rechnung zu tragen. Damit soll der steigenden Anzahl an Meldungen über Sicherheitslücken in Softwareprogrammen, neue Viren, Würmer und Trojaner Rechnung getragen werden, die die Frage aufwerfen, wie Pflichten, Verantwortlichkeit und Haftung derjenigen nach geltendem Recht aussehen, die an Herstellung, Einsatz und Nutzung von IT-Produkten beteiligt sind.

Die Studie läutet einen neuen Abschnitt der Diskussion um sichere Software(entwicklung) und die Haftbarkeit im deutschen Rechtsraum ein und liefert Impulse dafür, die Handlungsnotwendigkeit mit dem Geldbeutel des Managements zu verknüpfen.

Secorvo News

Secorvo College aktuell

Das (noch junge) Qualifikationszertifikat T.I.S.P. hat seinen Siegeszug angetreten: Die Nachfrage nach T.I.S.P.-Seminaren ist so groß, dass die akkreditierten Anbieter Zusatzseminare auflegen. Bis Ende 2007 wird die Zahl der Absolventen voraussichtlich die Schwelle von 200 überschreiten – und nähert sich damit rapide der Zahl der seit 1989 angebotenen (ISC)²-Abschlüsse (CISSP, CAP und SSCP) in Deutschland: Im Mai 2007 waren es gerade einmal 477. Secorvo College führt vom 25.-30.06. ein T.I.S.P.-Seminar durch; auch für den Termin vom 05.-10.11.2007 gibt es bereits zahlreiche Buchungen – lassen auch Sie Ihre Qualifikation zertifizieren (Online-Anmeldung).

Whitepaper “PKI-Policy”

Im aktuellen Secorvo White Paper vom 06.06.2007 fassen Petra Barzin und Stefan Kelm die Erfahrungen von Secorvo mit Policy-Rahmenwerken für PKIs zusammen. Das Whitepaper gibt eine strukturierte Einführung in drei zentralen Dokumente Certificate Policy (CP), Certification Practice Statement (CPS) und PKI Disclosure Statement (PDS). Der Schwerpunkt liegt auf der Darstellung des jeweiligen Zwecks und Inhalts und gibt Hilfestellung bei der Wahl der geeigneten Policy-Dokumente.

Security Awareness Symposium

Vom 12. bis 13.06.2007 fand das fünfte „Security Awareness Symposium“ mit knapp 60 Teilnehmern aus Wirtschaft und öffentlicher Verwaltung statt. Die präsentierten Kampagnen und Erfahrungen von BSI, Carl Zeiss, European Investment Bank, FIDUCIA, M. Dumont Schauberg und e.on Ruhrgas zeigten, dass die Sensibilisierung der Mitarbeiter für Informationssicherheit inzwischen in vielen Unternehmen zum festen Bestandteil der Sicherheitsstrategie geworden ist. Dabei hat sich gezeigt, dass vor allem die Gewinnung und Einbindung des Managements von entscheidender Bedeutung für den Erfolg einer Kampagne ist. Die Dokumentation des Symposiums (sowie aller vorausgegangenen) kann online bestellt werden.

Software ist sicher ...

... und die Erde eine Scheibe. Am **28.06.2007** (18 Uhr) werden Dr. Boris Hemkemeier (Commerzbank AG) und Tom Schröer (SAP AG) im Karlsruher Schlosshotel im Rahmen eines Events der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) die Ergebnisse des vom BMWi geförderten Projekts „Secologic“ vorstellen. In dessen Rahmen wurden u. a. Goldene Regeln für Auftraggeber entwickelt, die helfen sollen, die Zahl sicherheitsrelevanter Fehler in Software systematisch zu reduzieren. Für ein spannendes Net(t)working wird nicht nur das Ambiente sorgen – auch die zahlreichen Anmeldungen lassen interessante Diskussionen und Gespräche erwarten. Online-Anmeldung über http://www.ka-it-si.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2007	
25.-29.06.	T.I.S.P. Schulung (Secorvo, Karlsruhe)
28.06.	Software ist fehlerfrei. Und die Erde eine Scheibe. (KA-IT-Si, Karlsruhe)
30.06.	T.I.S.P. Zertifikatsprüfung (Secorvo, Karlsruhe)
Juli 2007	
12.-13.07.	DIMVA 2007 (GI, Luzern/CH)
28.07.-02.08.	Black Hat USA 2007 (Las Vegas/US)
August 2007	
03.-05.08.	Defcon 15 (Las Vegas/US)
06.-10.08.	USENIX Security Symposium (Boston/US)
19.-23.08.	Crypto 2007 (IACR, Santa Barbara/US)
28.-29.08.	XCon2007 (Beijing/CN)
September 2007	
18.-20.09.	IT-Sicherheit heute (Secorvo, Karlsruhe)

Fundsache

Auszug aus www.security-finder.de

Mitteilung der EU-Kommission zu den Vorteilen von Technologien zum Schutz der Privatsphäre. Die Mitteilung enthält die diesbezüglichen Ziele der Kommission, die durch eine Reihe gezielter Maßnahmen zur Förderung der Entwicklung solcher Technologien und ihrer Verwendung durch die für die Datenverarbeitung Verantwortlichen und die Verbraucher erreicht werden sollen.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Petra Barzin, Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch, Kai Jendrian, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Juli 2007



Editorial: Wiederentdeckung der Langsamkeit

Sten Nadolny war es, der vor fast 25 Jahren – zehn Jahre vor dem ersten WWW-Browser – die Langsamkeit zum deutschen Mega-Trend machte. Zumindest literarisch. In „Die Entdeckung der Langsamkeit" verklärt er sie in der Person des britischen Admirals Sir John Franklin zur entscheidenden Quelle von Zielstrebigkeit und Gründlichkeit, den späteren Erfolgsgaranten des Admirals bei Seegefechten und auf Forschungsreisen. Eine These, die, den Verkaufszahlen (1,7 Mio.) nach zu urteilen, wohl einen Kern der deutschen Seele traf.

Kurz darauf geriet die Welt in den Griff moderner Informations- und Kommunikationstechnik (WWW, E-Mail, SMS). Die Herausforderung der Globalisierung tat ein Übriges: Getrieben von der Furcht, wirtschaftlich den Anschluss zu verlieren, entdeckte Ende der 90er Jahre die Bundesregierung mit mehrjähriger Verspätung das Internet. Nun zählte Schnelligkeit. Um den internationalen Rückstand aufzuholen, wurden Unsummen in eGovernment-Programme gesteckt: allein 1,65 Mrd. € in „BundOnline 2005" (2002).

Langsamkeit ist jedoch geduldig. Nach dem Höhepunkt der Online-Euphorie meldete sie sich als „Entschleunigung" zurück. Ihre Renaissance erreicht nach der systematischen Beruhigung innerstädtischer Verkehrswege und der Erfindung von „Slow Food" nun auch das eGovernment. So wurden im Projekt „Deutschland-Online" seit 2003 ganze zwei von insgesamt 15 Vorhaben umgesetzt. Und über die Nutzung der seit 2002 möglichen elektronischen Steuererklärung mit digitaler Signatur werden lieber keine Zahlen veröffentlicht. Nun hat es auch die Bundesnetzagentur erwischt: Die Umstellung der Wurzel-Schlüssel und -Zertifikate auf die von ihr selbst empfohlenen Schlüssellängen und Hashfunktionen ist längst überfällig. Und für die Prüfung der von der (insolventen) Medizon AG ausgestellten qualifizierten Signaturzertifikate bietet sie neuerdings nicht etwa OCSP an, sondern empfiehlt das „SnailMail Certificate Status Protocol (SCSP)" – ein schriftliches Auskunftsersuchen per Post.



Inhalt

Editorial: Wiederentdeckung der Langsamkeit

Security News

Kriminelle Tools

Versteckspiel im Web

EAL 4+ für Red Hat – ein Plus?

Fluggastdatenaffäre

Click 'n Hack Tools

Populäres Filecarving

IIS – Bezahlpatch?

Awareness in YouTube

Secorvo News

Secorvo College aktuell

Sichere Software im Trend

Veranstaltungshinweise

Fundsachen

secorvo
security consulting

Security News

Kriminelle Tools

Aller Aufregung zum Trotz (siehe Editorial SSN 10/06) hat der Bundesrat die Änderung des § 202c StGB am 09.07.2007 durchgewunken. Der Wunsch des Gesetzgebers ist nachvollziehbar: Wenn einem Hacker nach gelungener Spurenverwischung schon die Tatdurchführung nicht nachgewiesen werden kann, dann soll wenigstens die Tatvorbereitung strafbar sein. Die publizistische Staubwolke um die Entscheidung ist vor dem Hintergrund der Gegenäußerung der Bundesregierung vom 30.11.2006 auch im Kontext der Anhörung vor dem Rechtsausschuss des Bundestages vom 18.04.2007 und der Empfehlung des Rechtsausschusses vom 23.05.2007 nur eingeschränkt nachzuvollziehen.

Eine Befürchtung bleibt allerdings: Wenn „Scheren im Kopf" zukünftig verhindern, dass Angriffstools weiterhin im Internet veröffentlicht und verbreitet werden, dann lassen sich die Möglichkeiten eines Angreifers weit weniger verlässlich abschätzen.

Versteckspiel im Web

Am 04.06.2007 hat finjan seinen vierteljährlichen Web Security Trends Report für das zweite Quartal 2007 veröffentlicht. Schlüsselfeststellung der Autoren: Durch sogenannten „Evasive Attacks" versuchen Angreifer mit immer ausgefeilteren Methoden der Entdeckung von Schadcode zu entgehen. Wurde Schadsoftware in der Vergangenheit hauptsächlich durch Verschleierung (Obfuscation) im Code versteckt, so finden sich heute ausgefeilte datenbankgestützte Mechanismen, durch die mit Hilfe spezieller Regeln angepasster Schadcode an Besucher infizierter Webseiten ausgeliefert wird. Der Code wird vor der weiteren Verteilung immer wieder verändert, so dass die Erkennbarkeit für herkömmliche Virenschutzlösungen erheblich erschwert wird. Daher gehört die Zukunft zweifellos geeigneten dynamischen Erkennungsverfahren als Ergänzung der derzeitigen signaturbasierten Methoden.

EAL 4+ für Red Hat – ein Plus?

Wieder einmal hat ein Hersteller den dornigen Weg einer Zertifizierung nach Common Criteria (CC) auf sich genommen: Am 07.06.2007 hat Red Hat Enterprise Linux 5 (RHEL) auf IBM-Hardware das begehrte Label „EAL 4+" erhalten. Wie immer lohnt für eine Bewertung dieser Evaluierung ein Blick in die zu Grunde liegenden Dokumente.

Jede CC-Evaluierung basiert auf so genannten „Schutzprofilen" (protection profiles), die auch Anforderungen an die Einsatzumgebung des zu untersuchenden Gegenstands beschreiben. Red Hat hat sein Betriebssystem gleich dreien dieser Profile ausgesetzt: Das schon von etlichen anderen Herstellern verwendete Controlled Access Protection Profile (CAPP) sowie Labeled Security Protection Profile (LSPP) und Role-Based Access Control Protection Profile (RBACPP). Im LSPP findet man Einschränkungen wie „The LSPP provides for a level of protection which is appropriate for an assumed non-hostile and wellmanaged user community", und auch das entsprechende Security Target bewertet die Schutzmechanismen als „appropriate for a controlled environment where attackers only have a low attack potential".

Bleibt die Frage nach der Aussagekraft dieser Evaluierung. Fakt ist, dass durch die Überprüfung die Sicherheit bestimmter Schutzmechanismen nachgewiesen wurde. Dennoch haben die Konfigurationen der evaluierten Gegenstände nicht selten wenig bis gar nichts mit einer realistischen Einsatzumgebung zu tun. Bei RHEL führt beispielsweise schon die Installation einer graphischen Benutzeroberfläche zum virtuellen Erlöschen des Gütesiegels.

Fluggastdatenaffäre

Am 28.06.2007 haben sich EU-Kommission und USA auf ein Fluggastdaten-Abkommen geeinigt – Meilenstein einer seit dem 05.03.2003 andauernden Posse. Seitdem zwingt die USA als Antiterror-Maßnahme ausländische Fluglinien unter Androhung des Entzugs der Landerechte, ihre Passagierdaten dem amerikanischen Zoll zu öffnen. Diese Praxis wurde am 09.10.2003 vom EU-Parlament wegen Verstoßes gegen EU-Datenschutzrecht gestoppt. In einer Einigung vom 16.12.2003 wurde die Zahl der zu übermittelnden Datensätze von 39 auf 34 reduziert und die Speicherdauer von sieben auf 3,5 Jahre gesenkt. Diese Einigung wurde von der EU-Kommission am 14.05.2004 bestätigt. Dagegen zog das EU-Parlament vor den Europäischen Gerichtshof – der die Einigung am 30.05.2006 als rechtswidrig kassierte.

Das Interim-Abkommen vom 16.10.2006 läuft am 31.07.2007 aus. Die Einigung vom 28.06.2007 sieht vor, dass von den 34 Datensätzen nunmehr lediglich 19 übermittelt werden. Allerdings beruht ein großer Teil der Reduktion auf der trickreichen Zusammenfassung von Datensätzen. Dafür wurde die Speicherdauer auf 15 Jahre erhöht.

Click 'n Hack Tools

Am 20.06.2007 wurde vom SANS Internet Storm Center auf das Untergrundprodukt „MPACK" hingewiesen, das für ca. 150 USD erworben werden kann. Dabei handelt es sich um eine hochspezialisierte

Software, die ungenügend gepatchte Clientsysteme mit Internet-Zugang zu Botnetzen für Clickbetrug und Pharming hinzufügt. Dazu werden Webseiten mit einer iframe-Seite präpariert, die beim Aufruf MPACK-Code nachlädt. Die Software unterstützt den Käufer unter anderem mit einer aktuellen Onlinedatenbank und wählt auf den Client zugeschnittene technische Schwachstellen aus (z. B. MS06-071, MS07-017, Buffer Overflows für WinZip, QuickTime etc.), bei Bedarf auch Phishing-Trojaner, Dialer, Backdoors oder Spamfunktionen.

Offenbar gibt es einen Markt für Malware. Damit dürfte die Motivation weiter sinken, effektiven Exploit-Code zu veröffentlichen. Ohne die Meldung gefundener Schwachstellen an die Hersteller wird sich die Bereitstellung von Patches jedoch weiter verzögern. Damit verschwände guter Angriffscode in Untergrund-Tools – „geschützt" vom neuen § 202c StGB (siehe oben).

Populäres Filecarving

Carving ist nicht nur unter Skifahrern sehr beliebt. Auch IT-Forensiker finden immer mehr Gefallen daran: Filecarving-Tools werten Header- und Footer-Informationen aus forensischen Images aus und können anschließend die entsprechenden Dateitypen extrahieren. Dies funktioniert auch dann, wenn kein „regulärer" Zugriff mehr auf die Dateien möglich ist – bspw. weil die Dateien gelöscht wurden oder die Dateizuordnungstabelle (FAT) defekt ist.

Scalpel ist ein solcher hoch-performanter Filecarver, der kostenlos ist und unter Unix/Linux, Windows (ohne Installation) sowie Mac OS X läuft. Scalpel ist eine Weiterentwicklung von Foremost und kann dd-Images direkt lesen, ohne dass diese zuvor gemountet werden müssen. Jedes Image wird dabei doppelt „durchforstet". Die Erkennungsraten sind sehr gut, so dass Scalpel auch regelmäßig von Secorvo in forensischen Analysen eingesetzt wird.

Noch einen Schritt weiter gehen Tools, die das sog. „In Place Carving" beherrschen. Tools wie CarvFS extrahieren die Dateien nicht, die in einem Image gefunden wurden: sie legen symbolische Links an, die direkt auf die entsprechende Stelle im Image verweisen. Diese Technik benötigt deutlich weniger Speicherplatz bei der forensischen Analyse, was sich im GB-Bereich positiv bemerkbar machen kann.

IIS – Bezahlpatch?

Am 05.06.2007 veröffentlichte Microsoft einen Knowledgebase-Artikel, in dem erläutert wurde, wie unter bestimmten Bedingungen die Authentifizierung von IIS 5.0/5.1 ausgehebelt werden kann. Inzwischen wurden diese Details aus dem Beitrag gestrichen; in Blogs und Diskussionsforen wird man jedoch schnell fündig. Nun ist die Veröffentlichung einer neu entdeckten Schwachstelle per se nichts Erwähnenswertes. Eigenartig ist jedoch, dass Details zur Ausnutzung der Schwachstelle fast im Stil einer Anleitung preisgegeben wurden. Und Microsoft liefert weder einen Patch, noch sind in dem Text Workarounds zu finden. Einzige Empfehlung für Betroffene: Ein kostenpflichtiges Upgrade auf IIS 6.0. Da drängt sich der Eindruck auf, dass Microsoft seine Kunden mit eigenwilliger Methode zu einem Serverversionswechsel zwingen will. Tatsächlich gibt es kostenlose Workarounds wie der Einsatz von URLScan, detailliert beschrieben im o. g. Blog.

Awareness in YouTube

Im Stil etwas überzeichnet, aber gut erläutert und inhaltlich zutreffend sensibilisiert ein knapp siebenminütiges, bereits am 15.10.2006 in YouTube veröffentlichtes Video der „American International Group" für die Bedrohung durch Externe, die sich Zugang zum Unternehmen verschaffen. Es wird gezeigt, wie leicht es sein kann, wertvolle Informationen zu gewinnen, wenn die Mitarbeiter auf Unbekannte im eigenen Unternehmen nicht angemessen reagieren. Trotz der etwas schwachen Bildqualität eine gute Ergänzung zum Secorvo-Video „Social Engineering".

Secorvo News

Secorvo College aktuell

Im September 2007 startet College nach der Sommerpause mit dem Seminar „IT-Sicherheit heute" (18.-20.09.2007) – dank reger Nachfrage mit nur noch wenigen freien Plätzen. Und auch für das nächste T.I.S.P.-Seminar (05.-10.11.2007) liegen bereits viele Anmeldungen vor – Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Sichere Software im Trend

Am 28.06.2007 präsentierten Dr. Boris Hemkemeier (Commerzbank) und Tom Schröer (SAP) auf einem Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) vor über 60 Teilnehmern „Goldene Regeln der IT-Sicherheit bei der Beauftragung und Erstellung von Software" – ein Ergebnis des Projekts Secologic (Vortragsunterlagen auf der Webseite der KA-IT-Si). Erst Mitte Juni hatte Secorvo für eine sechsköpfige Delegation von Vertretern unterschiedlicher Ministerien der indischen Regierung das Seminar „Sichere Softwareentwicklung" durchgeführt, erweitert um zwei Praxistage. Die Resonanz zeigt, dass das Thema nicht nur in Deutschland eine hohe Aufmerksamkeit genießt. Nächste Gelegenheit zum Besuch des Seminars: **13.-15.11.2007**.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2007	
03.-05.08.	Defcon 15 (Las Vegas/US)
06.-10.08.	USENIX Security Symposium (Boston/US)
19.-23.08.	Crypto 2007 (IACR, Santa Barbara/US)
28.-29.08.	XCon2007 (Beijing/CN)
September 2007	
10.-13.09.	CHES 2007 (IACR, Wien/AT)
18.-20.09.	IT-Sicherheit heute (Secorvo, Karlsruhe)
24.-26.09.	ESORICS 2007 (TU Dresden, Dresden)
Oktober 2007	
04.-05.10.	3rd European Conference on Computer Network Defense (EC2ND) (Enisa, Heraklion/GR)
09.-12.10.	Public Key Infrastrukturen (Secorvo, Karlsruhe)
16.-19.10.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo, Karlsruhe)

Fundsachen

Auszug aus www.security-finder.de

Dass die Version 2.0 des SSL-Protokolls mehrere Sicherheitsschwachstellen aufweist und man daher nur noch Versionen ab SSL 3.0 einsetzen sollte, gehört fast zum Allgemeinwissen. Doch welche Schwachstellen gibt es eigentlich? In Abschnitt 2 der Analysis of the SSL 3.0 Protocol, die ursprünglich beim USENIX Workshop on Electronic Commerce 1996 veröffentlicht wurde, wird man fündig.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

August 2007



Editorial: Digitaler Blockwart

Irren ist menschlich. Aber wenn man richtig Mist bauen will, braucht man einen Computer.
Dan Rather

Seit dem 11.07.2007 liegt der offizielle Abschlussbericht des BKA-Feldversuchs zur Foto-Fahndung vor. Von Oktober 2006 bis Januar 2007 war im Hauptbahnhof Mainz die automatische Gesichtserkennung als Fahndungshilfsmittel mit 200 Freiwilligen untersucht worden. Die Ergebnisse sind in verschiedener Hinsicht ernüchternd. Statt der erhofften 80% lag die Erkennungsrate der drei evaluierten Systeme zwischen 17% und 29%, bei im Schnitt mehr als 22.000 Passanten täglich und einer False-Acceptance-Rate (FAR) von 0,1% (23 Personen/Tag). Bei guten Lichtverhältnissen stieg die Erkennungsrate auf bis zu 60%, nachts lag sie unter 20%. Damit sind die Systeme nach Überzeugung des BKA-Präsidenten Jörg Ziercke für den polizeilichen Einsatz untauglich.

Nun übertrifft aber schon ein System, das in Stoßzeiten aus 50-100 Personen pro Minute bei Tageslicht mehr als die Hälfte von 200 Gesuchten herausfiltert, bei weitem die Erkennungsleistung menschlicher Beobachter. Und zweifellos wird die Systemleistung in den kommenden Jahren steigen: Höher auflösende Bilder, verbesserte dreidimensionale Erkennungsalgorithmen und schnellere Prozessoren werden ihren Teil dazu beitragen. Auch durch einfache Maßnahmen wie eine Aufmerksamkeit heischende Laufschrift in Kameranähe lässt sich die Erkennungsrate deutlich verbessern.

Sobald öffentliche Räume hierzulande ähnlich umfassend mit Videokameras ausgeleuchtet sind wie in London ist es nicht mehr weit bis zur „Knopfdruckfahndung“: Bilddaten eingespeist, und kurz darauf laufen die Treffer ein. Der Preis, den wir für die automatisierte Verbrecherjagd zahlen werden, wird hoch sein. Denn selbst bei einer FAR von 0,001% (im Bereich der natürlichen Ähnlichkeiten) müssten wir allein in Ballungszentren jährlich mit über 100.000 Fehlidentifikationen rechen.

Deutschland, Land der Verdächtigen.



Inhalt

Editorial: Digitaler Blockwart

Security News

CrypTool 1.4.10 erschienen

Der König ist tot ...

Sicherer Fensterln

Virtual Honeypots

Neugefasster Leitfaden

Botnetz-Bedrohung

RFIDIOt live

Secorvo News

Secorvo College aktuell

Forensische Checkliste

Bericht aus der Schlangengrube

Preiswürdig

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

CrypTool 1.4.10 erschienen

Das von der Deutschen Bank und der TH Darmstadt entwickelte freie E-Learning-Programm „Cryptool" erschien am 30.07.2007 in Version 1.4.10. Neu enthalten sind u. a. eine über 100seitige Präsentation, eine erheblich erweiterte und verbesserte Online-Hilfe, hybride Verschlüsselungsverfahren auf der Basis Elliptischer Kurven, Flash-Animationen für Enigma und AES sowie ein Dialog zur Bestimmung der Qualität eines Passworts. Das inzwischen 230seitige CrypTool-Skript wurde um aktuelle Erkenntnisse der Kryptographie ergänzt und glänzt mit verständlichen Beispielen. Die inhaltliche Dichte macht es vor allem für Leser mit Grundkenntnissen der Kryptographie zu einer Goldgrube.

Der König ist tot ...

... es lebe der König: Am 01.07.2007 wurde durch das Technical Committee JTC 1/SC 27 der ISO der ISMS-Standard ISO/IEC 17799:2005 in ISO/IEC 27002:2005 „Information technology – Security techniques – Code of practice for information security management" umbenannt. Inhaltlich blieb er dabei unverändert.

Mit der Umbenennung hat die ISO einen wichtigen Beitrag zur Bereinigung der babylonischen Namensverwirrung im Bereich der sicherheitsrelevanten Standards geleistet – nach den Standards ISO/IEC 27001:2005 und ISO/IEC 27006:2007 existiert jetzt der dritte Standard im Nummernkreis 270xx. Die Numerierung verdeutlicht die „Verwandtschaft" zu ISO 9001 (Qualitätsmanagement) und ISO 14001 (Umweltmanagement).

Sicherer Fensterln

Fast 20 Monate – genauer seit dem 27.12.2005 – im Netz, aber bisher ohne Erwähnung in den Security News: das lesenswerte und hilfreiche Microsoft TechNet-Handbuch „Bedrohungen und Gegenmaßnahmen". Es fasst in 12 Kapiteln alle wesentlichen Sicherheitseinstellungen für Windows Server 2003 und Windows XP zusammen, verlinkt auf alle in diesem Kontext wichtigen Microsoft-Dokumente und ergänzt so die beiden Sicherheitshandbücher für Windows XP und Windows 2003 Server. Die Struktur wurde an den Aufbau der Benutzeroberfläche des Gruppenrichtlinien-Editors angelehnt. Nur das englische Original ist als zusammenhängende PDF-Datei verfügbar; die deutsche Fassung ist ein 14teiliges Online-Dokument.

Virtual Honeypots

Dass das Thema Honeypots immer wichtiger wird, verdeutlichen nicht nur zahlreiche Tools (SSN 08/2005, 12/2006). Auch Veröffentlichungen auf Konferenzen und White Paper nehmen zu. Dies hat zwei deutsche Autoren zu dem im Juli 2007 erschienenen Fachbuch „Virtual Honeypots – From Botnet Tracking to Intrusion Detection" motiviert: Niels Provos und Thorsten Holz prägen seit vielen Jahren die „Honeypot-Szene" und haben nun ihre Erfahrungen dokumentiert. Heraus gekommen ist eine Publikation, die das Zeug zum Standardwerk hat: Alle aktuellen Themen rund um Honeypots/ Honeynets werden detailliert beschrieben. Dabei kommt die Praxis nicht zu kurz – die Autoren geben Installationshinweise für eine Reihe unterschiedlicher Tools und runden das Thema durch mehrere Fallstudien ab. Lance Spitzner – Gründer des Honeynet-Projekts – hält das Buch für „the best reference for honeypots today". Kaufempfehlung.

Neugefasster Leitfaden

Am 20.06.2007 wurde der Bitkom-Leitfaden zur Nutzung von E-Mail und Internet im Unternehmen in einer überarbeiteten Version 1.4 veröffentlicht. Darin werden alle im Zusammenhang mit der dienstlichen und privaten Nutzung relevanten und bei Regelungen zu berücksichtigenden gesetzlichen Bestimmungen aus dem Steuer-, Telekommunikations-, Datenschutz-, Mitbestimmungs- und Strafrecht zusammengefasst. Die neue Version berücksichtigt aktuelle Entwicklungen in der Rechtsprechung sowie die Bestimmungen des am 01.03.2007 in Kraft getretenen Telemediengesetzes (TMG), das das Teledienstegesetz (TDG), das Teledienstedatenschutzgesetz (TDDSG) sowie weitgehend auch den Mediendienste-Staatsvertrag (MdStV) abgelöst hat. Für Datenschutzbeauftragte und Betriebsräte ist die Lektüre dieses 50seitigen Leitfadens ein absolutes "Muss".

Botnetz-Bedrohung

Das seit Jahresanfang vom „Storm Worm" aufgebaute Botnetz, dessen Schädling sich zunächst als Anhang vermeintlicher Gruß-E-Mails verbreitete, ist nach Einschätzung von Joe Stewart von SecureWorks inzwischen auf 1,7 Mio. infizierte Rechner (Zombies) angewachsen. Damit wäre es das bisher größte bekannte Botnetz – konzentriert auf eine einzelne Domäne wäre gegen die Gewalt eines konzertierten Denial of Service-Angriffs (DoS) wenig auszurichten.

Mikko Hyppönen, Chefanalyst von F-Secure, hält die Meldung jedoch für Hysterie: Seiner Einschätzung nach seien bis Mitte August keine 100.000 Rechner infiziert worden, und auch ein DoS-Angriff sei nicht zu befürchten – Botnetze dieser Größe ließen sich durch Vermietung viel attraktiver vermarkten. Mit

dieser Einschätzung liegt er jedoch falsch: Etliche Wissenschaftler, die „Storm Worm" untersuchten, berichten von Denial of Service-Attacken gegen ihre Systeme.

Außerdem zeichnen sich die „Storm Worm"-Betreiber durch eine gefährliche Kreativität aus. Die jüngste Variante des Wurms tauscht den Treiber tcpip.sys gegen eine Version, die den eigentlichen Schadcode nachlädt – und ist damit nach einem Eintrag in McAfees Labs Blog offenbar sehr erfolgreich. Ferner ändern die „Betreiber" solcher Botnetze über so genannte „Fast Flux" die DNS-Einträge sehr oft – teilweise im Minutentakt – so dass die Verursacher schwerer zu finden sind. Dass ein großes Botnetz eine erhebliche Bedrohung darstellt, steht außer Frage: Nicht nur als Spam-Quelle, sondern auch für Erpresserdrohungen z. B. gegen Sportwettenanbieter wurden Botnetze in der Vergangenheit „erfolgreich" eingesetzt.

RFIDIOt live

Auf der diesjährigen Blackhat führte Adam Laurie am 02.08.2007 auf recht unterhaltsame Weise das RFID-Tool RFIDIOt vor. Mit Hilfe des Tools können Daten von RFID-Chips ausgelesen und auf neue RFID-Chips übertragen werden („rfid cloning"). Damit können Zugangskontrollsysteme auf Basis einfacher RFID-Techniken kompromittiert werden.

Auch europäische Reisepässe lassen sich, wie wir feststellen mussten, mit RFIDIOt und einem handelsüblichen RFID-Lesegerät problemlos inklusive der gespeicherten Bilder auslesen – trotz Verschlüsselung, da die verwendeten Schlüssel aus dem maschinenlesbaren Bereich des Passes entnommen werden können. Zum Schutz vor Fälschung sind die RFID-Daten digital signiert; eine Veränderung der Informationen kann also prinzipiell erkannt werden. Da aber nicht alle Länder die Zertifikate überprüfen, werden selbstsignierte Informationen nicht überall als Fälschung erkannt. Wie sagte Manfred Rommel so treffend: „Halb richtig ist meistens ganz falsch."

Secorvo News

Secorvo College aktuell

Das zweite Halbjahr beginnt für Secorvo College am 18.09.2007 mit dem Klassiker „IT-Sicherheit heute" (nur noch wenige Plätze frei). Im Oktober folgen die Seminare „Public-Key-Infrastrukturen" (09.-12.10.2007) und „Information Security Management" (16.-19.10.2007). Anfang November bietet sich die nächste Gelegenheit zur T.I.S.P.-Zertifizierung (05.-10.11.2007); es folgt das Seminar „Sichere Softwareentwicklung" (13.-15.11.2007).

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Forensische Checkliste

Die ersten Schritte nach einem Sicherheitsvorfall sind oft die entscheidenden, insbesondere dann, wenn das Ereignis im Rahmen einer forensischen Analyse im Detail untersucht werden soll. Viele Fehler werden in den ersten Minuten danach gemacht – etliche wichtige Informationen gehen unwiederbringlich verloren oder werden nicht ausreichend dokumentiert.

Um diese Informationserhebung zu erleichtern, hat Secorvo eine forensische Checkliste entwickelt, die die zu Beginn einer Analyse wichtigsten Fragen beinhaltet. Diese Checkliste hilft bei jedem wichtigen Sicherheitsvorfall – unabhängig davon, ob die anschließende Untersuchung selbst oder mit externer Unterstützung durchgeführt werden soll.

Bericht aus der Schlangengrube

Es war einmal – vor 20 Jahren: Der erste PC-Virus erblickt das Licht der Welt; er verbreitet sich über Disketten (wissen Sie noch, was das ist?). Vor 10 Jahren: Macro-Viren kommen auf, die sich in Word-Dokumenten via E-Mail verbreiten; 3-5 neue Varianten am Tag. Paradiesische Zustände. Denn 2007 sind es 16.000 neue Schädlinge pro Jahr, durchschnittlich 45 an jedem Kalendertag, weltweit verbreitet innerhalb von Sekunden über Botnetze.

Wie werden sie gefunden? Wie identifiziert? Was bedeutet diese Entwicklung für den Alltag im Viren-Labor? Und was droht für die kommenden 10 Jahre? Ein Live-Bericht über das Leben in der Schlangengrube von Angel Jodra, Virenanalyst bei Kaspersky Labs, auf dem kommenden Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 27.09.2007, 18 Uhr (Schlosshotel Karlsruhe). Online-Anmeldung erforderlich.

Preiswürdig

Am 14.09.2007 wird der in diesem Jahr erstmals ausgelobte „Sicherheitspreis Baden-Württemberg 2007" im Rahmen der Fachmesse SafeKon von Innenminister Heribert Rech verliehen. Prämiert werden „herausragende Projekte der betrieblichen Sicherheit mit Zielsetzung Know-how-Schutz" und „mustergültige Projekte zur praxisgerechten Konzeption, Realisierung und Kontrolle unternehmensinterner Sicherheitsmaßnahmen".

So viel dürfen wir bereits verraten: Zu den vier Projekten, die diese in Deutschland einmalige Auszeichnung erhalten, zählt die von Secorvo unterstützte Security-Awareness-Kampagne der T-Systems Enterprise Services GmbH. Mehr in den September-News...

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2007	
10.-13.09.	CHES 2007 (IACR, Wien/AT)
11.-13.09.	3rd International Conference on IT-Incident Management & IT-Forensics (GI, Stuttgart)
18.-20.09.	IT-Sicherheit heute (Secorvo, Karlsruhe)
24.-26.09.	ESORICS 2007 (TU Dresden, Dresden)
27.09.	Leben in der Schlangengrube (KA-IT-Si, Karlsruhe)
Oktober 2007	
09.-12.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.10.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo, Karlsruhe)
November 2007	
05.-09.11.	T.I.S.P. Schulung (Secorvo, Karlsruhe)
13.-15.11.	Sichere Software-Entwicklung (Secorvo, Karlsruhe)

Fundsache

Auszug aus www.security-finder.de

Das lesenswerte White-Paper „Exploiting SAP Internals – a Security Analysis of the RFC Interface Implementation“ von Mariano Nunez Di Croce vom 08.03.2007 beschreibt zahlreiche Sicherheitslücken der RFC (Remote Function Call) Schnittstelle innerhalb von SAP und zeigt Gegenmaßnahmen auf. Die Ergebnisse wurden auch auf der Black Hat Europe 2007 präsentiert (siehe auch SSN 05/2007).

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

September 2007



Editorial: Über die rote Ampel

Seit nunmehr 30 Jahren soll das deutsche Datenschutzrecht den Einzelnen „unter den Bedingungen der modernen Datenverarbeitung“ vor „unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten“ schützen. So gewährleistet das allgemeine Persönlichkeitsrecht des Art. 2 Grundgesetz „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf ‚informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig.“ (BverfGE 65, „Volkszählungsurteil“ vom 15.12.1983)

Zwar wurde der Datenschutz im Jahr 2000 als Art. 8 in die Charta der Grundrechte der EU aufgenommen. Seit 1983 haben sich aber die „Bedingungen der modernen Datenverarbeitung“ erheblich verändert. Und erweiterte Befugnisse von Staatsorganen der Inneren Sicherheit kratzen an der Substanz dieses Grundrechts.

Am schlimmsten aber ist das herrschende Vollzugsdefizit, das auf einen verbreiteten Mangel an Respekt vor der Individualität und Persönlichkeit anderer Menschen schließen lässt. In zahlreichen Unternehmen ist die Neigung zu beobachten, unzweideutige Bestimmungen des Bundesdatenschutzgesetzes sophistisch zu verbiegen – oft mit Duldung oder gar Unterstützung der Rechtsabteilung. Da werden hemmungslos Personaldaten an amerikanische Mutterkonzerne übermittelt, Whistleblowing-Systeme ohne Rücksicht auf die Persönlichkeitsrechte anonym Verdächtigter installiert oder versteckte Videoüberwachungsanlagen eingerichtet und ohne Benachrichtigung Betroffener ausgewertet.

Diese Verstöße gegen geltendes Recht zeugen von derselben Respektlosigkeit vor der Unversehrtheit anderer Menschen, wie ein Autofahrer, der unter Inkaufnahme der Gefährdung Dritter eine Ampel bei Rot passiert. Schade nur, dass sich Datenschutzvergehen in der Regel weder „blitzen“ noch durch den Entzug einer „Verarbeitungserlaubnis“ ahnden lassen.



Inhalt

Editorial: Über die rote Ampel

Security News

Security Leck in VMware

Passworte in Tor

OWASP German Chapter

Germany versus Freeworld

Kryptologen als Autoknacker

Herausforderung Gütesiegel

Neues Sicherheitszertifikat

Sichere Software bei eco

Secorvo News

Secorvo College aktuell

Sicherheitspreis

Weitere KA-IT-Si-Events

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Security Leck in VMware

Mit dem Einsatz von Virtualisierungslösungen sind auch neue Risiken verbunden, wie beispielsweise eine am 30.07.2007 veröffentlichte Schwachstelle in VMware Workstation 6.0.0 zeigt: die mitgelieferte Library vielib.dll erlaubt es, neue Prozesse zu starten. Nach unseren eigenen Tests ist auch die Version 5.5 betroffen. Behoben wurde das Leck in der am 18.09.2007 veröffentlichten Version 6.0.1 – ein Update empfehlen wir dringend.

Zwar bietet die Virtualisierung von Server-Systemen und Test-Clients aus Sicherheitssicht einige wesentliche Vorteile, sie ist jedoch kein Allheilmittel. So werden einige Risiken nur verlagert, andere Risiken beeinflusst die Virtualisierung überhaupt nicht. Am 25.09.2007 wird Stefan Gora das Für- und Wider auf dem IT-Virtualisierungsforum 2007 vorstellen.

Passworte in Tor

Am 30.08.2007 veröffentlichte Dan Egerstad 100 E-Mail-Passwörter von Botschafts- und Regierungsangehörigen so unterschiedlicher Länder wie Iran, Usbekistan und Japan. Am 10.09.2007 enthüllte er, wie er an diese Passwörter gelangt war: Er hatte einen „Exitknoten" für das Anonymisierungsnetzwerk Tor installiert und betrieben (was man auch den Geheimdiensten von USA und China sowie kriminellen Organisationen nachsagt).

Über diesen Server konnte er Verbindungen von Tor-Nutzern weltweit beim Ausgang aus dem Tor-Netzwerk mitlesen. Denn Tor schützt zwar die Anonymität von Web-Nutzern auf TCP/IP-Ebene (und das nach heutiger Kenntnis wirksam), sorgt aber nur innerhalb des Netzwerks für Vertraulichkeit – die Verbindung bis zum Exitknoten muss man zusätzlich z.B. per TLS verschlüsseln.

Nicht auszuschließen ist allerdings, dass nicht alle betroffenen Tor-Verbindungen von Regierungsangehörigen stammten: möglicherweise waren einige Passworte längst kompromittiert, und die Angreifer nutzten Tor zur Verschleierung ihrer Spuren.

OWASP German Chapter

Am 07.09.2007 trafen sich 16 Sicherheitsexperten in Frankfurt zum Relaunch des German Chapter des Open Web Application Security Project (OWASP). Bei dieser konstituierenden Sitzung wurden die verschiedenen Erwartungen an einen deutschen Ableger diskutiert sowie die ersten Projekte mit lokalem Fokus initiiert. Interessierte sind herzlich eingeladen, sich an der Arbeit des OWASP durch Anregungen zu beteiligen (Kontakt: owasp@secorvo.de).

Germany versus Freeworld

Am 10.08.2007 wurde im Bundesgesetzblatt das Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) veröffentlicht. Der umstrittene „Hackerparagraph" §202c ist damit geltendes Recht. Jetzt erfüllen sich unsere Befürchtungen (siehe SSN 7/07): Am Tag der Veröffentlichung hat der PHP-Sicherheitsexperte Stefan Esser alle „Proof of Concept"-Exploits, die im Rahmen des Month of PHP Bugs entwickelt wurden, von seiner Webseite entfernt. Und The Hackers's Choice (THC) hat seine Aktivitäten in Deutschland eingestellt: So gibt es bei THC jetzt zwei verschiedene Webseiten: germany.thc.org und freeworld.thc.org.

Offen ist derzeit, wie die Justiz den Paragraphen in der Praxis auslegen wird. Um in diesem Punkt Rechtssicherheit zu gewinnen, hat das IT-Magzin tecchannel.de am 14.09.2007 angesichts der Verbreitung des Hacker-Tools „John the Ripper" auf der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) verbreiteten BOSS-CD Strafanzeige gegen Unbekannt wegen des Verdachts des Verstoßes gegen §202c StGB erstattet.

Kryptologen als Autoknacker

Wenn es in der Kryptologie unumstößliche Erkenntnisse gibt, dann sind dies das Kerckhoffsche Prinzip und das Mooresche Gesetz. Ersteres fordert, dass die Sicherheit eines Algorithmus nie von dessen Geheimhaltung, sondern nur von einem Schlüssel abhängen darf, letzteres, dass die Sicherheit der Schlüssellänge – dank Verdoppelung der Rechenleistung alle zwei Jahre – ständig sinkt. Aus diesem Grund aktualisiert die BNetzA jährlich den Algorithmenkatalog zum Signaturgesetz in Abstimmung mit dem BSI und zahlreichen Experten.

Dies dürfte nun auch der Hersteller gelernt haben, der das vor etwa 20 Jahren entworfene KeeLoq Verfahren in Wegfahrsperren-Chips für Autoschlüssel einsetzt. Als der geheim gehaltene Algorithmus 2006 publik wurde, begannen Kryptologen, aktuelle Analysemethoden darauf anzuwenden.

Am 21.08.2007 präsentierte eine Forschergruppe – darunter zwei Schwergewichte der Szene – auf der Rump Session der Crypto 2007 eine Methode, um binnen 48 Stunden einen Wegfahrsperrenschlüssel zu duplizieren. Erforderlich sind dafür 50 Dual-Core PCs und ca. 65 Minuten RFID-Kontakt zum Autoschlüssel des Fahrers, beispielsweise mit einem präparierten Stuhl im Wartezimmer. Schlimmer noch: Stimmt die vermutete Schlüsselableitung, sind so gleich die Wegfahrsperren der ganzen Fahrzeugserie gebrochen.

secorvo
security consulting

Herausforderung Gütesiegel

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) ist um seine selbst gewählte Herausforderung nicht zu beneiden: Wie überzeugt man die Menschheit von einem Datenschutz-Gütesiegel, wenn man nur für Behörden des Landes Schleswig-Holstein zuständig ist?

Da die bereits 2001 im BMI-Gutachten „Modernisierung des Datenschutzrechts" geforderte gesetzliche Produktzertifizierung auf sich warten lässt, hat das ULD nun Europa für das Gütesiegel begeistert: Im Projekt European Privacy Seal (EuroPriSe) werden ab November 2007 unter der Leitung des ULD europäische Pilot-Zertifizierungen durchgeführt.

Aber ein Gütesiegel braucht auch prominente Träger. Mit der Verleihung an Microsofts Update Service landete das ULD im Februar 2007 einen Medien-Coup (siehe SSN 3/07). Das damit betretene Eis ist aber dünn: Dies wurde bei der Verleihung des Gütesiegels für den Lizenzprüfdienst WGA von Windows XP am 03.09.2007 deutlich. Der Schutz der personenbezogenen Daten stützt sich teilweise (bei Fälschungsverdacht) auf rein organisatorische Maßnahmen bei Microsoft – eine Maßnahme, die weder für den Betroffenen nachvollziehbar (nur ein Kurzgutachten ist öffentlich) noch kontrollierbar ist. Auch ist wie bei Sicherheitszertifikaten die Zertifizierung von Teildiensten inhaltlich zumindest fragwürdig, denn das „pars pro toto"-Denken beim Verbraucher kann nicht verhindert werden. Dass hier nicht Microsoft oder Windows ein Datenschutzgütesiegel erhalten haben, sondern ein winziger Dienst des Betriebssystems XP, wird so differenziert nur von einer Minderheit wahrgenommen. Dies könnte mittelfristig das Vertrauen in das Gütesiegel selbst gefährden.

Neues Sicherheitszertifikat

Das International Software Quality Institute (iSQI) hat gemeinsam mit u.a. SAP, Secunet, Virtual Forge und Secorvo die Entwicklung eines Zertifizierungsstandards für Softwareentwickler („Certified Professional for Secure Software Engineering") initiiert. Secorvo wird seine Erfahrungen mit dem Seminar „Sichere Softwareentwicklung„ in dieses Zertifikat einbringen.

Sichere Software bei eco

Wer die gut besuchte Veranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zu sicherer Software-Entwicklung am 28.06.2007 verpasst hat, dem sei die Sitzung des Arbeitskreises Sicherheit des eco – Verband der deutschen Internetwirtschaft e.V. am 26.09.2007 in Frankfurt ans Herz gelegt. Die Teilnahme ist kostenlos, eine Online-Anmeldung erforderlich.

Secorvo News

Secorvo College aktuell

In das vierte Quartal startet Secorvo College mit vollem Programm und vollen Seminaren – noch wenige Plätze gibt es für das PKI-Seminar am **09.-12.10.2007**, das Seminar Information Security Management am **16.-19.10.2007** und die T.I.S.P.-Schulung am **05.-09.11.2007**.

Auch die Seminare Sichere Software-Entwicklung am **13.-15.11.2007** und IT-Sicherheitsaudits in der Praxis am **04.-06.12.2007** füllen sich bereits.

Programme und Online-Anmeldung unter
http://www.secorvo.de/college

Sicherheitspreis

Am 14.09.2007 wurde im Rahmen der Security-Fachmesse Safekon in Karlsruhe die Security Awareness-Kampagne „Mission Security" der T-Systems Enterprise Services GmbH, die von Secorvo und der Agentur Südpol konzipiert und unterstützt wurde, als eines von vier beispielhaften Projekten zum Schutz vor Wirtschaftsspionage und Konkurrenzausspähung von Innenminister Heribert Rech mit dem erstmals verliehenen „Sicherheitspreis Baden-Württemberg" ausgezeichnet (zweiter Preis).

Der Innenminister lobte in seiner Laudatio das „psychologisch einfühlsam aufbereitete Konzept" der Kampagne, in der der fiktive Mitarbeiter James Bit als Leitfigur und Vorbild diente (Motto: „Mir ist es nicht egal!").

Weitere KA-IT-Si-Events

Angesichts der großen und wachsenden Resonanz, der sich die Events der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) erfreuen, sind für 2007 noch drei Veranstaltungen geplant. Zwei Termine sollten Sie sich bereits vormerken:

- **Leben in der Schlangengrube**
  Am 27.09.2007 gewährt Angel Jodra (Kaspersky Labs) einen Einblick in die zu erwartende Entwicklung der Bedrohung durch Viren, Trojaner und andere Malware (Anmeldung).

- **Wer wird FIDUCIA Security Champ?**
  Am 18.10.2007 ist die FIDUCIA IT AG Gastgeber der KA-IT-Si und wird ihre mit dem Sicherheitspreis Baden-Württemberg 2007 (2. Preis) ausgezeichnete Security-Awareness-Kampagne vorstellen. Das sollten Sie nicht verpassen ...

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2007	
25.-27.09.	ISSE 2007 (TeleTrusT et al., Warsaw/PL)
26.09.	Sichere Softwareentwicklung (eco AK Sicherheit, Frankfurt)
27.09.	Leben in der Schlangengrube (KA-IT-Si, Karlsruhe)
Oktober 2007	
04.-05.10.	3rd European Conference on Computer Network Defense (FORTH-ICS & ENISA, Heraklion/GR)
09.10.	Verdeckte Online-Durchsuchung (a-i3, Bochum)
09.-12.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.10.	Information Security Management – von A(udit) bis Z(ertifizierung) (Secorvo, Karlsruhe)
18.10.	Wer wird FIDUCIA Security Champ? (KA-IT-Si, Karlsruhe)
November 2007	
05.-09.11.	T.I.S.P. Schulung (Secorvo, Karlsruhe)
13.-15.11.	Sichere Software-Entwicklung (Secorvo, Karlsruhe)

Fundsache

Auf den Punkt gebracht werden zahlreiche Sicherheitsthemen auf der Cartoon-Seite SecurityCartoon.com. Eine thematische Gliederung erleichtert die Recherche. Deren nichtkommerzielle Nutzung – z. B. zur gestalterischen Aufwertung einer Security-Intranet-Seite – ist mit Quellenangabe zugelassen.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting, Karin Schuler

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Oktober 2007



Editorial: Angehört

Ein Erlebnis der besonderen Art war die Anhörung des Bundesverfassungsgerichts zur „Online-Durchsuchung“ am 10.10.2007. Mit beeindruckender Konzentration folgte der erste Senat vor vollen Besucherbänken der Erörterung wichtiger Fragen, die für die Bewertung der Verfassungsmäßigkeit einer Online-Durchsuchung eine Rolle spielen dürften. Diskutiert wurden u. a. die Eingriffstiefe von Online-Durchsuchung und „Quellen-Telekommunikationsüberwachung“ sowie die Frage, ob sich beides technisch unterscheiden lässt. Kritisch beleuchtet wurde auch, ob eine Online-Durchsuchung zielgerichtet möglich ist: Wie kann sicher gestellt werden, dass das „richtige“ System durchsucht wird? Entlarvend die Antwort eines BKA-Vertreters: Das wisse er erst, „wenn die Daten zu ihm sprechen“.

Die Stellungnahmen der fünf geladenen sachkundigen Auskunftspersonen Bogk (CCC), Fox (Secorvo), Prof. Freiling (Uni Mannheim), Prof. Pfitzmann (TU Dresden) und Prof. Sieber (MPI Freiburg) sind inzwischen online verfügbar.

Deutlich wurde, dass das NRW-Gesetz kippen wird – schon aufgrund der mangelnden Normenklarheit. Nach den Ausführungen des Bevollmächtigten der NRW-Landesregierung, Prof. Heckmann, fragte Verfassungsgerichtspräsident Prof. Papier dezent süffisant: „Sprechen wir über dasselbe Gesetz?“. Auf die Erwiderung Heckmanns, das Gesetz sei „auslegungsfähig“, konterte Papier, die Auslegung sei „ansprechend“, das Gericht habe jedoch „nicht die Auslegung eines Prozessbevollmächtigten zu beurteilen, sondern den Wortlaut des Gesetzes.“ Das für 2008 erwartete Urteil dürfte wegweisend ausfallen – vergleichbar dem "Volkszählungsurteil" von 1983, das die "Informationelle Selbstbestimmung" prägte. Möglicherweise wird das BVerfG den Schutz des Kernbereichs privater Lebensgestaltung neu definieren, und zweifellos wird eine Online-Überwachung an hohe Hürden geknüpft, mindestens an die einer G10-Ermächtigung.

Solange wir solche Verfassungsrichter haben, können stümperhafte Gesetzgeber zum Glück nur begrenzten Schaden anrichten.



Inhalt

Editorial: Angehört

Security News

Last Orders, please!

Risiko Kreditkarte

SQL-Nahkämpfer

Material zum Bundestrojaner

BBA 2007

Nichts zu verbergen

iPhone out of Jail

Secorvo News

Secorvo College aktuell

Spionage für Anfänger

Virtuelle IT-Sicherheit

Wie dick ist Ihr Bunker?

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Last Orders, please!

Am 01.11.2007 beginnen die deutschen Einwohnermeldeämter mit der Erfassung von Fingerabdrücken für den neuen Reisepass („ePass"). Allen Sicherheitsbedenken zum Trotz werden jedem Antragsteller zwei Fingerabdrücke abgenommen, die als weiteres biometrisches Merkmal – zusätzlich zu dem bereits 2005 eingeführten digitalen Passbild – auf einem im Pass befindlichen RFID-Chip gespeichert werden.

Dabei hat sich offenbar bei den Behörden noch nicht herumgesprochen, dass das Auslesen der RFID-Chips geradezu trivial ist (siehe SSN 08/2007): sogar das Bundesinnenministerium behauptet auf seinen Informationsseiten: „*Schon die elektronischen Pässe der ersten Generation sind durch einen wirkungsvollen Mechanismus gegen unberechtigtes Auslesen geschützt.*" Vertrauensbildung sieht anders aus. Wer schnell handelt, sichert sich noch eine zehnjährige Karenzzeit.

Risiko Kreditkarte

Am 04.10.2007 hat der amerikanische Großhändlerverband NRF die Kreditkartenorganisationen aufgefordert, auf die Verpflichtung zur Speicherung der vollständigen Kreditkartendaten beim Händler gemäß den Best-Practice-Vorgaben des Payment Card Industry Security Standards Council zu verzichten. Danach müssen die Daten 12 bis 18 Monate für laufende Abfragen bereit gehalten werden.

Auch wenn das nicht das einzige Motiv der NRF sein dürfte, verringert die Reduktion sensibler Daten zweifellos die Gefahr unerwünschten Datenabflusses. Just an eben diesem 04.10.2007 waren dem Eintrittskarten-Shop Kartenhaus.de Kreditkartendaten von ca. 66.000 Kunden der vergangenen 12 Monate gestohlen worden.

Vorfälle dieser Art täuschen jedoch darüber hinweg, dass Kreditkartenbetrug in der Regel „klassisch" erfolgt: Angeblich finden 70% aller Kreditkartenbetrügereien der USA in Restaurants statt. Selbst wenn die Kreditkarte nicht vom Personal mitgenommen wird, ist es mit geeigneten Lesegeräten trivial, den Magnetstreifen unbemerkt am Tisch auszulesen – und die Karte später zu „klonen".

SQL-Nahkämpfer

Am 08.10.2007 wurde Version 0.2.1 des SQL-Angriffswerkzeugs SQLNinja veröffentlicht. Das auf Microsofts SQL-Server spezialisierte Open-Source-Tool versucht, bekannte SQL-Schwachstellen auszunutzen und kann bei Penetrationstests zur Analyse von Webapplikationen eingesetzt werden.

Die Angriffsoptionen reichen von der Informationsbeschaffung bis zur Durchführung von Bruteforce-Attacken auf Datenbank-Accounts. Im „besten" Fall startet SQLNinja eine remote shell auf dem betroffenen System. Im Mai 2007 wurde es in die Top 15-Liste der kostenfreien SQL Injection Scanner aufgenommen.

Material zum Bundestrojaner

In den vergangenen Wochen wurden einige erhellende Dokumente zum Thema „Online-Durchsuchung" veröffentlicht, allen voran zwei Stellungnahmen des BMI vom 22.08.2007 zu einem Fragenkatalog des BMJ und einem Fragenkatalog der SPD-Bundestagsfraktion. Eine gute Übersicht enthält auch der in HRRS erschienene Beitrag von Ulf Buermeyer. Nach Überzeugung von Prof. Hartmut Pohl (Beitrag in DuD 9/2007) wurden vom Bundesnachrichtendienst Online-Durchsuchungen unter Verwendung von „Less-Than-Zero-Day-Exploits" durchgeführt – unabhängig von dem dafür erforderlichen Aufwand ein gefährlicher Ansatz, wird durch die Geheimhaltung von Sicherheitslücken doch zugleich der Zeitraum verlängert, in dem Systeme von Unternehmen, Behörden und Bundesbürgern angreifbar sind.

Inzwischen sind auch die Stellungnahmen der fünf vom Bundesverfassungsgericht befragten und zur Anhörung am 10.10.2007 geladenen sachkundigen Auskunftspersonen Bogk (CCC), Fox (Secorvo), Prof. Freiling (Uni Mannheim), Prof. Pfitzmann (TU Dresden) und Prof. Sieber (MPI Freiburg) online.

BBA 2007

In Deutschland erstmals im Jahr 2000 ausgelobt wurden sie am 12.10.2007 zum achten Mal verliehen: die „Big Brother Awards", unerwünschte Auszeichnungen für Datenkraken. Erstmals überstieg die Zahl der Nominierungen die Marke 500, so dass die Jury in diesem Jahr zahlreiche Auswahlrunden zu bewältigen hatte, ehe die endgültigen acht Preisträger fest standen.

In der Kategorie „Arbeitswelt" siegte die Novartis Pharma GmbH mit der Bespitzelung des eigenen Außendienstes, der Öffnung von Betriebsratspost und der Missachtung der Vertraulichkeit von Mitarbeiterumfrageergebnissen. Die internationalen Hotelketten in Deutschland – stellvertretend Hyatt, Marriott und Intercontinental – errangen den Award in der Kategorie „Verbraucherschutz" für die heimliche Erfassung und Speicherung von Gastdaten (Trink- und Essgewohnheiten, Pay-TV-Nutzung, Allergien, Kontaktadressen, Kreditkartendaten, Sonderwünsche und Beschwerden) sowie deren rechtswidrige Übermittlung in die USA.

In der Kategorie „Politik“ setzte sich Bundesfinanzminister Peer Steinbrück mit seiner lebenslangen „Steuer-ID“ durch.

Für die hochwirksame Schärfung des Datenschutzbewusstseins in der Öffentlichkeit (mittels zahlloser Vorschläge zur Einschränkung von Freiheitsrechten zu Gunsten wirksamerer Terrorismusbekämpfung) wurde Bundesinnenminister Wolfgang Schäuble die Ehrenmitgliedschaft in der Deutschen Vereinigung für Datenschutz (DVD) angetragen.

Nichts zu verbergen

Was ist Privatsphäre, warum ist diese schützenswert, und ist es so, dass wir wirklich nichts zu verbergen haben? Mit diesen Fragestellungen beschäftigt sich das am 12.07.2007 veröffentlichte Essay 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy von Professor Daniel J. Solove. In dem 25-seitigen Papier entkräftet der Autor anhand grundsätzlicher Überlegungen und zahlreichen Beispielen die verbreitete, undifferenzierte „Ich-habe-nichts-zu-verbergen“-Haltung sowie die simplifizierende Gegenüberstellung von Sicherheitsinteressen und dem Schutz von Privatsphäre.

iPhone out of Jail

Seit dem 08.10.2007 können Besitzer infizierter iPhones wieder die alleinige Kontrolle über ihr Eigentum zurück erlangen. Die Portierung eines seit 2006 bekannten Buffer Overflows der TIFF library (libtiff), der – im Kontext des Browsers Mobile Safari erfolgreich ausgeführt – Root-Berechtigungskontext gewährt, bedrohte iPhones bis Version 1.02.

Die Gefährdung mobiler Geräte durch eben diesen Bug wurde bereits Anfang 2006 an Sonys Playstation demonstriert. Bedenklich, dass ein führender Hersteller sein mobiles Äpfelchen nicht besser vor der Root-Fäule schützt – fachkundige, lesbare Impfanleitungen für gesundes Obst gibt es mindestens seit 2002 von Forschern wie Steven M. Bellovin.

Sollte die Sicherheit von Embedded Systems nicht bald ebenso ernst genommen werden wie die Sicherheit von Servern und Arbeitsplatzrechnern, werden in den SSN demnächst wohl Hersteller von intelligenten IP-Kühlschränken gegen Navigationssysteme antreten.

Secorvo News

Secorvo College aktuell

Drei Weiterbildungsgelegenheiten bietet Secorvo College noch in 2007: die T.I.S.P.-Schulung am **05.–09.11.2007** (mit anschließender Prüfung) sowie die Seminare Sichere Softwareentwicklung (**13.–15.11.2007**) und IT-Sicherheitsaudits in der Praxis (**04.–06.12.2007**). Weitere Seminare und Termine finden sich im druckfrischen Jahresprogramm 2008.

Alle Termine, Programme und Online-Anmeldung unter http://www.secorvo.de/college

Spionage für Anfänger

Auf Einladung der Firma Vollack und der „badischen Wirtschaftswoche“, dem Magazin econo, gewährt Secorvo am 15.11.2007 ab 18:30 Uhr in der Vollack Culturwerkstatt (Karlsruhe, Fettweisstraße 42) einen Einblick in Techniken der Wirtschaftsspionage – und zeigt an Beispielen die Bedeutung von IT-Sicherheit für den Mittelstand auf; typische Bedrohungen werden live demonstriert. Im Anschluss gibt es Gelegenheit zur Diskussion am Buffet. Eintritt 30 Euro, Anmeldung bis 08.11.2007 an Frau Cornelia Braun, cbraun@vollack.de (0721/4768126).

Virtuelle IT-Sicherheit

Virtualisierungslösungen besitzen aus der Perspektive der IT-Sicherheit zahlreiche Vor-, aber auch einige Nachteile. Stefan Gora stellte auf dem Forum IT-Virtualisierung 2007 im September die wichtigsten Aspekte gegenüber. Zum selben Thema wird er auf dem Forum IT-Revision am 06.-07.11.2007 vortragen.

Wie dick ist Ihr Bunker?

So aktiv war die Karlsruher IT-Sicherheitsinitiative noch nie: Fünf Events zu spannenden Themen in 2007 mit mehreren hundert Teilnehmern – und ein sechstes Event in Vorbereitung: Unter der Leitfrage „Wie dick ist Ihr Bunker?“ werden am 22.11.2007 (18 Uhr) die physischen Gefährdungen von Rechenzentren und die damit verbundenen Haftungsrisiken diskutiert.

Die Unternehmen Lampertz und Rittal werden zusammen mit Professor Bartsch von der Kanzlei Bartsch und Partner die besonderen Herausforderungen des Rechenzentrumsbetriebs aus technischer und rechtlicher Perspektive beleuchten. Anschließend gibt es Gelegenheit zum Networking am Buffet (bitte um Anmeldung bis 20.11.2007).

Die Vortragsunterlagen des KA-IT-Si-Events „Trau, schau, wem“ am 18.10.2007 bei der FIDUCIA IT AG, auf dem die mit dem Sicherheitspreis Baden-Württemberg 2007 ausgezeichneten Security Awareness Kampagnen der FIDUCIA IT AG und der T-Systems Enterprise Services GmbH präsentiert wurden, sind inzwischen vom Server der KA-IT-Si abrufbar.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2007	
23.-26.10.	4. Black Hat Japan Briefings & Training 2007 (Tokyo)
November 2007	
05.-09.11.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
06.-07.11.	Forum IT-Revision (IIR, Frankfurt)
09.11.	Security Symposium (TelekomForum, Hamburg)
13.-15.11.	Sichere Softwareentwicklung (Secorvo College, Karlsruhe)
15.11.	Wirtschaftsspionage für Anfänger (Vollack Culturwerkstatt, Karlsruhe)
15.-16.11.	1. T.I.S.P.-Community-Workshop (TeleTrusT/Secorvo College, Karlsruhe)
22.11.	Wie dick ist Ihr Bunker? (KA-IT-Si, Karlsruhe)
Dezember 2007	
04.-06.12.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)

Fundsache

Das am 17.09.2007 publizierte 35seitige SAP-Whitepaper SSO mit Windows und SAP stellt die unterschiedlichen Authentifizierungsverfahren von Microsoft (IIS, .NET, MOSS, WCF) und SAP NetWeaver (SAP GUI, ICM, PAS, JAAS), die Kopplungsmöglichkeiten mit externen Verfahren (LDAP) sowie die unterschiedlichen Mechanismen – von ID/Passwort bis zum Client-Zertifikat – vor. Dabei werden unterschiedliche Szenarien für die gegenseitige Nutzung der Mechanismen – von Windows zu SAP ebenso wie von SAP-Applikationen zu Windows-Services – präsentiert.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting, Karin Schuler

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

November 2007



Editorial: Quod licet Jovi...

Der Streit um die datenschutzrechtliche Zulässigkeit der Speicherung von Zugriffsdaten auf Web-Angebote fußt auf der Kernfrage, ob es sich bei IP-Adressen um personenbezogene Daten handelt. Dazu liegt inzwischen ein einschlägiges Urteil vor: Das Landgericht Berlin hat am 23.11. 2006 festgestellt, dass IP-Adressen auch dann als personenbeziehbar (und damit als personenbezogene Daten) gelten, wenn zwar nicht die speichernde Stelle, wohl aber ein Dritter den Personenbezug herstellen kann. Die Konsequenz ist klar: Ohne Einwilligung der Betroffenen ist damit jede Speicherung unzulässig, die für den Betrieb des Web-Angebots nicht erforderlich ist. Auf dieser Grundlage untersagte das Landgericht Berlin am 27.03.2007 dem Bundesjustizministerium (sic!) die Speicherung von Zugriffsdaten über das Ende des Nutzungszeitraums hinaus, da dies das Persönlichkeitsrecht der Betroffenen verletze.

In der Antwort der Bundesregierung vom 30.10. 2007 auf eine kleine Anfrage von FDP-Bundestagsabgeordneten und einer Antwort vom 07.11.2007 auf eine Anfrage der Linksfraktion wurde nun bekannt, dass das Bundeskriminalamt (BKA) seit Juli 2001 die IP-Adressen von Besuchern der BKA-Webseite „Militante Gruppen“ nicht nur registriert, sondern bei „signifikanter Zugriffsfrequenz“ eine „Anschlussinhaberfeststellung über den Provider gemäß § 100g StPO“ vornimmt.

Bemerkenswert ist daran die datenschutzrechtliche Position der Bundesregierung: Eine „Aussage zur Gesamtmenge der überprüften IP-Adressen“ sei nicht möglich, da datenschutzkonform gelöscht werde; eine Information der Betroffenen erfolge nicht. Und: „Inwieweit IP-Adressen personenbezogene Daten darstellen, ist nicht abschließend geklärt.“ Da möchte man der Bundesregierung doch die Lektüre der Entscheidung des BVerfG vom 23.10.1952 zum SRP-Verbot ans Herz legen: „Zu den grundlegenden Prinzipien dieser Ordnung sind mindestens zu rechnen: die Achtung (...) vor allem vor dem Recht der Persönlichkeit auf Leben und freie Entfaltung, (...) die Gesetzmäßigkeit der Verwaltung (...).“ Schön wär's.



Inhalt

Editorial: Quod licet Jovi...

Security News

GSM-Hacking

ISF Good Practice

SANS Top 20

Denial of Car Service

Vorratsdatenspeicherung

Leitfaden IT-Sicherheit

Anstieg der IuK-Straftaten

Tag des Informationsrechts

T.I.S.P.-Boom

Secorvo News

Secorvo College aktuell

“Wie dick ist Ihr Bunker?”

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

GSM-Hacking

Auf dem diesjährigen Chaos Communication Camp in Berlin präsentierten David Hulton und Joshua Lackey am 10.08.2007 Angriffe auf GSM-Verbindungen. Sie stellten einen „GSM Traffic Sniffer" und eine Implementierung des Cyphertext Only Angriffs (siehe SSN 09/2003) von Eli Biham, einem der weltweit führenden Kryptologen vom Israel Institute of Technology in Haifa, auf den Verschlüsselungsalgorithmus A5 vor, mit der sie kürzeste SMS- oder Telefonie-Verbindungen innerhalb von 3-5 Minuten mit einem handelsüblichen PC entschlüsseln können. Der Vortrag ist als einstündiger Film abrufbar; auch gibt es umfangreiche Hintergrundinformationen zum A5 Cracking Projekt wie die Original-Veröffentlichungen aller Angriffe, sehr viele Beispielprogramme und einen Überblick über die weltweite Nutzung des A5 in GSM-Netzen.

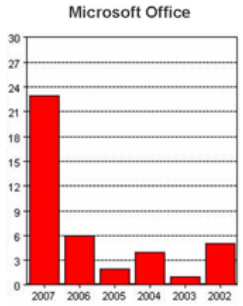
Damit hat der von den meisten GSM-Netzbetreibern genutzte Verschlüsselungsalgorithmus A5 ein unrühmliches Ende gefunden. Immerhin: Nun gibt es einen prominenten weiteren Beleg dafür, dass die Nutzung proprietärer und geheim gehaltener Verschlüsselungsverfahren in der Regel der Anfang vom Ende der Vertraulichkeit ist. Bleibt zu hoffen, dass die Lehre ankommt.

ISF Good Practice

Am 16.10.2007 veröffentlichte das Information Security Forum (ISF) eine neue Version des "Standard of Good Practice for Information Security". Die 372 Seiten umfassende Neufassung wurde an die jüngsten Standards in der Informationssicherheit wie ISO/IEC 27002:2007 und COBIT v4.1 angepasst. Da auch aktuelle Entwicklungen wie Virtualisierung und EuroSOX, die in den Unternehmen derzeit eine große Rolle spielen, berücksichtigt wurden, hilft das Dokument, den derzeitigen Stand der „Best Practice" in der Informationssicherheit zu bestimmen.

SANS Top 20

Am 28.11.2007 publizierte SANS die aktuelle Version der „TOP-20"-Liste der größten Security Risiken. Viele Positionen blieben unverändert, wie die der Web-Applications auf Platz 1 der Server-seitigen Verletzlichkeiten. Auffällig ist allerdings die signifikante Zunahme hochkritischer Sicherheitslücken in Office-Anwendungen von Microsoft: Patchen dringend anzuraten.



Denial of Car Service

Eine ganz neue Klasse von Denial of Service (DoS) Angriffen könnte uns zukünftig bevorstehen. So wurde am 01.11.2007 in einem Parkhaus in Kent (GB) als Verursacher einer seit mehreren Wochen andauernden Störung von Dutzenden Fahrzeugen das Familienauto eines Pendlers identifiziert. Es gab periodisch Signale ab, die in einem Umkreis von 50 m die Bordelektronik anderer Automobile verwirrten. Die dadurch verursachten Effekte reichten von einer Selbstauslösung der Diebstahl-Alarmierung über die Blockierung der Zentralverriegelung bis zur Sperrung der Zündung. Wenn das schon unbeabsichtigt so wirksam funktioniert – mit welchen Wirkungen ist dann erst bei gezielten „DoCS"-Angriffen zu rechnen?

Vorratsdatenspeicherung

Am 09.11.2007 hat der Bundestag die Telekommunikationsüberwachung neu geregelt. Damit wurden unter anderem die Zugriffsmöglichkeiten der Strafverfolgungsbehörden auf Verkehrsdaten erheblich ausgeweitet. So sind TK-Provider nun verpflichtet, im manuellen Auskunftsverfahren (§ 113 TKG), d. h. auch ohne Vorlage eines richterlichen Beschlusses, zu einer dynamischen IP-Adresse mit Zeitangabe den Namen des Anschlussinhabers preiszugeben.

Auch wurde die Pflicht zur Benachrichtigung Betroffener nach Abschluss einer Maßnahme (§ 101 StPO) erheblich abgeschwächt: Der neue Absatz 7 erlaubt, mit Zustimmung des Gerichts von einer Benachrichtigung abzusehen, wenn sie für insgesamt fünf Jahre zurückgestellt worden ist und die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden.

Schließlich macht der neue § 113a TKG eine sechsmonatige Vorratspeicherung aller Verkehrsdaten demjenigen zur Pflicht, der „öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt". Die bei Telefondiensten, Internet-Nutzung und E-Mail-Diensten jeweils zu speichernden Verkehrsdaten sind vollständig aufgeführt – und schließen explizit auch nicht zu Stande gekommene Verbindungsversuche ein; Mobilfunknetzbetreiber haben den Standort aller Funkzellen und die zugehörigen Hauptstrahlrichtungen vorzuhalten.

Mit dieser Regelung bricht der Gesetzgeber ein zentrales Grundprinzip des Datenschutz- und Strafrechts: Eine verdachts- und anlassunabhängige Erhebung und Speicherung von Verkehrsdaten galt bisher als unvereinbar mit den Prinzipien einer freiheitlichen Ordnung.

Die Neuregelungen treten am 01.01.2008 in Kraft – sofern der Bundespräsident dieser erheblichen Ausweitung sicherheitsbehördlicher Eingriffsbefugnisse nicht seine Unterschrift verweigert. Dann bleibt nur noch, auf einen Erfolg der Initiative gegen die Vorratsdatenspeicherung zu hoffen, die eine Sammel-Verfassungsbeschwerde initiiert hat. Eine Beteiligung daran ist noch bis 24.12.2007 möglich.

Leitfaden IT-Sicherheit

Am 25.10.2007 gab das BSI eine aktualisierte Fassung des "Leitfaden IT-Sicherheit" heraus. Darin werden die 50 wichtigsten organisatorischen und technischen Maßnahmen insbesondere für kleinere und mittelständische Unternehmen sowie Behörden als „IT-Grundschutz kompakt" anschaulich zusammengefasst. Der Leitfaden bietet eine gute Übersicht und Checklisten zur (Selbst-) Überprüfung.

Pikanterweise haben sich die Autoren darin gegenüber der Version vom September 2003 (siehe SSN 10/2003) sang- und klanglos vom Begriff „... Härten in der IT-Sicherheit ..." verabschiedet. Vielleicht lassen sich ja so die Grundschutzanforderungen an Behörden im Kontext des Umsetzungsplans Bund (UP Bund) besser erfüllen.

Anstieg der IuK-Straftaten

Das Bundeskriminalamt (BKA) veröffentlichte am 20.11.2007 die offizielle Statistik der Entwicklung von „IuK-Straftaten" im Jahr 2006. Einschließlich Warenkreditbetrug stieg die Gesamtfallzahl um 40% auf über 165.000 Straftaten. Zur „IuK-Kriminalität im engeren Sinne" zählte das BKA knapp 30.000 Fälle – ein Plus von knapp 10 %. Dabei verzeichneten die „Fälschung beweiserheblicher Daten und Täuschung im Rechtsverkehr bei der Datenverarbeitung" und das „Ausspähen von Daten" (Plus von 140 % bzw. 26 %) die höchsten Zuwachsraten.

Tag des Informationsrechts

Eine spannende Veranstaltung zur Online-Durchsuchung des Zentrums für Angewandte Rechtswissenschaft in Kooperation mit den Jungen Juristen Karlsruhe e.V. ist für den „Karlsruher Tag des Informationsrechts" am 10.12.2007 geplant. Neben Gerhart Rudolf Baum, Bundesinnenminister a.D. und einer der Beschwerdeführer vor dem Bundesverfassungsgericht, werden der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar und der BKA-Präsident Jörg Ziercke zu der dreistündigen Veranstaltung in der Städtischen Galerie beim ZKM erwartet. Die Teilnehmerzahl ist begrenzt, eine Anmeldung erforderlich.

T.I.S.P.-Boom

Die wachsende Bedeutung des T.I.S.P.-Zertifikats verdeutlichte das erste T.I.S.P.-Community-Treffen am 15.-16.11.2007 in Karlsruhe. Neben Fachvorträgen zu „Security bei SAP", „IT won't happen to me" und „Abhörschutz" wurden Workshops zu den Themen „Awarenesskampagnen", „Herausforderungen im Arbeitalltag" und „Projektleitung und IT-Sicherheit" geboten. Gelegenheit zu Erfahrungsaustausch und Networking, u. a. beim abendlichen Dinner, rundeten die gut besuchte Veranstaltung ab.

Dr. Günther Welsch, Geschäftsführer von TeleTrusT Deutschland e.V., erwartet für Ende 2007 mehr als 200 zertifizierte T.I.S.P.-Absolventen – eine Verdoppelung innerhalb eines Jahres. Diese Entwicklung belege die steigende Akzeptanz und Bedeutung des T.I.S.P. als beruflicher Qualifikationsnachweis.

Secorvo News

Secorvo College aktuell

Eine letzte Weiterbildungsgelegenheit in 2007 bietet Secorvo College mit dem Seminar IT-Sicherheitsaudits in der Praxis am **04.-06.12.2007**. Alle Seminare und Termine für das kommende Jahr finden Sie im noch druckfrischen Jahresprogramm 2008.

Auf Grund der großen Nachfrage bietet Secorvo College die Möglichkeit zur T.I.S.P.-Zertifizierung im Jahr 2008 insgesamt vier Mal an. Termin des ersten T.I.S.P.-Seminars ist der **25.-29.02.2008**.

Termine, Programme und Online-Anmeldung unter http://www.secorvo.de/college

"Wie dick ist Ihr Bunker?"

Für den 22.11.2007 hatte die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zu Vortrag und Diskussion über physikalische Gefährdungen von Rechenzentren und den damit verbundenen Haftungsrisiken geladen. Prägnant und eindrucksvoll spannten Prof. Dr. Michael Bartsch (Bartsch und Partner) und Hans-Jürgen Frase (Litcos) den Bogen von der Verantwortung des Managements für die Risikovorsorge bis zu den konkreten Bedrohungen der IT-Verfügbarkeit durch Überhitzung, Stromausfall, Feuer und Wasser sowie einem systematischen Vorgehen zur Entwicklung von Schutzmaßnahmen. Die Unterlagen der Referenten sind online abrufbar.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2007	
04.-06.12.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
10.12.	Tag des Informationsrechts: Onlinedurchsuchung (ZAR, Karlsruhe)
27.-30.12.	The 24th Chaos Communication Congress (24C3) (Chaos Computer Club, Berlin)
Februar 2008	
10.-13.02.	Fast Software Encryption Workshop (FSE 08) (IACR, Lausanne/CH)
11.-14.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
13.-14.02.	15. DFN CERT & PCA Workshop - Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
19.-20.02.	Identity Management Symposium 2008 (vps & Secorvo, Karlsruhe)
25.-29.02.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)

Fundsache

Der seit dem 13.07.2007 öffentliche Aufsatz "Fast-Flux Service Networks" des Honeynet Projects erläutert die immer ausgefeilteren Methoden von Angreifern zur Verschleierung des Ursprungs von Viren-, Würmer- und Spam-E-Mails oder Phishing-Angriffen. Kern der Analyse ist eine neue Technologie namens "Fast Flux", mit der Angreifer ihre DNS-Einträge sowie die zugeordneten IP-Adressen regelmäßig – teilweise im Minutentakt – ändern, um unentdeckt zu bleiben.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Dezember 2007



Editorial: Ganz einfach

Alles Große und Edle ist einfacher Art.
Gottfried Keller (1819-1890)

Die Komplexität hat uns im Griff. Sowohl im Großen (Termine, Aufgaben) als auch im Detail (Umsetzungsprobleme, Prozesse, Tools). Schleichend haben wir die Übersicht der Vielfalt geopfert. Der Trend zum Komplexen verursacht Mehraufwände, Ärger und Verzögerungen, die von keinem Controller gemessen werden – und gefährdet die Sicherheit unserer Systeme. Denn Komplexität erhöht die Anfälligkeit für Fehler (Software, Bedienung, Hardware), erschwert zugleich die Kontrolle und verbaut den Blick auf das Wesentliche: Sind Prioritäten ereignisgetrieben und vernebeln diffuse Ziele die Aufgaben, geht leicht der Überblick verloren.

Die Erkenntnis, dass Konzentration auf das Wesentliche die Effektivität steigert, ist ebenso banal wie bekannt – aber selten beachtet. Doch Vorsicht: Einfachheit ist harte Arbeit. Sie erfordert drei Dinge:

- **Klarheit**: Formulieren Sie Sicherheitsziele und Regeln verständlich, nachvollziehbar und eindeutig – und vor allem: im Kontext Ihrer Unternehmensziele. Jede Policy und jede Maßnahme sollte sich daraus mit „gesundem Menschenverstand" ableiten lassen.
- **Konsequenz**: Sorgen Sie für die Umsetzung Ihrer Basis-Sicherheitsmaßnahmen – wie personalisierte Accounts, Mindestanforderungen an die Passwortqualität, Unterbindung von Passwortweitergaben, „Need-to-Know"-Prinzip für Administratorrechte, Schutz mobiler Systeme. Damit schließen Sie die „Löcher im Zaun" und erzielen die mit Abstand beste Wirkung.
- **Verzicht**: Verhindern Sie nebulöse Floskeln, vermeidbare Regelungen, nicht konsequent umsetzbare Maßnahmen. Sie gewinnen Sicherheit, wenn Vereinfachung die Umsetzung erleichtert.

Ingenieure lieben es, Komplexität zu konstruieren.
Die Konstruktion von Einfachheit ist um Einiges schwieriger. Shai Agassi



Inhalt

Editorial: Ganz einfach

Security News

Wireless Hacking

Mobile Bots

Selbst-Inspektion

EU-Signatur-Studien

BCM bald zertifizierbar

Sicherheitspreis 2008

Eichhörnchen mit Backdoor

Trojaner 2.0

Erratum

Secorvo News

Secorvo College aktuell

Veranstaltungshinweise

secorvo
security consulting

Security News

Wireless Hacking

Am 30.11.2007 veröffentlichte die Schweizer Firma Dreamlab Technologies ein Whitepaper, in dem sie Details der Verschlüsselung in Microsofts Funktastaturen offen legt. So werden die Tastatureingaben lediglich durch einen einfachen XOR-Mechanismus mit einem ein Byte langen Zufallswert kryptiert (Vigenère-Chiffre, vor 151 Jahren von Charles Babbage gebrochen); dieser Zufalls-„Schlüssel" wird nach einem „Connect" der Tastatur im Klartext an den Receiver geschickt. Da es nur 256 mögliche Schlüssel gibt, lohnt es nicht, den Wert abzufangen – schon nach wenigen Tastatureingaben (20-50) kann die Zufallszahl bestimmt werden. Manchmal lohnt es, sich mit seiner eigenen Geschichte zu beschäftigen: Mit demselben „Verschlüsselungsmechanismus" hatte Microsoft sich schon bei Office 95 blamiert.

Immerhin gibt es zahlreiche Funktastaturen am Markt, die selbst auf eine solche Verschleierung verzichten. Daher sind nach Geheimschutzhandbuch des BMWi für IT-Systeme, mit denen Verschlusssachen verarbeitet werden, gemäß Abschnitt 6.11.2 (1) Funktastaturen nicht zugelassen.

Mobile Bots

Das am 27.11.2007 von der ENISA publizierte Positionspapier „Botnets - The Silent Threat" liefert eine aktuelle Analyse der Botnet-Szene. Die statistischen Daten stammen überwiegend aus dem ATLAS-System (SSN 02/2007). Danach werden 65% der „Zombie"-Systeme über Browser-Exploits infiziert.

Nach Überzeugung der ENISA sind Botnetze (mit insgesamt ca. 6 Mio. Bots) ein Werkzeug der organisierten Kriminalität. Sie stuft sie aufgrund der technischen Ausgereiftheit und andauernden Weiterentwicklung als mittelfristig ernsthafte Gefährdung der globalen Netzwerkinfrastruktur ein. Insbesondere mobile, vernetzte Endgeräte mit ständigem Netzzugang dürften zukünftig eine bevorzugte Zielplattform für Botnetze darstellen (s. a. iPhone out of Jail, SSN 10/2007).

Der Kern des Problems, die Unsicherheit von Programmen und Betriebssystemen, wird in dem Papier zwar angesprochen, mündet jedoch in der wenig spektakulären Forderung, „*Vendors should continuously improve the security of their products*". Statt der Hersteller (Produkthaftung) nimmt die ENISA die ISPs in die Pflicht: Sie sollen Botnetz-E-Mails erkennen und blockieren.

Selbst-Inspektion

Nach einer einjährigen Beta-Phase hat das dänische Unternehmen Secunia am 18.12.2007 Release 1 des Personal Software Inspectors (PSI) freigegeben. Das für Privatnutzer lizenzfrei nutzbare Tool überprüft Windows-Betriebssysteme und zahlreiche installierte Standard-Anwendungen, ob technische Schwachstellen existieren, Softwareversionen veraltet sind oder Programme nicht mehr vom Hersteller unterstützt werden. PSI erkennt mehr als 4.700 Programm(versionen) anhand einer eigenen Signatur-Datenbank. Praktischerweise liefert das Analyseergebnis auch die direkten Download-Links der erforderlichen Sicherheits-Updates. Ein wertvolles Hilfsmittel, will man sich durch konsequentes Securitypatch-Management vor Bedrohungen schützen, die von bekannten Fehlern installierter Programme und Betriebssysteme ausgehen.

EU-Signatur-Studien

Pünktlich zur besinnlichen Adventszeit legte die EU-Kommission zwei Studien zum Thema elektronische Signaturen auf den virtuellen Gabentisch. Sie sind „Nachfolger" der Study on legal and market aspects of electronic signatures (2003), an der auch Secorvo mitwirkte und die der Kommission eine Reihe von Empfehlungen mit auf den Weg gab (vgl. SSN 10/2003). Die Studien untersuchen erneut den Stand der Umsetzung der EU-Signaturrichtlinie in ausgewählten Bereichen. Beide Studien wurden am 12.12.2007 in Brüssel der Öffentlichkeit vorgestellt.

Die am 22.11.2007 fertig gestellte Study on the standardisation aspects of eSignature analysiert die zahlreichen Initiativen en Detail, die entweder innerhalb oder außerhalb offizieller Gremien die Standardisierung im Bereich Signaturen voran getrieben haben. Dabei werden die existierenden Standards sehr unterschiedlich bewertet (von „zu vage" bis „zu detailliert"); Probleme sehen die Autoren vor allem bei der Veröffentlichung von Standards im Amtsblatt der Europäischen Union. Zur Verbesserung werden eine Reihe von teilweise sehr pragmatischen Maßnahmen empfohlen.

Eine gänzlich andere Fragestellung untersucht die – bislang nur als Vorstudie publizierte – Study on mutual recognition of eSignatures for eGovernment applications. Sie analysiert wie die gegenseitige Anerkennung elektronischer Signaturen im E-Government innerhalb Europas verbessert werden kann, und richtet zahlreiche Empfehlungen an die EU (insbesondere die Einrichtung einer „European Generic Validation Authority"), die Mitgliedsstaaten sowie an die für PKI-Anwendungen Verantwortlichen. Man darf gespannt sein, wie viele der Empfehlungen diesmal umgesetzt werden.

BCM bald zertifizierbar

Im November 2006 wurde der Empfehlungsstandard BS 25999-1:2006 „Business continuity management. Code of Practice“ veröffentlicht. Ein Jahr später erschien nun dessen Pendant, der Anforderungsstandard BS 25999-2:2007 „Specification for business continuity management“ des englischen BSI (British Standards Institute), der die Grundlage für den Nachweis eines BCM-Systems bilden kann.

Die Ähnlichkeiten zum ISO/IEC 27001:2005, der aus dem BS 7799-2:2002 hervorging, sind nicht zufällig. Auch der BCM-Standard setzt auf das bewährte PDCA-Modell (Plan-Do-Check-Act) als Grundlage eines „lebendigen“ Management-Systems. Generell bewegt sich der nur 28seitige Standard auf einem abstrakten Niveau und enthält im Gegensatz zum ISO/IEC 27001:2005 keinen Katalog mit konkreten Umsetzungsmaßnahmen.

Damit steht nur noch die Veröffentlichung des neuen BSI-Standards 100-4 zum Thema Notfallmanagement aus. Darin wird der Praktiker zweifellos konkretere Hilfestellungen finden.

Sicherheitspreis 2008

Zum zweiten Mal hat die Horst-Görtz-Stiftung des Utimaco-Gründers am 08.12.2007 den mit insgesamt 200.000 Euro dotierten Deutschen IT-Sicherheitspreis ausgelobt. Prämiert werden innovative Konzepte und Lösungen aus den Bereichen Kryptografie, System- und Netzwerksicherheit. Eine Bewerbung ist schriftlich bis 18.02.2008, online bis 28.02.2008 möglich. Die Preisverleihung erfolgt im Oktober 2008 in Darmstadt.

Eichhörnchen mit Backdoor

Am 13.12.2007 entdeckten die Entwickler des beliebten Open-Source Webmailers SquirrelMail, dass die MD5-Summen der veröffentlichten Software-Pakete von Version 1.4.12 nicht stimmten. Tatsächlich konnte eine nachträgliche Veränderung des Codes festgestellt werden, durch die die Ausführung beliebigen Programmcodes – und damit bösartige Angriffe – ermöglicht wurden. Wir raten daher dringend zum Update auf die neueste Version 1.4.13. Und: Vor der Installation von öffentlich zugänglicher Software sollte immer die Integrität geprüft werden! Das kleine Tool Hashtab (Version 2.07 vom 13.12.2007) vereinfacht dies für Dateien unter Windows erheblich. Es unterstützt zehn auswählbare Hash-Algorithmen (u. a. RIPEMD, MD5 und SHA-1).

Trojaner 2.0

Der Internet-Sicherheitsspezialist finjan hat am 10.12.2007 seinen Web Security Trends Report (Q4 2007) veröffentlicht. Interessantester Schwerpunkt dieses Berichts ist die Prognose für die Entwicklung der Steuerung von Trojanern auf infizierten PCs. Die traditionellen Wege – Nutzung von IRC und IRC über HTTP als dedizierte Kommunikationszentren – erlaubte ein (mühseliges) Blacklisting dieser Dienste.

Der finjan-Report sagt voraus, dass mit der Verbreitung von Web 2.0-Techniken diese vermehrt auch zur Steuerung von infizierten Drohnen genutzt werden. Die Übertragung von Daten zum infizierten Rechner erfolge per RSS-Feed, während als Rückkanal Blog-Services oder offene Web 2.0-Plattformen genutzt würden. Moderne verteilte APIs verschiedener Plattformen erleichterten diesen Ansatz. Dies würde eine effektive Verteidigung signifikant erschweren, da der bösartige Datenverkehr transparent in zulässige Datenströme eingeflochten und somit kaum noch zu filtern sein würde. Perimeter-Schutz hilft da nicht weiter: Die Nutzung wirksamer Sicherheitsmechanismen in Applikationen gewönne weiter an Bedeutung.

Erratum

Anders als in den SSN 11/2007 behauptet wurde in der Neufassung des BSI-„Leitfadens IT-Sicherheit“ keineswegs der Begriff „Härten (...) in der IT-Sicherheit“ gestrichen. Wir bitten um Entschuldigung. Über die Feiertage üben wir Lesen. Versprochen.

Secorvo News

Secorvo College aktuell

Noch nie haben so viele Teilnehmer unsere Seminare besucht wie 2007 – sogar Zusatztermine mussten wir kurzfristig einschieben. Stolz machen uns vor allem die hervorragenden Bewertungen und die zahlreichen Empfehlungen aus berufenem Mund wie diese: „*Secorvo überzeugt durch exzellente Fachkompetenz, den Bezug von IT-Sicherheit zur Wirtschaftlichkeit, die Professionalität der Dozenten und nicht zuletzt die hervorragende Organisation der Schulung. Ich habe Secorvo weiterempfohlen.*“ (Markus Hieb, Roche Diagnostics GmbH).

Wir danken Ihnen für Ihr Vertrauen und freuen uns auf ein Wiedersehen in 2008 auf einem unserer zahlreichen Seminare.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2007	
24.12.	Heiligabend
27.-30.12.	The 24th Chaos Communication Congress (24C3) (Chaos Computer Club, Berlin)
Januar 2008	
16.-18.01.	Omicard 2008 (inTIME, Berlin)
Februar 2008	
05.-06.02.	18. SmartCard Workshop (Fraunhofer, Darmstadt)
10.-13.02.	Fast Software Encryption Workshop (FSE 08) (IACR, Lausanne/CH)
11.-14.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
13.-14.02.	15. DFN CERT & PCA Workshop - Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
19.-20.02.	Identity Management Symposium 2008 (vps & Secorvo, Karlsruhe)
25.-29.02.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
März 2008	
09.-12.03.	11. International Workshop on Practice and Theory in Public Key Cryptography (IACR, Barcelona/ES)
11.-14.03.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
19.-21.03.	5. Theory of Cryptography Conference (TCC 2008) (IACR, New York/US)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Januar 2008



Editorial: Abgeschöpft

Skimming („Abschöpfen") heißt die neue Kampfansage an bargeldlose Zahlungsmittel, nachdem es zumindest in Deutschland schwieriger geworden ist, mit Phishing reich zu werden. Zwar ist das Abgreifen der PIN am Geldautomaten keine ganz frische Idee: Erste Betrugsfälle, bei denen mittels präparierter Tastatur (Pulver o.ä.) die PIN-Ziffern am Geldautomaten ausgespäht und anschließend die EC-Karte entwendet wurde, gab es schon vor über 15 Jahren.

Die Entwicklung kleinster digitaler Kameras und Kartenleser ermöglicht heute jedoch „Massenattacken" durch die Konstruktion täuschend echter Attrappen für Kartenleser und Tastatur. Dabei werden die Daten der eingeschobenen EC-Karte vom aufgesetzten Lesegerät kopiert und die PIN-Eingabe mit einem Tastaturaufsatz oder mittels winziger verborgener Video-Kameras aufgezeichnet. Anschließend übermittelt die Attrappe die Daten per Funk oder speichert sie auf einem Flash-Chip. Die damit geklonten EC-Karten funktionieren zwar nur im Ausland – dafür kann das Tageslimit meist mehrmals abgeschöpft werden, bevor das Konto gesperrt wird.

2007 wurden in Deutschland 10.400 Skimming-Fälle mit insgesamt 41.000 betrügerischen Abhebungen gezählt – fast doppelt so viele wie 2006. Einige der Täter ließen sich bei der Montage der Attrappen sogar fotografieren und filmen. Und es dürfte noch schlimmer kommen: Denn nicht nur 53.000 Geldautomaten sondern auch die rund 600.000 Point-of-Sales-Terminals sind ein attraktives Ziel – erste manipulierte Geräte, die PIN und Daten per SMS verschicken, wurden bereits entdeckt. Und die PIN-Zahlungen im EC-Cash-Verfahren steigen seit Jahren. Quelle des Übels ist die Speicherung der Kartendaten auf Magnetstreifen statt auf zugriffsgeschützten Chips, einer seit über 15 Jahren verfügbaren Technik. Bis zur Nachrüstung hilft manchmal das Abdecken der PIN-Eingabe mit der freien Hand. Vom Rütteln am Automaten hingegen wird abgeraten – ein Zerstören der Attrappe könnte den Zorn in der Nähe wartender Täter erregen.



Inhalt

Editorial: Abgeschöpft

Security News

Router ohne Hosen

Kompass IT-Sicherheitsstandards

OpenSource Grundschutztool

Infra-Root

Mit Spammern Geld verdienen

15 Jahre und kein bisschen leise...

Kreditscoring im Fokus

Hackers Challenge

Sicherheitsstudie 2008

Secorvo News

Secorvo College aktuell

Veranstaltungshinweise

Security News

Router ohne Hosen

Von Tomaz Bratusa wurde am 07.01.2008 eine Session-Riding-Schwachstelle in der Router-Serie Linksys WRT54GL veröffentlicht. Ist ein Benutzer per Browser auf dem Router angemeldet, kann die Firewall des Routers durch einfaches Klicken auf einen präparierten Link deaktiviert werden. Die Routereinstellungen werden gemäß den in der URL übergebenen Parametern ohne weitere Bestätigung verändert, wenn ein Browser-Cookie der authentifizierten Sitzung hinterlegt ist.

Da bei Heimarbeitsplätzen die Firewall des Routers oft die einzige Schutzbarriere zum Internet darstellt und nicht immer zusätzlich eine Personal Firewall eingesetzt wird, besteht eine direkte Gefährdung für die dem Router nachgelagerten Endsysteme. Daher wird dringend empfohlen, administrative Tätigkeiten am Router und Surfen – auch das Recherchieren von Routerkonfigurationen – nicht zeitgleich oder zumindest nicht mit demselben Browser durchzuführen.

Grundsätzlich ist es ohnehin empfehlenswert, die Standardeinstellungen des Routers (wie Kennworte und voreingestellte IP-Netzbereiche) vor Inbetriebnahme zu ändern.

Kompass IT-Sicherheitsstandards

Der in Zusammenarbeit zwischen dem NIA und dem Bitkom erarbeitete Kompass der IT-Sicherheitsstandards wurde am 03.12.2007 in einer neuen Version 3.0 vorgestellt. Der Kompass gibt eine aktuelle Übersicht und Bewertung aller verfügbaren nationalen und internationalen Standards mit Bezug zur IT-Sicherheit. Den Autoren ist es gelungen, eine knappe und sehr hilfreiche Handreichung zu erstellen, die sowohl für IT-Sicherheitsverantwortliche als auch für Geschäftsführer und IT-Führungskräfte ein Leitfaden bei der Planung und Umsetzung von IT-Sicherheitskonzepten sein kann.

Im Rahmen des Sicherheitsmanagements spielen qualifizierte Audits eine immer wichtigere Rolle, daher haben wir den Standard ISO 19011:2002 „Guidelines for quality and/or environmental management systems auditing" vermisst. Auch auf die aktuelle Weiterentwicklung der ISO Standards 27xxx wird nicht eingegangen: So fehlt der Ausblick auf die Standards zu Benchmarking (ISO 27004), Management von Informationssicherheits-Risiken (ISO 27005) und Disaster Recovery Services (ISO 27006). Dies trübt den ansonsten sehr positiven Gesamteindruck allerdings nur minimal.

OpenSource Grundschutztool

Die SerNet GmbH publizierte am 21.01.2008 das OpenSource Grundschutztool Verinice in der Version 0.6. Es unterstützt das Sicherheitsmanagement und die Durchführung von Audits auf der Basis von IT-Grundschutz und ist – im Unterschied zu den etablierten Grundschutztools – kostenfrei erhältlich, sowohl für Windows, als auch für Linux und MacOS. Alle Versionen des Tools sind als Download verfügbar.

Unsere ersten Testeindrücke waren sehr positiv. Das Werkzeug zeichnet sich durch eine intuitive Bedienbarkeit, ein erweiterbares Objektmodell und die Möglichkeit zur Anbindung an verschiedene Datenbanken aus.

Infra-Root

Am 11.01.2008 berichtete die Online-Ausgabe der britischen „Telegraph", dass es einem Jugendlichen gelungen sei, mittels einer TV-Fernbedienung Wiechen der U-Bahn in Lodz umzustellen und so mindestens eine Entgleisung zu verursachen. Die technischen Details bleiben in dem Bericht im Dunkeln – zweifellos aber war die fehlende gegenseitige Authentisierung der beteiligten Geräte wieder einmal (vgl. SSN 04/2007) Hauptursache für das Problem. Statt eines Challenge-Response-Verfahrens wird bei Infrarot-Steuerungen bestenfalls ein Authentisierungscode übermittelt, der grundsätzlich (mit mehr oder weniger hohem Aufwand) kopiert und erneut „eingespielt" werden kann. Bei einfachen Systemen werden moderne programmierbare Fernbedienungen sowie viele PDAs bzw. Mobiltelefone so im virtuellen Handumdrehen über ihre Infrarot-Schnittstelle zum Angriffswerkzeug.

Die meisten Automobilhersteller haben bei ihren Zentralverriegelungen inzwischen professionellere Lösungen implementiert, die von einer einfachen Fernbedienung nicht „erlernt" werden können. Man sollte also erwarten können, dass Systeme mit einem höheren Gefährdungspotential mit mindestens der gleichen Sorgfalt konzipiert werden. Dennoch hat es in der Vergangenheit weitere und ähnliche Vorfälle gegeben. Unsere Empfehlung für's neue Jahr: Hausaufgaben nachholen!

Mit Spammern Geld verdienen

Nicht immer enthalten Spam-E-Mails URLs, auf die man klicken soll, oder Bilder von beworbenen Produkten. Seit einiger Zeit werden reine Text-E-Mails verschickt, die den Kauf bestimmter Aktien bewerben – so genannter „Stock Spam".

Wer sich immer schon gefragt hat, wie und warum derartige Aktionen erfolgreich sein können, dem sei die 39-seitige Anklageschrift zu Alan Ralsky als Lektüre empfohlen: Ralsky gilt seit vielen Jahren als einer der internationalen Top-Spammer, konnte aber nie verhaftet werden. Am 03.01.2008 nun wurden er sowie zehn weitere Personen weltweit angeklagt. Ihnen wird vorgeworfen, über einen Zeitraum von mindestens 21 Monaten durch das Versenden von bis zu mehreren Millionen Spam-E-Mails pro Tag einen Gewinn von geschätzten 2,6 Millionen US-Dollar eingestrichen zu haben.

Dazu kauften sie zunächst gezielt die (niedrig-preisigen) Aktien chinesischer Unternehmen und bewarben diese anschließend via Spam. Etliche Käufer trieben dann den Wert der Aktien in die Höhe, so dass die Spammer ihre Aktienpakete teuer verkaufen konnten. Die gesamte „Aktion" umfasste die Manipulation von Aktienpaketen, Registrierung gefälschter Domains, Bestechung von E-Mail-Server-Administratoren sowie das Mieten von Botnetzen (vgl. SSN 05/2005).

15 Jahre und kein bisschen leise...

Kaum eine andere Security-Veranstaltung zieht seit so vielen Jahren so viele Sicherheitsexperten an: Der DFN Workshop „Sicherheit in vernetzten Systemen" findet in diesem Jahr schon zum 15. Mal statt. Wieder einmal verspricht das Programm, an dessen Erstellung Stefan Kelm als Mitglied des Programmkomitees mitgewirkt hat, sowie die schon legendäre Abendveranstaltung Highlights zu aktuellen Themen der IT-Sicherheit. Auch Secorvo ist – wie in jedem Jahr – an dem Workshop beteiligt: Dirk Fox wird über Realisierung, Grenzen und Risiken der 'Online-Durchsuchung' vortragen.

Kreditscoring im Fokus

Für viele Datenschützer ist der Einsatz von Scoring-Verfahren, mit denen Banken die Bonität ihrer Kunden analysieren, ein rotes Tuch. Denn dabei wird bei Privatkunden oft erheblich in der Persönlichkeitssphäre „gewühlt" – und die unterliegt dem Schutz des Bundesdatenschutzgesetzes (BDSG).

Zahlreiche Kreditinstitute nehmen es jedoch offenbar mit dem BDSG nicht so genau, wie eine am 23.01.2008 vom Bundesverband der Verbraucherzentralen vorgelegte Studie zur Kreditscoring-Praxis in Deutschland zeigt. In über 90% der Stichproben wurden Testpersonen nicht über den Scoring-Wert informiert, in 30% der Fälle wurde nicht einmal eine Einwilligung zur Schufa-Anfrage eingeholt. Schließlich wurden z.T. äußerst fragwürdige Angaben wie „Wohndauer", „Arbeitgeber", „berufliche Stellung" und „Umzugshäufigkeit" erhoben.

Hackers Challenge

Die US-amerikanische Firma Digital Armaments Inc. hat am 04.01.2008 eine Hacker Challenge gestartet, die jede bis zum 29.02.2008 eingereichte neue Schwachstelle mit funktionsfähigem Exploit-Code mit 20.000 US$ prämiert. Das Geschäftsmodell des 2003 gegründeten Unternehmens ist interessant: Es versucht, Hacker zur Zusammenarbeit zu gewinnen und schreibt seit April 2006 immer wieder thematische Hacker Challenges aus. Geld verdient das Unternehmen mit dem Verkauf exklusiver Reports über die eingereichten (und möglicherweise auch selbst gefundenen) Schwachstellen.

Genau so müsste es das organisierte Verbrechen wohl machen, um günstig an unveröffentlichte Exploits zu kommen. Oder BND, BKA und Verfassungsschutz – für die Online-Durchsuchung.

Sicherheitsstudie 2008

Seit vielen Jahren sind die Ergebnisse der IT-Sicherheitsstudie der Zeitschrift KES, die alle zwei Jahre erstellt wird, für viele Sicherheitsbeauftragte eine große Hilfe – denn „belastbare" Zahlen, mit denen sich eigene Risikoeinschätzungen und Investitionsentscheidungen stützen lassen, gibt es viel zu wenig.

Den pdf-Fragebogen für die Sicherheitsstudie 2008 gibt es online unter www.kes.info/studie2008. Die Auswertung erfolgt anonym. Alle Teilnehmer erhalten exklusiven Zugriff auf die tabellarische Auswertung sowie ein Präsent. Einsendeschluss für den ausgefüllten Fragebogen ist der 01.03.2008.

Secorvo News

Secorvo College aktuell

Im vergangenen Jahr hat sich die Zahl der TISP-Absolventen auf mehr als 200 verdoppelt – und die Nachfrage reißt nicht ab. Damit ist der TISP auf dem Weg zum führenden beruflichen Weiterbildungszertifikat im Gebiet IT-Sicherheit. Vom **25.–29.02.2008** bietet Secorvo College mit der fünftägigen T.I.S.P.-Schulung die nächste Gelegenheit, ein TISP-Zertifikat zu erwerben.

Anfang März (**11.–14.03.2008**) bietet das Seminar PKI - Grundlagen, Vertiefung, Realisierung genau das Wissen und die Erfahrung, die für die zielorientierte Entwicklung und den effizienten Betrieb einer PKI unabdingbar sind.

Das gesamte Seminarangebot 2008 sowie ein Online-Anmeldeformular finden Sie unter http://www.secorvo.de/college.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2008	
05.-06.02.	18. SmartCard Workshop (Fraunhofer, Darmstadt)
10.-13.02.	Fast Software Encryption Workshop (FSE 08) (IACR, Lausanne/CH)
13.-14.02.	15. DFN CERT & PCA Workshop - Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
25.-29.02.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
März 2008	
09.-12.03.	11. International Workshop on Practice and Theory in Public Key Cryptography (IACR, Barcelona/ES)
11.-14.03.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
19.-21.03.	5. Theory of Cryptography Conference (TCC 2008) (IACR, New York/US)
April 2008	
01.-03.04.	Forensik - Verfahren, Tools, Praxiserfahrung (Secorvo College, Karlsruhe)
14.-17.04.	Eurocrypt 2008 (IACR, Istanbul/TR)
15.-18.04.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
15.04.	First USENIX Workshop on Large-scale Exploits and Emergent Threats (Usenix, San Francisco/US)
22.-23.04.	Identity Management Symposium 2008 (Secorvo, Karlsruhe-Ettlingen)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Februar 2008



Editorial: Captcha

Informatiker kennen den nach seinem Erfinder Alan Turing (1912-1954) benannten Turing-Test, in dessen Verlauf ein Mensch in fünf Minuten entscheiden soll, welcher von zwei mit ihm über einen Computer verbundenen Gesprächspartnern eine Maschine und welcher ein Mensch ist. Bis heute hat es kein Computerprogramm geschafft, einen menschlichen Tester zu täuschen.

Diese Frage nach der Unterscheidbarkeit von „künstlicher" und „menschlicher" Intelligenz, die in den 80er Jahren die Informatik aufwühlte, ist heute hinter eine andere zurückgetreten: Kann ein *Computer* entscheiden, ob ein Computer mit ihm spricht? Dieser gewissermaßen „umgekehrte Turing-Test" entwickelt sich zur Schlüsselfrage zahlreicher Web-Angebote. Denn vielfach sind automatische „Gesprächspartner" unerwünscht, wie z. B. Antwort-Automaten bei Wissenstests, Trojaner beim Online-Banking oder Spam-Bots, die Suchmaschinen für die Recherche von E-Mail-Adressen einspannen und News-Weiterleitungen für Postings missbrauchen.

Als Fachbegriff für solche Tests hat sich das Akronym „CAPTCHA" durchgesetzt: *Completely Automated Public Turing test to tell Computers and Humans Apart*. Dabei wird dem Nutzer des Angebots eine Aufgabe gestellt, die möglichst nur ein Mensch lösen kann – meist das Herauslesen verfremdeter Ziffern und Buchstaben aus einer Grafik. In zahlreichen Anwendungen werden solche Bild-CAPTCHAs inzwischen als Sicherheitsmechanismus eingesetzt. Ein Problem dieser CAPTCHA-Mechanismen ist, dass für viele nach und nach automatische Lösungen entwickelt werden, und daher deren Komplexität ständig zunimmt. Je komplizierter aber das CAPTCHA, desto schwerer ist es auch für einen Menschen zu lösen.

Austricksen lassen sich CAPTCHAs aber noch viel einfacher: Präsentiert ein Online-Banking-Trojaner ein abgefangenes CAPTCHA auf einer vielbesuchten Erotik-Seite, erhält er die Lösung in Sekunden „frei Haus" – beantwortet von einem unwissentlichen Mittäter. Sicherheit ist eben mehr als die Summe guter Mechanismen.



Inhalt

Editorial: Captcha

Security News

TrueCrypt 5

Leitfaden Kritis

ITGK-Ergänzung 9

Metasploit 3.1

Shmoocon 2008

Protokollierung

OWASP Publikationen

Der neue Gola/Wronka

Secorvo News

Secorvo College aktuell

Identity Management Symposium

Veranstaltungshinweise

secorvo
security consulting

Security News

TrueCrypt 5

Die freie Software TrueCrypt zur Verschlüsselung von Daten auf Festplatten ist am 05.02.2008 in der Version 5 erschienen. Highlight der Neuerungen ist die Möglichkeit, nun auch die komplette Festplatte inklusive Betriebssystem zu verschlüsseln. Weiter wurde erstmals eine Version für Mac OS X veröffentlicht, und Linux-Benutzer können sich endlich über eine grafische Oberfläche freuen. Zusätzlich gab es einige Detailänderungen bei den genutzten kryptografischen Verfahren.

Erste Tests bestätigen den guten Eindruck früherer Versionen der Software. Sowohl die Vollverschlüsselung als auch die Kompatibilität mit alten Versionen funktionierten problemlos. TrueCrypt ist eine gut gemachte, kostenlose Verschlüsselungssoftware. Neben vielen guten Eigenschaften lässt sie allerdings einige für den Einsatz in Enterprise-Umgebungen wichtige Funktionalitäten wie z. B. Mehrbenutzerfähigkeit und PKI-Anbindung vermissen.

Leitfaden Kritis

Am 24.01.2008 stellte Staatssekretär Dr. August Hanning vom Bundesministerium des Inneren den neuen Leitfaden „Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement" vor. Das 87-seitige Dokument wendet sich primär an Behörden und Unternehmen mit Verantwortung im Bereich KRITIS. Der Leitfaden beschreibt die Phasen Vorplanung, Risikoanalyse, Vorbeugende Maßnahmen und Krisenmanagement und stellt einen umfangreichen Anhang mit Literatur, Gefahrenlisten, Checklisten und einer beispielhaften Risikoanalyse zur Verfügung. Auch für Unternehmen und Behörden, die nicht zu den primären Adressaten des Leitfadens zählen, enthält das Dokument interessante Ansätze für Risiko- und Krisenmanagement. Weitere gute Dokumente zum Thema bietet die Risk Management Series der amerikanischen Federal Emergency Management Agency (FEMA).

ITGK-Ergänzung 9

Seit dem 15.02.2008 ist die 9. Ergänzungslieferung der IT-Grundschutzkataloge online und zum Download auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verfügbar. Eine angepasste Version des Grundschutztools GSTOOL ist angekündigt.

Die Weiterentwicklung umfasst neue Bausteine, die sich u. a. mit Themen wie elektrotechnischer und IT-Verkabelung, Netzdruckern, Datenträgeraustausch und dem unscheinbaren, aber immer wichtigeren Thema „mobile Datenträger" beschäftigen. Zusätzlich sind neue Maßnahmen und Gefährdungen in die Kataloge eingearbeitet worden.

Auch sprachlich passt das BSI die Kataloge dem wachsenden Bedürfnis nach umfassender Informationssicherheit an. Sukzessive wird der etablierte Begriff „IT-Sicherheit" durch „Informationssicherheit" ersetzt – das ist ein sehr sinnvoller Schritt, geht es doch um den Schutz von Informationen unabhängig von der Form, in der sie vorliegen.

Metasploit 3.1

Am 28.01.2008 wurde Version 3.1 des Metasploit Project vorgestellt, dessen Ziel es ist, Penetrationstestern, Forschern und Exploit-Entwicklern aktuelle Informationen und Hilfsmittel zu Exploit-Techniken verfügbar zu machen. Die neue Version enthält Werkzeuge beispielsweise zur Sicherheitsüberprüfung von WLANs und des neuen Apple iPhone, wurde um weitere Funktionen ergänzt und bietet nun auch unter Windows eine vollständige grafische Oberfläche.

Ergonomie und Leistungsfähigkeit des Werkzeugs sind beachtlich. Wie so viele „dual use"-Produkte wird es in den falschen Händen allerdings zu einem mächtigen Angriffswerkzeug, mit dem sich erheblicher Schaden anrichten lässt.

Shmoocon 2008

Auf der diesjährigen Shmoocon (15.-17.02.2008) wurden eine ganze Reihe neuer Angriffstechniken vorgestellt. Besonders interessant waren das Entschlüsseln von GSM-Verbindungen mit vertretbaren Investitionskosten, potentielle Schwachstellen auf Citrix-Servern und das Einbringen von echten Exploits in virtuelle Welten wie „second live". Daneben wurden auch gesellschaftspolitische Themen wie die soziale Verantwortung der Hacker-Community diskutiert und Hilfsprojekte wie Hackers for Charity vorgestellt.

In seiner Keynote am 15.02.2008 stellte Alex Halderman unglaubliche Sicherheitsmängel amerikanischer Wahlcomputer vor. Stimmt der Dateiname, wird ein infiziertes Systemimage anstandslos geladen und kann sich über eine PCMCIA-Speicherkarte auf weitere Wahlcomputer verbreiten. Prüfsummen und kryptografische Schutzmechanismen sucht man vergeblich; der PCMCIA-Schacht kann nur mit einem Schloss physikalisch gesperrt werden – das bau- und „schlüsselidentisch" mit einem bei Jukeboxen und Geldspielgeräten eingesetzten ist. Nach dem holländisch-deutschen Wahlmaschinen-Debakel (siehe SSN 10/2006) ist nun vielleicht auf politische Einsicht zu hoffen – auch bei der Entwicklung und Prüfung von Wahlmaschinen

sollte man jemanden fragen, der etwas davon versteht. Die Vortragsunterlagen und Videos der gelungenen Veranstaltung können in Kürze von der Website geladen werden.

Protokollierung

Das Thema Protokollierung ist so etwas wie die Achillesferse der IT-Sicherheit: fast jedes System bietet Protokolldaten, die Auswertungstools sind meist primitiv, die Formate uneinheitlich – und nicht jede Protokollierung ist zulässig. Mit der am 17.01.2008 veröffentlichten „Studie über die Nutzung von Log- und Monitoringdaten im Rahmen der IT-Frühwarnung und für einen sicheren IT-Betrieb“ will das BSI Licht in den Logdatendschungel bringen – und hat dem Thema möglicherweise einen Bärendienst erwiesen.

Die 294 Seiten umfassende Fleißarbeit listet die Merkmale von Logdateien wichtiger Systeme und Anwendungen auf, ignoriert aber die rechtlichen Anforderungen praktisch vollständig. Die wenigen Andeutungen zu Anforderungen des Datenschutzrechts sind irreführend bis falsch und lassen diesbezügliche Unkenntnis der Autoren vermuten; Hinweise auf Mitbestimmungspflicht und die Unzulässigkeit der Speicherung von Verbindungsdaten nach Telekommunikationsgesetz fehlen ganz. Von einer Umsetzung der Empfehlungen der Studie ohne vorausgehende Betrachtung der rechtlichen Anforderungen wird daher dringend abgeraten.

OWASP Publikationen

Veröffentlichungen der OWASP-Initiative sind seit Kurzem über den digitalen Verlagsmarktplatz LULU in gedruckter Form oder als formatiertes PDF verfügbar. Die Prints sind preislich sehr attraktiv, die PDFs kostenlos und tragen hoffentlich dazu bei, die qualitativ sehr hochwertigen Informationen der OWASP weiter zu verbreiten.

Der neue Gola/Wronka

Peter Gola und Georg Wronka haben Ihr Standardwerk „Handbuch zum Arbeitnehmerdatenschutz“ erneut überarbeitet und am 28.11.2007 in einer aktualisierten 4. Auflage herausgebracht.

Leider konnten sich die Autoren nicht von ihrem Konzept trennen, das sich an Verarbeitungsphasen orientiert, wodurch die Erörterung praktisch zusammenhängender Themen häufig in unterschiedlichen Kapiteln erfolgt. Auch wenn der Praktiker einige brandaktuelle Themen vermisst (z. B. Forensische Untersuchungen) und andere sehr allgemein abgehandelt werden (z. B. Whistleblowing), so bietet das Werk doch nach wie vor einen guten Überblick und stellt insbesondere die Verschränkung mit Mitbestimmungsfragen umfassend dar.

Secorvo News

Secorvo College aktuell

Die CeBIT wird es wieder zeigen: PKIs leben – wenn auch oft versteckt als „Treibsatz“ z. B. hinter E-Mail-Verschlüsselungslösungen. Wer verstehen will, wie PKIs funktionieren, wie sie aufgebaut und in Anwendungen und Verzeichnisdienste integriert werden, dem sei das Seminar PKI – Grundlagen, Vertiefung, Realisierung vom **11.–14.03.2008** ans Herz gelegt. Das Seminar umfasst praktische Übungen.

Der „Klassiker“ IT-Sicherheit heute wird wegen der hohen Nachfrage als Zusatztermin vom **27.–30.05.2008** stattfinden. Nach einer grundlegenden Überarbeitung und Aktualisierung deckt die Agenda jetzt in vier Tagen die wichtigsten aktuellen Themen der IT-Sicherheit ab. Eine Einführung in das Information Security Management von A(udit) bis Z(ertifizierung) mit Umsetzungsworkshop bietet Secorvo College vom **15.–18.04.2008**.

Detaillierte Programme, vollständige Jahresübersicht und Online-Anmeldung unter http://www.secorvo.de/college

Identity Management Symposium

In vielen Unternehmen existieren historisch bedingt zwei „Identitäts-Management“-Systeme unverbunden nebeneinander: Der Betriebsausweis, meist im Verantwortungsbereich der Corporate Security, und die Benutzerauthentifikation mit Rechnerzugang, in der Regel in der Zuständigkeit der IT-Security. Dabei kommt es zu Doppelarbeit, denn für beide Bereiche ist das Management eines „Berechtigungs-Lebenszyklus“ erforderlich.

Mit der Verbreitung elektronischer Zugangssysteme und Authentifikationslösungen, die Passworte durch Token ersetzen, rücken beide Systeme zusammen: Idealerweise sollten alle an die Identität eines Mitarbeiters gekoppelten Dienste über eine Karte möglich sein. Erste Unternehmen haben inzwischen ihre Identity Management-Systeme zusammengeführt. Die Komplexität dieser Projekte lag dabei sowohl in der Technik als auch in zahlreichen zu bewältigenden praktischen „Fallstricken“.

Gemeinsam mit der vps GmbH will Secorvo mit dem „Identity Management Symposium“ am **22.–23.04.2008** einen intensiven Erfahrungsaustausch mit und zwischen Unternehmen und Behörden initiieren, die ein solches integriertes „Identity Management“ vorbereiten oder bereits eingeführt haben (Programm, Online-Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2008	
09.-12.03.	11. International Workshop on Practice and Theory in Public Key Cryptography (IACR, Barcelona/ES)
11.-14.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
19.-21.03.	5. Theory of Cryptography Conference (TCC 2008) (IACR, New York/US)
April 2008	
02.-04.04.	Sicherheit 2008 (GI, Saarbrücken)
14.-17.04.	Eurocrypt 2008 (IACR, Istanbul/TR)
15.-18.04.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
15.04.	First USENIX Workshop on Large-scale Exploits and Emergent Threats (Usenix, San Francisco/US)
22.-23.04.	Identity Management Symposium 2008 (Secorvo, Karlsruhe-Ettlingen)
Mai 2008	
06.-07.05.	9. Datenschutzkongress 2008 (Euroforum, Berlin)
06.-08.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
26.-29.05.	IT Sicherheitsforum 2008 (GAI Netconsult, Frankfurt)
27.-30.05.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Karin Schuler

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

März 2008



Editorial: Ach wie gut!

Heute back' ich, morgen brau' ich,
übermorgen hol' ich der Königin ihr Kind;
ach, wie gut dass niemand weiß,
dass ich Rumpelstilzchen heiß!

Das war es also. Dieses Märchen unserer Kindheit erklärt unser gespaltenes Verhältnis zum Datenschutz. Tief verinnerlicht haben wir, dass nur derjenige seinen richtigen Namen verheimlicht, der Böses im Schilde führt – wird er erkannt, reißt er sich selbst in Stücke. Und so glauben wir im Umkehrschluss, dass der Unbescholtene nichts zu verbergen habe. Streift man durch „soziale Netzwerke" wie myspace, facebook, Xing oder SchülerVZ, so drängt sich der Eindruck auf, als wollten Millionen aus dieser tief verankerten Überzeugung ihre Unbescholtenheit durch exzessives Nichtverbergen unter Beweis stellen.

Wehe aber, wenn die Erkenntnis dämmert, dass es vielleicht nicht immer gut ist, Dritten umfangreiche persönliche Informationen zur Verfügung zu stellen. So geschehen, als facebook ab 07.11.2007 zur Nutzung des verkaufsfördernden „me too"-Effekts die aktuellen Online-Einkäufe der registrierten Benutzer an deren Freundeslisten schickte. Aber auch unwissentlich geben viele Nutzer persönliche Informationen im Internet preis – so weiß beispielsweise nicht jeder, dass die private Wunschliste beim Online-Buchhändler Amazon von jedermann eingesehen werden kann, wenn die Voreinstellung nicht geändert wurde. Daher lohnt es, gelegentlich bei einer Personensuchmaschine wie Yasni das eigene „Bild im Netz" zu überprüfen.

Zugleich nimmt die Überwachung im Windschatten der Terrordrohung zu – ungeachtet der jüngsten Urteile des BVerfG zu Online-Durchsuchung und Vorratsdatenspeicherung, die dem behördlichen Zugriff auf persönliche Daten hohe Hürden auferlegen. Dabei gibt die älteste Demokratie Europas den Schritt vor: Nach der flächendeckenden Installation von Videokameras in britischen Großstädten soll zukünftig eine Bilddatenbank die automatische Identifikation Verdächtiger erlauben. Ein 18-monatiges Pilotprojekt mit 750.000 Fotos verlief offenbar vielversprechend. Ob es hilft, den Namen des Ideengebers herauszufinden – damit er sich selbst in Stücke reißt?



Inhalt

Editorial: Ach wie gut!

Security News

Mifare-Cloning

Fingerwischerei

Einsatz von WAFs

Citrix-Ausbruch

Rechenfehlerangriff

VMware-Hacks

Druckfrischer Entwurf

Krypto-Historie

Secorvo News

Secorvo College aktuell

Aktualisierte White Paper

Identity Management Symposium

ITSF 2008

Veranstaltungshinweise

secorvo
security consulting

Security News

Mifare-Cloning

Auf dem Jahreskongress des Chaos Computer Clubs stellten Karsten Nohl und Henryk Plötz am 28.12.2007 einen Angriff auf das Authentifikationsverfahren kontaktloser Mifare-Chipkarten vor. Dem vom Hersteller geheimgehaltenen, etwa 15 Jahre alten "CRYPTO1"-Algorithmus waren sie mit einer Mikroskop-Analyse des Chip auf die Spur gekommen, um dann nach kryptographischen Schwächen (zu kleiner Zufallswert, lineares Schieberegister) darin zu suchen. Zu dieser Krypto-Schwachstelle gibt es nun den passenden „Mifare-Cloner“: Am 12.03. 2008 haben Forscher der Radboud Universiteit Nijmegen ein Video in YouTube veröffentlicht, auf dem sie zeigen, wie sie mit minimalem Aufwand Mifare-basierte Zugangskarten duplizieren.

Von der Attacke betroffen sind Tausende von Anwendungen mit einer Milliarde ausgegebenen Karten, vom Betriebsausweis über die Kantinenkarte bis zum bargeldlosen Bezahlsystem im öffentlichen Nahverkehr, sofern sie Mifare-Chips des Typs MF1 IC S50 oder S70 verwenden. Fein raus ist, wer seine Anwendung bereits auf den neueren Mifare DESFire (MF3 IC D40) migriert hat – statt einer etwas ältlichen Stromchiffre verwendet er bei der Authentifikation wahlweise DES oder TripleDES.

Fingerwischerei

In einem am 12.03.2008 online veröffentlichten Beitrag aus c't 05/08 beschreibt Daniel Bachfeld eine simple Methode, wie auf zahlreiche USB-Sticks unter Umgehung des Fingerprint-Schutz zugegriffen werden kann. Verwendet der Stick den Controller USBest UT176 oder UT 169 von Afa Technology, so erfolgt zwar die Fingerprint-Prüfung auf dem Chip – das Freigabe-Kommando für die „geschützte“ Partition sendet jedoch die Systemsoftware vom PC. Mit dem Open-Source-Tool PLscsi gelingt der Zugriff ohne Fingerkuppen-Imitat in nur drei Schritten.

Das Beispiel zeigt (leider) wieder einmal, dass es meist wenig hilft, einen Sicherheitsmechanismus nachträglich an eine bestehende Lösung „anzuflanschen“ – ist er nicht geeignet im System verankert, lässt sich das Verfahren an der Nahtstelle oft allzu leicht wieder auftrennen.

Einsatz von WAFs

Das OWASP German Chapter veröffentlichte am 18.03.2008 den deutschsprachigen Guide „Best Practices: Einsatz von Web Appliction Firewalls“. Das lesenswerte 25-seitige Dokument wendet sich an technische Entscheider im Bereich der Sicherheit von Web-Applikationen. Nach einer Einordnung von Web Application Firewalls (WAF) wird deren Haupteinsatzzweck erläutert – die nachträgliche Absicherung des externen Verhaltens von produktiven Web-Anwendungen, mit vertretbarem Aufwand und ohne Änderung der Applikation.

Die Betrachtung der Schutzmechanismen fokussiert auf den Schutz gegen die OWASP Top 10 (siehe SSN 06/2007). Abschließend werden Kriterien zur Einsatz-Entscheidung, Checklisten und Rollenmodelle für die Einführung sowie Best Practices für den Betrieb vorgestellt. Positiv fällt auf, dass in dem Dokument in allen Phasen Wert auf die Berücksichtigung von Aufwandsschätzungen gelegt wird.

Citrix-Ausbruch

Nicht nur bei einer Betriebssystemvirtualisierung sondern auch bei der Desktopvirtualisierung ist der Ausbruch aus einem beschränkten Kontext ein Risiko. So deckte Stefan Gora am 07.03.2008 auf, dass in Citrix-Umgebungen über den Microsoft-Taschenrechner auf weitere Applikationen zugegriffen werden kann, für die keine Berechtigung besteht. Denn unter Windows 2003 Server werden die Lizenzbedingungen des Taschenrechners mit dem Editor angezeigt, der über die Funktion „Datei öffnen“ das Starten weiterer Anwendungen ermöglicht.

Die Sicherheitslücke ist ein schönes Beispiel dafür, dass Hintertüren in komplexen Umgebungen manchmal ganz harmlos daherkommen. Zwar erlaubt der Taschenrechner unter den aktuelleren Microsoft-Server-Versionen diesen „Ausbruch“ nicht; dennoch empfehlen wir die Nutzung verschiedener Terminal-Server-Plattformen für Benutzergruppen mit unterschiedlichen Berechtigungen.

Rechenfehlerangriff

Zwei japanische Wissenschaftler veröffentlichten am 27.12.2007 einen Angriff auf den Advanced Encryption Standard (AES), der unter bestimmten Voraussetzungen 88 Bit eines 128-Bit-AES-Schlüssels rekonstruiert. Sie verwendeten dazu die auf den ersten Blick befremdlich anmutende Methode der „Differentiellen Fehleranalyse“ (DFA). In diesem speziellen Fall muss dazu ein bekannter Klartext mehrfach mit demselben Schlüssel verschlüsselt werden: Einmal ungestört, ein anderes Mal mit einem gezielt induzierten Fehler. Dabei muss der Angreifer erreichen, dass bei der neunten von zehn Runden eine bestimmte 32-Bit-Variable einen fehlerhaften Wert annimmt.

In der Praxis dürfte ein derartiger Angriff bei den meisten Anwendungen des AES nur äußerst schwer erfolgreich durchzuführen sein. Wer dennoch auf

Nummer sicher gehen will und die vierzigprozentige Leistungseinbuße nicht scheut, sollte den AES mit der maximalen 256 Bit Schlüssellänge verwenden – mit weiteren 128 Schlüsselbits und vier zusätzlichen Runden.

VMware-Hacks

Die am 25.02.2008 von Coresecurity veröffentlichte und vom Hersteller bestätigte Schwachstelle in VMware-Workstation und dem VMware-Player sollte nicht unterschätzt werden: Durch den Bug im Mechanismus der „Shared Folder" ist es möglich, von Wirtsbetriebssystemen aus auf das Hostsystem – und damit auf weitere Wirtssysteme – zuzugreifen. Die Abschottung der Systeme kann so vollständig ausgehebelt werden.

Unverständlich ist, dass bisher seitens VMware nur ein primitiver Workaround für die schon am 16.10. 2007 an den Hersteller gemeldete Schwachstelle vorliegt: die Empfehlung, „Shared Folder" zu deaktivieren.

Druckfrischer Entwurf

Auf den Webseiten des Bundesamt für Sicherheit in der Informationstechnik (BSI) steht der druckfrische Entwurf des „BSI Standards 100-4: Notfall-Management" in der Version 0.7 vom 19.03.2008 zum Download bereit. Die Veröffentlichung dieses schon lange erwarteten BSI-Standards zum Thema Business Continuity (BCM) und Notfall-Management verzögerte sich durch die Abstimmung mit den britischen Standards BS 25999-1:2006 und BS 25999-2:2007.

Das BSI bittet um kritische Prüfung und Kommentierung des aktuellen 82-seitigen Entwurfs bis Ende April 2008.

Krypto-Historie

Auf der Tagung „Día Internacional de la Seguridad de la Información" (DISI) gab Martin E. Hellman am 03.12.2007 an der Universidad Politécnica de Madrid einen spannenden Einblick in die Geburtsstunden der modernen Kryptographie („A Fool's Errand"). Sowohl seine Vortragsfolien als auch ein Video der Keynote sind inzwischen online verfügbar – die Dokumentation einer der Sternstunden der IT-Sicherheit.

Überraschend sein wenig technischer Ausblick: „What is the most important unsolved problem in cryptography? Lack of user awareness."

Secorvo News

Secorvo College aktuell

Eine Einführung in das Information Security Management von A(udit) bis Z(ertifizierung) inklusive Umsetzungsworkshop bietet Secorvo College vom **15.–18.04.2008.** Ein guter Einstieg für alle, die ihr Sicherheitsmanagement auf Standard-Konformität „abklopfen" möchten.

Das tatsächlich erreichte Sicherheitsniveau lässt sich auch durch ein Audit prüfen. Dazu bietet das Seminar IT-Sicherheitsaudits in der Praxis am **06.–08.05.2008** zahlreiche Hilfestellungen.

Am **27.–30.05.2008** wird der Klassiker IT-Sicherheit heute wieder aufgelegt – und deckt nach einer gründlichen Überarbeitung und Aktualisierung in vier Tagen die wichtigsten aktuellen Themen der IT-Sicherheit ab.

Und im Juni bietet sich Ihnen die nächste Gelegenheit, Ihre Fachkunde zu zertifizieren: auf dem T.I.S.P.-Seminar am **02.–06.06.2008**, mit anschließender Prüfung (Achtung: frühzeitige Anmeldung empfohlen).

Detaillierte Programme, vollständige Jahresübersicht und Online-Anmeldung unter http://www.secorvo.de/college

Aktualisierte White Paper

Eine aktualisierte Fassung des Secorvo White Papers „Das Policy-Rahmenwerk einer PKI" (Petra Barzin, Stefan Kelm) ist seit dem 27.03.2008 verfügbar.

Ebenfalls aktualisiert wurde die Forensik-Checkliste von Stefan Kelm (Version 1.2 vom 05.03.2008).

Identity Management Symposium

Gemeinsam mit der vps ID Systeme GmbH veranstaltet Secorvo am **22.–23.04.2008** das erste „Identity Management Symposium" in Ettlingen (bei Karlsruhe). Im Stil der bewährten Secorvo-Symposien wird es einen intensiven Erfahrungsaustausch mit und zwischen Unternehmen und Behörden bieten, die ein integriertes Identity Management vorbereiten oder bereits eingeführt haben. Unter anderem werden die Lösungen von BASF, BMW, ESG, Evonik, Fraunhofer und Swisscom vorgestellt (vollständiges Programm und Online-Anmeldung).

ITSF 2008

Das von GAI Netconsult und der ComConsult Akademie veranstaltete IT-Sicherheits-Forum 2008 findet in diesem Jahr vom 26.-29.05.2008 in Frankfurt statt. Auch diesmal wirkt Secorvo am Programm der etablierten Veranstaltung mit einem Tutorium zu „Security Awareness" und einer Keynote mit. Die Frühbucherphase endet am 31.03.2008.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2008	
02.-04.04.	Sicherheit 2008 (GI, Saarbrücken)
14.-17.04.	Eurocrypt 2008 (IACR, Istanbul/TR)
15.-18.04.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo College)
15.04.	First USENIX Workshop on Large-scale Exploits and Emergent Threats (Usenix, San Francisco/US)
22.-23.04.	1. Identity Management Symposium 2008 (Secorvo & vps, Karlsruhe-Ettlingen)
Mai 2008	
06.-07.05.	9. Datenschutzkongress 2008 (Euroforum, Berlin)
06.-08.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
26.-29.05.	IT Sicherheitsforum 2008 (GAI Netconsult, Frankfurt)
27.-30.05.	IT-Sicherheit heute (Secorvo College)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College)
09.-10.06.	DuD 2008 (Computas, Berlin)
17.-18.06.	6. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)
24.-25.06.	D-A-CH Security 2008 (GI/OCG/Bitkom/TTT, Berlin)
24.-26.06.	Sichere Softwareentwicklung (Secorvo College)
Juli 2008	
01.-03.07.	Forensik (Secorvo College)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

April 2008



Editorial: „(T)Räumst du noch oder identifizierst du schon?“

Kontaktlose Chipkarten haben sich inzwischen auch in mittelständischen Unternehmen als Betriebsausweis durchgesetzt. Sie dienen als bargeldloses Zahlungsmittel im Betriebsrestaurant, regeln den Gebäudezugang und vereinfachen die Zeiterfassung. Von einer ähnlichen Infrastruktur träumt auch die IT: Gesteuert durch aktuelle HR-Prozesse (Eintritt, Austritt, interner Wechsel etc.) ließen sich Zugriffsrechte für zentrale Systeme und kryptographische Schlüssel (VPN-Einwahl, E-Mail- und Festplattenverschlüsselung) automatisch vergeben und wieder entziehen – abhängig von Aufgabe und Stellenbeschreibung, mit striktem Freigabeprozess nach dem Need-to-Know-Prinzip. Schließlich kann der Ausweis als Single-Sign-On-Token leidige Mehrfach-Logins ablösen.

Der Sicherheitsgewinn wäre erheblich – keine „vagabundierenden“ Accounts mehr, Schluss mit notierten, weitergegebenen oder trivialen Passworten, Ende der „Rechteakkumulation“ bei Mitarbeitern, die häufig den Zuständigkeitsbereich wechseln. Administrationsprozesse würden einfach, Hotline-Anrufe zur Passwortrücksetzung entfallen. Die subjektive Wahrnehmung von Sicherheitsmechanismen als Arbeitsbehinderung wäre endlich Geschichte.

Technisch ist dies keine Zauberei mehr. In der Praxis sind zuvor jedoch ein paar Aufräumarbeiten zu erledigen, die schon in mittelgroßen Unternehmen wie die Reinigung des Augiasstalls anmuten: So müssen Rechte in Rollen verdichtet, Freigabeprozesse etabliert und HR-Daten konsolidiert werden. Die Bewältigung dieser Herausforderungen, die ohne höchsten Management-Support nicht gelingen kann, lohnt jedoch – das zeigten die Vorträge und Diskussionen auf dem ersten „Identity Management Symposium“ in Ettlingen: Wer Ordnung schafft, gewinnt – Geld, Überblick und Sicherheit.

Wer beim Schachspiel nicht einmal die Figuren in Ordnung zu stellen weiß, der wird es schlecht zu spielen verstehen; und wer nicht Schach bieten kann, der wird auch nie schachmatt setzen können." - *Theresa von Ávila*



Inhalt

Editorial: „(T)Räumst du noch oder identifizierst du schon?“

Security News

Online-Durchsuchung in der EU

Registry Ripper

Datenschutz international

Voreingestellte WPA-Keys

All Your iFrames Point to Us

Wurm inklusive

Finger-Logger

Vorratsdatenspeicherung

Secorvo News

Secorvo College aktuell

DuD 2008 – die zehnte

Pimp your web

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Online-Durchsuchung in der EU

Am 09.04.2008 hat die 42köpfige interministerielle Arbeitsgruppe „Online-Durchsuchung“ des österreichischen BMJ/BMI ihren Schlussbericht zur Online-Durchsuchung vorgelegt. In dem knapp 100seitigen Dokument kommen die Autoren zu dem Schluss, „dass die geheime Überwachung von privaten Rechnern ein besonders schwer wiegender Eingriff ist“, der unter Gesetzesvorbehalt stehe – und für den es derzeit in Österreich keine Rechtsgrundlage gibt. Der öffentlich gewordene Einsatz einer „Remote Forensik“-Software vom Herbst 2007, bei dem in kurzen Abständen Screenshots eines überwachten Systems an die Strafverfolgungsbehörden gesandt worden waren, wird in einem rechtlichen „Graubereich“ angesiedelt. Lesenswert ist die vergleichende aktuelle Übersicht der Regulierung und des Standes der politischen Diskussion zur Online-Durchsuchung in den Mitgliedsstaaten der EU.

Registry Ripper

Immer öfter erfordert die forensische Analyse von Windows-Rechnern eine zeitaufwändige Untersuchung der Registry (NTUSER.DAT, etc.), da das Betriebssystem dort eine Vielzahl von Aktionen protokolliert, beispielsweise die zuletzt geöffneten Dateien und eine Liste gestarteter Anwendungen, geöffneter Netzwerk-Ports und besuchter Webseiten.

Obwohl nicht nur frei verfügbare Registry-Viewer, sondern auch (fast) alle Forensik-Toolkits detaillierte Auswertungsmöglichkeiten für die Registry bieten, artet die Analyse in der Praxis oft in "Herumgestochere" mit manueller Auswertung bestimmter Registry-Schlüssel aus. Dagegen hilft das am 09.04.2008 veröffentlichte Tool RegRipper (v2.01A vom 20.04.2008): Es wertet die ca. 50 wichtigsten in der Registry vorhandenen Schlüssel aus, kodiert dabei Binärwerte in eine lesbare Form, extrahiert vorhandene Zeitstempel und speichert das Ergebnis in einer effizient weiter zu bearbeitenden Textdatei. Die zu untersuchenden Teilbäume der Registry werden über programmierbare, leicht anpassbare Plugins gesteuert. Das Tool erfordert dabei keine Installation und verfügt neben einer Kommandozeile auch über eine graphische Benutzeroberfläche; außerdem wird der Perl-Quellcode mitgeliefert. Bereits diese vom Autor "Basic edition" genannte Version sollte in keiner forensischen Tool-Sammlung fehlen – der Autor hat bereits angekündigt, an einer stark erweiterten Version zu arbeiten.

Datenschutz international

Im Auftrag der Europäischen Kommission erstellten wik-Consult und RAND Europe eine Gegenüberstellung der Datenschutz-Regulierung in Europa, den USA, Japan, Südkorea, Malaysia und Indien. Die vom 20.07.2007 datierende Endfassung der Studie wurde am 29.02.2008 von der EU-Kommission publiziert.

Bewertet wurden insbesondere der Rechtsschutz, der Grad an Selbstregulierung, die Effektivität, die Rechtsdurchsetzung und das Spannungsverhältnis zu Sicherheitsgesetzen. Die 230seitige Studie basiert auf rund 40 Interviews mit Experten aus unterschiedlichen gesellschaftlichen Bereichen (Unternehmen, Regierungen, Datenschutzbehörden, Juristen und Verbraucherschutzverbänden) und bietet einen guten Überblick der Datenschutz-Gesetzgebung der jeweiligen Länder sowie des dahinter stehenden Regulierungskonzepts.

Voreingestellte WPA-Keys

Am 14.04.2008 veröffentlichte Kevin Devine unter gnucitizen.org den von Britisch Telekom für den WLAN-Router Thompson Speedtouch verwendeten Algorithmus zur Erzeugung der voreingestellten WEP- und WPA-Schlüssel: ein einfacher SHA-1-Hash der hexadezimal dargestellten Seriennummer. Für die WEP-Keys von Netopia-Routern entdeckte und publizierte er das Verfahren schon am 29.09.2007: ein SHA-1-Hash der Seriennummer mit angehängter Textzeile aus „Third Stone From The Sun" von Jimi Hendrix liefert den Schlüssel. Von „James67“ wurde kürzlich auch der Erzeugungsalgorithmus der Default-Keys des Routers Netgear V1 DG834GT gefunden – am 21.02.2008 riet Sky Broadband zum sofortigen Wechsel des WiFi-Keys.

Ursache des Übels, von dem viele weitere WLAN-Router unterschiedlicher Hersteller und vielleicht auch deutsche Provider betroffen sein dürften, sind das fehlende Verständnis für die Wichtigkeit einer *zufälligen* Schlüssel-Wahl – und die Bequemlichkeit der meisten Nutzer, die den voreingestellten Schlüssel nicht wechseln. Dazu raten wir dringend – denn auch wenn der Erzeugungsalgorithmus nicht veröffentlicht ist oder sogar Zufallswerte erzeugt, kennen Hersteller oder Online-Provider den Schlüssel. Damit ist die Kommunikation – auch ohne „Bundestrojaner“ – potentiell Dritten zugänglich.

All Your iFrames Point to Us

Seit mehr als 1,5 Jahren untersucht Google Webseiten auf Malware, die automatisch beim Aufruf der Seite installiert wird. Dabei wurden über drei Millionen unterschiedliche, mit Malware verseuchte URLs auf mehr als 180.000 Webseiten gefunden, wie Niels Provos am 11.02.2008 berichtete. Der

Anteil infizierter Seiten hat sich dabei von April 2007 bis Januar 2008 auf ca. 1,3% verdreifacht; mehr als die Hälfte (über 60%) der Seiten stammt aus China.

Details der zusammen mit der Johns Hopkins University durchgeführten Untersuchung finden sich in einem von Niels Provos veröffentlichten, 22seitigen Technical Report. Besonders lesenswert ist das vom 07.04.2007 datierende (9seitige) Grundlagenpapier The Ghost in the Browser, in dem Provos mit seinen Koautoren an Javascript-Beispielen erläutert, wie Webseiten-Malware arbeitet – und entdeckt werden kann.

Wurm inklusive

Am 03.04.2008 wurde bekannt, dass „USB Floppy Drive Keys" der Firma HP, eine optionale Ergänzung für ca. 40 Modellvarianten der Proliant-Serie, mit zwei Würmern verseucht ausgeliefert worden waren. Bei den Würmern handelte es sich um Fakerecy und SillyFDC, die sich auf alle angeschlossen lokalen und vernetzen Laufwerken verbreiten. Sie waren erstmals Mitte Januar bzw. Ende Februar 2008 aufgetaucht. Über eine Schadfunktion verfügen beide Würmer glücklicherweise nicht, und aktuelle Virenscanner erkennen und beseitigen sie vollständig. Dennoch zeigt der Vorfall, was bei mangelhafter Qualitätssicherung in der Hardwareproduktion drohen kann – erst im September 2007 waren einzelne iPods mit dem Virus RavMon.Exe ausgeliefert worden. Der nächste Wurm kommt bestimmt. Hoffentlich einer, den der Virenscanner erkennt.

Finger-Logger

Nicht erst seit der Ausspähung und Publikation des Fingerabdrucks des Bundesinnenministers durch den Chaos Computer Club Ende März 2008 ist bekannt, dass biometrische Merkmale gefälscht werden können – siehe z.B. den von Matsumoto auf der Eurocrypt 2002 publizierten Beitrag „Gummi Fingers" (SSN 1/2002).

Auf der Blackhat Europe wurde am 04.04.2008 eine exemplarische Analyse für einen biometrischen Scanner nebst Infrastruktur (Türzugang) vorgestellt. Durch eine Man-in-the-Middle-Attacke wurden die Daten aus dem Kommunikationsstrom erfolgreich rekonstruiert, da sie unverschlüsselt übertragen wurden. Die gewonnen Datenschablonen (Position, Datensatz und Fingerfolge) und Bilddaten wurden nach einem bekannten Verfahren zu einem funktionsfähigen Fingerabdruck weiterverarbeitet. Nach Keyloggern, Mini-Videokameras und Skimming-Attrappen müssen wir uns möglicherweise bald auch nach Biodaten-Loggern umschauen.

Vorratsdatenspeicherung

Am 11.3.2008 entschied das Bundesverfassungsgericht im Eilverfahren über die Verfassungsbeschwerde von über 34.000 Beschwerdeführern gegen die mit der Änderung von TKG und StPO eingeführte Vorratsdatenspeicherung. Zwar setzte es nicht – wie von den Beschwerdeführern erhofft – die Speicherung selbst außer Vollzug, sondern verbot befristet bis zum 11.09.2008 lediglich die Datenherausgabe an die Strafverfolgungsbehörden.

Das Gericht verpflichtete die Bundesregierung zur Abfassung eines Berichts über die praktischen Auswirkungen der Sperrung. Damit traf das BVerfG keine Vorentscheidung über die Speicherung, sondern vermied zunächst nur etwaige negative Folgen für die Betroffenen im Falle einer späteren Feststellung der Verfassungswidrigkeit der Regelungen.

Secorvo News

Secorvo College aktuell

Einen tiefen Einblick in IT-Sicherheitsaudits in der Praxis bietet Secorvo College am **06.–08.05.2008**. Am **27.–30.05.2008** findet wieder der „aktuelle Klassiker" statt – IT-Sicherheit heute. Nur noch wenige Plätze gibt es für das TISP-Seminar, das Secorvo College am **02.–06.06.2008** mit anschließender Prüfung durchführen wird. Programm und Online-Anmeldung unter http://www.secorvo.de/college.

DuD 2008 – die zehnte

Für die diesjährige 10. Fachkonferenz „DuD 2008" am **09.–10.06.2008** in Berlin unter der fachlichen Leitung der Herausgeber der Zeitschrift „Datenschutz und Datensicherheit" konnten wieder spannende Vorträge gewonnen werden. Darunter finden sich die Themen Whistleblowing, Internet-Bewertungen von Lehrkräften, IT-Virtualisierung, das Audit-Gesetz, Computerkriminalität und das „Web 2.0". Burkhard Hirsch, Bundesinnenminister a.D., wird zu den gesellschaftlichen Folgen staatlicher Überwachung Stellung beziehen, Prof. Christof Paar seine Attacke auf Wegfahrsperren vorstellen und Jan Krissler vom Chaos Computer Club über die jüngsten Angriffe auf Biometrie-Systeme berichten.

Pimp your web

Am **29.05.2008** widmet sich die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) dem Schutz von Web-Applikationen. Maximilian Dermann von Lufthansa Technik wird vorstellen, wie diese sich insbesondere vor DoS-Angriffen schützen lassen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2008	
06.-07.05.	9. Datenschutzkongress 2008 (Euroforum, Berlin)
06.-08.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
26.-29.05.	IT Sicherheitsforum 2008 (GAI Netconsult, Frankfurt)
27.-30.05.	IT-Sicherheit heute (Secorvo College)
29.05.	Pimp your web (KA-IT-Si, Karlsruhe)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College)
09.-10.06.	DuD 2008 (Computas, Berlin)
17.-18.06.	6. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)
24.-25.06.	D-A-CH Security 2008 (GI/OCG/Bitkom/TTT, Berlin)
24.-26.06.	Sichere Softwareentwicklung (Secorvo College)
Juli 2008	
01.-03.07.	Forensik (Secorvo College)

Fundsache

Das freie E-Book „Security Concepts“ von Travis Howard, veröffentlicht am 12.04.2008, hat zwar mit 120 Seiten noch Projektcharakter, aber die übersichtliche Struktur, die Inhalte und insbesondere die starke Verlinkung zu externen Quellen machen das Werk zu einem lesenswerten Reiseführer für Sicherheitsinteressierte. Bemerkenswert ist der Versuch des Autors, zentrale und allgemeingültige Sicherheitsprinzipien herauszuarbeiten.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Mai 2008



Editorial: Geistige Brandstifter

Der 11. September 2001 wird uns nicht nur als der Tag eines schockierenden Massenmords in Erinnerung bleiben. Er wird auch als Wendepunkt in die Annalen der Inneren Sicherheit eingehen. Mit beispielloser Geschwindigkeit zauberten Sicherheitsbehörden westlicher Regierungen gleich welcher politischen Couleur in den darauffolgenden Monaten neue Sicherheitsgesetze aus den Schubladen, die ohne nennenswerten politischen oder öffentlichen Widerstand die demokratischen Entscheidungsgremien passierten. Auch bestehende Befugnisse wurden ausgeweitet. In Deutschland stieg die ohnehin schon rekordverdächtig hohe Zahl angeordneter Telekommunikationsüberwachungen rapide: sie verdoppelte sich seit 2001 auf knapp 45.000 Fälle. 2007 war es für einen Bundesbürger 74 mal so wahrscheinlich, abgehört zu werden, wie für einen Nordamerikaner.

Erst in den vergangenen Monaten regt sich nennenswerter öffentlicher Widerstand – gegen die Pläne einer Online-Durchsuchung, den biometrischen Personalausweis und die Vorratsdatenspeicherung; ermutigt vom Bundesverfassungsgericht, das die rechtsstaatlichen Grenzen staatlicher Überwachung in Erinnerung gebracht hat.

Schlimmer noch als die schleichende Ausdehnung von Überwachungsbefugnissen ist jedoch der Geist, den die scheinbar widerspruchsfreie Beschränkung bürgerlicher Freiheitsrechte gesät hat. So sollte es eigentlich niemanden wundern, dass in der herrschenden Atmosphäre des Misstrauens Verantwortliche in Unternehmen auf die Idee kommen, Mitarbeiter, Aufsichtsräte und Investoren zu überwachen. Das Bewusstsein der Strafbarkeit solcher Maßnahmen kann in einem politischen Kontext abhanden kommen, in dem Datenschutz als „Täterschutz“ diffamiert wird, Abschüsse von Linienflugzeugen, Online-Überwachung und Vorratsdatenspeicherung ohne Rücksicht auf elementare Grundrechte in Gesetze gegossen werden und Nachrichtendienste rechtswidrig Journalisten bespitzeln. Die geistigen Brandstifter – die sitzen in den Innenministerien.



Inhalt

Editorial: Geistige Brandstifter

Security News

WLAN-Missbrauch strafbar

Botnetz-Analyse

Schwerer Lotus Domino Bug

Verbindungsdatenauskünfte

Pseudozufall

Leitfäden zum “Hackerparagraf”

Malware mit Copyright

Firewire macht Feuer

Secorvo News

Secorvo College aktuell

Security Awareness Symposium

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

WLAN-Missbrauch strafbar

Erstmalig hat ein deutsches Gericht den Missbrauch eines ungeschützten privaten WLANs als Straftatbestand gewertet: Das Amtsgericht Wuppertal verurteilte in einem am 03.04.2008 publizierten Urteil (Az. 22 Ds 70 Js 6906/06) den „Schwarzsurfer" wegen unerlaubten Abhörens eines Funknetzes (§ 89 TKG) sowie nach § 44 BDSG wegen der widerrechtlichen Aneignung einer privaten IP-Adresse – die ihm der Router zugeteilt hatte. Die Strafe (20 Tagessätze) wurde zur Bewährung ausgesetzt, der Laptop des Täters jedoch als „Tatwerkzeug" eingezogen (NStZ 03/2008, S. 161 ff.). Auch wenn Kritik an der Rechtsauffassung des Gerichts angebracht erscheint, sollte man von der ungenehmigten Nutzung fremder WLANs tunlichst Abstand nehmen.

Botnetz-Analyse

Vitaly Kamluk, Virenanalyst bei Kaspersky Lab, veröffentlichte am 13.05.2008 eine lesenswerte Analyse über Botnetze. Neben einer systematischen Klassifizierung nach Architektur und verwendeten Netzprotokollen und einer anschaulichen Darstellung der Entwicklung der Botnetz-Technologie beleuchtet der Autor den gefährlichen Trend zu Peer-to-Peer-Botnetzen. Diese kommen ohne eine zentrale Kommandostelle aus, indem sie Befehle mit ihren „Nachbarn" austauschen. Besonders das „Sturmwurm"-Botnetz (SSN 08/2007) stellt eine erhebliche Bedrohung dar, da es sich über stündlich neue Mutationen verbreitet und bis zu seinem Einsatz unauffällig und „ruhig" verhält.

Die Analyse, die bei Kaspersky Lab auch als pdf-Datei heruntergeladen werden kann, schließt mit der Veranschaulichung einiger Geschäftsmodelle der „Botnetz-Industrie". Die zunehmende Professionalisierung von Konzeption, Infizierung und Steuerung von Zombie-PCs über Botnetze belegt, dass mit der Nutzung von Bots Geld verdient werden kann. Austrocknen lässt sich dieser Cyber-Sumpf nur an den Wurzeln: den Löchern in Systemen, die die Einnistung von Bots erst ermöglichen.

Schwerer Lotus Domino Bug

Am 20.05.2008 meldete MWR InfoSecurity einen Stack Overflow für IBMs Lotus Domino Web Server, der einem Angreifer die Ausführung beliebigen Codes unter System-Privilegien erlaubt – und der via Fernzugriff ausgelöst werden kann. Nachgewiesen wurde der Bug für die Versionen 7.0.3 und 8.0; mit hoher Wahrscheinlichkeit sind auch ältere Versionen betroffen. IBM hat passende Update-Patches bereitgestellt. Wer einen Lotus Domino Web Server im Internet betreibt sollte schnell reagieren.

Verbindungsdatenauskünfte

Neben den Inhalten unterliegen auch die „näheren Umstände" der Telekommunikation (Wer? Wo? Mit wem? Wann? Wie lange?), „Verbindungsdaten" genannt, dem Fernmeldegeheimnis (§ 88 TKG). Dessen Verletzung ist eine Straftat (§ 206 StGB) und kann mit bis zu fünf Jahren Freiheitsstrafe geahndet werden. Ausnahme: Strafverfolgungsbehörden dürfen im Zusammenhang mit Straftaten von „im Einzelfall erheblicher Bedeutung" (insbesondere die „Katalogstraftaten" des § 100a Abs. 2 StPO) auch ohne Wissen des Betroffenen Verkehrsdaten erheben (§ 100g StPO).

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat am 13.02.2008 ihre knapp 500 Seiten starke, im Auftrag des BMJ erstellte Langzeitstudie zur „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO" vorgelegt. Danach ist die Zahl der Verkehrsdatenabfragen in den vergangenen Jahren explodiert: Waren es im Jahr 2000 noch 5.000, stieg die Anzahl 2005 auf das Achtfache (40.000 Abfragen). Eine wachsende Rolle spielen dabei offenbar Standort- und Funkzellenabfragen (18% bzw. 10%), mit denen der Aufenthaltsort Verdächtiger ermittelt werden kann – oder auch alle Personen, die sich zum Tatzeitpunkt mit eingeschaltetem Handy in einer bestimmten Funkzelle aufhielten.

Mängel stellt die Untersuchung insbesondere bei der Benachrichtigung der Betroffenen fest: lediglich in 4% der Fälle war die Benachrichtigung in den Akten dokumentiert; die Vernichtung der Daten konnte nur in 3% der untersuchten Verfahren den Akten entnommen werden. Wer mag sich da noch wundern, dass die derzeit vor dem Bundesverfassungsgericht verhandelte Vorratsdatenspeicherung von Verbindungsdaten Befürchtungen weckt?

Pseudozufall

Am 13.05.2008 veröffentliche das Debian Projekt eine korrigierte Version des OpenSSL-Packets, da alle OpenSSL-Versionen seit September 2006 (Versionen 0.9.8c-1 bis 0.9.8g-9) auf Debian-Distributionen wie Ubuntu kompromittierbare kryptografische Schlüssel erzeugen. Ursache: Die Funktion, die für zufällige Startwerte im Zufallszahlengenerator sorgen sollte, war im Quellcode auskommentiert. Der Zufallszahlengenerator nutzte daher die Linux Prozess ID als Zufallswert, die nur 32.767 mögliche

Werte annehmen kann. Daher lassen sich die geheimen Schlüssel von u.a. SSL, SSH, DNSSEC sowie X.509-Zertifikaten via Brute-Force-Angriff finden. Betroffen sind alle Programme, die OpenSSL zur Erzeugung kryptografischer Schlüssel verwenden, darunter Apache, Sendmail, Exim und OpenVPN.

Zweck der nicht mit dem OpenSSL-Entwicklungsteam abgestimmten Auskommentierung durch den Debian OpenSSL Maintainer war die Unterdrückung von Fehlermeldungen, die das Softwareanalysewerkzeug valgrind festgestellt und fälschlich als Softwarefehler interpretiert hatte. Da kommt der Draft der NIST-Publikation SP 800-108 „Recommendation for Key Derivation Using Pseudorandom Functions“ vom 01.05.2008 leider zu spät: Jetzt müssen zahlreiche Schlüssel getauscht werden – ein gutes Geschäft für Certificate Authorities.

Leitfäden zum “Hackerparagraf”

Am 17.04.2008 hatte die EICAR einen von Christian Hawellek und Dennis Jlussi von der Universität Hannover entwickelten Leitfaden zur strafrechtlichen Relevanz von IT-Sicherheitsaudits veröffentlicht, der Empfehlungen zur Durchführung von Audits im Kontext des neuen § 202c StGB (der „Hackerparagraf“, siehe SSN 07/2007) zusammenfasst. Er geht unter anderem ausführlich auf die Gestaltung von Einverständniserklärungen zur Vermeidung von Strafbarkeitsrisiken ein. Ebenfalls 16 Seiten umfasst der am 23.05.2008 vom Bitkom publizierte Praktische Leitfaden für die Bewertung von Software im Hinblick auf den § 202c, StGB. Neben einer Kriterienliste zur Beurteilung, ob eine Software unter die Bestimmungen des § 202c fällt, schlägt der Leitfaden „Best Practice“-Regelungen für den Umgang mit „Dual-Use“-Software im Unternehmen vor. Beide enthalten vernünftige Empfehlungen zur Absicherung, insbesondere im Falle einer externen Durchführung von IT-Sicherheitsaudits.

Malware mit Copyright

Am 25.04.2008 veröffentlichte Liam O. Murchu im Symantec Security Response Blog beispielhaft die Copyright- und Lizenzhinweise der ZeuS-Crimeware – eines russischen Malware-Construction-Kits zum Aufbau von Botnetzen. Darin droht der „Anbieter“ damit, jede nicht vertragskonforme Nutzung durch die Versendung der Signatur der spezifischen Binärdatei an führende Antiviren-Hersteller zu unterbinden. Eine interessante Rolle für die AV-Industrie – Copyright Enforcement für Schadsoftware-Baukästen. Möglicherweise kann sie sich dieser Rollenzuweisung nicht einmal entziehen.

Firewire macht Feuer

In der Theorie ist es ein alter Hut: Schon am 30.09.2006 hatte Adam Boileau auf der damaligen Ruxcon über Angriffe via Firewire vorgetragen. Seine ausführliche Präsentation „Hit by a bus: Physical Attacks with Firewire“ wurde damals von einer Live-Demo begleitet. Knapp zwei Jahre später nun unterlegt er seine akademische Attacke mit einem „Proof of concept“: Anfang März 2008 stellte Boileau das Tool winlockpwn auf seiner Website zur Verfügung. Mit diesem Tool kann von einem via Firewire verbundenen Computer ein Login an einem Rechner unter Windows XP (SP2) als Administrator erzwungen werden. Die erschreckende Eleganz dieses Angriffs lässt sich auf YouTube bewundern. Boileau nutzt dabei die Eigenschaft der Firewire-Schnittstelle, den Speicher des angeschlossenen Rechners direkt zu adressieren – und ihm so z.B. eine modifizierte DLL unterzuschieben.

Die Existenz von winlockpwn fordert in vielen Bereichen das Überdenken existierender Sicherheitskonzepte. Beispielhaft sei hier der – nicht zu empfehlende – Einsatz von Festplattenvollverschlüsselungslösungen ohne „Pre Boot Authentication“ genannt.

Secorvo News

Secorvo College aktuell

Die Nachfrage nach dem TISP-Zertifikat wächst ungebrochen: Schon weit über 200 deutsche Security Professionals dürfen sich mit diesem Titel schmücken, und 2008 werden voraussichtlich weitere 100 Absolventen das Zertifikat erwerben. Noch zwei letzte freie Plätze für Kurzentschlossene gibt es auf dem TISP-Seminar am **02.–06.06.2008**.

Die nächste Gelegenheit zur TISP-Zertifizierung bietet College nach der Sommerpause vom **08.–12.09.2008**. Vorher führt College vom **01.–03.07.2008** noch mit einem dreitägigen Seminar in die Durchführung von forensischen Analysen ein.

Security Awareness Symposium

Vom 17.-18.06.2008 findet das sechste „Security Awareness Symposium“ statt, das sich zum jährlichen Treffpunkt von Security-Awareness-Verantwortlichen entwickelt hat. Auf dem von Secorvo zusammen mit den E-Learning-Experten von digital spirit und der Agentur DauthKaun veranstalten Symposium in den stilvollen Räumen der Buhlschen Mühle in Ettlingen werden unter anderem die Erfahrungen der Münchener Rück, SAP, T-Systems und MDS vorgestellt und diskutiert.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2008	
29.05.	Pimp your web (KA-IT-Si, Karlsruhe)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College)
09.-10.06.	DuD 2008 (Computas, Berlin)
17.-18.06.	6. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)
24.-25.06.	D-A-CH Security 2008 (GI/OCG/Bitkom/TTT, Berlin)
24.-26.06.	Sichere Softwareentwicklung (Secorvo College)
Juli 2008	
01.-03.07.	Forensik (Secorvo College)
10.-11.07.	DIMVA 2008 (GI)
28.07.-1.08.	17th USENIX Security Symposium 2008 (San José/US)
August 2008	
17.-21.08.	Crypto 2008 (IACR, Santa Barbara/US)

Fundsache

Symantec hat am 08.04.2008 den 13. „Global Internet Thread Report" für den Sechsmonatszeitraum Juli bis Dezember 2007 publiziert. Er enthält eine umfangreiche Analyse der Entwicklung aktueller Bedrohungen durch Malware, Botnetze und sicherheitskritische Softwarefehler. Explodiert ist die Menge bösartigen „Malicious Code": Gegenüber dem Vorjahreszeitraum hat sich deren Zahl auf 500.000 mehr als versechsfacht.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Kai Jendrian, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Juni 2008



Editorial: Reden ist Silber

Schweiger erfreuen sich in westlichen Gesellschaften eines guten Rufs. Wer wenig redet, den umgibt der Nimbus des Vergeistigten – denn „Stille Wasser sind tief", wie der Volksmund weiß. Oder er gilt gar als weise: Von Ernest Hemingway (1899-1961) ist der Ausspruch überliefert, man brauche „zwei Jahre, um sprechen zu lernen, und fünfzig, um schweigen zu lernen". Zumeist gilt Schweigen als ein Indiz für Nachdenken – wenigstens bis zum Beweis des Gegenteils: „Wo Männer schweigen, reden die Gedanken" (Carl Spitteler, 1845-1924).

Nicht immer aber stimmt das Klischee. Denn Schweigen kann auch mehr Schein als Sein verbergen. Das wird oft erst deutlich, wenn sich ein stilles Wasser als seichte Pfütze outet. Ein fast 1.500 Jahre altes Bonmot belegt die lange Tradition des Schweigens als potemkinsches Dorf: „Si tacuisses, philosophus mansisses" reimte der Philosoph Boethius (ca. 475–525 n. Chr.) – „Hättest Du geschwiegen, wärst Du Philosoph geblieben." Die Motivation des taktischen Schweigens hat der französische Schriftsteller François Duc de La Rochefoucauld (1613-1680) auf den Punkt gebracht: „Schweigen ist der beste Ausweg für den, der seiner Sache nicht sicher ist." Bei hartnäckigem Schweigen ist daher Vorsicht angeraten.

Die Geschichte der Kryptographie kennt unzählige Beispiele für dünne Bretter, die allein durch Schweigen hielten: Crypto-1 (Mifare) und KeeLoq sind zwei der jüngsten. Auch wenn es immer wieder behauptet wird: Die Sicherheit eines (Krypto-)Verfahrens steigt nicht durch Verschweigen. Im Gegenteil: „Security by Obscurity" erhöht das Risiko eines schlagartigen Sicherheitsverlustes, falls das Verfahren bekannt wird. Immer wieder bestätigt sich der von Auguste Kerckhoffs vor 125 Jahren in „La Cryptographie Mililtaire" formulierte Fundamentalsatz der modernen Kryptographie: Die Sicherheit eines kryptographischen Mechanismus' darf nur von der Geheimhaltung des Schlüssels abhängen. Oder kurz: Reden ist Silber. Schweigen ist ... Mist. Zumindest in der Kryptographie.



Inhalt

Editorial: Reden ist Silber

Security News

OpenSSL Nachwehen

ISO-Risikomanagement

Cisco Rootkits

Automatische Exploits

PTK Forensics

Exponierte Leittechnik

Reaktorabschaltung per Patch

Nessus-Lizenz

Secorvo News

Secorvo College aktuell

Team(ver)stärkung

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

OpenSSL Nachwehen

Die meisten Probleme des am 13.05.2008 bekannt gewordenen Sicherheits-Desasters von OpenSSL in Debian-basierten Linux-Distributionen sind umfänglich beschrieben und diskutiert worden (siehe auch SSN 05/2008). Möglicherweise betroffene Server-Schlüssel können seit dem 09.06.2008 mit dem SSL-Online-Check des Heise-Verlags überprüft werden.

Auf ein etwas vernachlässigtes Risiko wollen wir jedoch hinweisen: Auch Schlüssel, die auf Systemen erzeugt wurden, die von der OpenSSL-Problematik nicht betroffen waren, müssen als kompromittiert gelten, wenn sie auf einem betroffenen System zur Public-Key-Authentifizierung mit DSA, wie z. B. bei SSH, eingesetzt wurden. DSA benötigt zum Signieren eine vom Client-System erzeugte Zufallszahl, die geheim bleiben muss. Mit Kenntnis dieser Zufallszahl kann mit einfacher Mathematik in wenigen Schritten der private Schlüssel aus einer veröffentlichten DSA-Signatur herausgerechnet werden. Noch einfacher ist es bei einem Diffie-Hellman-Schlüsselaustausch: Die kleine Menge möglicher Zufallszahlen auf einem betroffenen Client erlaubt es einem Angreifer, mit begrenztem Aufwand den Session-Key aus mitgeschnittenen SSH-Sessions zu gewinnen.

ISO-Risikomanagement

Mit dem am 04.06.2008 veröffentlichten Standard ISO/IEC 27005:2008 "Information technology – Security techniques – Information security risk management" hat die ISO die Normenreihe ISO/IEC 2700x um einen wichtigen Baustein ergänzt. Neben einer verallgemeinerten Herangehensweise an das Thema Risikomanagement werden darin wesentliche Prozessschritte wie beispielsweise die Risiko-Identifikation, -Bewertung und -Akzeptanz beschrieben und konkrete Hilfestellung zur Anwendung gegeben. Der neue Standard konkretisiert damit die Anforderungen an das Risikomanagement aus ISO/IEC 27001:2005.

Cisco Rootkits

Am 22.05.2008 stellte Sebastian Muniz auf der EuSecWest in London ein funktionsfähiges Rootkit für Cisco IOS vor. Dessen Wirksamkeit wurde inzwischen durch eine offizielle Stellungnahme des Herstellers bestätigt. Einen Tag zuvor hatte Cisco drei außerplanmäßige Patches veröffentlicht, die mit der IOS-Rootkit-Thematik zusammenhängen dürften. Insbesondere der Cisco IOS SSHService Denial of Service-Fehler wird als reengineer-bar eingestuft, daher sollte mit Angriffen auf diese Schwachstelle gerechnet werden. Wir empfehlen, betroffene Systeme umgehend zu patchen.

Automatische Exploits

David Brumley, Pongsin Poosankam, Dawn Song, und Jiang Zheng veröffentlichten am 18.04.2008 einen Ansatz zur automatischen Erzeugung von Exploits aus Patches. Die Kernidee: Sie vergleichen das gepatchte mit dem ursprünglichen Programm. Identifizieren sie dabei beispielsweise eine Input-Validierung, so erzeugen sie daraus Angriffscode, der gegen genau diese Validierung verstößt – und können nun jedes ungepatchte System attackieren. Zwar lassen sich mit diesem Ansatz (noch) nicht alle Exploits zu jedem Patch finden; für ausgewählte Microsoft-Patches konnten sie jedoch in weniger als 30 Sekunden funktionsfähige Exploits gewinnen. Sollte dieser Ansatz weiter entwickelt werden, könnten Hersteller und Anwender in Zugzwang geraten und müssten sich um geeignete Gegenmaßnahmen und zügigeres Patchen bemühen.

PTK Forensics

Seit dem 30.05.2008 läuft der öffentliche Beta-Test für PTK – eine neue, völlig überarbeitete graphische Benutzeroberfläche für das altehrwürdige Forensik-Tool The Sleuthkit (TSK). Dabei handelt es sich nicht bloß um eine aktuellere Version der bereits etwas in die Tage gekommenen Sleuthkit-Benutzeroberfläche Autopsy. Die Entwickler der italienischen DF LABS srl wollten vielmehr komplett neue Funktionen zur Verfügung stellen.

Wir haben das Tool einem ausgiebigen Test unterzogen. Vor der eigentlichen Analyse extrahiert die neue "Indexing Engine" Textpassagen, sucht nach bekannten Dateitypen, führt File-Carving durch, berechnet bei Bedarf kryptographische Prüfsummen und legt die Ergebnisse in einer SQL-Datenbank ab. Anschließend kann der Forensiker über eine Ajax-basierte Web-Schnittstelle auf zahlreiche Funktionen zugreifen. Dabei überzeugen Features wie die "Gallery", die eine Vorschau auf gefundene Bilder erlaubt, oder eine nützliche "Bookmark"-Funktion zur Hervorhebung wichtiger Suchtreffer.

Der Beta-Test läuft bis September 2008. Da es gelegentlich zu Fehlermeldungen kommt und noch nicht alle Funktionen aus TSK und Autopsy implementiert sind, stellt PTK zur Zeit noch keinen vollwertigen Ersatz dar.

Exponierte Leittechnik

Nun ist es ja nicht so, dass analoge Leittechnik unangreifbar wäre: Ein durchgetrenntes Kabel kann die Verfügbarkeit von Anlagen gefährden, und das

Drehen an einem Potentiometer könnte Signale verfälschen. Allein der Umstand, dass man hierzu einen physikalischen Zugriff vor Ort benötigt, erschwert derartige Angriffe erheblich. Anders sieht es dagegen bei der digitalen Leittechnik aus: Durch TCP/IP verbundende Systeme können über hunderte von Kilometern hinweg beeinflusst werden.

Schutz bieten hier durchdachte Netzwerk-Zonenkonzepte und entsprechend restriktiv konfigurierte Firewalls. Dass es daran gelegentlich mangelt, zeigen die Feststellungen der US-amerikanischen Überwachungsbehörde Government Accountability Office (GOA) bei einem der größten Energieversorger, der Tennessee Valley Authority (TVA); nachlesbar in einem Prüfbericht vom 21.05.2008. Darin werden unter anderem Verbindungen zwischen Anlagennetzen und Office-Netzsegmenten und zu offen konfigurierte Firewallsysteme bemängelt. Kein Wunder, dass in den USA die Angst vor einem Hacker-Angriff auf die Energieversorgung umgeht.

Reaktorabschaltung per Patch

Am 05.06.2008 wurde ein peinlicher Zwischenfall in einem amerikanischen Atomkraftwerk bekannt: Ein Service-Techniker hatte im Kraftwerk Hatch auf einem PC im Office-Netzsegment ein Update installiert, das durch eine fehlerhafte Synchronisierung Daten auf einem Kontrollsystem im Anlagennetz löschte. Die fehlenden Daten wurden von den Schutzsystemen des Reaktors als zu niedriger Kühlwasserstand interpretiert – und daher eine Notabschaltung ausgelöst, so die Darstellung im NRC-Bericht (Nuclear Regulatory Commission).

Zwar ist zu hoffen, dass ein solcher Vorfall in einem deutschen Kraftwerk nicht möglich wäre. Aber beunruhigend ist auch schon die Vorstellung, dass ein einfaches Systemupdate solche Aktionen auslösen kann – selbst bei einem 7.400 km entfernten Kernkraftwerk.

Nessus-Lizenz

Der Security-Scanners Nessus, einstmals Open Source, seit 2005 als Closed Source weiterentwickelt (vgl. SSN 02/2005), erfreut sich auch in Unternehmen großer Beliebtheit. Mit dem bisherigen Nutzungsmodell, nach dem Updates und Plugins mit etwas Verzögerung kostenfrei zum Download bereitgestellt wurden, ist es für den kommerziellen Einsatz am 31.07.2008 vorbei: In einem Schreiben informierte der Hersteller Tenable registrierte Nutzer am 14.05.2008 über die bevorstehenden Änderungen der Lizenzbedingungen.

Ab dem 01.08.2008 ist nur noch die private Nutzung kostenfrei. Auf die Reaktion der Nessus-Fangemeinde darf man gespannt sein. Vielleicht hätte Tenable lieber die Reaktion des Marktes auf die am 06.06.2008 angekündigte 33%ige Preiserhöhung des Kultgetränks Bionade (um sich so „von seinen Nachahmern abzusetzen“) abgewartet – schließlich lernt man immer am billigsten aus den Fehlern anderer. Die Kommerzialisierung von Nessus dürfte dem vom BSI unterstützen und am 21.05.2008 auf dem LinuxTag 2008 vorgestellten Projekt OpenVAS Vortrieb leisten: einem auf Basis der letzten frei verfügbaren Quellen von Nessus entwickelten kostenfreien Security-Scanner.

Secorvo News

Secorvo College aktuell

Vom **01.–03.07.2008** entführen Stefan Kelm, Stefan Gora und Jochen Schlichting in die Tiefen der Forensik – inklusive praktischer Übungen an elementaren Tools und einer Einführung in den rechtlichen Kontext. Der Termin ist seit einigen Wochen ausgebucht – die nächste Gelegenheit zur Teilnahme bietet sich am **11.–13.11.2008**. Interessierten empfehlen wir eine frühzeitige Anmeldung.

Das Programm des zweiten Halbjahrs beginnt nach der Sommerpause mit einer T.I.S.P.-Schulung vom **08.–12.09.2008** mit anschließender Zertifizierung. Die große Nachfrage nach dem T.I.S.P.-Zertifikat lässt erwarten, dass sich die Zahl der Absolventen in 2008 erneut verdoppelt.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Team(ver)stärkung

Das Secorvo-Team ist zum 01.06.2008 weiter gewachsen: Alexander Göbel – T.I.S.P., CISM, CISO und BSI-zertifizierter Audit-Teamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz – bringt vieljährige Erfahrung aus dem IT-Risk-Management eines DAX-Unternehmens und der Zertifizierung eines Rechenzentrums nach ISO 27001 auf der Basis von IT-Grundschutz mit. Neben allen Facetten des Sicherheitsmanagements ist der betriebliche Datenschutz eines seiner Schwerpunktthemen.

Ebenfalls gewachsen ist die inzwischen lange Liste der Zertifizierungen der Secorvo-Consultants: Petra Barzin erhielt die Zertifizierung als CISSP, und Jochen Schlichting darf neben seinen Zertifizierungen als CISA und CISSP nun auch das CISM-Zertifikat (Certified Information Security Manager) der ISACA führen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2008	
01.-03.07.	Forensik (Secorvo College)
10.07.	Die Mifare-Attacke und andere Krypto-Desaster (KA-IT-Si, Karlsruhe)
10.-11.07.	DIMVA 2008 (GI, Paris)
28.07.-01.08.	17th USENIX Security Symposium 2008 (Usenix, San José/US)
August 2008	
17.-21.08.	Crypto 2008 (IACR, Santa Barbara/US)
September 2008	
07.-10.09.	OSSCoNF 08 (IFIP, Mailand)
08.-12.09.	T.I.S.P.-Schulung (Secorvo College)
23.-25.09.	IMF 2008 (GI, Mannheim)
23.-26.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2008	
07.-10.10.	IT-Sicherheit heute (Secorvo College)

Fundsache

Am 09.05.2008 veröffentlichte die schweizerische Melde- und Analyse-stelle Informationssicherung (Melani) den Halbjahresbericht 2007/2, der die Entwicklung der Gefährdungslage in der Schweiz und international beleuchtet. Als Beispiel wird ein sehr professioneller Phising-Angriff auf Systeme der Schweizer Bundesverwaltung detailreich dargestellt – der die Grenzen des etablierten Virenschutzes aufzeigte.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Juli 2008

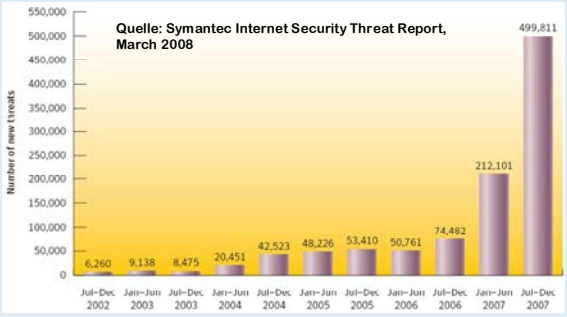


Editorial: Geburtstagstorte

Wer Kinder hat, kennt Pettersson und Findus – den alten, schrulligen, liebenswerten Bauern mit seinem quirligen sprechenden Kater in grüner Hose, detailreich gezeichnet von Sven Nordqvist. „Eine Geburtstagstorte für die Katze“ heißt das 1984 erschienene erste Bilderbuch der Kultserie. Die Geschichte ist fix erzählt: Findus beschließt, Geburtstag zu haben – denn dann gibt es Pfannkuchentorte. Das ist jedoch leichter gesagt als getan: Das Mehl ist ausgegangen, und das Fahrrad hat einen Platten. Pettersson muss es reparieren, bevor er zum Einkaufen fahren kann – das Werkzeug aber liegt im verschlossenen Schuppen, und den Schlüssel entdeckt Findus im Brunnen. Um ihn herauszufischen braucht er die Angel vom Dachboden, aber an der Leiter lehnt ein schlafender Stier. Also muss Findus mit einer Gardine den Matador geben, reißt aber dabei den Eierkorb um.

Natürlich kommt der Kater doch noch zu seiner Geburtstagstorte. Aber das war jedenfalls für meine Kinder ganz unwichtig – gebannt verfolgten sie die immer neuen Widrigkeiten und deren kreative Beseitigung. Der Umweg war das Ziel, und die Torte bestenfalls die Belohnung für die erfolgreiche Problemlösung.

Sehr ähnlich müssen die Autoren von Malware empfinden. Wie anders ist zu erklären, dass sie sich weder von immer besseren Schutzmaßnahmen noch von schärferen Strafgesetzen abschrecken lassen? Statt dessen ersinnen sie raffiniertere Angriffsmethoden. Offenbar spornt der Widerstand an, das belegen die Zahlen. Und dahinter steht heute meist ein Investor, der auf die Torte scharf ist.





Inhalt

Editorial: Geburtstagstorte

Security News

BSI-Krypto-Richtlinie

Survival of the Fittest

Schlecht versteckt

Evilgrade

CrypTool 1.4.2x

BSI-Standards 2.0

Bluetooth Security

Link-Prefetching im Firefox

WAF-Pflicht

Secorvo News

Secorvo College aktuell

Symposium Wirtschaftsspionage

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

BSI-Krypto-Richtlinie

Seit Inkrafttreten des deutschen Signaturgesetzes vor mehr als 10 Jahren erstellt das BSI jährlich eine aktuelle Übersicht geeigneter kryptographischer Algorithmen und Schlüssellängen für digitale Signaturen. Verschlüsselungsverfahren spielen darin naturgemäß keine Rolle – gleichwohl sind sie in der Praxis viel verbreiteter als digitale Signaturen.

Mit der Veröffentlichung einer technischen Richtlinie „Kryptographische Verfahren: Algorithmen und Schlüssellängen“ (TR 02102) hat das BSI am 20.06. 2008 nun auch bei Verschlüsselungsverfahren, Authentisierungsmechanismen, Zufallszahlengeneratoren und Schlüsselvereinbarungsprotokollen Farbe bekannt. Eine wertvolle Orientierung für die Praxis.

Survival of the Fittest

Am 14.07.2008 veröffentlichte Torsten Holz in seinem Blog die Ergebnisse einer 12monatigen Honeynetanalyse zur Überlebenszeit ungepatchter IT-Systeme. Untersucht wurde die Dauer einer erfolgreichen Kompromittierung durch autonome Malware, die alte, lange bekannte Schwachstellen ausnutzen. Ergebnis: Im Schnitt überlebt ein System ca. 12 Minuten, etwas länger als die vom Internet Storm Center gemessenen knapp fünf Minuten.

Die Analyse, die auf den Vorarbeiten von Laura Itzel aufbaut, weist eine erhebliche Abhängigkeit der Überlebenszeit vom jeweiligen Internet Service Provider nach: ISPs, die bevorzugt von Malware genutzte Ports sperren, erhöhen die Überlebenszeit angeschlossener Systeme um ein Vielfaches. Angesichts des deutlich größeren Zeitfensters zwischen Bekanntwerden einer Schwachstelle und Verfügbarkeit des Patches („Window of Exposure“) erscheint es jedoch in keinem Fall angeraten, eine Internet-Verbindung ohne gut konfigurierte Personal Firewall aufzubauen.

Schlecht versteckt

Dass Blicke über den Tellerrand auch in der Kryptographie wichtig sind, belegt eine Arbeit, die Forscher der University of Washington zusammen mit Bruce Schneier am 29.07.2008 auf einem USENIX Workshop vorgestellt haben. Darin untersuchten sie die Sicherheit von „Deniable File Systems“, mit deren Hilfe die Existenz verschlüsselter Daten verschleiert werden soll – beispielsweise mit „Hidden Volumes“ des Verschlüsselungstools TrueCrypt. Aber auch versteckte Dateisysteme hinterlassen im Betriebssystem unvermeidlich Spuren, wenn sie aktiviert werden, z. B. als kürzlich geöffnete „Recent Items“. Im schlimmsten Fall findet sich, lange nach der Deaktivierung des „Hidden Volumes“, Klartext-Inhalt einer versteckten Datei im Cache von Google-Desktop.

Was des einen Leid, ist des anderen Freud’ – die Forensiker reiben sich die Hände. Einige der aufgedeckten Probleme wurden in der am 06.07.2008 erschienenen Version 6 von TrueCrypt behoben.

Evilgrade

Am 28.07.2008 veröffentlichte Francisco Amato das Framework Evilgrade. Der Schadsoftware-Baukasten nutzt als Verbreitungsmechanismus verbreitete Updatemechanismen und tarnt sich als automatischer Patch. Derzeit werden u.a. Java Plugins, Winzip, Winamp und iTunes simuliert; Schadcode kann für beliebige Zielplattformen ergänzt werden. Die Integration der am 08.07.2008 von Dan Kaminsky publizierten DNS Cache Poisoning Variante in das Metasploit-Attackframework vereinfacht die Anwendbarkeit von Evilgrade erheblich – und macht es sehr gefährlich: Fast alle DNS-Server waren bzw. sind ohne aktuelle Updates von dieser Schwäche betroffen. Wer nicht Teil des Problems sein möchte, sollte schnell patchen.

CrypTool 1.4.2x

Fast genau ein Jahr nach der Veröffentlichung von Version 1.4.10 ist am 11.07.2008 CrypTool als neues Release 1.4.21 erschienen. Neben vielen kleinen Korrekturen und akribischer Detailpflege an Bedienungsfreundlichkeit und Dokumentation wurden der Passwort-Qualitätsmesser optimiert und die Hashfunktionenfamilie SHA-2 integriert. Der Passwort-Generator erzeugt zufällige Passworte aus einem voreinstellbaren Alphabet – auch für WLANs.

Besonders erwähnenswert ist die jüngste Auszeichnung des Open Source Projekts: In einer Festveranstaltung wurde CrypTool am 22.07.2008 an der Uni Siegen im Rahmen der Kampagne „Deutschland Land der Ideen“ als „Ausgewählter Ort 2008“ ausgezeichnet.

BSI-Standards 2.0

Am 23.06.2008 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die zweite Auflage der überarbeiteten BSI-Standards 100-1 „Managementsysteme für Informationssicherheit“, 100-2 „IT-Grundschutz-Vorgehensweise“ und 100-3 „Risikoanalyse auf Basis von IT-Grundschutz“ veröffentlicht. Diese drei Standards bilden die Grundlage für den nach ISO 27001 ausgerichteten IT-Grundschutz. Die Neuauflage verschiebt den Blickwinkel von der reinen IT-Sicherheit zur Informationssicherheit; außerdem wurden die Standards um Datenschutzaspekte erweitert. Und schließlich wurde die

Fortschreibung der relevanten ISO-Standards der 2700x-Reihe berücksichtigt. Der neue BSI-Standard 100-4 zum Notfall-Management liegt nach wie vor nur als Entwurf vor.

Bluetooth Security

Zwar ist Bluetooth schon lange keine neue Technik mehr – kaum ein IT-Gerät, das etwas auf sich hält, kommt noch ohne daher. Und obwohl Security-Mechanismen und potentielle Schwachstellen schon lange dokumentiert sind, kommt es immer wieder zu fehlerhaften Implementierungen – Handys, die sich via Bluetooth Malware einfangen oder ferngesteuert werden können, oder Headsets, die aus der Ferne als Überwachungsmikrofon missbraucht werden können. Mit den 2004 und 2005 entwickelten Tools der trifinity-Gruppe – darunter Bluebug, Bluesnarf, Blueprint, Bluedump und Car Whisperer – ist das bei betroffenen Systemen ein Kinderspiel.

Nun hat offenbar auch das US-amerikanische NIST gemerkt, dass hier ein reales Risiko steckt und am 09.07.2008 einen Guide to Bluetooth Security (Draft SP 800-121) publiziert – mit der Bitte um Kommentierung bis 22.08.2008. Eine nette Urlaubslektüre ...

Link-Prefetching im Firefox

Nicht neu, aber nicht überall bekannt: Im Mozilla-Browser Firefox ist die Funktion Link-Prefetching in den Voreinstellungen aktiviert. Webseiten, die diese Funktion zum Einbinden von Links verwenden, sorgen dafür, dass die Inhalte der Links schon im Voraus geladen werden, ohne dass der Nutzer den Link angeklickt hat – in der Regel merkt er davon nicht einmal etwas.

Dafür liegt der möglicherweise rechtswidrige Inhalt der verlinkten Seite im Cache. Auch aus Sicherheitsperspektive ist diese Funktion nicht unbedenklich: Da sich Trojaner angesichts immer wirksamerer Spam- und Virenscanner in wachsendem Umfang über präparierte Webseiten statt per E-Mail verbreiten, können Angreifer Prefetching-Links auf eine einzige mit Schadcode versehene Webseite auf vielen unzureichend geschützten Seiten Dritter verstecken und so zahlreiche Systeme unbemerkt infizieren. Vorteil für den Angreifer: Schadcode-Updates muss er nur auf einer Webseite einspielen, und zur Spurenverwischung genügt die Entfernung genau dieses Codes. Abhilfe ist jedoch einfach: Zum Deaktivieren muss unter der URL „about:config“ der Wert des Parameters „network.prefetch-next“ durch Anklicken von true auf false gesetzt werden.

WAF-Pflicht

Die Anforderungen des Payment Card Industry (PCI) Data Security Standard V.1.1 vom 15.04.2008 an den Schutz von Web-Applikationen (Abschnitt 6.6) sind seit dem 30.06.2008 keine Empfehlung mehr, sondern eine verbindliche Vorgabe: Code-Reviews, eine automatisierte Schwachstellen-Analyse und die Nutzung von Web Application Firewalls (WAF) sind nunmehr Pflicht. Ein ergänzendes Dokument des PCI Security Standards Council erläutert die Anforderungen stichwortartig auf wenigen Seiten – für einige Anbieter sicher eine Herausforderung.

Secorvo News

Secorvo College aktuell

Nach der Sommerpause startet das Programm von Secorvo College am **08.–12.09.2008** mit einer T.I.S.P.-Schulung in das zweite Halbjahr – gefolgt von einer komplett unabhängigen Zertifikats-Prüfung durch iSQI am 13.09.2008 in den Räumen von Secorvo. Es folgt ein Klassiker in aktuellem Gewand: PKI – Grundlagen, Vertiefung, Realisierung am **23.–25.09. 2008** – baldige Anmeldung empfohlen.

Schon jetzt möchten wir Sie auf unser Forensik-Seminar vom **11.–13.11.2008** hinweisen. Die „Premiere“ im Juli war ausgebucht – und wurde von den Teilnehmern euphorisch gelobt („Mit dem Seminar hat sich Secorvo selbst übertroffen. (...) Ich kann jedem, der mit IT-Security zu tun hat, dieses Seminar nur wärmstens empfehlen. Drei Tage voller Information, Spannung, Überraschungen, Aha-Effekte und optimaler Mischung aus Theorie und Praxis.“ – Matthias Grund, Siemens AG).

Termine, Programme und Online-Anmeldung unter http://www.secorvo.de/college

Symposium Wirtschaftsspionage

Schutzmassnahmen gegen die ungezielte Bedrohung durch Schadsoftware und Hacker sind bei Unternehmen heute eine Selbstverständlichkeit. Seit etwa zwei Jahren belegen Studien jedoch einen unheilvollen Trend: Im Schatten wachsender Spam- und Trojaner-Wellen nehmen gezielte Spionageattacken zu – nicht nur unter Nutzung technischer Hilfsmittel.

Das "Symposium Wirtschaftsspionage" von Econo und Secorvo wird sich am **03.09.2008** diesem Thema widmen. Ulf Tietge, Chefredakteur von Econo, wird das Symposium moderieren, auf dem sowohl Fachexperten (u. a. Dr. Udo Ulfkotte und Hans Schlumpberger vom Landesamt für Verfassungsschutz BaWü) als auch Unternehmen die tatsächliche Bedrohungslage analysieren und ihre Schutzmaßnahmen vorstellen (vollständiges Programm, Online-Anmeldung und Anfahrtskizze).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2008	
17.-21.08.	Crypto 2008 (IACR, Santa Barbara/US)
September 2008	
03.09.	Symposium Wirtschaftsspionage (Secorvo, Ettlingen)
08.-12.09.	T.I.S.P.-Schulung (Secorvo College)
23.-26.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
23.-25.09.	IMF 2008: 4th International Conference on IT-Incident Management & IT-Forensics (GI, Mannheim)
Oktober 2008	
07.-09.10.	ISSE 2008 (EEMA/TeleTrusT, Madrid/ES)
07.-10.10.	IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College)
28.-30.10.	IT-Sicherheitsaudits in der Praxis – Konzeption, Durchführung, Bewertung (Secorvo College)

Fundsache

Das Verizon Business RISK Team hat im 2008 Data Breach Investigations Report die Ergebnisse seiner forensischen Analysen der letzten vier Jahre ausgewertet und zusammengefasst. Dabei wurde neben der Komplexität der Angriffe analysiert, wie der Datendiebstahl zu Stande kam und wer der Urheber war. Abweichend von der verbreiteten Überzeugung, dass Insider die meisten Angriffe verursachen, zeigt die Auswertung, dass in fast 80% der untersuchten Fälle der Zugriff von außen erfolgte, dabei allerdings häufig Geschäftspartner involviert waren.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian,
Hans-Joachim Knobloch, Natalie Mareth, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

August 2008



Editorial: Vom Urteilen

Ein Urteil, so die eingängige Definition in Wikipedia, ist „eine wertende Entscheidung über einen Sachverhalt oder Erkenntnisgegenstand". Entscheidungen zwischen alternativen Bewertungsmöglichkeiten treffen wir ständig – mit mehr oder weniger guter Kenntnis der Zusammenhänge. Viele unserer Urteile sind daher genau besehen Vorurteile, also eine „im Allgemeinen wenig reflektierte Meinung – ohne vollständige Würdigung aller relevanten Eigenschaften eines gewerteten Sachverhalts oder einer Person". Vorurteile sind voreilige Urteile, sie verallgemeinern ohne Berücksichtigung des Einzelfalls.

Das ist nicht notwendig schlecht und manchmal überlebenswichtig. Für viele unserer wertenden Entscheidungen steht uns zu wenig Zeit zur Verfügung, um den Sachverhalt angemessen zu analysieren. Vorurteile geben eine (erste) Orientierung und erlauben sofortiges Handeln. Dabei müssen wir uns aber bewusst machen, dass das Vorurteil nur ein vorläufiges Urteil sein kann, das durch zusätzliche Informationen oder Erkenntnisse in ein reiferes münden sollte.

Die „vollständige Würdigung aller relevanten Eigenschaften" erfordert Disziplin, Zeit und die Offenheit für die Revision eines (Fehl-)Urteils. Daher wurde für Urteile mit besonderer Tragweite für Betroffene das Amt des Richters geschaffen und die Möglichkeit zur Revision institutionalisiert. Im Finanzwesen ist derzeit jedoch ein Trend zur vermeintlichen Objektivierung von z. B. Kreditentscheidungen durch den Rückgriff auf personenbezogene Informationen Dritter zu beobachten, verschleiernd „Rating" genannt. Verständlich vielleicht, dass ein Online-Anbieter nicht gegenüber einem notorischen Zahlungsverweigerer in Vorleistung gehen möchte. Aber soll eine Bank die Kreditbedingungen verschärfen dürfen, weil ein direkter Verwandter des Kunden Privatinsolvenz angemeldet hat? Oder einen Kredit verweigern, weil der Kunde in einem schlecht beleumundeten Viertel wohnt? Da fehlt nicht viel, und aus „automatisierten Einzelentscheidungen" werden nicht-revidierbare Vorurteile – und damit gesamtgesellschaftliche Freiheitsbegrenzer.



Inhalt

Editorial: Vom Urteilen

Security News

Rutkowska strikes again

Schwachstellen-Primus Browser

Phalanx2-Rootkit

Update legt ESX-Server lahm

Eisspray gegen Krypto-Schlüssel

Verflüchtigung 1.3

Secorvo News

Secorvo College aktuell

Symposium Wirtschaftsspionage

Gut gemeint

10 Jahre weiser

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Rutkowska strikes again

Die auf virtuelle Rootkits spezialisierte Forscherin Joanna Rutkowska hat wieder zugeschlagen: Auf der diesjährigen Blackhat stellte sie am 07.08.2008 mit ihren Kollegen Rafal Wojtczuk und Alexander Tershkin vor, wie man den Hypervisor der Virtualisierung Xen mit Rootkits trojanisieren kann. Die technischen Details sind anspruchsvoll und interessant: Der modifizierte Code wird dem bereits laufenden Hypervisor über eine Netzwerkkartentreiber-Software oder den Festplattencontroller untergeschoben und im laufenden Betrieb über Direct Memory Access (DMA) zur Ausführung gebracht.

Wie bereits bei ihrem 2006 vorgestellten Rootkit BluePill (siehe SSN 8/06), das die Virtualisierungsfunktionen von AMD-Prozessoren nutzt, ist die Erkennung dieser Angriffssoftware sehr schwierig. Derzeit entwickeln Rutkowska und ihre Kollegen im Projekt HyperGuard die BIOS-Funktionen von Mainboards weiter, um einen Integritätsschutz der Hypervisor-Software zu ermöglichen – damit wäre wirksame Abhilfe möglich.

Schwachstellen-Primus Browser

In einer am 14.08.2008 vom Deutschen Sicherheitsnetz e.V. vorgestellten Untersuchung wurde festgestellt, dass von 253 geprüften privaten PC-Systemen gut die Hälfte Browserschwachstellen aufwies. Deutlich repräsentativer, aber im Ergebnis vergleichbar sind die am 10.08.2008 vorgestellten Ergebnisse einer von der ETH Zürich gemeinsam mit Google und IBM durchgeführten Studie: Von ca. 1,4 Milliarden PCs setzten danach 45,2 % nicht die aktuellen Versionen der jeweiligen Browser ein.

Je nach Art der Schwachstelle reicht es aus, eine entsprechend präparierte Website zu besuchen, um im schlimmsten Fall einem Angreifer die vollständige Kontrolle über das System zu überlassen. In der Tat tauchen – wie beispielsweise eine von Google am 30.07.2008 vorgestellte Studie zeigt – gerade vor Großereignissen wie den olympischen Spielen immer wieder zahlreiche manipulierte Webseiten auf, deren Besuch mit anfälligen Browsern zur Kompromittierung des Systems führen kann.

Dabei ist zu beachten, dass die Schwachstellen nicht nur die Kernkomponenten des Browsers, sondern in vielen Fällen auch Erweiterungen wie Java, Flash und Quicktime betreffen. Diese Komponenten werden gelegentlich beim Patch-Management übersehen. Eine Überprüfung der Aktualität eigener Browser-Erweiterungen und die Suche nach weiteren Schwachstellen kann bei Secunia online erfolgen. Empfehlenswert sind auch die Browserchecks vom Deutschen Sicherheitsnetz und Heise online.

Phalanx2-Rootkit

Das DFN-CERT warnte am 04.08.2008 vor einer neuen Version des bereits seit 2005 bekannten Linux-Rootkits „Phalanx“, welches in aktuellen Angriffen aus dem Internet beobachtet wurde. Phalanx2 manipuliert dabei – wie andere Rootkits auch – bestimmte Systemdateien, um sich vor Benutzer und Administrator zu verstecken. Die Infektion des Systems erfolgt überwiegend über gestohlene SSH-Schlüssel.

Linux-Administratoren sollten demnach kurzfristig überprüfen, ob ihre Systeme betroffen sind: Das DFN-CERT stellt in dem entsprechenden Security Advisory ein einfaches Shell-Skript zur Verfügung, welches nach Phalanx2-Spuren sucht.

Update legt ESX-Server lahm

Wer der Überzeugung ist, seine Sicherheit durch den Einsatz von Virtualisierung automatisch gesteigert zu haben, ist einem populären Irrglauben erlegen. Zwar kann beispielsweise durch den Einsatz von VMware ESX Server die Verfügbarkeit von Serversystemen erhöht werden. Damit handelt man sich jedoch auch zusätzliche Risiken ein. So führte ein Update für ESX in den Versionen 3.5/3.5i vom 12.08.2008 dazu, dass virtuelle Systeme auf dem ESX Server nicht mehr gestartet werden konnten. Kritisch ist dabei, dass von ESX-Fehlfunktionen unvermeidlich zahlreiche virtualisierte Serversysteme betroffen sein können. Schlimmstenfalls können komplette Serverlandschaften ausfallen.

Das Beispiel zeigt, dass bei der Einführung von Virtualisierung die damit verbundenen Risiken zu betrachten sind und – wie bei jeder kritischen Komponente einer Infrastruktur – ein besonderes Augenmerk auf den Patch-Prozess gelegt werden muss.

Eisspray gegen Krypto-Schlüssel

Dass die Inhalte des Hauptspeichers (RAM) weniger flüchtig sind als lange Zeit angenommen, weiß man aufgrund forensischer Analysen bereits seit einiger Zeit: Je nach betroffener Hardware-Betriebssystem-Kombination „überleben“ große Mengen interessanter Daten sogar das (mehrfache) Booten des Rechners.

Forscher aus Princeton, die ihre (vorab schon am 21.02.2008 unter anderem als Film in YouTube publizierten) Ergebnisse am 30.07.2008 auf dem diesjährigen USENIX Security Symposium präsentierten, gingen noch einige Schritte weiter. So fanden sie heraus, dass sich auch mehr als 60 Sekunden nach dem kompletten Ausschalten des Rechners Inhalte

aus bestimmten DRAM-Speicherchips größtenteils rekonstruieren lassen. „Behandelten" sie die Speicherriegel eines Laptops zusätzlich mit Eisspray, bevor sie den Rechner ausschalteten, und bauten sie die gekühlten RAM-Bausteine in ein anderes Laptop ein, so konnten sie auch noch nach mehreren Minuten ohne Strom problemlos auf sämtliche RAM-Inhalte zugreifen.

Spektakulärer wird dieser Angriff durch die Tatsache, dass die Forscher zeitgleich Algorithmen und Tools zum Auffinden kryptographischer RSA- sowie AES-Schlüssel entwickelten: Mit deren Hilfe muss auf der Suche nach BitLocker-, FileVault-, dm-crypt- oder TrueCrypt-Schlüsseln nicht mehr der komplette Speicherinhalt manuell „durchstöbert" werden. Vielleicht sollten Laptop-Nutzer zukünftig ein Wärmepflaster als Zubehör mit sich führen.

Verflüchtigung 1.3

Die künstliche Verlängerung der Flüchtigkeit von RAM-Inhalten könnte zukünftig auch bei forensischen Analysen interessant werden, da die Untersuchung des Hauptspeichers im Rahmen so genannter „Live-Analysen" immer wichtiger wird. Längst spielt die dynamische Analyse in vielen Forensik-Projekten eine größere Rolle als die rein statische. Anzahl und Qualität der entsprechenden Tools zur Untersuchung des Hauptspeichers hielten sich bislang jedoch in Grenzen – viele Tools besaßen diesbezüglich nur rudimentäre Funktionen.

Die am 14.08.2008 erschienene neue Version der Tool-Sammlung Volatility – von ihren Entwicklern als v1.3_Beta bezeichnet – ist eine sehr mächtige, aus der Open-Source-Welt stammende kostenlose Software für Live-Analysen. Sie unterstützt Speicherdumps von Windows XP (SP2 und SP3) sowie ansatzweise Linux, kann die laufenden Prozesse anzeigen, Binaries extrahieren und offene Netzwerkverbindungen auflisten. Sie darf in keinem forensischen Werkzeugkasten fehlen.

Secorvo News

Secorvo College aktuell

Für die nächste T.I.S.P.-Schulung in der zweiten Septemberwoche (**08.–12.09.2008**) mit anschließender Zertifikats-Prüfung durch iSQI gibt es nur noch wenige freie Plätze, und auch unser „aktueller Klassiker" mit umfangreichem Demo- und Praxisteil, das Seminar PKI – Grundlagen, Vertiefung, Realisierung am **23.–25.09. 2008**, erfreut sich großer Nachfrage – baldige Anmeldung empfohlen. Im Oktober folgen das Grundlagenseminar IT-Sicherheit heute am **07.–10.10.2008** und IT-Sicherheitsaudits in der Praxis am **28.–30.10.2008**. Termine, Programme und Online-Anmeldung unter http://www.secorvo.de/college

Symposium Wirtschaftsspionage

Im Schatten wachsender Spam- und Trojaner-Wellen nehmen gezielte Spionageattacken zu. Angesichts dieser besorgniserregenden Entwicklung führen wir gemeinsam mit dem Wirtschaftsmagazin Econo am **03.09.2008** ein eintägiges Symposium zur "Wirtschaftsspionage" durch. Ulf Tietge, Chefredakteur von Econo, wird das Symposium moderieren, für das wir zahlreiche Fachexperten wie Dr. Udo Ulfkotte und Unternehmensvertreter gewinnen konnten, die die tatsächliche Bedrohungslage analysieren und Schutzmaßnahmen vorstellen. Mit voraussichtlich über 70 Teilnehmern verspricht auch das Auditorium spannende Diskussionen. Für Schnellentschlossene gibt es noch freie Plätze (Programm, Online-Anmeldung und Anfahrtskizze).

Gut gemeint

Was ist ein "gutes" Passwort? Verbessern die verbreiteten Komplexitätsanforderungen tatsächlich die Güte gewählter Passworte? Und wie lässt sich verhindern, dass die Passworte notiert oder weitergegeben werden? Auf diese Fragen gibt eine aktuelle Untersuchung überraschende Antworten, die Thomas Maus auf dem nächsten Event der Karlsruher IT-Sicherheitsinitiative am 25.09.2008 im Schlosshotel Karlsruhe vorstellen wird. Er räumt mit einigen liebgewonnenen "Glaubenssätzen" auf und legt ein Umdenken im Umgang mit Passworten nahe. Anmeldung und weitere Informationen unter http://www.ka-it-si.de.

10 Jahre weiser

In wenigen Tagen, am 01.09.2008, wird Secorvo zehn Jahre alt. Dann werden über 550 herausfordernde Projekte, mehr als 200 veröffentlichte Aufsätze, über 70 Ausgaben der "Security News" und mehrere hundert Seminare, Symposien und Vortragsveranstaltungen hinter uns liegen. Dass wir die Chance hatten, über einen solchen - im IT-Zeitalter geradezu astronomisch langen – Zeitraum die IT-Sicherheit und den Datenschutz in Deutschland mitzugestalten, verdanken wir nicht zuletzt unseren Kunden: Deren Vertrauen in unsere Arbeit, die fruchtbare Zusammenarbeit und wohl auch die eine oder andere Empfehlung waren wesentliche Voraussetzung für diesen Erfolg.

Auch bei unseren treuen Lesern der Security News möchten wir uns bei dieser Gelegenheit bedanken. Die monatlich mehreren tausend Abrufe der News sind eine wichtige Motivation für unsere Arbeit. Und falls Sie uns schon immer einmal ein Lob aussprechen wollten – anlässlich unseres runden Geburtstags würde uns das besonders freuen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2008	
03.09.	Symposium Wirtschaftsspionage (Secorvo, Ettlingen)
07.-10.09.	OSS 2008 – 1st Workshop on Open Source Software for Computer and Network Forensics (IFIP, Milano/IT)
08.-12.09.	T.I.S.P.-Schulung (Secorvo College)
23.-26.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
23.-25.09.	IMF 2008 – 4th International Conference on IT-Incident Management & IT-Forensics (GI, Mannheim)
Oktober 2008	
07.-10.10.	IT-Sicherheit heute (Secorvo College)
28.-30.10.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
November 2008	
04.-05.11.	Security Awareness - Methoden, Konzepte, Best Practice (Secorvo College)
11.-13.11.	Forensik - Verfahren, Tools, Praxis (Secorvo College)

Fundsache

Die Kryptoanalyse mathematischer Algorithmen ist seit vielen Jahrhunderten eine anspruchsvolle Wissenschaft. Zahlreiche Fachbücher existieren zu diesem Thema; nicht immer sind die Erläuterungen aber für Einsteiger verständlich. Der Google-Mitarbeiter Mark Chu-Carroll hat am 15.08.2008 in seinem Blog eine sehr informative Einführung in die Kryptoanalyse „zum Nachmachen" gegeben – auch die Kommentare sind lesenswert.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Stefan Kelm

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

September 2008



Editorial: Verhältnisunmäßig

Große Erregung: Millionen Kontendaten, für kleines Geld zu erwerben, bieten fette Beute für Betrüger, die Banken glaubhaft versichern, im Besitz von Einzugsermächtigungen zu sein. Verbraucherschützer trommeln, die Republik ist empört, und der Bundesinnenminister gipfelt.

Die richtige Aufregung, aber zum falschen Anlass. Seit 1998 wertet Google täglich Milliarden Suchanfragen zur Erstellung und Verfeinerung von Abfrageprofilen aus. Zähneknirschend hat Google am 08.09.2008 auf Druck der Artikel-29-Gruppe den europäischen Datenschutzbeauftragten angekündigt, „damit zu beginnen", die IP-Adressen in den Such-Logs schon (sic!) nach neun Monaten zu anonymisieren. Sechs Tage zuvor hatte Google seinen neuen Browser Chrome publiziert. Welch Koinzidenz. Millionenfach heruntergeladen, erlaubt Chrome die Verknüpfung von Suchanfragen mit Webseitenaufrufen – und einer eindeutigen Browser-ID. Abgleiche der Suchprofile mit den Webseiten von Social Networks, Personensuchmaschinen wie 123people oder yasni, den Adressangaben in Telefonbüchern oder Nachbarbeschimpfungen liefern Google (und z.T. auch dessen Nutzern) von immer mehr Menschen ein Persönlichkeitsprofil. Von da zum Großen Bruder ist es nur noch einen klitzekleiner Klick. Wer braucht da noch die sechsmonatige Vorratsdatenspeicherung?

Immerhin regt sich inzwischen etwas im Innenministerium. Sogar in die seit sieben Jahren überfällige Verabschiedung eines Datenschutz-Audit-Gesetzes, an die kein Datenschützer mehr zu Glauben wagte, kommt Bewegung. Allerdings lassen einige der Gipfelergebnisse eher operative Hektik befürchten: Durch die Abschaffung des Listenprivilegs würde keine einzige Kontonummer gerettet, und ein Kopplungsverbot wiese Google nicht in die Schranken.

„Wer weiß, wie Gesetze und Würste zu Stande kommen, kann nachts nicht mehr gut schlafen", soll Otto von Bismarck gesagt haben. Den meisten Metzgern würde er heute damit Unrecht tun.



Inhalt

Editorial: Verhältnisunmäßig

Security News

WASC Studie

Nmap auswerten

Rootkit für Jedermann

Botnetz-Wachstum

Endlich DNSSEC?

Datenschutz-Bußen

Secorvo News

Secorvo College aktuell

Gut gemeint

Jubiläums-Nachlese

Veranstaltungshinweise

Fundsache

Security News

WASC Studie

Am 08.09.2008 hat das Web Appliction Security Consortium (WASC) die Ergebnisse des Projekts „Web Application Security Statistics 2007" veröffentlicht. Im Rahmen dieser Studie wurden zum besseren Verständnis der Sicherheitslage bei Web-Anwendungen über 32.000 Sites automatisiert und manuell untersucht. Die im Detail vorgestellten Ergebnisse sind aufschlussreich und erschreckend zugleich: Wenn auch nur knapp über 7% der untersuchten Anwendungen automatisiert kompromittiert werden konnten, wurden in über 96% der Anwendungen bei manueller Suche schwerwiegende Schwachstellen gefunden. Insbesondere handelte es sich um Anfälligkeiten für Cross-Site-Scripting, Information Leakage, SQL-Injection und Predictable Resource Location.

Als Basis diente die WASC Threat Classification 1.0 aus dem Jahr 2005. Trotz der etwas betagteren Grundlage bietet die Studie eine umfassende Analyse der benutzten Methoden und erzielten Ergebnisse. In diesem Zusammenhang triff es sich gut, dass am 15.09.2008 der Aufruf zur Mitarbeit an der Weiterentwicklung zur WASC Threat Classification 2.0 erfolgte. Allen an Web-Sicherheit Interessierten legen wir die Beobachtung dieser Entwicklung sehr ans Herz.

Nmap auswerten

Am 07.09.2008 ist der Netzwerkscanner Nmap in Version 4.75 erschienen. Darin wurde das GUI Zenmap um die Visualisierungskomponente Radialnet erweitert. Zwei sehr sinnvolle Funktionen – Datenaggregation mehrerer Scans und eine Netztopologiedarstellung – stehen nun zur Verfügung, sofern die Scan-Ergebnisse im XML-Format vorliegen.

Dies vereinfacht die Analyse der Scanergebnisse erheblich, da zeitlich auseinanderliegende Scans in einer Auswertung darstellbar sind – der Praktiker weiß: Nicht immer sind alle Hosts online oder dürfen im selben Arbeitsablauf gescannt werden. Erfreulicherweise funktioniert die Aggregation auch mit älteren XML-Dateien des 4.60-Releases. Die Topologie des Netzwerks ist konzentrisch und mit relativer Hopdistanz darstellbar, inklusive Ergebnisdetails für gescannte IPs. Ein übersichtlicher Netzplan als Nebenprodukt eines Audits ist ein erheblicher Mehrwert. Ein Wermutstropfen bleibt: Für umfangreiche IP-Ranges braucht man viel CPU-Zeit – und scharfe Augen.

Rootkit für Jedermann

Am 03.09.2008 wurde das voll funktionsfähige Open Source Rootkit „Debug Register" (DR) in der Version 0.1 für Linux-Kernels 2.6.x (Intel-IA32-Architekturen) vom Penetrationstest-Werkzeughersteller Immunity Inc. zum Download veröffentlicht. Seine Funktionen umfassen die Unterstützung für versteckte Prozesse, Netzwerksockets, Daten sowie eine Backdoor.

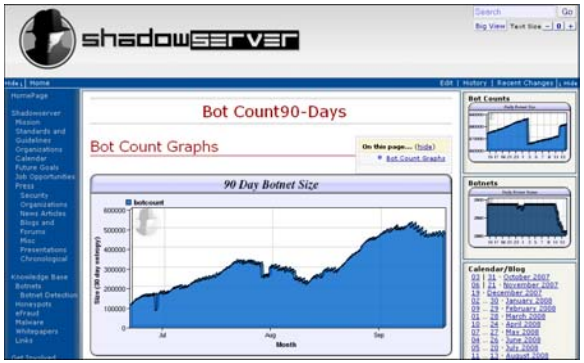
Das Rootkit arbeitet wie ein Kernel-Debugger und nutzt vorhandene System-Interrupts der Intel-CPUs – eine Technik, die bisher von Malware kaum eingesetzt wurde, da dafür ein tiefes Systemverständnis erforderlich ist. Mit einem Entwicklungsaufwand von ca. zwei Wochen lässt sich der Code um eine Tarnung auf Kernel-Ebene erweitern.

Damit wurde die Entwicklung leistungsfähiger Malware im Linux-Umfeld erheblich beschleunigt. Ohne einen wirksamen Integritätsschutz der Systemumgebung ist gegen derartige Low-Level-Angriffe kein Kraut gewachsen.

Botnetz-Wachstum

Die 2004 gegründete Shadowserver Foundation hat sich zur Aufgabe gemacht, die „dunklen Seiten des Internet" zu beleuchten. Von Sicherheitsspezialisten werden die Entwicklungen bei Viren und Malware sowie von Botnetzen beobachtet; Ergebnisse und weitere Informationen werden auf den Webseiten der Initiative veröffentlicht.

Dabei wurde in den vergangenen drei Monaten ein sprunghaftes Wachstum von Botnetzen beobachtet: Die geschätzte Anzahl der übernommenen Systeme hat sich fast vervierfacht. Ursache hierfür dürften unter anderem Malware-Mailings anlässlich der Olympiade sein. Auch wurden PCs verstärkt über kompromittierte Webserver infiziert.



Die Entwicklung zeigt, dass es weiterer technischer und organisatorischer Maßnahmen bedarf, um Client-Systeme adäquat zu schützen. Nutzern empfehlen wir die Beachtung entsprechender Warnungen, beispielsweise unter www.bsi-fuer-buerger.de.

Endlich DNSSEC?

Die Schwächen des Internet Domain Name Systems (DNS), die bei den unlängst veröffentlichten Cache Poisoning Attacken (siehe SSN 07/08) zu Tage traten, kommen nicht überraschend. Bereits im Januar 1997 wurde in RFC 2065 die erste Version der DNS Security Extensions (DNSSEC) veröffentlicht. Nach zwei Überarbeitungen ist DNSSEC seit März 2005 in den RFCs 4033 ff. spezifiziert und in verbreiteter DNS-Software, z. B. BIND, integriert – kann also nach Internet-Zeitmaßstäben als ausgereift gelten.

DNSSEC nutzt elektronische Signaturen zur Sicherung der erteilten Auskünfte. Die dabei benötigte PKI wird jedoch nicht wie üblich über X.509-Zertifikate realisiert; statt dessen erteilen Nameserver direkt Auskunft über die Public Keys der Nameserver darunter liegender Ebenen. Hierin liegt auch einer der Gründe, dass DNSSEC trotz langer Vorlaufzeit noch nicht global eingesetzt wird: Genau so umstritten wie die Kontrolle über die Root-Nameserver ist auch die politische Frage, wer deren Schlüsselpaar als „Trust Anchor" des Internet kontrollieren soll.

Mit Erlass vom 22.08.2008 ordnete die US-Regierung – kaum zufällig zeitgleich mit den jüngsten DNS-Attacken – für die von ihr kontrollierte Government Top-Level Domain („gov") die flächendeckende Einführung von DNSSEC bis Ende 2009 an. Die einschlägigen Umsetzungsempfehlungen der NIST Special Publication 800-81 sind für jeden DNS-Verantwortlichen einen Blick wert.

Ein Multiplikator-Effekt könnte sich einstellen, wenn Service-Provider, die für einzelne Behörden deren .gov-Domains hosten, ihre Insfrastruktur fit für DNSSEC machen müssen und diesen Zusatz-Dienst dann auch anderen Kunden anbieten.

Datenschutz-Bußen

Weder die öffentliche Zerknirschung noch der Rückgriff auf den ehemaligen Bundesdatenschutzbeauftragten Jakob haben Lidl geholfen: Am 11.09.2008 verkündeten die Datenschutzaufsichtsbehörden die Verhängung von Bußgeldern in einer Gesamthöhe von knapp 1,5 Mio. Euro, nachdem Lidl seine Mitarbeiter in persönlichkeitsverletzender Weise hatte ausspionieren lassen. Eigenwillige Interpretationen von Arbeitnehmerrechten hatten bereits 2004 zur Verleihung des BigBrotherAward geführt.

Dass es sich beim persönlichkeitsverletzenden Einsatz von Videoüberwachung nicht um ein Kavaliersdelikt handelt, wird auch durch das am 15.09.2008 von der nordrhein-westfälischen Aufsichtsbehörde gegen den Fleischverarbeiter Tönnies verhängte Bußgeld in Höhe von 80.000 Euro bekräftigt. Zur Diebstahlsvorbeugung wurden die Beschäftigten mit über 200 Kameras unter anderem auch in Umkleidekabinen und Sozialräumen überwacht.

Eine gesetzeskonforme Gestaltung der Verarbeitung personenbezogener Daten gebietet inzwischen auch die ökonomische Vernunft. Die Zeiten, in denen sich Datenschutzverstöße aussitzen ließen, sind vorbei.

Secorvo News

Secorvo College aktuell

Pünktlich zu den in Karlsruhe gelegentlich auch im Spätsommer noch südländischen Temperaturen lockt Secorvo College nun mit klimatisierten Räumen. Das scheint sich schnell herumgesprochen zu haben, denn mehrere Seminare waren schon kurz nach dem Ende der Urlaubszeit ausgebucht.

Noch freie Plätze gibt es für die Seminare IT-Sicherheit heute (**07.–10.10.**), IT-Sicherheitsaudits (**28.–30.10.**), Security Awareness (**04.–05.11.**) und das T.I.S.P.-Seminar (**24.–28.11.**).

Programm und Online-Anmeldung unter http://www.secorvo.de/college

Für das Seminar Forensik, das sich ganz besonderer Nachfrage erfreut, haben wir eine Warteliste eingerichtet. Voraussichtlich im Januar 2009 wird es einen zusätzlichen Termin geben. Bitte wenden Sie sich bei Interesse an college@secorvo.de.

Gut gemeint

„Das Gegenteil von gut ist nicht böse, sondern gut gemeint." Das gilt leider auch für verbreitete Passwort-Policies, wie Thomas Maus in seinem Vortrag im Rahmen der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 25.09.2008 (18 Uhr im Schlosshotel Karlsruhe) zeigen wird. Dabei räumt er mit vielen lieb gewonnenen und, wie das obige Zitat von Gottfried Benn, gerne kopierten „Wahrheiten" auf. Im Anschluss an den Vortrag gibt es, wie gewohnt, Gelegenheit zum Buffet-Networking. Um Anmeldung wird gebeten.

Jubiläums-Nachlese

Für die zahlreichen Glückwünsche, die uns zu unserem 10jährigen Firmenjubiläum erreicht haben, bedanken wir uns auch an dieser Stelle sehr herzlich. Auch die vielen „Geburtstagslob"-E-Mails zu unseren News haben uns sehr gefreut – wir bleiben am Ball, versprochen. Mit den Vorbereitungen für den 20sten Jahrestag haben wir auch schon begonnen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2008	
25.09.	Das Gegenteil von gut ist - gut gemeint (KA-IT-Si)
Oktober 2008	
07.-10.10.	IT-Sicherheit heute (Secorvo College)
07.-09.10.	ISSE (TeleTrust), Madrid/ES
27.-30.10.	Hack-in-the-Box 2008, Kuala Lumpur/MY
28.-30.10.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
November 2008	
04.-05.11.	Security Awareness - Methoden, Konzepte, Best Practice (Secorvo College)
11.-13.11.	Forensik – Verfahren, Tools, Praxis (Secorvo College)
18.-21.11.	Information Security Management (Secorvo College)
24.-28.11.	T.I.S.P.-Schulung (Secorvo College)
Dezember 2008	
02.-04.12.	Sichere Softwareentwicklung (Secorvo College)

Fundsache

Bei der Betätigung des „Home Buttons" eines iPhones schrumpft die aktuell offene Anwendung und blendet sich aus. Dieser optische Effekt wird im iPhone durch das Erstellen von Bildschirmfotos realisiert – SubSeven lässt grüßen. Das iPhone löscht ältere Fotos zwar, aber bei einer forensischen Untersuchung des iPhones treten diese Spuren offenbar wieder hervor. Ein Feature für die Strafverfolgung – oder ein Westentaschenspion?

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Karin Schuler, Hans-Joachim Knobloch, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Oktober 2008



Editorial: One man – no vote?

Wählen mit Computerhilfe – der Traum aller Wahlhelfer, die unter Zeitdruck tausende Stimmzettel auszählen müssen. Einfach bestechend: Per Mausklick lassen sich Auszählung und Wahlvorgang beschleunigen und Zählfehler ausschließen.

Elektronische Wahlen sind nichts Neues in Deutschland. Die Gesellschaft für Informatik wählt ihr Präsidium seit 2004 über das Internet, an Universitäten wird die Selbstverwaltung mit Computerhilfe bestimmt und in mehreren Bundesländern werden Wahlcomputer bei Kommunal-, Landtags- und Bundestagswahlen eingesetzt. Am 24.10.2008 erhielt Bingo Voting, ein an der Universität Karlsruhe entwickeltes Verfahren mit der Möglichkeit zur Prüfung der korrekten Zählung der eigenen Stimme, den Deutschen Sicherheitspreis 2008.

Tatsächlich ist E-Voting nicht so einfach, wie es scheint. Denn aus der Perspektive des Wählers ist ein Wahlcomputer eine Black Box, der er bei Stimmabgabe blind vertrauen muss. Nicht immer ist dieses Vertrauen berechtigt. So wird in Deutschland der Nedap-Wahlcomputer eingesetzt, ein Gerät, dessen Version ES3B der Chaos Computer Club (CCC) 2006 analysiert hat – mit bitteren Ergebnissen: Der Manipulationsschutz beruht auf simplen, leicht fälschbaren Papiersiegeln, das Master-Passwort war mit „GEHEIM" vorbelegt, und durch einen Firmwaretausch ließ sich der Wahlcomputer in einen Schachcomputer verwandeln (siehe SSN 10/2006). In Brandenburg stellten Wahlbeobachter des CCC am 28.09.2008 – wie zuvor in Hessen – erhebliche Mängel beim Umgang mit den Wahlcomputern fest: Fehlende Siegel, unbeaufsichtigte Lagerung, Fehlbedienung und unerklärliche Zähldifferenzen.

Manipulierbare Wahlcomputer wären eine gefährliche Waffe in den Händen einer Partei oder Regierung. Stimmzettel lassen sich durch Unabhängige nachzählen – Computerdaten nicht. Das wurde auch in der öffentlichen Anhörung vor dem Bundesverfassungsgericht am 28.10.2008 deutlich. Bleibt zu hoffen, dass Papier und Bleistift noch eine Chance haben – wenigstens dann, wenn der Souverän wählt.



Inhalt

Editorial: One man – no vote?

Security News

Clickjacking

Forensische Spirale 2.0

Neue Hash-Funktionen

Virenschutz für VMs

Surf-CD vom BSI

OWASP Appsec 2008

Mifare-Exploit online

BSI meets ISACA

Secorvo News

Secorvo College aktuell

Original oder Fälschung?

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Clickjacking

Auf der diesjährigen amerikanischen OWASP-Konferenz sorgte das Zurückziehen eines Vortrags zum Thema „Clickjacking“ durch die Autoren Robert „RSnake“ Hansen und Jeremiah Grossman für einiges Aufsehen. Inzwischen sind durch einen Blog-Eintrag Robert Hansens vom 07.10.2008 sowie die Veröffentlichung eines Proof of Concept und eines Videos erste Details zu der architektonisch bedingten Schwachstelle bekannt. Darin werden verschiedene Ausprägungen vorgestellt.

Clickjacking wird das Platzieren eines „unsichtbaren“ Click-Buttons auf einer Webseite genannt, auf den der Nutzer klickt, während er vermeintlich einen darunter liegenden Link auswählt. Bis zur Beseitigung dieser Browserschwachstelle bietet das – auch in anderem Kontext sehr nützliche – Firefox Add-On „NoScript“ mit „ClearClick“ einen gewissen Schutz.

Forensische Spirale 2.0

Seit vielen Jahren schon gehört die Live-CD Helix in den virtuellen Werkzeugkasten jeder Forensikerin. Helix ist eine der wenigen umfangreichen Tool-Sammlungen, die sowohl unter Windows als auch unter Linux zu verwenden sind – sie war allerdings schon etwas in die Jahre gekommen.

Am 15.09.2008 wurde endlich die von vielen herbei gesehnte Helix Version 2.0 veröffentlicht. Wir haben die neue Version in unserem forensischen Labor ausgiebig getestet. Ergebnis: Das Warten hat sich gelohnt. Zunächst wurden die einzelnen Tools auf den neuesten Stand gebracht bzw. um neue Software ergänzt. Die größte Änderung ist jedoch der Umstieg der Boot-Partition auf Ubuntu, was u. a. die Unterstützung neuer Hardware spürbar verbessert. Helix 2.0 ist und bleibt damit eine interessante Ergänzung oder sogar Alternative zu kommerziellen forensischen Tools. Wir werden Helix 2.0 bereits im kommenden Forensik-Seminar berücksichtigen.

Neue Hash-Funktionen

SHA, der Secure Hash Standard, war die erste standardisierte Hashfunktion, 1994 vom US-amerikanischen NIST veröffentlicht. Am 01.08.2002 legte das NIST mit einer erweiterten Spezifikation nach, die vier Varianten der nun SHA-2 genannten Algorithmenfamilie mit unterschiedlich langen Hashwerten umfasste (FIPS PUB 180-2). 2004 wurde die Spezifikation um die Variante SHA-224 ergänzt; eine Endfassung des Standards erschien am 17.10.2008 (FIPS PUB 180-3).

Doch die Tage des in die Jahre gekommenen SHA-2 sind gezählt. Da für einen Nachfolger keine geeigneten alternativen Verfahren in Sicht waren, schrieb das NIST am 02.11.2007 – wie beim AES – einen Wettbewerb für SHA-3 aus. Wenige Tag vor der Einreichungsfrist (31.10.2008) waren schon über 30 Verfahren beim NIST eingegangen. Ein sehr aussichtsreicher Kandidat ist der Skein getaufte Algorithmus einer Kryptographengruppe um Bruce Schneier. Auch ein „Veteran“ ist dabei: Ron Rivest, einer der Väter des RSA-Verfahrens, hat MD6 ins Rennen geschickt.

Virenschutz für VMs

Vom Virenschutz-Anbieter McAfee wurden am 17.09.2008 Lösungen zum Scannen von virtuellen Maschinen vom Virtualisierungs-Host aus (VMware ESX) vorgestellt. Auf den ersten Blick ein vorteilhafter Ansatz: Virtuelle Maschinen werden, auch wenn sie nicht verwendet werden, zentral überprüft, und bei Bedarf wird sogar der auf den Gastsystemen installierte Virenschutz aktualisiert.

Aber Vorsicht: Jedes Gastsystem sollte – wie bei „echten“ physikalischen Servern – über einen installierten und regelmäßig aktualisierten Virenschutz verfügen. Einen Mehrwert bietet die neue Produktserie nur dann, wenn die Systeme gerade ausgeschaltet sind. Auch besteht die Gefahr, sich durch die zusätzliche Software auf dem Hostsystem Angriffsmöglichkeiten und Sicherheitsprobleme einzuhandeln. Denn in den Listen von Produkten mit sicherheitskritischen Fehlern fanden sich in den vergangenen Jahren zahlreiche Hersteller und Produkte von Sicherheitssoftware.

Unsere Empfehlung lautet daher: Keep it simple. ESX-Systeme sollten ohne Verwässerung der Sicherheitsfunktionen wie guter schottischer Whisky genossen werden: pur – und ohne Eis.

Surf-CD vom BSI

Am 08.08.2008 wurde vom BSI eine auf Knoppix basierende „Surf-CD“ vorgestellt. Die Idee dahinter ist, durch Booten von CD ein sauberes System zu erhalten und damit bspw. sicheres Online-Banking zu ermöglichen. Dazu wurde das von CD zu startende System durch mehrere Maßnahmen gehärtet und der verwendete Browser „Iceweasel“, die Debian-Variante von Firefox, durch Sicherheits-Plugins aufgepeppt. Im Vergleich zu anderen Boot-CDs überzeugt unter anderem, dass ein schreibender Zugriff auf weitere Datenträger, beispielsweise auf interne oder externe Festplatten des Systems, kernelseitig unterbunden wird.

Eine gute Lösung für Anwender, die ihr System beim Surfen vor eingefangener Schadsoftware

schützen möchten – oder dem vom Filius zum Spielen genutzten System nicht mehr ihre PINs und TANs anvertrauen mögen.

OWASP Appsec 2008

Am 24.-25.09.2008 fand die OWASP NYC Appsec 2008 Conference im Big Apple statt. Das wachsende Interesse an Applikationssicherheit wurde durch die ansehnliche Zahl von über 850 Teilnehmern eindrucksvoll verdeutlicht. Die an der einen oder anderen Stelle dadurch verursachten Reibungsverluste wurden durch die engagierte Konferenzorganisation überkompensiert.

Fachlich hatte die Tagung einige Highlights zu bieten. Hervorzuheben sind die Vorträge von Gunter Ollmann zum Thema „Multidisciplinary Bank Attacks", Ausflüge in die Praxis von Angriffen wie „Get Rich or Die Trying – Making Money on The Web, The Black Hat Way" von Tom Brennan, Jeremiah Grossman und Trey Ford. Für Interessierte, die nicht an der Konferenz teilnehmen konnten oder verpasste Parallelvorträge ansehen möchten, stehen die Videos der Vorträge online bereit.

Die vorgestellten theoretischen und praktischen Arbeiten sind für die Beschäftigung mit verschiedenen Aspekten der Applikationssicherheit wertvoll. Daher sollte man den Termin der OWASP Germany 2008 Conference am 25.11.2008 in Frankfurt vormerken.

Mifare-Exploit online

Jetzt ist es passiert: Am 27.10.2008 hat ein Hacker unter dem Pseudonym 'Bla' eine C-Implementierung des von der Radboud Universiteit Nijmegen auf der europäischen Sicherheitskonferenz Esorics am 06.-08.10.2008 publizierten Angriffs auf Mifare Classic mit dem Titel „crapto1" auf der Open Source Platform Google Code veröffentlicht. Zwar fehlt zu einer „Plug-and-Play"-Attacke noch die Software für Proxmark oder den OpenRFID Sniffer. Für deren Implementierung sind jedoch keine kryptologischen Kenntnisse erforderlich; die öffentliche Bereitstellung ist daher nur eine Frage der Zeit.

Jetzt hilft kein Abwiegeln mehr: Das Clonen und Manipulieren von Mifare-basierten Chipkarten wird in Kürze ein Kinderspiel sein. Wer Mifare Classic einsetzt, sollte sich daher baldigst geeignete Migrationsstrategien einfallen lassen, um nicht gegen Sorgfaltspflichten zu verstoßen.

BSI meets ISACA

Der bereits am 01.09.2008 veröffentlichte „Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" bildet die Grundlage für die Durchführung von IS-Revisionen in Bundesbehörden gemäß des UP Bund. Das konzeptionell klar strukturierte, 37-seitige Dokument enthält neben den konkreten Durchführungsschritten auch eine Aufwandsschätzung über 30 bis 100 Personentage für die so genannte Querschnittsprüfung. Daraus wird ersichtlich, dass Initial- und Betriebsaufwand für das Thema Informationssicherheit deutlich höher sind als das, was viele Behörden operativ investieren. Als Fachqualifikation für die Befähigung zur IS-Revision wird allgemein auf einen „Nachweis der Qualifikation durch Zertifikate" verwiesen. Eine Chance für den IT-Grundschutz?

Im Oktober 2008 hat das ISACA Germany Chapter den – nur in Papierform erhältlichen – „Leitfaden zur Durchführung eines Quality Assurance Reviews der Internen IT-Revision (QAR-IT)" veröffentlicht. Der zehnseitige Prüfungskatalog ist eindeutig und sehr aussagefähig und wird durch eine vollständige Liste aller Prüfungsstandards abgerundet. Er ist zudem so universal einsetzbar, dass damit auch eine QAR für eine IS-Revision durchgeführt werden kann. In Kombination mit dem Leitfaden des BSI lässt sich damit auch die Frage nach der „Kontrolle des Kontrolleurs" beantworten.

Secorvo News

Secorvo College aktuell

Für Schnellentschlossene bietet Secorvo College 2008 noch zwei Weiterbildungschancen:

- Information Security Management von A(udit) bis Z(erzifizierung) am **18.–21.11.2008** sowie eine
- T.I.S.P.-Schulung am **24.–28.11.2008** mit anschließender Prüfung.

Die Termine der Seminare 2009 stehen inzwischen ebenfalls fest – eine praktische Übersicht bietet der ganzjährige College-Kalender.

Detaillierte Seminarprogramme und die Möglichkeit zur Online-Anmeldung (auch schon für 2009) finden Sie unter http://www.secorvo.de/college.

Original oder Fälschung?

Seit fast 20 Jahren prägt ein Karlsruher Unternehmen, die WIBU-Systems AG, die weltweite Entwicklung des „Digital Rights Managements" zum Schutz digitaler Produkte – Software, Dokumente, Medien. Auf dem letzten diesjährigen Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 04.12.2008 wird Rüdiger Kügler spannende Einblicke in die rasante Entwicklung der DRM-Technologie geben – und zeigen, was uns hinsichtlich des Schutzes digitaler Güter in den kommenden Jahren erwartet.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2008	
04.-05.11.	Praxistage Datenschutz (BvD, Stuttgart)
11.-13.11.	Forensik (Secorvo College)
18.-21.11.	Information Security Management (Secorvo College)
24.-28.11.	T.I.S.P - Schulung (Secorvo College)
25.11.	OWASP Germany 2008 Conference (www.owasp.org, Frankfurt)
29.-30.11.	ruxcon 2008 (ruxcon.org, Sydney/AU)
Dezember 2008	
04.12.	„Das Original ist die beste Kopie“ (KA-IT-Si, Karlsruhe)
27.-30.12.	25th Chaos Communication Congress (CCC, Berlin)
Januar 2009	
20.-22.01.	Omnicard 2009 (inTIME, Berlin)

Fundsache

Am 29.09.2008 hat das US-amerikanische NIST in der Reihe Special Publication einen 80seitigen „Technical Guide to Information Security Testing and Assessment“ (NIST Special Publication 800-115) veröffentlicht, das eine sehr hilfreiche und praktisch-konkrete Handreichung zur Durchführung von Information Security Audits darstellt. Alle wesentlichen Risiken einer Netzwerkinfrastruktur werden betrachtet und eine systematische Vorgehensweise für deren Analyse vorgeschlagen. Abgerundet wird das instruktive Dokument durch eine aktuelle Liste frei verfügbarer Tools und Informationsquellen über bekannte Schwächen.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Alexander Göbel, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

November 2008



Editorial: Geschichtsvergessen

Das aktuelle Politbarometer der Mannheimer Forschungsgruppe Wahlen vom 21.11. 2008 enthält die erste repräsentative Befragung zur geplanten Ermächtigung des BKA zu Online-Durchsuchungen. Das ernüchternde Ergebnis: 57% der Deutschen halten die Befugnis für grundsätzlich richtig, 39% sprachen sich dagegen aus.

Ist das stereotype „ceterum censeo" des BKA-Präsidenten, eine verbreitete „Ich-hab-nichts-zu-verbergen"-Mentalität oder die mediale Beschwörung der terroristischen Bedrohung (zum Vergleich: 2007 starben in Deutschland 340 Menschen durch Mord, 600 bei Brandkatastrophen und knapp 5.000 bei Verkehrsunfällen – und niemand bei einem Terroranschlag) für dieses Ergebnis verantwortlich?

Vor 40 Jahren, im Sommer 1968, trieben die als „Ermächtigungsgesetz" geziehenen Notstandsgesetze der Großen Koalition Jugendliche und Studenten zu Tausenden auf die Straßen. Die Ermächtigung der Nachrichtendienste im G-10-Gesetz zu Eingriffen in das Post- und Fernmeldegeheimnis – unter strenger parlamentarischer Kontrolle durch die G-10-Kommission – war eines der zentralen politischen Reibungspunkte der Außerparlamentarischen Opposition, aus deren Trümmern zwei Jahre später die RAF hervorging.

Heute bleibt Deutschland angesichts der fortschreitenden Aushöhlung des Fernmeldegeheimnisses gelassen. Während die Liste der Katalogstraftaten in § 100 StPO, die Abhörmaßnahmen rechtfertigen, schrittweise ausgeweitet wurde und die Zahl der Abhöranordnungen von 1985 (1.400) bis 2007 (44.280) auf das 30-fache anstieg (vgl. SSN 06/2006), wirkt selbst die Aufregung über die Auswertung der Verbindungsdaten von Journalisten durch die Deutsche Telekom angestrengt. Bei der verfassungswidrigen Durchsuchung der Redaktionsräume des „Spiegel" im Jahr 1962 hatte es noch zu einer Entscheidung des BVerfG, dem Spiegel-Urteil vom 05.08.1966 gereicht.

Wie formulierte Alexis de Tocqueville 1835 doch so zutreffend: „Die schlimmsten Feinde der Freiheit – sind die glücklichen Sklaven."



Inhalt

Editorial: Geschichtsvergessen

Security News

Kryptographie bleibt schwierig

Neue Schlüssel – gute Schlüssel?

WPA-Erbsünde rächt sich

Sicherere Software

Mühsam nährt sich der Spammer

Social Communities für Eltern

Neuer NIST-Signaturstandard

Secorvo News

Secorvo College aktuell

Über Originale und Fälschungen

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Kryptographie bleibt schwierig

Mitglieder des Google Security Teams meldeten am 11.08.2008 in ihrem Blog eine Lösung für das Problem, wie Anwendungsentwickler Kryptoverfahren einfach und sicher einsetzen können: das bei Google gehostete Open-Source Crypto-Toolkit Keyczar. Zielpublikum für die in Java und Phyton vorliegende Keyczar-Implementierung sind primär Web-Entwickler – und zwar solche, die den Keyczar-Autoren zufolge schlimmstenfalls Schlüssel fest im Quellcode ihrer Anwendung hinterlegen würden.

Für Entwickler der letztgenannten Ignoranzklasse mag das Toolkit tatsächlich eine Hilfe sein. Ansonsten aber zeigt ein Blick in das Designdokument, dass Keyczar keine Konkurrenz für die direkte Nutzung von OpenSSL & Co. ist und hinter den eigenen Ansprüchen zurück bleibt. Denn nicht nur für die Bundesnetzagentur zählen SHA-1 und 1024 Bit DSA schon lange nicht mehr zu den „safe default algorithms and key lengths".

Schlimmer wiegt, dass Keyczar zwar optional geheime Schlüssel auch verschlüsselt ablegt, dafür aber einen unverschlüsselten Masterkey im eigenen Format braucht. Die Gefahr ist groß, dass Web-Entwickler die Schlüssel zwar nicht mehr im Quellcode „verstecken", dafür aber den Masterkey offen als Datei ablegen - und sich dabei sicher wähnen.

Das Zweitschlimmste nach dem Irrtum, Sicherheitsverfahren wären einfach selbst zu entwickeln, sind wohl Systeme, die vorgeben, dem Entwickler die nötigen Kenntnisse zu deren Einsatz zu ersparen.

Neue Schlüssel – gute Schlüssel?

Die am 07.11.2008 veröffentlichte NIST Special Publication 800-108 zum Thema „Key Derivation" zeigt, dass ein erläuternder Standard anstelle eines Black-Box-Toolkits wie Keyczar die Anwendung von Kryptoverfahren vielleicht nachhaltiger erleichtern kann.

Auf 20 Seiten wird dargestellt, wie sich aus einem vorhandenen Schlüssel viele (z. B. für automatisierte Schlüsselwechsel) ableiten lassen, wird hingewiesen, worauf beim Einsatz dieser Verfahren zu achten ist, und wird motiviert, warum manch scheinbar unnützer „Schnörkel" dabei hilfreich ist.

Das Dokument legen wir jedem Entwickler dringend ans Herz, der eine sichere Schlüsselverwaltung entwerfen will.

WPA-Erbsünde rächt sich

Als im Jahr 2001 nach erfolgreichen Angriffen auf das Wired Equivalent Privacy (WEP) Protokoll dringend Abhilfe für die Sicherung von WLANs gesucht wurde, war der erste Wurf für das neue Wifi Protected Access (WPA) Verfahren gar nicht so neu: Das Temporal Key Integrity Protocol (TKIP) des Standards IEEE 802.11i setzt auf der WEP-Verschlüsselung auf, ergänzt um weitere Sicherheitsmechanismen und regelmäßige Schlüsselwechsel. Durch diesen Trick wurde es möglich, allein per Firmware-Update aus vorhandenen, unsicheren WEP-Produkten neue WPA-Produkte zu machen.

Am 08.11.2008 veröffentlichten Martin Beck und Erik Tews, Forscher der Unis Dresden und Darmstadt (woher 2007 schon die bis heute schnellste WEP-Attacke stammt, vgl. SSN 04/07), einen Weg, um trotz der zusätzlichen Vorkehrungen in TKIP über eine ererbte WEP-Schwachstelle einen Teil des RC4-Schlüsselstroms von WEP bzw. TKIP zu ermitteln. Diese Information erlaubt es, einige wenige Datenpakete vom Access Point an WLAN-Clients zu fälschen, beispielsweise zum gezielten Umleiten von Verbindungen.

Wie vor zehn Jahren bei Daniel Bleichenbachers Angriff auf SSL mit RSA hilft hier wieder das Entgegenkommen der Protokolldesigner: Erst die Rückmeldung, die verrät, an welcher Stelle Entschlüsseln und Prüfen eingeschleuster Daten fehlschlagen, zeigt dem Angreifer, wie weit er vorgedrungen ist. Der neue alte Angriff ist nicht so fatal wie die WEP-Attacken und eröffnet keine völlig neuen Angriffswege gegen WPA oder den Nachfolger WPA2. Dennoch sollte man der AES-CCMP Verschlüsselung von WPA2 den Vorzug vor TKIP geben – oder zumindest die TKIP-Schlüsselwechsel auf unter 120 s beschleunigen.

Sicherere Software

Die Entwicklung sicherer Software liegt im Trend: Endlich wird das Problem „unsichere Software" an der Wurzel gepackt. Am 08.10.2008 hat das Software Assurance Forum for Excellence in Code (kurz SAFECode) den Leitfaden Fundamental Practices for Secure Software Development veröffentlicht. Die Organisation, der u. a. Microsoft, EMC und SAP angehören, hat sich zum Ziel gesetzt, zur Verbesserung von Methoden der Softwareentwicklung beizutragen – mit dem besonderen Schwerpunkt Sicherheit.

Das 22-seitige Dokument fasst nach Einschätzung der Autoren die zur Zeit effektivsten Methoden zur sicheren Entwicklung von Software zusammen. Die Darstellung praxiserprobter Vorgehensweisen wird ergänzt durch Verweise auf weiterführende Informationen. Daher kann der Leitfaden gut als Einstieg in die sichere Softwareentwicklung genutzt

werden. Er ergänzt die Übersicht über Fallstudien zum Thema sichere Softwareentwicklung, Software Assurance: An Overview of Current Industry Best Practices, die im Februar 2008 von SAFECode publiziert wurde.

Mühsam nährt sich der Spammer

Nicht nur Stammzellenforschung bringt Ethikkonflikte mit sich – bisweilen auch die IT-Sicherheit: Dürfen Forscher Spam-Mails verschicken, um deren Erfolg oder Misserfolg zu bestimmen? Ein Team aus Berkeley und San Diego (UCSD) stellt in einem Konferenzbeitrag vom 28.10.2008 dar, wie es einen Teil eines Bot-Netzes „zurückkaperte", um die ohnehin darüber versandten Spam-Mails zur statistischen Auswertung zu markieren. Neben dem Wirkungsgrad verschiedener Spam-Filter zeigte sich: Nur knapp eine von zehn Millionen Mails führt zum Kauf der beworbenen blauen Pillen.

Wie die Forscher aus der Strichprobe hochrechnen, dürfte die Marge bei diesem Aufwand-Ertrags-Verhältnis so gering sein, dass weiter verbesserte Anti-Spam-Techniken das Geschäftsmodell empfindlich treffen könnten. Das gibt Hoffnung auf ein mögliches Ende der Plage.

Social Communities für Eltern

Am 04.09.2008 veröffentlichte die Medienkompetenz-Initiative Klicksafe, ein Projekt der Landeszentrale für Medien und Kommunikation Rheinland-Pfalz (LMK), der Landesanstalt für Medien Nordrhein-Westfalen (LfM) und des Europäischen Zentrums für Medienkompetenz (ecmc) eine Handreichung für Eltern zum Thema Social Communities.

Der Kurzratgeber erklärt auf 12 Seiten kompakt und gut verständlich, welche Risiken auf Kinder und Jugendliche bei der Nutzung von Communities wie SchülerVZ & Co. sowie in den beliebten Chatrooms lauern. Die wichtigsten Punkte, die man mit seinen Kindern besprechen sollte, werden erläutert und durch Links auf weiterführende Informationen und Kontaktadressen ergänzt.

Unserer Ansicht nach eine empfehlenswerte Lektüre und ein gutes Hilfsmittel für Eltern – im übrigen nicht das einzige, das sich in der umfangreichen Materialsammlung der Initiative findet.

Neuer NIST-Signaturstandard

Das US-amerikanische National Institute of Standards and Technology (NIST) hat am 12.11.2008 die Entwurfsfassung eines neuen Standards für Digitale Signaturen (FIPS-186-3) veröffentlicht. Der Nachfolger des angejährten FIPS 186-2 vom Januar 2000 unterscheidet sich schon im Umfang erheblich: Aus 76 Seiten wurden 125, allein der „Kern" des Standards (ohne Anhänge) wuchs von vier auf 19 Seiten. Neben den auf dem Diskreten Logarithmusproblem basierenden Signaturverfahren DSA und ECDSA sind nun auch RSA-Signaturen Teil des Standards – nicht mehr nur als kurzer Verweis auf ANSI X.9.31, sondern mit einer mehrseitigen Darstellung der Anforderungen z. B. an die Schlüsselgenerierung. Deutlich erweitert wurden die Anhänge zur Primzahl- und Parameterberechnung.

Die Neufassung des Standards geht deutlich über den eigentlichen Zweck hinaus: Er wurde zu einem ausgewachsenen Leitfaden für Einsteiger und Programmierer erweitert. Der Qualität zukünftiger Implementierungen könnte das zuträglich sein.

Secorvo News

Secorvo College aktuell

Für die rechtzeitige Planung der Weiterbildung 2009 lohnt ein Blick in den Seminarkalender 2009. Neben vier Terminen zum Abschluss der TISP-Zertifizierung bietet Secorvo College 2009 erstmals – im Februar und im Oktober – die Zertifizierung zum CPSSE an: dem Certified Professional for Secure Software Engineering. Das Zertifikat wurde von ISSECO, dem International Secure Software Engineering Council, unter Beteiligung von u. a. der SAP AG entwickelt.

Detaillierte Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Über Originale und Fälschungen

Mit Dongles fing alles an – zwanzig Jahre später spricht man vom „Digital Rights Management", wenn es um den Schutz digitaler Güter geht. War es zunächst nur Software, die vor lizenzwidriger Verbreitung geschützt werden musste, zählen heute auch Daten zu den Schutzgütern – Musikaufnahmen, (Hör-) Bücher, Filme.

Auf dem letzten diesjährigen Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) wird Rüdiger Kügler von Wibu Systems, einem der Pioniere auf diesem Gebiet, am 04.12.2008 (Schlosshotel Karlsruhe, Beginn: 18 Uhr) spannende Rück-, Ein- und Ausblicke in die rasante Entwicklung des Lizenzmanagements geben. Im Anschluss gibt es wie gewohnt Gelegenheit zum „Buffet-Networking". Um Anmeldung wird gebeten.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2008	
25.11.	OWASP Germany 2008 Conference (www.owasp.org, Frankfurt)
Dezember 2008	
02.-04.12.	Sichere Softwareentwicklung (Secorvo, Karlsruhe)
04.12.	Das Original ist die beste Kopie (KA-IT-Si, Karlsruhe)
27.-30.12.	25th Chaos Communication Congress (CCC, Berlin)
Januar 2009	
20.-22.01.	Omnicard 2009 (inTIME, Berlin)
Februar 2009	
03.-04.02.	19. SmartCard-Workshop (Fraunhofer, Darmstadt)
10.-12.02.	Certified Professional for Secure Software Engineering (CPSSE) (Secorvo College, Karlsruhe)
22.-25.02.	16th Int. Workshop on Fast Software Encryption (IACR, Leuven/BE)
23.-26.02.	13th Financial Cryptography and Data Security 2009 (Int. Financial Cryptography Association, Barbados)

Fundsache

Der lesenswerte Leitfaden zur Nutzung von E-Mail und Internet im Unternehmen des BITKOM erschien im Januar 2008 in der aktualisierten Version 1.5. Das Dokument gibt einen Überblick über die Rechtslage, leitet daraus Empfehlungen für die rechtskonforme Gestaltung der E-Mail- und Internetnutzung ab und schließt mit Formulierungsvorschlägen für eine Betriebsvereinbarung.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Dezember 2008



Editorial: Pyrrhussiege

Einige zehntausend Kreditkartennummern der Landesbank Berlin auf Microfiche, vom Kurier gegen einen Christstollen getauscht. Bankverbindungen von 21 Mio. Bundesbürgern auf dem Schwarzmarkt, für kleines Geld von Call-Center-Mitarbeitern eingesammelt. CD mit 17 Mio. Kundendaten von T-Mobile aufgetaucht, von einem Dienstleister mit umfangreichen Berechtigungen entwendet. Alles Variationen desselben Themas: Zunehmend vertrauen Unternehmen sensible Unternehmens- und Personendaten Dritten an – die das Vertrauen nicht immer verdienen.

Zwar sind die Motive für eine Auslagerung von Tätigkeiten an externe Dienstleister ebenso berechtigt wie nachvollziehbar. Für größere Flexibilität und transparentere Kosten zahlt man aber einen versteckten Preis: geringere Loyalität und Bindung an das beauftragende Unternehmen, eingeschränkter Einfluss auf die Prozesse und geringes Verständnis der Kerngeschäftsprozesse beim Dienstleister.

Für zahlreiche Tätigkeiten mag das unproblematisch sein. Immer öfter aber sind sensible Daten betroffen, die eine hohe Zuverlässigkeit und Vertrauenswürdigkeit des Personals erfordern: Reinigungskräfte, die sich außerhalb der regulären Arbeitszeiten im Unternehmen bewegen; Kuriere, die vertrauliche Daten unverschlüsselt transportieren; IT-Dienstleister, die Zugriff auf unternehmenskritische Daten erhalten.

Unabhängig von der erforderlichen Basis-Qualifikation, die für eine Dienstleistung erforderlich ist, erfordert ein angemessener Umgang mit sensiblen Daten jedoch sowohl hohe Loyalität und Vertrauenswürdigkeit als auch ein Mindestmaß an Verständnis für die Bedeutung der Daten, um Schäden durch Nachlässigkeit zu vermeiden.

So entpuppen sich die schönen Reduktionen auf der Ausgabenseite der Bilanz immer öfter als Pyrrhussieg. Denn externe Dienstleistung erfordert sorgfältige Auswahl und Kontrolle – wer das vernachlässigt, zahlt meist einen hohen Preis, wenn etwas schief geht.



Inhalt

Editorial: Pyrrhussiege

Security News

Autorun deaktiviert?

Handys aller Orten

Blackberry zertifiziert

ePA-Akteptanzstellen gesucht

Forensische Päckchen

OWASP-Start in Deutschland

Flickwerk Patchen

Secorvo News

Secorvo College aktuell

Zum Schluss ...

Veranstaltungshinweise

Fundsache

Security News

Autorun deaktiviert?

Seit vielen Jahren predigen Security-Experten, wie gefährlich das automatische Starten von Anwendungen auf Wechseldatenträgern mittels Autorun-Funktionalität ist, haben Viren und Würmer so doch leichtes Spiel. Glücklicherweise ist das Deaktivieren der Autorun-Funktion in Windows technisch trivial und wird daher in vielen Unternehmen zentral über Group Policy Objekte durchgesetzt.

Aber ist es wirklich so trivial? Still und heimlich gestand Microsoft in einem Technet-Artikel vom 10.10.2008, dass das Setzen von NoDriveTypeAutorun in der Windows-Registry nicht ausreicht – und beschrieb die korrekte Erzwingung der Deaktivierung des Autorun-Registrierungsschlüssels in Windows. In vielen Umgebungen wird „die Autorun-Features nicht ordnungsgemäß deaktiviert", selbst wenn die Registry-Schlüssel korrekt gesetzt waren. Microsoft reagierte nun mit zahlreichen Updates sowie einem weiteren Registry-Schlüssel, genannt „HonorAutorunSetting". Nomen est omen. Peinlich, peinlich.

Handys aller Orten

Die Positionsbestimmung von Mobiltelefonen durch eifersüchtige Ehepartner und andere Bedarfsträger ist schon seit einer Weile einer der gefragtesten Location Based Serivices (LBS) für Mobilfunknetze. Zwar lassen sich LBS am Handy deaktivieren; dazu haben die deutschen Provider am 14.10.2008 eine Selbstverpflichtung auf ein einheitliches Verfahren veröffentlicht. Aber auch wenn auf dem Handy keine LBS aktiviert sind, werden Bewegungsdaten an Dritte weiter gegeben: So meldete T-Traffic am 03.11.2008, dass für die Stauprognose auf die Bewegungsdaten von 34 Millionen Handys im Netz der T-Mobile zugegriffen wird – „natürlich anonym". Pikant: T-Traffic wurde am 20.11.2008 von einer Nokia-Tochter in den USA übernommen; die Daten verlassen also den Geltungsbereich der EU-Datenschutzrichtlinie. Auch der Mitbewerb gibt sich nicht zugeknöpfter: Bereits am 14.01.2008 vereinbarte Vodafone Ähnliches mit TomTom.

Dass Handy-Ortung mit besseren Funkmessdaten noch präziser funktioniert als auf den Radius der mehr oder minder großen Funkzelle genau, gehört zur Lehrbuchweisheit. Am 01.12.2008 verkündete Bayerns Innenminister den praktischen Vollzug: Das dortige LKA hat in einer Art „Wardriving per Streifenwagen" einen Großteil der Mobilfunkzellen im Land vermessen und kartografiert. Eingesetzt wird das System zur Suche nach Verunglückten – und „noch nicht" zur Fahndung.

Alles in allem ein paar gute Gründe (mehr), das Handy immer öfter einfach abzuschalten.

Blackberry zertifiziert

Vor mehr als drei Jahren wurde nach einem umstrittenen Kurzgutachten des BSI das Testlabor des Fraunhofer Instituts SIT in Darmstadt vom Hersteller Research in Motion (RIM) mit einer Analyse der Sicherheit des Blackberry-Dienstes beauftragt. Am 24.11.2008 wurden nun das lange erwartete Zertifikat (gültig für BES v4.1.6) und der 33seitige Zertifizierungsbericht veröffentlicht.

Das Ergebnis ist eindeutig und belegt die Sorgfaltsmängel des BSI-Gutachtens vom Herbst 2005: „In our analysis of the BlackBerry Enterprise Solution, we did not find any evidence for the existence of a master key, back door or a function that would allow RIM to read customer's emails." Es ergänzt die von Secorvo im November 2005 publizierte Analyse der Blackberry-Architektur um eine Bestätigung der korrekten Implementierung des AES-256 und des Schlüsselmanagements.

Neben den im Zertifizierungsbericht enthaltenen Hinweisen zur sicheren Konfiguration des BES ist der „Blackberry Hardening Guide" des australischen Department of Defense vom 18.12.2007 zu empfehlen. Er enthält auf 27 Seiten zahlreiche detaillierte Konfigurationstipps für die sichere Nutzung des Blackberry – einschließlich Vorgaben für die Nutzung von S/MIME, PGP und TLS.

ePA-Akteptanzstellen gesucht

Es hat etwas von einem Gewinnspiel: Aus Unternehmen, Institutionen und Behörden, die bis zum 28.02.2009 dem Aufruf zum Anwendungstest für den elektronischen Personalausweis (ePA) – nicht zu verwechseln mit EPa – folgen, werden zehn ausgewählt. Sie können schon ab 01.10.2009 mit fachlicher Unterstützung des Bundesministeriums des Innern (BMI) die Nutzung des Identitätsnachweises über den ePA im Internet, an Automaten oder anderen Akzeptanzstellen erproben.

Leichtfertig sollte man dem Aufruf vom IT-Gipfel in Darmstadt am 20.11.2008 jedoch nicht mit seiner Registrierung folgen. Denn auch dieses Gewinnspiel hat einen Haken: Alle Bewerber – auch die nicht ausgewählten, deren Testphase nach Zeitplan am 01.12. 2009 beginnt – verpflichten sich, zahlreiche Eigenleistungen zu erbringen, von der Beschaffung bisher noch nicht verfügbarer Komponenten über die Akquise von Probanden bis zu gemeinsamen Marketing-Aktionen mit dem BMI. Bei positivem Testverlauf müssen sie ab dem Stichtag der ePA-Ausgabe am 01.11.2010 den ePA-Identitätsnach-

weis auch produktiv allen Ausweisinhabern unter ihren Nutzern anbieten.

Forensische Päckchen

Helix hat es vorgemacht (vgl. SSN 10/2008) – nun haben zwei weitere Anbieter neue Versionen ihrer kostenlosen forensischen Live-CDs veröffentlicht.

DEFT Linux (Digital Evidence & Forensic Toolkit) erschien am 28.11.2008 bereits in Version 4.01. Die Unterschiede zu Helix sind allerdings marginal: neben zu erwartenden Tools wie Autopsy, Sleuthkit oder foremost umfasst DEFT Linux Tools für Penetrationstests, bspw. Nessus und nmap. Vorsicht ist jedoch beim Anschluss externer Analyseplatten geboten: entgegen forensischer Best Practice werden diese nicht „read only“ eingebunden.

Äußerst vielversprechend sieht Version 0.4 von CAINE (Computer Aided INvestigative Environment) aus, die am 05.12.2008 veröffentlicht wurde. Auch CAINE bringt Standard-Tools mit, beinhaltet aber auch unbekanntere Forensiktools wie guymager, SFDumper oder Fundl. Herausragend ist das für Forensiker so wichtige Erstellen von Reports: CAINE stellt Mechanismen zur Verfügung, den Output der unterschiedlichen Tools in einem einheitlichen Format zu integrieren und erleichtert damit den Analyseprozess erheblich.

OWASP-Start in Deutschland

Über 100 Teilnehmer konnten sich am 25.11.2008 in Frankfurt davon überzeugen, dass das Thema Web Application Security inzwischen auch in Deutschland angekommen ist. Trotz äußerst kurzer Vorlaufzeit war die erste OWASP-Konferenz OWASP Germany 2008 sowohl im Hinblick auf die inhaltliche Qualität als auch auf die Teilnehmerzahl ein voller Erfolg. Es wurden technische Themen wie z. B. "Server- und Browser-basierte XSS Erkennung" oder "SOA Sicherheitsarchitektur" und nicht-technische Themen wie z. B. "Wirtschaftlichkeitsbetrachtungen von IT-Sicherheitsmaßnahmen" behandelt. Den Besuchern früherer KA-IT-Si-Veranstaltungen wird der Vortrag "Goldene Regeln der IT-Sicherheit bei der Beauftragung und Erstellung von Software" bekannt vorgekommen sein. Auch diese Konferenz bestätigt, dass sich die OWASP-Organisation national und international zu einer festen Größe im Zusammenhang mit der Sicherheit von (Web-)Applikationen entwickelt hat. Allen, die die Konferenz nicht besuchen konnten oder die Vorträge noch einmal nachvollziehen möchten, stehen die Präsentationsfolien auf der Konferenzseite zur Verfügung.

Flickwerk Patchen

Dass das Aktualisieren von Systemen und Anwendungen inzwischen eine herausfordernde und aufwändige Aufgabe darstellt, ist nichts Neues. Lücken im Patch-Management finden sich daher nicht selten – und sollten zügig geschlossen werden. Das unterstreicht eine aktuelle Veröffentlichung des Anbieters Secunia, der am 25.11.2008 Version 1.0 des für den Privatgebrauch kostenlosen Personal Software Inspector veröffentlichte. Die Auswertung der Analyseergebnisse von über 20.000 (überwiegend privaten) Client-Systemen nach einer Woche zeigte, dass weniger als 2 % der Systeme sowohl beim Betriebssystem als auch bei weiteren installierten Programmen auf einem aktuellen Stand waren.

Angesichts der Zunahme aufgedeckter sicherheitskritischer Bugs und immer kürzerer Reaktionszeiten der Angreifer-Szene ist eine regelmäßige Analyse des Patch-Stands sehr zu empfehlen.

Secorvo News

Secorvo College aktuell

Für Ihr großes Interesse am Weiterbildungsangebot von Secorvo College im Jahr 2008 danken wir Ihnen. Die starke Nachfrage und die vielen positiven Rückmeldungen haben uns sehr gefreut. Wir hoffen, Sie im kommenden Jahr auf einer unserer Veranstaltungen wiederzusehen – einen aktuellen Überblick finden Sie in unserem Seminarkalender 2009.

Auch für Ihre Anregungen und Themenwünsche an college@secorvo.de sind wir dankbar. Detaillierte Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Zum Schluss ...

Hinter uns liegen 10 Jahre aktiver Mitwirkung an IT-Sicherheit und Datenschutz in Deutschland – und das erfolgreichste Jahr unserer Firmengeschichte. Wir danken Ihnen für Ihr Vertrauen und freuen uns auf viele weitere herausfordernde und spannende Jahre der Zusammenarbeit.



Wir wünschen Ihnen besinnliche Feiertage – und für 2009 neue Ideen, Visionen und gutes Gelingen!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2008	
27.-30.12.	25th Chaos Communication Congress (CCC, Berlin)
Januar 2009	
20.-22.01.	Omnicard 2009 (inTIME, Berlin)
Februar 2009	
03.-04.02.	19. SmartCard-Workshop (Fraunhofer, Darmstadt)
10.-12.02.	Certified Professional for Secure Software Engineering (CPSSE) (Secorvo College, Karlsruhe)
19.02.	Bingo-Voting - verifizierbare elektronische Wahlen (KA-IT-Si, Karlsruhe)
22.-25.02.	16th Int. Workshop on Fast Software Encryption (IACR, Leuven/BE)
März 2009	
09.-13.03.	T.I.S.P.-Schulung (Secorvo College)
17.-18.03.	16. DFN Workshop - Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
17.-19.03.	IT-Sicherheitsaudits (Secorvo College)

Fundsache

Microsoft hat am 10.11.2008 eine öffentliche Beta-Version des "SDL Threat Modelling Tool v3.1" zum Download bereitgestellt. Die Bedrohungsanalyse (Threat Modelling) spielt im Secure Development Lifecycle (SDL) eine wichtige Rolle. Erste Tests mit diesem Tool hinterließen einen positiven Eindruck. Das Threat Modelling Tool findet sich u. a. im Tools Repository zum SDL.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Januar 2009



Editorial: Sammler

Die Begehrlichkeit kennt keine Schranken, nur Steigerung.
Lucius Annaeus Seneca (ca. 1-65 n. Chr.)

Wer die Datenschutzpraxis nicht nur aus den Gazetten kennt, den wundert eher Seltenheit als Ausmaß der aktuellen Datenschutzvorfälle. Technikentwicklung und explodierende Speicherkapazitäten lassen den Umfang personenbezogener Datensammlungen ständig anschwellen – deutlich schneller als die Sensibilität der für die Datenverarbeitung Verantwortlichen, und wohl auch die der Betroffenen.

Natürlich erfolgt die Verarbeitung immer zu deren eigenem Wohle: Schließlich geht es um zielgenauere Angebote, bedienungsfreundlichere Webseiten und Fehlerbeseitigung. Sobald ein „Mehrwert" winkt, sind die Betroffenen selbst nur zu gerne bereit, die Sammlungen um sensibelste Daten zu ergänzen.

Nirgendwo wird das deutlicher als am Beispiel von Google. Erst am 27.01.2009 hat das Unternehmen lautlos seine Datenschutzerklärung geändert: Neben den üblichen Web-Log-Daten (deren Zulässigkeit in Deutschland umstritten ist) und Cookies, die den Surfer eindeutig identifizieren, speichert Google nun auch Daten über die Nutzung der Google-Dienste. Chrome transferiert außerdem alle URLs, die der Nutzer besucht, direkt an Google. Und wer auf Seiten surft, die Google Analytics verwenden (99 % der Webseitenbetreiber ignorieren Googles Kennzeichnungspflicht), liefert Google sein komplettes Bewegungsprofil im Cyberspace. Schließlich sind da noch Google Mail und das Handybetriebssystem Android, bei denen Mail-Verzeichnisse, Adressbücher und Terminkalender nicht direkt mit dem lokalen PC, sondern über Googles Server abgeglichen werden.

Eine mächtige Datensammlung in den Händen eines einzelnen Unternehmens. Selbstverständlich werden diese Daten zu keinen anderen Zwecken genutzt als zu den in der Datenschutzerklärung angegebenen. Zumindest bisher. Wenigstens angeblich. Und gelöscht wird nach neun Monaten. Frühestens. Sagt Google.



Inhalt

Editorial: Sammler

Security News

PKI-Praxisprobleme

No Risk – No Web

Passwörter in Browsern

Gelöscht ist gelöscht

Common PKI 2.0 erschienen

Secorvo News

Secorvo College aktuell

Trau keiner Wahl ...

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

PKI-Praxisprobleme

Eine möglichst weitgehende Kompatibilität mit unterschiedlichen, besonders auch älteren Datenformaten ist in den meisten Fällen ein erwünschtes Merkmal von IT-Systemen – für die Sicherheit ist sie es häufig jedoch nicht. Ein Beispiel aus der PKI-Welt: Während Kryptologen wegen der Schwachstellen im Hashalgorithmus SHA-1 bereits einen SHA-3 suchen (SSN 10/2008), akzeptieren gängige Systeme immer noch klaglos dessen mittlerweile gebrochenen Urgroßvater MD5 (SSN 3/2005).

Am 30.12.2008 präsentierte Alexander Sotirov beim 25C3 Kongress, wie er zusammen mit Kollegen amerikanischer und europäischer Forschungseinrichtungen ein Sub-CA Zertifikat erzeugen konnte, das denselben MD5-Hashwert hat wie ein SSL-Zertifikat, das die Forscher von einem öffentlichen Trustcenter signieren ließen. Über den heimlichen Zwilling des regulär bezogenen Serverzertifikats wurden die Forscher quasi zum ebenso unautorisierten wie unkontrollierten Unterverkäufer des betroffenen Anbieters – da es um eine Demonstration ging, rückwirkend nur bis Ende 2004. Während der Nutzen von SSL ohnehin umstritten ist, löste der Beitrag bei Trustcentern natürlich umgehend Aktivitäten und Klarstellungen aus.

Aber das Problem ist nicht auf SSL beschränkt: Am 17.01.2009 veröffentlichte Didier Stevens ein per Authenticode signiertes „Hello, World!"-Programm, dessen böser MD5-Zwilling, der damit ebenso gültig signiert ist, glücklicherweise nur so tut, als ob er die Festplatte löscht. Obwohl für den offiziellen Zeitstempel SHA-1 verwendet wird, gilt dieser ebenso für beide Programme, da in Authenticode-Zeitstempel nur die angebrachte Code-Signatur, nicht aber der eigentliche Programmcode eingeht. Die Software von Peter Selinger zum Erstellen von Programm-Zwillingen ist ebenfalls im Netz verfügbar.

Nicht den MD5, sondern die in der Praxis eher ungebräuchlichen Signaturalgorithmen DSA und ECDSA betrifft ein Security Advisory des OpenSSL Projekts vom 07.01.2009. Die OpenSSL-Implementierung derartiger Signaturen liefert bei der Prüfung u. U. andere Fehlercodes als beim verbreiteten RSA-Verfahren. OpenSSL selbst und weitere betroffene Systeme lassen auch „rechnerisch falsche" Signaturen als gültig durchgehen, weil sie diese speziellen Fehlercodes nicht richtig auswerten.

Allen drei Fällen ist gemeinsam, dass ihnen am einfachsten beizukommen wäre, wenn es die PKI-Software erlaubte, die für Zertifikats- bzw. Signaturprüfung akzeptablen Algorithmen auf diejenigen zu beschränken, die als sicher gelten und auch tatsächlich gebraucht werden. Die Herausforderung für die Hersteller wäre dabei nicht, diese Funktionalität einzubauen, sondern sie so umzusetzen, dass Anwender sie einfach und effektiv nutzen können.

No Risk – No Web

Die detaillierte Analyse „Bootkits – die Herausforderung des Jahres 2008" von Kaspersky Lab, publiziert am 18.12.2008, führt erneut eindrucksvoll vor Augen, welchen Bedrohungen alle Nutzer beim Surfen im Web ausgesetzt sind. Die Erkenntnisse sind keine bahnbrechenden Neuigkeiten. Ein Google-Whitepaper vom 04.04.2007 mit dem Titel „The Ghost In The Browser" enthält umfangreiche Analysen ähnlicher Bedrohungen beim Surfen im Web. Allerdings wird in der Bootkits-Analyse verdeutlicht, wie verschiedene Eigenschaften und architekturbedingte Schwachstellen oder Mängel des Internets clever ausgenutzt werden, um zufällige Opfer mit Schadsoftware zu infiltrieren.

Zur Zeit gibt es keine umfassenden Schutzmechanismen gegen entsprechende Attacken durch Drive-by-Downloads. Die meisten Ansätze erfordern entweder hohe Anpassungs- und Wartungsaufwände oder werden als Einschränkung des „Surfgenusses" empfunden; beides ist mit geringer Akzeptanz verbunden. Trotzdem sind aktuelle Virenscannersuites, spezielle Surftools (z. B. NoScript, RequestPolicy und zukünftig auch Application Boundaries Enforcer) sowie eine gehörige Portion Vorsicht angeraten, um wenigstens gegen die häufigsten Angriffe gewappnet zu sein. Unter Umständen kann ein Werkzeug wie Bothunter helfen, Fälle aufzuspüren, bei denen das Kind schon in den Brunnen gefallen ist. Leider ist das in der Regel nicht leicht zu erkennen.

Passwörter in Browsern

Am 12.12.2008 veröffentlichte Robert Chapin die Ergebnisse eines umfangreichen Tests der Passwortmanager aktueller Versionen der Windows-Browser Firefox, Chrome, Opera, Safari und Internet Explorer. Die Ergebnisse sind ernüchternd: Von 21 Tests bestanden Firefox und Opera ganze sieben – und schnitten damit am besten ab. Chrome und Safari erfüllten nur zwei Sicherheitsanforderungen.

Besonders ernüchternd: Allein Firefox und Opera überprüfen, ob das automatisiert eingetragene Passwort auch von derselben Internet-Adresse stammt, für die es gespeichert wurde, und ob das Protokoll (bspw. http vs. https) übereinstimmt. Und lediglich Firefox erwartet – als einziger der getesteten Browser – die Zustimmung des Nutzers, wenn Herkunftsadresse oder das Übermittlungsprotokoll im entsprechenden Eintrag des Passwortmanagers überschrieben werden soll.

Zwar sollte man zumindest auf mobilen Geräten ohnehin von der Nutzung eines Browser-Passwortmanagers absehen, sofern das System nicht vollständig verschlüsselt ist. Denn der verschlüsselte Passwort-Speicher könnte auf einem verlorenen System einer Brute Force-Attacke zum Opfer fallen. Dennoch ist eine Browser-Attacke für einen Angreifer sehr viel attraktiver: Mühe- und spurenlos lassen sich bei entsprechender Verbreitung der Schadsoftware in kürzester Zeit Millionen Passwort-Datensätze einsammeln – und sogar automatisiert missbrauchen. Ein Browser mit fehlerhaftem Passwortmanager ist ein Blankoscheck für „Drive-by"-Angreifer.

Wer sicher gehen will, dass der Passwortmanager seiner Browser-Version zumindest den wichtigsten Anforderungen genügt, sollte sie der von Chapin entwickelten Online-Überprüfung unterziehen.

Gelöscht ist gelöscht

Bekanntlich führt das Löschen einer Datei in modernen Betriebssystemen nicht zur Beseitigung der Daten vom Speichermedium. Zur großen Freude von Forensikern lassen sich daher oft alle Dateien rekonstruieren, die jemals auf einer Festplatte gespeichert wurden. In der Maßnahmenempfehlung M 2.167 der IT-Grundschutz-Kataloge des BSI wird für das sichere Löschen von Dateien folgerichtig ein zwei- bis dreimaliges Überschreiben empfohlen.

Datenschützer gehen noch weiter: Im IT-Grundschutz-Baustein B 1.5 „Datenschutz" vom 04.07.2007 werden für das datenschutzgerechte Löschen von personenbezogenen Daten mindestens sieben, bei Daten hoher Schutzstufe sogar 33 Überschreibzyklen gefordert. Diese Forderung dürfte auf eine (missverstandene) Veröffentlichung von Peter Gutmann („Secure Deletion of Data from Magnetic and Solid-State Memory") vom 22.07.1996 zurück gehen – die sich auf inzwischen veraltete Festplattentechnologie bezog. Daher sorgte der Beitrag „Overwriting Hard Drive Data: The Great Wiping Controversy" von Craig Wright, Dave Kleiman und Shyaam Sundhar auf der ICISS 2008 (16.-20.12.2008) für Wirbel: Abgesehen von ein paar technischen Fehlern (siehe „Further Epilogue" in Gutmanns Papier) stellen die Autoren überzeugend klar, dass die Rekonstruktion eines einzigen, einmal überschriebenen Bits immer nur mit einer gewissen Wahrscheinlichkeit gelingt. Selbst wenn die Erfolgsaussicht 99,9 % erreicht, liegt die Wahrscheinlichkeit, eine nur 2 kB große Datei zu rekonstruieren, bei 0,000076 % (so viel wie ein 6er im Lotto). Merke: Ein einfaches, einmaliges und vollständiges Überschreiben genügt für ein sicheres Löschen.

Common PKI 2.0 erschienen

Am 20.01.2009 wurde Version 2.0 der Common PKI-Spezifikation (ehemals ISIS-MTT) vom T7 e. V., dem Verband der Trustcenter-Betreiber, und dem TeleTrusT e. V. veröffentlicht. Die neue Version wurde – unter Mitwirkung von Secorvo – dem aktuellen Stand der in der Common PKI zusammengestellten und profilierten internationalen Standards angepasst und trägt so der Entwicklung auf dem Gebiet der PKI-Standardisierung seit der Publikation von ISIS-MTT 1.1 (am 16.03.2004) Rechnung.

Eine wesentliche Neuerung von Common PKI 2.0 stellt die Signatur-API dar, die das PKCS#11-Profil von ISIS-MTT 1.1 ersetzt. Sie basiert auf der eCard-API-Spezifikation des Bundes, ist aber deutlich kompakter, da sie sich auf die Funktionen beschränkt, die zur Anwendung der in Common PKI definierten Datenformate für Signatur und Verschlüsselung benötigt werden.

Secorvo News

Secorvo College aktuell

Seit 2004 haben mehr als 250 Sicherheitsexperten das T.I.S.P.-Zertifikat erworben. Im März steht das erste T.I.S.P.-Seminar bei Secorvo College auf dem Programm. Frühbucher sollten sich bis zum 09.02.2009 die letzten vergünstigten Plätze sichern.

Damit Softwareentwicklung in Zukunft sicherer wird, hat ISSECO einen international Zertifizierungsstandard für Software-Engineers entwickelt. Eine Schulung mit Prüfung zum CPSSE (Certified Professional for Secure Software Engineering) bietet Secorvo erstmals im Februar und September an.

Neben Klassikern wie IT-Sicherheit heute und PKI hält Secorvo College spannende neue Themen aus allen Bereichen der IT-Sicherheit für Sie bereit. Termine und Seminar-Details finden Sie im Seminarkalender und den ausführlichen Seminarprogrammen.

Trau keiner Wahl ...

... die du nicht selbst gefälscht hast: Auf dem ersten Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-SI) im neuen Jahr wird Dr. Jörn Müller-Quade das mit dem Deutschen IT-Sicherheitspreis 2008 ausgezeichnete "Bingo Voting" vorstellen – ein Verfahren, bei dem der Wähler einen Beleg erhält, der es ihm ermöglicht, die korrekte Zählung der eigenen Stimme zu überprüfen. Dr. Müller-Quade war einer der Gutachter vor dem Bundesverfassungsgericht zu elektronischen Wahlmaschinen und leitet das Europäische Institut für Systemsicherheit (E.I.S.S.). Der Vortrag findet statt am 19.02.2009 im Schlosshotel Karlsruhe, Beginn: 18 Uhr. Im Anschluss gibt es – wie gewohnt – Gelegenheit zum "Buffet-Net(t)working". Um Anmeldung wird gebeten.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2009	
03.-04.02.	19. SmartCard-Workshop (Fraunhofer, Darmstadt)
19.02.	Trau keiner Wahl, die du nicht selbst gefälscht hast (KA-IT-Si, Karlsruhe)
22.-25.02.	16th Int. Workshop on Fast Software Encryption (IACR, Leuven/BE)
März 2009	
09.-13.03.	T.I.S.P.-Schulung (Secorvo College)
15.-17.03.	Sixth IACR Theory of Cryptography Conference (IACR, San Francisco, US)
16.-19.03.	Third International Workshop on Secure Software Engineering (SINTEF, Fukuoka/JP)
17.-18.03.	16. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
17.-19.03.	IT-Sicherheitsaudits (Secorvo College)
24.-25.03.	Security Awareness (Secorvo College)
31.03.-03.04.	Forensik - Verfahren, Tools, Praxiserfahrung (Secorvo College)

Fundsache

Einer der häufigsten Fehler in Datenbank basierten Web-Anwendungen ist die Anfälligkeit für SQL-Injection (Platz zwei der OWASP Top 10). Am 05.12.2008 haben die Oracle-Mitarbeiter Mark Fallon, Bryn Llewellyn und Howard Smith ein 67seitiges White Paper („How to write SQL injection proof PL/SQL") mit wertvollen Hinweisen veröffentlicht, wie sich sichere SQL-Abfragen entwickeln lassen.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2009



Editorial: Double Cross

NSA offering ‚billions' for Skype eavesdrop solution.
The register, 12.02.2009

Der Psychologe und Kommunikationswissenschaftler Paul Watzlawick wäre begeistert gewesen. In „Wie wirklich ist die Wirklichkeit" erläuterte er 1976 anschaulich das Phänomen der Interdependenz, illustriert am Beispiel geheimdienstlicher Desinformation („XX"). Hier finden wir nun ein Exempel in Reinkultur. Was lässt sich aus dem angeblichen Angebot der NSA lernen? Dass sie Skype tatsächlich nicht abhören kann? Oder dass sie den Eindruck erwecken möchte, dass sie es kann, damit Nutzer sich auf die Vertraulichkeit verlassen – und hemmungslos offen kommunizieren?

Tatsächlich lässt sich die Aussage systematisch analysieren. Angenommen, das Gerücht ist wahr. Wann würde die NSA davon profitieren? Fall 1: Sie kann Skype bisher nicht entschlüsseln und findet jemanden, der Skype bricht. Dann kann sie es – und gewinnt, selbst wenn es bekannt wird (denn erstens wird das mglw. für eine Desinformation gehalten, und zweitens gibt es bisher keine gute Alternative). Allerdings kostet sie das einen Milliardenbetrag. Fall 2: Findet sie niemanden, bleibt die Situation, wie sie ist – die Nutzer wissen nicht, dass sie niemanden gefunden hat und nicht abhören kann. Fall 3: Sie kann Skype bereits entschlüsseln und findet niemanden, der es schafft. Auch dann gewinnt sie – denn das stärkt das Vertrauen der Nutzer in Skype. Kritisch ist allein Fall 4: Sie kann Skype entschlüsseln, und jemand bricht Skype. Dann kann sie verlieren – nicht nur einen Milliardenbetrag für etwas, das sie nicht braucht, sondern auch die Nutzer, die bisher darauf vertrauten, dass die NSA nicht mithören kann. Daraus lernen wir: Die NSA ist sich sicher, dass das Brechen von Skype schwierig ist – es ist ihr entweder sehr viel Geld wert, oder sie ist überzeugt, dass es niemandem gelingen wird.

Übrigens: Man munkelt, Secorvo habe Skype gebrochen, wolle das Wissen aber nicht an die NSA verkaufen.

Jetzt sind Sie dran.



Inhalt

Editorial: Double Cross

Security News

Wurm drin

Druckerpatch

Schwächelnde Profis

Web Apps – kritisch betrachtet

Sametime – Same Password

Helix ist tot, es lebe Helix

Online Games – Serious Business

TCG-versiegelt

Secorvo News

Secorvo College aktuell

Veranstaltungshinweise

Fundsache

Security News

Wurm drin

Nun gibt es sicherlich zahlreiche Gründe, sich für einen Computer des Herstellers Apple zu entscheiden. Ein Grund hat allerdings inzwischen nur noch wenig Überzeugungskraft: Das Betriebssystem OS X sei erheblich sicherer als Windows. Am 13.02.2009 veröffentlichte Apple das Sicherheitsupdate 2009-001 für Mac OS X 10.4 und 10.5. Damit stopft Apple insgesamt 48 Sicherheitslücken in über 20 Betriebssystemkomponenten, darunter ein kritischer Zero-Day-Bug im Safari-Browser. Wer – ungeachtet des schlechten Abschneidens beim Umgang mit Passworten (siehe SSN 01/2009) – die Windows-Version von Safari nutzt, sollte umgehend auf Version 3.2.2 wechseln.

Spätestens jetzt wird es Zeit, auch unter OS X die Software-Update-Funktion zu aktivieren. Denn nun ist auch für Apple-Nutzer das Paradies zu Ende. (Vielleicht hätten sie besser nicht hineingebissen.)

Druckerpatch

Es ist so weit: Die Sicherheitsdisziplin des Patchens hat nicht nur Apple, sondern auch die Peripheriegeräte erreicht. Am 04.02.2009 veröffentlichte HP einen Security Patch für seine Laser- und Farbdrucker, der eine kritische Sicherheitslücke schließt. Geschickt ausgenutzt kann sie Unberechtigten den Zugriff auf Druckdateien ermöglichen.

Angesichts immer leistungsfähigerer „Embedded Systems“ und der zunehmenden Vernetzung von Kleinstgeräten wird es nun nicht mehr lange dauern, bis Security Patches auch beim digitalen Bilderrahmen, dem MP3-Player und dem E-Book-Reader zur Gewohnheit werden – sofern die Hersteller nicht endlich beginnen, ihre Entwickler in sicherer Softwareentwicklung zu trainieren. Dann könnte es bald Zeit werden, vom PC zur Schreibmaschine „upzugraden“.

Schwächelnde Profis

Nachdem der Hashalgorithmus MD5 gebrochen und der Secure Hash Standard (SHA) von 1993 erst 2002 und erneut im Oktober 2008 wegen neuerer Angriffe aktualisiert werden musste, schrieb das US-amerikanische NIST am 02.11.2007 ähnlich wie 10 Jahre zuvor beim AES eine „Cryptographic Hash Algorithm Competition“ aus. Bis zum 31.10.2008 konnten Kandidaten für einen Nachfolger des SHA-2 (Arbeitstitel: SHA-3) gemeldet werden.

Zwei Tage vor Beginn der ersten Hash Function Candidate Conference an der Universität Leuven veröffentlichte Fortify am 20.02.2009 die Ergebnisse einer Analyse der Referenzimplementierungen von 42 der vom NIST für Runde 1 akzeptierten und noch nicht gebrochenen Kandidateneinreichungen.

Ergebnis: Bei sechs Kandidaten fand Fortify mit seinem Source Code Analyser sicherheitskritische Bugs. Besonders peinlich: Die Implementierung des MD6 von Ron Rivest enthielt allein drei (!) Buffer Overflows – und das, nachdem ein Buffer Overflow in der RSA-Referenzimplementierung erst 1999 fast alle SSL- und SSH-Implementierungen kaltgestellt hatte. Merke: Trau' keiner Referenzimplementierung, die Du nicht selbst geprüft hast. Erst recht, wenn sie von einem Kryptologen stammt.

Web Apps – kritisch betrachtet

Mit der am 18.12.2008 erstmalig auf der OWASP-Webseite erwähnten Neuauflage des „OWASP Testing Guide“ wurde ein bewährtes Standardwerk zur Analyse von Web-Applikationen aktuellen Anforderungen angepasst und noch einmal erweitert. Die aktuelle Version v3 erleichtert durch die Einführung von Referenznummern für Testfälle die Kommunikation über Applikationstests gegenüber der Vorgängerversion v2 erheblich.

Inhaltlich wurden die meisten technischen Tests aktualisiert. Einige Testfälle wurden neu sortiert, so dass der neue Guide sich deutlich flüssiger liest, obwohl er um knapp 80 Seiten gewachsen ist. Bei den Tests stechen folgende Änderungen ins Auge: die ausführliche Erweiterung um den Bereich „Configuration Management Testing“, die Ergänzung um Aspekte von „Authorization Testing“ und weitere Änderungen beim „Data Validation Testing“.

Der Ansatz einer ganzheitlichen Betrachtung der Sicherheit von Applikationen über deren gesamten Lebenszyklus steht auch weiterhin im Vordergrund des Guides.

Ergänzend zu dem OWASP-Guide, der eine analytische Sicht der Sicherheit bietet, beleuchtet ein Positionspapier der ENISA zu „Web 2.0 Security and Privacy“ aus dem Dezember 2008 Sicherheits- und Datenschutzrisiken bei aktuellen Trends im World Wide Web. Die Kombination aus motivierendem Überblick und technischem Handwerkszeug gibt Verantwortlichen ausgiebiges Know-How zur Verbesserung der Sicherheit im WWW an die Hand.

Sametime – Same Password

Am 31.01.2009 veröffentlichte Carl Tyler in seinem Blog ein aus Sicherheitssicht kritisches Feature von Lotus Sametime: Ab Version 7.5 kann durch ein Plugin auf die gespeicherten Kennwörter im Klartext zugegriffen werden. Diese Funktion unter-

stützt die Realisierung von Single-Sing-On, könnte aber in verschiedenen Angriffsszenarien ausgenutzt werden: Meldet sich ein Benutzer in einer anderen Community an, die die Installation von Plugins zulässt, können dort ein Plugin installiert und die Sametime-Kennwörter ausgespäht werden. Auch könnte sich über diese Funktion ein Sametime/ Notes-Administrator Zugang zu den Kennwörtern verschaffen. Beide Szenarien sind besonders kritisch, wenn die Sametime-Kennwörter (benutzerfreundlich per Passwortsynchronisation) auch für weitere Anwendungen verwendet werden und somit ein unbefugter Zugriff auf weitere Daten möglich ist.

Sofern nur die im Notes Client integrierte Version von Sametime verwendet oder Samtetime über IBMs LTPA-Token authentifiziert wird, kann die Funktion nicht genutzt werden. In der Stellungnahme des Herstellers IBM vom 06.02.2009 wird darauf hingewiesen, dass derartige Funktionen beabsichtigt sind – und auch bei anderen Produkten wie Browsern verwendet werden, um beispielsweise ein Single-Sign-On zu ermöglichen. Um den eigenen Sicherheitsansprüchen gerecht zu werden, ist vorgesehen, in einer Technote auf die potentiellen Sicherheitsprobleme hinzuweisen und zu definieren, wie ein Schutz – beispielsweise durch eine digitale Signatur und Autorisierung für Plugins – erreicht werden kann. Betroffene Unternehmen sollten diese Diskussion verfolgen.

Helix ist tot, es lebe Helix

Nessus hat es vorgemacht (vgl. SSN 06/2008) – nun hat auch e-fense als Entwickler des äußerst populären Forensik-Werkzeugkastens Helix sein Lizenzmodell geändert. Seit dem 23.01.2009 ist Helix weder Open Source noch frei verfügbar. Wer künftig „Helix Pro“ einsetzen möchte, muss sich für ca. 15 Dollar pro Monat beim Hersteller registrieren lassen – was freilich noch immer deutlich preisgünstiger ist als die meisten anderen kommerziellen Forensik-Tools. Glücklich schätzen können sich diejenigen, die vor wenigen Monaten die letzte freie Version heruntergeladen haben (vgl. SSN 10/2008).

Fast zeitgleich mit der Kommerzialisierung von Helix ist übrigens am 11.02.2009 eine Beta-Version von Backtrack erschienen – eine Live-Distribution, die zumindest rudimentäre Forensik-Funktionen enthält.

Online Games – Serious Business

Am 28.01.2009 wurde im Presseportal der Polizei Nordrhein-Westfalen über eine kuriose Diebstahlanzeige berichtet: Ein Spieler eines Online-Rollenspiels war seiner virtuellen, mit viel zeitlichem und finanziellem Aufwand erworbenen Ausrüstungsgegenstände beraubt worden.

Die Anzeige wirft zahlreiche technische und rechtliche Fragen auf. Interessant ist allerdings, dass die Fragestellung deutlich präsenter ist, als vielleicht angenommen. Schon im November 2008 beleuchteten 18 Autoren in einem ENISA-Bericht „Virtual Worlds, Real Money“ auf 80 Seiten Sicherheitsrisiken und Empfehlungen für „Massively-Multiplayer Online Games and Social and Corporate Virtual World“. Ereignisse in zahlreichen „virtuellen Welten“ – nicht nur in Second Life – dürften in den kommenden Jahren in wachsendem Maße Auswirkungen in der „realen Welt“ haben. Der kurzweilig geschriebene Bericht gibt davon einen ersten Eindruck.

TCG-versiegelt

Die Trusted Computing Group (TCG), der u. a. Hersteller wie HP, IBM, Lenovo und Sun Microsystems angehören, hat am 27.01.2009 zwei richtungsweisende Standards zur Verschlüsselung von Speichersystemen sowohl für Desktops und Laptops als auch für Enterprise Lösungen veröffentlicht.

Angesichts der schwer verdaulichen 80 bzw. 130seitigen Standards gerät leicht aus dem Blick, dass die TCG damit die Grundlage für eine einheitliche und von den Chips der PC-Hardware-Hersteller unterstützte Verschlüsselung von Speichermedien gelegt hat. Sollte sich der Ansatz durchsetzen, könnten verschlüsselte Festplatten in wenigen Jahren der „Hardware-Standard“ sein – und die heutigen Spezialanbieter einschlägiger Softwarelösungen sich auf die allein schon herausfordernde Aufgabe des Schlüsselmanagements konzentrieren.

Secorvo News

Secorvo College aktuell

Nur noch wenige Seminarplätze sind im März für Sie frei: Vom 09.-14.03.2009 können Sie Ihr Wissen mit dem begehrten T.I.S.P.-Zertifikat besiegeln. Wertvolle Tipps für die erfolgreiche Umsetzung von Sicherheitsmaßnahmen zur Schließung von Sicherheitslücken bekommen Sie im Seminar "IT-Sicherheitsaudits in der Praxis" - nutzen Sie Ihre Chance, bevor auch dieses Seminar vom 17.-19. 03.2009 ausgebucht ist.

Im April halten wir einen Klassiker zu Grundlagenthemen für Sie bereit: "IT-Sicherheit heute" vom 21.-24.04.2009. Buchen Sie Ihren Platz noch bis zum 16.03.2009 mit Frühbucherrabatt. Alle weiteren Termine und Infos finden Sie auch in unserem Seminarkalender 2009.

Programme und Online-Anmeldung unter
http://www.secorvo.de/college

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2009	
09.-13.03.	T.I.S.P.-Schulung (Secorvo College)
15.-17.03.	Sixth IACR Theory of Cryptography Conference (IACR, San Francisco, US)
16.-19.03.	Third International Workshop on Secure Software Engineering (SINTEF, Fukuoka/JP)
17.-18.03.	16. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
17.-19.03.	IT-Sicherheitsaudits (Secorvo College)
24.-25.03.	Security Awareness (Secorvo College)
31.03.-03.04.	Forensik - Verfahren, Tools, Praxiserfahrung (Secorvo College)
April 2009	
21.04.	2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (Usenix, Boston/US)
21.-24.04.	IT-Sicherheit heute (Secorvo College)
26.-30.04.	Eurocrypt 2009 (IACR, Köln)

Fundsache

Bereits am 10.12.2008 hat Google sein "Browser Security Handbook" unter Google Code veröffentlicht, um die Entwicklung sicherer Web 2.0-Anwendungen zu fördern. Seitdem haben die Autoren um Michal Zalewski die Gegenüberstellung der Sicherheitsfeatures aktueller Browser-Versionen aufgrund jüngster Tests mehrfach aktualisiert. Die Übersicht gibt wertvolle Hinweise zur Sicherheit aktueller Browser und geht damit über die Untersuchung von Robert Chapin (SSN 01/2009) hinaus.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2009



Editorial: Zwangsbeglückung

Vor 22 Jahren erblickte der erste E-Mail-Sicherheitsstandard das Licht der Welt: In RFC 989 spezifizierte John Linn im Februar 1987 „Privacy Enhancement for Internet Electronic Mail“, einen frühen Vorläufer von S/MIME. Obwohl zahlreiche E-Mail-Clients, darunter Thunderbird, Notes und Outlook, heute S/MIME-basierte E-Mail-Verschlüsselung standardmäßig unterstützen und OpenPGP-Verschlüsselung sogar über die freie GnuPG-Programmfamilie komfortabel genutzt werden kann, sind E-Mails nach wie vor zumeist elektronische Postkarten.

Eine willkommene Gelegenheit, behütend einzugreifen: „*Der moderne Staat steht deshalb vor der Aufgabe, im elektronischen Kommunikationsraum für eine Grundversorgung an Verbindlichkeit und Vertraulichkeit zu sorgen*“, so das BSI im BSI-Forum der Fachzeitschrift <KES> (1/2008). „De-Mail“ soll der Dienst heißen, der ab 2010 mit Hilfe privatwirtschaftlicher „Bürgerportale“ einen Schlussstrich unter die chaotische Internet-Kommunikation ziehen soll.

Bei genauer Betrachtung entpuppt sich De-Mail als missratener Versuch, der digitalen Signatur nach 12 Jahren Misserfolgsgeschichte doch noch in den Sattel zu helfen. Das Konzept krankt an denselben Designfehlern: Wer De-Mail nutzt, schickt eine nicht abstreitbare Nachricht. Der Empfänger wiederum ist verantwortlich für das fristgerechte Abholen elektronischer Zustellurkunden. Eine Verschlüsselung erfolgt hingegen nur zwischen Nutzern und Bürgerportalen.

Am 23.03.2009 erlitt der Gesetzentwurf zur Regelung der Bürgerportale vom 04.02.2009 eine empfindliche Schlappe: Die Empfehlung der Ausschüsse des Bundesrats ist ebenso klarsichtig wie vernichtend: So seien die „konkreten Sicherheitsanforderungen an mehreren Stellen unklar“ und die Pflicht des Empfängers zur regelmäßigen Leerung des Postfaches ein unzumutbarer Grundrechtseingriff. Offenbar gibt es noch Volksvertreter, die nicht vergessen haben, dass der Idealtypus des „modernen Staates“ kein Leviathan, sondern eine freiheitliche Ordnung ist.



Inhalt

Editorial: Zwangsbeglückung

Security News

Klare Absage

SSL-Authentifikation für alle

„Man in the Middle“ is back

Aktuelle Fehlerübersicht

Umstrittenes BDSG

AutoRun Revisited

Secorvo News

Secorvo College aktuell

Das Original ist die beste Kopie

Veranstaltungshinweise

Fundsache

Security News

Klare Absage

So deutlich hat das Bundesverfassungsgericht weder bei der Online-Durchsuchung noch bei der Vorratsdatenspeicherung geurteilt: Am 03.03.2009 erklärte es den Einsatz von Nedap-Wahlcomputern und die Bundeswahlgeräteverordnung (BWahlGV) vom 20.04.1999 für verfassungswidrig, da „sie keine dem verfassungsrechtlichen Grundsatz der Öffentlichkeit der Wahl entsprechende Kontrolle sicherstellt". Denn es gilt: „Beim Einsatz von elektronischen Wahlgeräten müssen die wesentlichen Schritte von Wahlhandlung und Ergebnisermittlung [vom Wähler] zuverlässig und ohne besondere Sachkenntnis überprüft werden können." Ein klares Votum für die Souveränität des Souveräns (siehe SSN 10/2008) – und das an der Universität Karlsruhe entwickelte und mit dem IT-Sicherheitspreis 2008 ausgezeichnete „Bingo Voting" (Kurzbeschreibung).

Keine drei Wochen nach dem Urteil berichtete Matt Blaze, Mitautor einer Studie über Sicherheitsmängel einer in den USA verbreiteten elektronischen Wahlmaschine, am 23.03.2009 über die Aufdeckung systematischer Wahlfälschungen in Kentucky: Sechs Wahlhelfer hatten eine Schwäche in der Benutzerschnittstelle der Wahlmaschine zur Veränderung von Stimmabgaben genutzt.

SSL-Authentifikation für alle

SSL – seit zehn Jahren unter dem Namen Transport Layer Security (TLS) genormt – ist ein bekanntes, bewährtes und deshalb von seinem ursprünglichen Zweck, der Absicherung von Webzugriffen, auch auf andere Bereiche wie z. B. VPN oder WLAN übertragenes Sicherheitsprotokoll. Sollte man meinen. Auch sollte sich im Jahr 20 nach der Erstveröffentlichung des X.509 Standards herumgesprochen haben, dass Zertifikate naturgemäß öffentliche Daten sind und für sicherheitsrelevante Operationen das private Gegenstück des per Zertifikat bestätigten öffentlichen Schlüssels benötigt wird.

Umso größer die Verwunderung, als Microsoft am 10.03.2009 im Security Bulletin MS09-007 einräumte, dass die SSL-Komponente in Windows – vom Veteranen Windows 2000 bis zum neuesten 64-Bit-System – bei der Client-Authentifikation jahrelang patzte: Zwar wurde die Gültigkeit des vorgelegten Zertifikats geprüft; der im Standard vorgeschriebene Schritt, per Signatur der ausgetauschten Protokollnachrichten zu verifizieren, dass der Client auch den passenden privaten Schlüssel verwendet, wurde jedoch eingespart. Tatsächlich akzeptierte der Server also jeden Client mit irgend einem gültigen Zertifikat - ob nun dem eigenen oder einem fremden.

Durch das weite Einsatzspektrum von SSL/TLS sind wahrscheinlich nicht nur IIS-basierte Webanwendungen von diesem Bug betroffen, sondern jede zertifikatsbasierte VPN-, WLAN- und NAC-Anmeldung, sofern dabei der Microsoft-eigene RADIUS-Dienst IAS zum Einsatz kommt.

Vielleicht haben sich die Microsoft-Entwickler bei der Implementierung auf das SSL-Diagramm in Wikipedia verlassen – das den wichtigen Verifikationsschritt ebenfalls fehlerhaft darstellt. Manchmal geht Studieren doch über Probieren.

„Man in the Middle" is back

Nachdem in der jüngeren Vergangenheit andere Themen öffentlich diskutiert wurden, ist kürzlich die Bedrohung durch "Man in the Middle"-Attacken wieder ins Zentrum der Aufmerksamkeit gerückt, insbesondere dank der Veröffentlichung des White Papers "Active Man in the Middle Attacks – A Security Advisory" von Roi Saltzman und Adi Sharabani aus der IBM Rational Application Security Group am 27.02.2009.

In der Präsentation und dem White Paper werden Szenarien vorgestellt, bei denen ein Angreifer als "Man in the Middle" nicht durch Mitlesen auf zufällig übertragene Credentials (Cookies) wartet, sondern Server-Antworten so manipuliert, dass der Client seine Credentials ohne Wissen des Benutzers an ausgesuchte Webseiten überträgt. Dabei wird kein Implementierungsfehler, sondern ein Design-Problem von HTTP ausgenutzt.

Erst wenige Tage zuvor war das Thema „Man in the Middle" (MitM) am 18.02.2009 auf der Blackhat 2009 von Moxie Marlinspike in seinem Vortrag "New Tricks For Defeating SSL In Practice" aus einem anderen Blickwinkel beleuchtet worden. Darin wurden MitM-Angriffe betrachtet, die mit Manipulationen an SSL-Zertifikaten arbeiten. Als „Proof of Concept" wurde das Tool sslstrip vorgestellt.

Die Präsentationen beider Autoren auf der OWASP AU 2009 wurden am 04.03.2009 von Robert Hansem („RSnake") auf ha.ckers.org kommentiert. Wir können uns seinem Fazit anschließen: Das Thema ist keineswegs neu, aber inzwischen stehen so mächtige Angriffswerkzeuge zur Verfügung, dass zu erwarten ist, dass diese in Zukunft verstärkt von Amateur-Hackern genutzt werden.

Aktuelle Fehlerübersicht

Am 10.03.2009 wurde Version 1.3 des von 50 führenden amerikanischen IT-Unternehmen und Organisationen getragenen Projekts Common Weakness Enumeration (CWE) vorgestellt. In dieser Liste

werden die aktuell wichtigsten und schwerwiegendsten Sicherheitsprobleme bei der Softwareentwicklung identifiziert. Dazu werden sicherheitsrelevante Fehlerquellen bei der Erstellung von Software systematisch erfasst und detailliert ausgewertet.

Entsprechend wurden die 2009 CWE/SANS Top 25 Most Dangerous Programming Errors an die Resultate der aktuellen Erhebung angepasst. Sie sollten an dem Arbeitsplatz eines jeden Softwareentwicklers hängen – gleich neben den OWASP Top 10.

Umstrittenes BDSG

In seiner Sitzung am 23.03.2009 befasste sich der Innenausschuss des Deutschen Bundestages mit den geplanten Änderungen im Bundesdatenschutzgesetz und dem Entwurf eines Datenschutzauditgesetzes (DSAG). Die Bundesregierung hatte hierzu im Dezember neue Texte vorgelegt, nachdem die Erstentwürfe vom Spätsommer in der Fachwelt insgesamt auf große Kritik gestoßen waren.

Leider folgt der aktuelle Entwurf des DSAG weiterhin einem einstufigen Verfahren, bei dem die Gutachter (Kontrollstellen) gleichzeitig die zertifizierende Stelle sein sollen. Es ist schlichtweg unerklärlich, warum die Bundesregierung hinter international übliche Standards zurückfallen will: Schließlich ist die Trennung von Begutachtung und Zertifizierung in einem zweistufigen Verfahren Voraussetzung für die Minimierung von Interessenskonflikten – und damit Garant für die Seriosität eines Zertifikats. Erwartungsgemäß erntete gerade diese Grundkonzeption allgemeines Kopfschütteln in der Expertenrunde.

Heftige Kontroversen wurden unter den Sachverständigen über die vorgesehenen Regelungen zum Listenprivileg ausgetragen. Sogar einige Abgeordnete ließen sich angesichts der teils recht emotional vorgetragenen Stellungnahmen zu flammenden Reden während der Anhörung hinreißen, die sonst der parlamentarischen Debatte vorbehalten sind.

Die auf dem Datenschutzgipfel im Herbst beschlossene Abkehr vom Opt-Out-Verfahren im Bereich der Werbung, Markt- und Meinungsforschung und des Adresshandels steht wieder zur Debatte. So sehr fühlen sich Versandhandel, Adresshändler und Verlage durch die Pflicht zur Einwilligungserteilung eingeschränkt, dass sie das Schreckgespenst tausender bedrohter Arbeitsplätze an die Wand malen. In wirtschaftlich problematischen Zeiten offenbar ein wirksames Argument, um das informationelle Selbstbestimmungsrecht wieder einmal hintenan zu stellen. Nun wird die Stellungnahme des Innenausschusses gespannt erwartet.

AutoRun Revisited

Schon am 08.11.2007 hatte Scott Dunn darauf hingewiesen – und war am 20.03.2008 vom US-Cert bestätigt worden: Die von Microsoft beschriebenen Maßnahmen zur Deaktivierung der AutoRun-Funktion funktionierten nicht korrekt (SSN 12/2008). Der von Microsoft am 08.07.2008 veröffentlichte Patch zur Behebung dieser Schwachstellen war allerdings zunächst nur für Windows Vista und Windows Server 2008 verfügbar – nicht für die weit verbreiteten Systeme unter Windows XP.

Wohl angesichts der Conficker-Wurm-Infektionen über USB-Sticks und eines neuen US-CERT Advisorys vom 20.01.2009 hat Microsoft endlich reagiert und am 24.02.2009 ein Security Advisory sowie Patches für Windows 2000, XP und Server 2003 zur Verfügung gestellt, die diese Gefährdung beseitigen.

Unsere Empfehlung: Wer zur Deaktivierung von AutoRun den neuen Patch installiert, sollte sicherheitshalber auch die Wirksamkeit überprüfen.

Secorvo News

Secorvo College aktuell

Nach der Zertifizierung ist vor der Zertifizierung: Vom **22. bis 26.06.2009** findet das zweite diesjährige T.I.S.P.-Seminar mit anschließender Zertifikatsprüfung statt. Vorher bietet Secorvo College mit dem „aktuellen Klassiker“ IT-Sicherheit heute vom **21. bis 24.04.2009** einen Überblick der zentralen Themen der IT-Sicherheit und vom **05. bis 08.05.2009** einen umfassenden Einblick in die Welt der Public Key Infrastrukturen, praktische Übungen inklusive.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Das Original ist die beste Kopie

Auf dem kommenden Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **07.05.2009** wird Rüdiger Kügler von WIBU SYSTEMS – einem der Pioniere auf dem Markt für Softwarelizenzmanagement – Hintergründe und aktuelle Herausforderungen des Schutzes digitaler Güter vor Plagiaten (vulgo Raubkopien) beleuchten und heutige "best practices" zur Realisierung des Lizenzhandlings vorstellen. Im Anschluss gibt es wie gewohnt Gelegenheit zum „Buffet-Networking“. Um Anmeldung wird gebeten.

Das darauffolgende KA-IT-Si-Event am **25.06.2009** – Vertrauen ist gut – Zertifizierung ist besser – ist einem Erfahrungsbereicht zur Zertifizierung nach dem Sicherheitsstandard ISO 27001 gewidmet.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2009	
21.04.	2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (Usenix, Boston/US)
21.-24.04.	IT-Sicherheit heute (Secorvo College)
26.-30.04.	Eurocrypt 2009 (IACR, Köln)
Mai 2009	
05.-07.05.	10. Datenschutzkongress 2009 (EUROFORUM, Berlin)
05.-08.05.	PKI (Secorvo College)
07.05.	Das Original ist die beste Kopie (KA-IT-Si, Karlsruhe)
18.-20.05.	IFIP SEC 2009 (IFIP, Zypern/CY)
20.-22.05.	2009 ADFSL Conference on Digital Forensics, Security and Law (ADFSL, Burlington/US)
Juni 2009	
08.-09.06.	DuD 2009 (Computas, Berlin)
22.-26.06.	T.I.S.P. Schulung (Secorvo College)

Fundsache

Am 25.03.2009 wurde Version 1.0 von OpenSAMM (Software Assurance Maturity Model) des Open Web Application Security Projects (OWASP) veröffentlicht. Das Modell beschäftigt sich mit der Bewertung der Sicherheit im Softwareentwicklungsprozesse. Dabei werden alle Aspekte von der Steuerung über die Entwicklung, die Tests bis hin zur Verteilung betrachtet. Auf 96 Seiten werden nicht nur abstrakte Anforderungen gestellt, sondern auch praktische Hinweise zum Einsatz verschiedener Maßnahmen zur Verbesserung der Softwareentwicklung gegeben.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Karin Schuler

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2009



Editorial: Kuckucks-Eier

Abgesehen von gesetzlichen Pflichten ist die Reduktion operationeller Risiken die einzige vertretbare Begründung für Investitionen in den Schutz sensibler Daten und Information.

Als Existenznachweis für solche Risiken erfreuen sich die Ergebnisse von Studien und Befragungen großer Beliebtheit – besonders, wenn Teilergebnisse die eigenen Argumente untermauern. Tatsächlich aber besitzen veröffentlichte Studien fast ausnahmslos dieselben Schwächen: die Zahl der Befragten ist gering, die Fragen unscharf und interpretationsbedürftig, was wiederum die Aussagekraft der Antworten schwächt, und die Auswertung ist oberflächlich bis tendenziös. Nicht zuletzt mündet die Auswahl der Befragten (überwiegend selbst IT-Sicherheitsbeauftragte) oft in der gegenseitigen Bestätigung gemeinsam geteilter Vorurteile.

Eindrucksvoll belegt dies der am 14.04.2009 publizierte 2009 Data Breach Investigations Report von Verizon, für den 90 Sicherheitsvorfälle systematisch analysiert wurden. Dabei zeigte sich: Die meisten Vorfälle hatten mehrere Ursachen und ließen sich nicht in die beliebten simplen Verursacherkategorien „Insider“ oder „Externer“ einordnen. Zahlreiche Hacking-Attacken wären ohne die Ahnungslosigkeit oder den Leichtsinn von Mitarbeitern nicht erfolgreich. Und: Die absolute Zahl bestimmter Angriffe und auch deren prozentualer Anteil sagt wenig über das tatsächliche Risiko, denn das wird wesentlich von dem durch den Angriff verursachten Schaden bestimmt.

Wer bei der Steuerung seiner Investitionen in die Informationssicherheit auf zweifelhafte Studienergebnisse setzt, lässt sich fremde Eier ins Nest legen. Belastbare Hinweise auf das tatsächliche eigene Risiko ergeben sich nur bei vorurteilsfreier und differenzierter Analyse und Bewertung der eigenen Schwachstellen.

Wer dennoch aus Scheu vor dem Ruf des „Propheten im eigenen Lande“ zu Studien greifen möchte, sollte es wenigstens mit Sir Winston Churchill halten: „Ich glaube nur der Statistik, die ich selbst gefälscht habe.“ Sofern das Zitat ihm nicht untergeschoben wurde.



Inhalt

Editorial: Kuckucks-Eier

Security News

Signatur-Ei

Konjunktur-Ei

RZ-Ei

Entwickler-Ei

Backbone-Ei

Ankündigungs-Ei

Datenbank-Ei

Wurm-Ei

Secorvo News

Secorvo College aktuell

Nächste KA-IT-Si-Events

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Signatur-Ei

Die Prüfung elektronischer Signaturen ist ein typisches Henne-Ei-Problem: Um eine Signatur zu prüfen, muss man auch das Zertifikat des Signierenden prüfen, das die Signatur einer ausstellenden Certification Authority (CA) trägt, die es wiederum zu prüfen gilt. Das Ganze muss man so lange fortsetzen, bis man am Ende der Kette bei einer vertrauenswürdigen, bekannten Henne (sprich: Root CA) bzw. deren Ei (sprich: Stammzertifikat) angekommen ist.

Doch damit nicht genug: Für jedes dieser Zertifikate im Eierkorb will auch noch validiert sein, ob es nicht bereits vor Erreichen seines aufgedruckten Haltbarkeitsendes als verdorben erkannt wurde. Dazu wird eine Sperrliste oder Online-Statusauskunft zu Rate gezogen, die – der Leser ahnt es sicher schon – ihrerseits signiert ist und über eine Kette von Zertifikaten geprüft werden muss, für die auch jeweils der Sperrstatus zu validieren ist – und so weiter und so fort ...

Und wie man beim Eierkauf schaut, ob die Eier auch keinen Knacks in der Schale haben, so ist zu prüfen, ob alle Signaturen mit sicheren Algorithmen und Schlüssellängen erstellt wurden. Weil aber bei letzteren nur besonders feine Nasen erkennen, wann sie faulig zu duften beginnen, veröffentlicht die Bundesnetzagentur (BNetzA) jährlich im Bundesanzeiger eine aktuelle Liste aller Algorithmen der Hkl. A (zuletzt am 27.01.2009).

Am 06.03.2009 nun wies die BNetzA darauf hin, dass einer vermeintlich qualifizierten Signatur ein gegenüber § 371a ZPO verminderter Beweiswert zukommt, wenn bei der Prüfung des ganzen Hühnerstalls voller Hennen und Eier ein fauler Algorithmus entdeckt wird, der nicht rechtzeitig durch eine neue Eierschale (sprich: Übersignatur) gekittet wurde. Damit ergibt sich als siebte Klasse elektronischer Signaturen (vgl. SSN 02/2003) die „qualifizierte Signatur Hkl. B“ – mit abgelaufener Mindesthaltbarkeit. Vielleicht sollten potenzielle Anwender schon einmal beim Eierkauf üben und die Augen für das Kleingedruckte offen halten.

Konjunktur-Ei

Die Bundesregierung verteilt gerade Ostergeschenke in Gestalt von Konjunkturpaketen. Darunter finden sich 30 Millionen Eier, die gemäß der Antwort auf eine Kleine Anfrage der FDP-Bundestagsfraktion vom 25.03.2009 zur Steigerung der IT-Sicherheit verwendet werden sollen.

So ist geplant, von Anfang 2010 an über eine Million „IT-Sicherheitskits“ in Form von Kartenlesern und Software zur Nutzung der optionalen Authentifikations- und Signaturfunktionen der elektronischen Gesundheitskarte und des künftigen elektronischen Personalausweises zu verschenken – bevorzugt an die Teilnehmer des geplanten Anwendungstests (vgl. SSN 12/2008). Wie praktisch: Ein Softwarepaket zur Installation auf Privatrechnern – „from the people who brought you the Bundestrojaner“. Wer wird sich wohl so ein Ei ins eigene Nest legen?

RZ-Ei

Die gleichzeitige Gewährleistung von Vertraulichkeit und Verfügbarkeit gespeicherter Daten ist oft ähnlich schwierig, wie ein Omelette zuzubereiten, ohne dabei die Eier zu zerschlagen – „wasch' mich, aber mach' mich nicht nass“. Ein besonders hübsches Beispiel für diese Quadratur des Eis ist die von der israelischen Firma Axxana vermarktete Daten-Black-Box (am 30.03.3009 von Gartner in den Rang eines „Cool Vendor in Storage Technology and Systems“ erhoben). Darin sollen die Daten eines Rechenzentrums ähnlich geschützt sein wie ein rohes Ei in der richtigen Verpackung.

Damit man dieses „Daten-Ei“ selbst in einem eingestürzten Gebäude schnell finden kann, hat es einen eingebauten Peilsender. Und will man auf die wertvollen Daten nicht warten, bis alle Trümmer beiseite geräumt sind, lässt sich über eine Fernbedienung das drahtlose Netzwerk der Box aktivieren. Fragt sich nur, woran die Box erkennen kann, dass sie unter Trümmern begraben liegt – und nicht die Aufmerksamkeit eines nicht-autorisierten Eiersuchers auf sich gezogen hat.

Entwickler-Ei

„Easter Eggs“ werden verborgene Funktionen in Programmen genannt, mit denen sich die Entwickler ein „Denkmal“ gesetzt haben. Alte Bekannte sind der Flugsimulator in Microsoft Excel oder Space Invadors in Word. Aber auch in zahlreichen aktuellen Programmversionen lassen sich „Easter Eggs“ finden. Oft sind sie im Umfeld der Versions- und Copyright-Angaben verborgen, und meist muss man Insider-Kenntnisse haben, um sie zu finden – wie die „about:robots“-Seite in Firefox. Eine der bekanntesten Sammlungen solcher Easter Eggs findet sich auf eeggs.com.

Derartige Eier sollten allerdings auch daran erinnern, dass sich in jedem Programm unbekannte Funktionen verbergen können – auch solche, die nicht einmal vom Programmierer intendiert waren. Und unter diesen Eiern kann das eine oder andere faul sein. Merke: Die Axt im Haus erspart den Zimmermann – und die Backdoor im Programm einen mühsamen Hackerangriff.

Backbone-Ei

Auch im Backbone-Bereich wurden erst kürzlich einige Eier gefunden, u. a. von Enno Rey und Daniel Mende, die diese am 16.04.2009 auf der Blackhat Europe vorstellten. In ihrer Präsentation zeigten sie, wie man die durch MD5 gesicherten Signaturen von BGP (Border Gateway Protocol) kompromittieren kann, zum Beispiel mit dem von ihnen entwickelten Tool bgp_md5crack. Außerdem stellten die Autoren fest, dass man die Vertrauensanker von MPLS-VPNs kritisch prüfen sollte.

Auch wenn die Angriffsmöglichkeiten durch Tools wie mpls_redirect entsprechende Zugangsmöglichkeiten im Core-Bereich voraussetzen, weist der Vortrag nach, dass der Zugang alleine ausreichen kann, um den Verkehr umzuleiten. Die unterhaltsamen Folien können von der Webseite der Autoren herunter geladen werden.

Ankündigungs-Ei

Am 20.03.2009 veröffentlichte das US Department of Homeland Security einen Bericht über eine Überprüfung der Sicherheitssysteme an verschiedenen amerikanischen Flughäfen, die im Vorfeld bei der TSA intern per E-Mail angekündigt worden war. Die Darlegung von Details der geplanten Tests in dieser E-Mail musste zwangsläufig zur Nutzlosigkeit der verdeckt geplanten Überprüfung führen.

Als Aprilscherz wäre der Bericht vielleicht lustig zu lesen; tatsächlich muss er als Lehrstück verstanden werden, wie Tests und Audits gerade nicht durchgeführt werden sollten.

Datenbank-Ei

Einen ganzen Korb fauler Eier präsentierte Oracle am 14.04.2009 in seinem vierteljährlichen Critical Patch Update Advisory (letzte Aktualisierung vom 22.04.2009): Insgesamt 43 kritische Sicherheitslücken stopfen die Patches. Darunter finden sich zwei, die durch Fernzugriff auf eine Oracle-Datenbank ohne Authentisierung ausgenutzt werden können, und zwei weitere, die auf dieselbe Weise Peoplesoft Enterprise betreffen – in vielen Unternehmen mit amerikanischen Müttern das führende HR-System.

Betroffene Unternehmen sollten umgehend patchen – und die Datenschutzbeauftragten kritisch nachfragen.

Wurm-Ei

Am 22.04.2009 entdeckte Manh Dzung, Senior Malware Analyst beim vietnamesischen Unternehmen Bach Khoa Internetwork Security in Hanoi, einen Wurm, der Captchas von Google Mail löst – und so in der Lage ist, anonym eine beliebige Anzahl von E-Mail-Konten anzulegen. Die Analyse der Captchas übernimmt ein auf einem kanadischen Server beheimateter Dienst, an den der Wurm die Captcha-Grafik per E-Mail sendet.

Den erhofften Schutz vor automatisierten Angriffen bieten Captchas (vgl. SSN 2/2008) nicht mehr – die Tricks von Würmern und Trojanern kombiniert mit der Leistungsfähigkeit heutiger Analyse-Algorithmen macht eine verlässliche Unterscheidung von Mensch und Maschine praktisch unmöglich.

Secorvo News

Secorvo College aktuell

Den Sommer beginnen wir mit der nächsten Gelegenheit zur Zertifizierung Ihrer persönlichen Qualifikation: Das zweite T.I.S.P.-Seminar dieses Jahres findet vom 22. bis 27.06.2009 statt – Zertifikatsprüfung inklusive.

Vom 20.06. bis 03.07.2009 erfahren Sie bei unserer einzigen diesjährigen Veranstaltung zum Thema Information Security Management alles über Konzepte, Praxiserfolge und konkrete Umsetzung.

Stichwort Umsetzung: Erfolgreiche Forensik benötigt komplexe organisatorische und technische Vorgehensweisen. Bei uns lernen Sie diese kennen und können sie aktiv einüben – vom 07. bis 10.07.2009.

Detaillierte Programme und Online-Anmeldung unter http://www.secorvo.de/college.

Nächste KA-IT-Si-Events

Die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) stellt seit ihrer Gründung im Januar 2001 auf fünf bis sechs Abendveranstaltungen pro Jahr aktuelle Themen der IT-Sicherheit in den Fokus. Am 07.05.2009 widmet sich Rüdiger Kügler von WIBU SYSTEMS – einem der Pioniere auf dem Markt für Softwarelizenzmanagement – in seinem Fachvortrag dem Schutz digitaler Güter vor Plagiaten. Im Anschluss werden die Diskussionen beim "Buffet-Networking" wie gewohnt vertieft.

Am 25.06.2009 wird Peter Zimmer von der prego services GmbH einen Erfahrungsbericht zur Zertifizierung nach dem Sicherheitsstandard ISO 27001 vorstellen. Für beide Events bitten wir um rechtzeitige Anmeldung unter www.ka-it-si.de.



Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2009	
05.-07.05.	10. Datenschutzkongress 2009 (EUROFORUM, Berlin)
07.05.	Das Original ist die beste Kopie (KA-IT-Si, Karlsruhe)
18.-20.05.	IFIP SEC 2009 (IFIP, Zypern/CY)
20.-22.05.	2009 ADFSL Conference on Digital Forensics, Security and Law (ADFSL, Burlington/US)
Juni 2009	
02.-05.06.	ACNS '09: International Conference on Applied Cryptography and Network Security (INRIA, Paris/FR)
03.-04.06.	ASIA '09: 4th Annual Symposium on Information Assurance (University at Albany, Albany/US)
08.-09.06.	DuD 2009 (Computas, Berlin)
21.-25.06.	Africacrypt 2009 (IACR, Gammarth/TN)
22.-26.06.	T.I.S.P. Schulung (Secorvo College)
30.06.-03.07.	Information Security Management (Secorvo College)

Fundsache

Die Mustervertragsanlage des Bitkom zur Auftragsdatenverarbeitung liegt nun in einer um eine englische Übersetzungshilfe erweiterten Fassung 2.1 vor. Die auf das Wesentliche beschränkte (und als Word-Formular verfügbare) Vertragsvorlage zur Umsetzung der Anforderungen aus § 11 BDSG an die Verarbeitung personenbezogener Daten im Auftrag liefert eine wertvolle Grundlage für die Erstellung angepasster Vertragsentwürfe – und wird insbesondere mittelständischen Unternehmen ans Herz gelegt.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Mai 2009



Der Feind in meinem PDA

„Es ist also die Geschichte der Natur wie der menschlichen Gesellschaft, aus der die Gesetze der Dialektik abstrahiert werden. (...) Und zwar reduzieren sie sich der Hauptsache nach auf drei: das Gesetz des Umschlagens von Quantität in Qualität und umgekehrt, (...)"
Friedrich Engels, Dialektik der Natur

Es gibt gute Gründe, der Neudefinition der Hegelschen Dialektik durch Marx und Engels mit Skepsis zu begegnen. Die rasante Entwicklung der Informationstechnik liefert jedoch zahlreiche Belege für die Plausibilität von Engels erstem dialektischen Gesetz: Immer wieder ist es deren Verbreitung, die zu qualitativ neuen Sichtweisen zwingt. Das gilt besonders für die IT-Sicherheit: Erst die Allgegenwart von PCs machte sie als Angriffsziel interessant, Client-Server-Architekturen erhöhten den Schutzbedarf, und deren universelle Vernetzung führte zu gänzlich neuen Schutzkonzepten.

Nun ist es wieder so weit: Der Siegeszug moderner Personal Digital Assistants (PDAs) fordert Sicherheitsarchitekturen heraus. Vor wenigen Jahren noch waren PDAs bestenfalls persönliche Kalender mit Adressbuch auf proprietären Spezialsystemen. Schadsoftware hatte Seltenheitswert, da Inkompatibilität und rudimentäre Kommunikationsschnittstellen eine nennenswerte Verbreitung verhinderte.

Das hat sich geändert. PDAs sind dabei, Laptops zu verdrängen. Die Beliebtheit von Blackberry und iPhone haben ebenso dazu beigetragen wie der Preisverfall bei Mobilfunk-Flatrates und die gestiegene Leistungsfähigkeit. Unternehmen reagieren auf diese Entwicklung, indem sie über Hersteller-APIs den PDA-Zugriff auf Unternehmenssoftware freigeben. Damit stellt ein PDA heute aus der Perspektive des Informationsschutzes dasselbe Risiko dar wie ein Laptop.

Allerdings: PDAs gehen häufiger verloren, sind ständig „online" (oft ohne Passwortsperre), werden selten „sauber" entsorgt und verfügen fast nie über eine Vollverschlüsselung. Und sind das perfekte Tool für Industriespione: Mit Kamera, Mikrofon, Online-Verbindung, GPS-Empfänger und Zugriffsrechten – und einem Nutzer, der jeden Hinweis auf eine „hippe" neue Applikation sofort dankbar umsetzt.



Inhalt

Der Feind in meinem PDA

Security News

Websecurity-Statistik

Malware explodiert

„GSG Botnetz"

News from OWASP

Offene Gesellschaften

Secorvo News

Secorvo College aktuell

... Zertifizierung ist besser

Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

Security News

Websecurity-Statistik

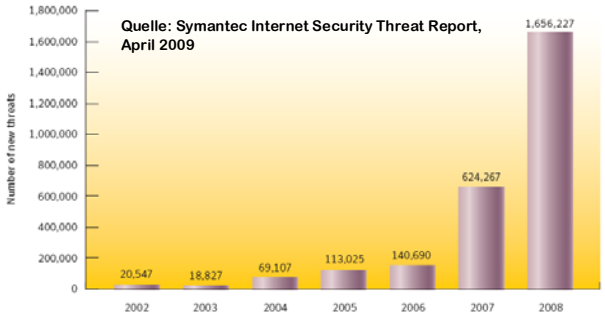
Zwar sollte man Statistiken grundsätzlich mit einer kritischen Distanz begegnen. Dennoch soll an dieser Stelle auf den Web Site Security Statistics Report der amerikanischen Firma WhiteHat Security, der am 18.05.2009 vorgestellt wurde, hingewiesen werden: Hinter diesem Bericht steckt unter anderem der Firmengründer und in Web-App-Security-Kreisen sehr geschätzte Jeremiah Grossman. Erschreckend ist, dass von den im ersten Quartal 2009 untersuchten Websites 82 % eine Schwachstelle aufwiesen, die von WhiteHat mit HIGH, CRITICAL oder URGENT bewertet wurde. Bei 63 % der Sites waren die Schwachstellen zum Veröffentlichungszeitpunkt noch nicht beseitigt.

Der Bericht stellt interessante aktuelle Entwicklungen vor und belegt viel diskutierte Sicherheitsprobleme von Webanwendungen mit konkreten Zahlen. Er kann auf der Webseite von WhiteHat zum Download angefordert werden.

Malware explodiert

Am 14.04.2009 hat Symantec den Internet Security Thread Report für 2008 veröffentlicht. Er dokumentiert die Fortsetzung einer beängstigenden Entwicklung: Die Zahl neuer Schadsoftware, die bereits 2007 auf mehr als das Vierfache angestiegen war, hat sich 2008 erneut vervielfacht – auf 1,65 Mio. Anders ausgedrückt: An jedem Kalendertag wurden 2008 im Schnitt über 4.500 neue Schadprogramme in die Welt entlassen.

Im vergangenen Jahr hatte die Zahl im Mittel noch bei etwa 1.700 gelegen. Eine solche Flutwelle lässt sich nur noch mit Heuristiken bewältigen: Virenscanner können neuartige Schadsoftware, die auf einen Schlag via Botnetz verteilt wird, nicht mehr an einer bekannten Signatur, sondern nur noch an „auffälligen" Eigenschaften erkennen. Daher steigt die Bedeutung einer alten Empfehlung wieder: Durch den Einsatz unterschiedlicher Scanner auf zentralen und lokalen Systemen und möglichst kurze Aktualisierungszyklen sollte die Qualität der Analyse optimiert werden. Und eine regelmäßige Komplettprüfung (vor allem mobiler) Endsysteme sollte ebenfalls etablierte „Best Practice" sein.



„GSG Botnetz"

Forschern der University of California ist es Anfang 2009 gelungen, das „Torping"-Botnetz zu übernehmen. In einem am 29.04.2009 veröffentlichten Forschungsbericht „Your Botnet is My Botnet" wird im Detail beschrieben, wie die dynamisch wechselnden Zieldomänen für die Command-und-Control-Server vorab bestimmt und reserviert werden konnten. Auf diese Weise konnten die Forscher – aus Sicht des Botnetz-Betreibers „feindliche" – C&C-Server aufbauen und darüber das Botnetz kontrollieren. Ein neues Binary des Botnetz-Betreibers, das an die infizierten Systeme verteilt wurde, unterband die Kontrolle nach zehn Tagen wieder.

Dennoch konnten in dieser Zeit über 70 Gigabyte an Botnetz-Daten, darunter zahlreiche Kennwörter gesammelt werden:

Data Type	Data Items (#)
Mailbox account	54,090
Email	1,258,862
Form data	11,966,532
HTTP account	411,039
FTP account	12,307
POP account	415,206
SMTP account	100,472
Windows password	1,235,122

Neben Details zur Funktionsweise stellten die Forscher fest, dass die Größe von Botnetzen vielfach überschätzt wird: Eine Unterscheidung zwischen infizierten Systemen und festgestellten IP-Adressen zeigt, dass aufgrund wechselnder IP-Adressen die reale Anzahl von „Zombies" erheblich kleiner ist als vermutet. Dennoch belegt das Beispiel eindrucksvoll die tatsächliche Gefährdung und verdeutlicht das Erfordernis, Systeme aktuell zu halten und Sicherheitssoftware wie Virenschutz und Personal Firewalls einzusetzen.

News from OWASP

Bei OWASP hat sich auch im Mai 2009 viel getan. Vom 13.-14.05.2009 fand in Warschau die OWASP AppSec Europe 2009 statt. Für Interessierte sind die Präsentationen von Tag 1 und Tag 2 inzwischen online verfügbar. Auf der Konferenz wurden in drei parallelen Tracks spannende Themen zur Sicherheit von Web-Anwendungen behandelt, darunter Vorträge zu den Themen „Threat Modeling", „The Bank in the Browser – Defending web infrastructures from banking malware", „CSRF: the nightmare becomes reality?" und „Factoring malware and

organized crime in to Web application security".

Im Schatten der OWASP-Konferenz wurde im Mai das OWASP PCI Project etabliert. Im Verlauf des Projekts sollen vereinheitlichte Anforderungen an Web-Anwendungen formuliert werden, die den Erfordernissen der Payment Card Industry Data Security Standards (PCI-DSS) der Kreditkartenorganisationen genügen.

Offene Gesellschaften

Bereits am 21.01.2009 veröffentlichte der ZEW-Forscher Dr. Wolfgang Sofka das Ergebnis einer in Zusammenarbeit mit Edlira Shehu von der Universität Hamburg durchgeführten Untersuchung über die Maßnahmen multinationaler Unternehmen zum Schutz vor unerwünschtem Informationsabfluss (Host Country Contingencies on Knowledge Protection Strategies of Multinational Firms).

Die zentrale Erkenntnis der Studie, gestützt durch eine Stichproben-Befragung von 1.500 deutschen Unternehmen, dürfte überraschen: Die ergriffenen Schutzmaßnahmen zur Verhinderung von Know-How-Diebstahl orientieren sich keineswegs an „Best Practices" oder etablierten Standards, sondern folgen überwiegend einem ökonomischen Kalkül: Hat ein ausländischer Standort den Status eines „Technologieführers", verlegen sich Unternehmen auf das Patentrecht und möglichst enge Kooperationen – mit dem Ziel eines für sie profitablen gegenseitigen Wissenstransfers. Umgekehrt steigt die Bedeutung von Abschottungsmaßnahmen, wenn ein Standort als technologisch rückständig gilt.

Selbstverständlich muss eine angemessene Klassifikation sensibler Daten in der Praxis einer realistischen Risikobewertung folgen. Zu kurz gesprungen erscheint allerdings die offensichtliche Zurückhaltung von Unternehmen in technologisch führenden Standorten – denn Wirtschaftsspionage ist schon lange kein nationales Problem mehr. So werden Patentschriften nicht nur im Inland gelesen, und die Spionageaktivitäten von Ländern mit technologischem Nachholbedarf konzentriert sich schon seit Jahren auf die „offenen" Gesellschaften des Westens, in denen das benötigte Wissen, wie die Studie belegt, oft viel leichter zugänglich ist.

Secorvo News

Secorvo College aktuell

In guten wie in schlechten Zeiten bleiben die Weiterentwicklung der persönlichen Qualifikation und deren Nachweis der Schlüssel für Ihre berufliche Entwicklung. Mit dem TISP bieten wir Ihnen die Möglichkeit, Ihre Kenntnisse auf hohem Niveau zu erweitern und mit einem anerkannten Zertifikat zu belegen. Acht Referenten bündeln ihr Wissen, ihre Expertise und ihre langjährige Berufserfahrung, um Ihnen in fünf Tagen die essentiellen Inhalte der Informationssicherheit zu präsentieren. Die nächsten TISP-Seminare finden statt am **22.–27.06.** und **07.–12.09.2009** (jeweils einschließlich Prüfung).

Vom **30.06.–03.07.2009** erfahren Sie bei unserer einzigen diesjährigen Veranstaltung zum Thema Information Security Management alles über Konzepte, Praxiserfolge und konkrete Umsetzung.

Detaillierte Programme, College-Jahreskalender und Online-Anmeldung unter http://www.secorvo.de/college.

… Zertifizierung ist besser

Am **25.06.2009** dreht sich bei der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) alles um das Thema ISO 27001: Im Rahmen des Events „Vertrauen ist gut – Zertifizierung ist besser" gibt Peter Zimmer von der prego services GmbH in Ludwigshafen mit einem Erfahrungsbericht Einblick in die notwendigen Vorbereitungen zur Erlangung der Zertifizierungsreife sowie die Wirkung des ISO-Standards im Geschäftsalltag. Um Anmeldung wird gebeten.

Tag der IT-Sicherheit

Gemeinsam mit dem Cyberforum und der IHK-Karlsruhe veranstaltet die KA-IT-Si am **16.07.2009** den ersten Karlsruher „Tag der IT-Sicherheit" im Saal Baden der IHK (Beginn: 14 Uhr, Teilnahmebeitrag 75 Euro). Neben Fragen der Haftung („Wer hastet, der haftet!") und einer aktuellen Einschätzung der Bedrohungen werden Unternehmen der TechnologieRegion in Erfahrungsberichten ihre „Best Practices" vorstellen: die Telemaxx Kommunikation GmbH, die Fiducia IT AG und die Edelstahl Rosswag GmbH – ausgezeichnet mit dem IT-Sicherheitspreis Baden-Württemberg 2007 bzw. 2009. Die Veranstaltung klingt ab ca. 18 Uhr mit einem KA-IT-Si-typischen „Buffet-Networking" aus.

Anmeldung bitte bis 09.07.2009 an Frau Helen Armbruster (IHK Karlsruhe), Tel.: 0721/174-190, helen.armbruster@karlsruhe.ihk.de.

Anschließend beginnt für die KA-IT-Si die Sommerpause – bevor es am **24.09.2009** mit dem Event „Pacta sunt servanda" zum Thema „Softwaresicherheit – Design by Contract" weitergeht.



Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2009	
02.-05.06.	ACNS '09: International Conference on Applied Cryptography and Network Security (INRIA, Paris/FR)
03.-04.06.	ASIA '09: 4th Annual Symposium on Information Assurance (University at Albany, Albany/US)
08.-09.06.	DuD 2009 (Computas, Berlin)
21.-25.06.	Africacrypt 2009 (IACR, Gammarth/TN)
22.-26.06.	T.I.S.P.-Schulung (Secorvo College)
25.06.	„Vertrauen ist gut – Zertifizierung ist besser“ (KA-IT-Si, Karlsruhe)
30.06.-03.07.	Information Security Management (Secorvo College)
Juli 2009	
06.-07.07.	SANS WhatWorks Summit in Forensics and Incident Response (SANS, Washington/US)
07.-10.07.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)

Fundsache

Ende August 2008 veröffentlichte Thomas Noon, inzwischen vereidigter Sachverständiger für IT-Systeme, seine Masterarbeit über „Geldspielgeräte und die SpielV“. Das Dokument ist ein weiteres erschütterndes Beispiel für die Risiken inkompetenter Digitalisierung ursprünglich analoger Geräte, wie erst unlängst bei Wahlmaschinen (SSN 10/2008) zu beobachten. Angesichts von Milliardenumsätzen geht es hier jedoch um Lizenzen zum Gelddrucken. Und wieder hat die PTB ihre Hand im Spiel ...



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2009



Riskante Mythen

Mythen erfreuen sich unausrottbarer Beliebtheit. Wie gerne glauben wir an einfache Erklärungen – besonders, wenn sie ein wohlfeiles Argument für vage Überzeugungen liefern, an unterschwellige Wünsche appellieren oder lieb gewonnene Vorurteile bestätigen.

1890 bestimmte der Physiologe Gustav von Bunge den Eisengehalt von 100 Gramm Spinat mit 35 Milligramm – von getrocknetem allerdings, dessen Eisengehalt zehnmal größer ist als der frischen Spinats. Das im Spinat enthaltene Eisen kann die menschliche Verdauung nicht einmal verwerten; dennoch glauben wir an dessen entwicklungsfördernde Kraft. Unzählige weitere Mythen bestimmen unsere Weltsicht: dass Lesen bei schlechtem Licht die Augen verdirbt oder wir nur einen Bruchteil der Kapazität unseres Gehirns nutzen. Alles Unsinn. Im Wochenmagazin DIE ZEIT geht Christoph Drösser seit 1997 in der Kolumne „Stimmt's?“ verbreiteten Alltagsüberzeugungen auf den Grund und konnte viele als überlieferten Irrglauben entlarven.

Offenbar hat auch das Fachgebiet IT-Sicherheit ein Alter erreicht, in dem sich Glaubenssätze einnisten, die ohne weitere Prüfung übernommen und weitergegeben werden. Selbst die IT-Grundschutz-Kataloge sind davor nicht gefeit, wie sich am Beispiel der Passwort-Empfehlungen (M 2.11) zeigen lässt. Dort wird eine Sperrung des Zugangs nach drei Fehleingaben empfohlen – eine Maßnahme, die keinerlei Sicherheitsgewinn bewirkt, jedoch kostspielige Kennwortrücksetzungen nach Urlauben und erzwungenen Passwortwechseln. Schlimmer noch: Sie ermöglicht simple Denial-of-Service-Angriffe – durch absichtliche Fehleingaben bei fremden Accounts. Ähnlich die Forderung nach Passworten mit mindestens einem nicht-alphabetischen Zeichen: Da die meisten Benutzer Ziffer oder Sonderzeichen anhängen, verkleinert sich dadurch der Suchraum. Viel wirksamer wäre eine um ein Zeichen erhöhte Mindestlänge.

Auch diese Mythen werden, so ist zu befürchten, weiterleben: „Es ist schwieriger, eine vorgefasste Meinung zu zertrümmern, als ein Atom“, wusste schon Albert Einstein.



Inhalt

Riskante Mythen

Security News

Windows 7 Security

SHA-1 auf Kollisionskurs

Opera Unite(d)

Security-Check für Anwendungen

Regenbogenbrecher

Phishing still alive

Secorvo News

Sicherheitsregion Karlsruhe

Veranstaltungshinweise

Fundsache

Security News

Windows 7 Security

Windows 7 soll im Oktober 2009 auf den Markt kommen und gegenüber Windows Vista verbesserte und neue Sicherheitsfunktionen enthalten. Eine Einführung in diese Funktionen bietet Chris Corio in einem Technet-Artikel vom 24.04.2009.

Neben der verbesserten Integration biometrischer Authentifzierungsverfahren und Verfeinerungen bei Bitlocker zur Festplattenverschlüsselung ist vor allem die neue Funktion „Applocker" viel versprechend. Durch eine zentrale Steuerung der Anwendungen, die durch einen Benutzer ausgeführt werden können, kann die Sicherheit maßgeblich gesteigert werden. Im Vergleich zu den bereits in XP und Vista vorhandenen „Software Restriction Policies" wurden das Management verbessert und weitere Funktionen etabliert, die es beispielsweise ermöglichen, die Auswirkungen von Policies vorab zu testen und den Umgang mit aktualisierten Programmversionen und Updates erheblich zu vereinfachen.

Sofern im Unternehmen Prozesse zur Freigabe von Software für die Benutzer etabliert sind, können diese durch diese neuen Funktionen technisch durchgesetzt werden – ein Gewinn vor allem für Unternehmen, die bisher über keine Kontrollmöglichkeit des Softwareeinsatzes verfügen.

SHA-1 auf Kollisionskurs

Die Krypto-Hashfunktion SHA-1 steht bekanntlich schon seit längerem unter Beschuss, und der Nach-Nachfolger SHA-3 macht sich bereit, in die Startblöcke zu steigen (siehe SSN 10/2008). In der Rump-Session der Eurocrypt 2009 kündigten drei australische Forscher am 28.04.2009 in Köln den bisher besten Angriff auf SHA-1 an, den sie am 02.06.2009 veröffentlichten. Er soll den Aufwand zum Finden einer Kollision auf 2^{52} Operationen reduzieren. Auch wenn bezweifelt wird, dass alle Annahmen der Autoren haltbar sind, und der Aufwand realistisch auf 2^{57} Operationen geschätzt wird, sinkt die Sicherheit des SHA-1 damit auf die des überholten DES (2^{56}).

Allerdings spielen Kollisionsattacken in der Praxis erst dann eine Rolle, wenn der Angreifer die beiden zur Kollision führenden Texte bzw. Dateien selbst konstruieren kann. Die Kunst besteht dann darin, ein „Zwillingspärchen" aus einem unverfänglichen Datum (z. B. einem Webserver-Zertifikat oder einem einfachen „Hello World"-Programm, SSN 01/2009), das man legal signieren lässt, und einem bösartigen Alter Ego (z. B. einem Zertifizierungsstellen-Zertifikat oder einem Programm mit Schadcode) zu wählen, das denselben Hashwert und damit dieselbe Signatur besitzt. Eine Signaturprüfung wird sowohl Jekyll als auch Hyde als gültig (und vertrauenswürdig) akzeptieren.

Eine solche Kollisionskonstruktion gelingt mit dem vorgestellten Angriff nur, wenn es gelingt, zu einer mehr oder weniger sinnlosen Zeichenfolge eine legale Signatur zu erschleichen. Und auch der Einsatz von SHA-1 zum Integritätsschutz per HMAC ist glücklicherweise nicht betroffen.

Opera Unite(d)

Am 16.06.2009 wurde die Opera-Browser-Nachfolger Unite (V10b1) verfügbar gemacht; eine portable Version soll folgen. Als Update ist er vollständig im Benutzerkontext installier- und nutzbar. Neu in Opera Unite sind „Social Network"-Server-Komponenten („Services"), durch die innerhalb von Minuten nach Beantragung eines (auch pseudonymen) Accounts bei Opera auf dem lokalen Clientsystem u. a. Filesharing und ein Webserver gestartet werden. Der Webserver ist direkt von Extern über einen Fully Qualified Domain Name (FQDN) erreichbar, sobald der Einstiegspunkt in die Dateiverzeichnisstruktur gesetzt wurde. Unter Windows sind auch Server-Shares in Gestalt zugewiesener Laufwerksbuchstaben möglich. Mit einer einfachen Google-Suche werden die Shares sichtbar.

Das verwendete Proxykonzept tunnelt dazu bestehende Firewallstrukturen, sofern ein Zugriff auf den Unite Proxy bei Opera auf Port 16680/tcp zugelassen ist. Ist der Unite Proxy nicht erreichbar und die UPnP-Option in Opera Unite aktiviert, wird ein Multicast auf Netz 239/8 nach RFC 3171 durchgeführt. Immerhin: Port Punching-Techniken à la Skype werden bisher nicht unterstützt – allerdings befindet sich die Software auch erst im Beta-Stadium.

Opera's Zielsetzung, mit diesem Konzept Daten in Social Networks wieder unter die Kontrolle der Besitzer zu stellen, in Ehren – ein Blick in Kapitel 7 der EULA („Use of Service") zeigt jedoch, dass es wohl eher auf eine Wahl zwischen Teufel und Beelzebub hinausläuft.

Security-Check für Anwendungen

Am 03.06.2009 wurde die erste Version des Application Security Verification Standard (ASVS) des Open Web Application Security Projekts (OWASP) veröffentlicht. Der Standard enthält eine Vorgehensweise zur einheitlichen Durchführung von Sicherheitstests von (Web-) Anwendungen und will damit vergleichbare Aussagen über das Sicherheitsniveau erreichen. Eine Überprüfung kann dabei auf einem von vier Ebenen erfolgen: Automatisierte Prüfung (L1), manuelle Prüfung (L2), Design-Prüfung (L3) oder interne Prüfung (L4).

Zu begrüßen ist, dass der Schwerpunkt des Standards auf der Überprüfung des Vorhandenseins effektiver Sicherheitsmechanismen liegt. Auf 42 Seiten werden neben der generellen Vorgehensweise der vier Überprüfungs-Level auch detaillierte Prüfvorgaben für jedes Level vorgegeben. Diese unterfallen in 14 Themengebiete, darunter Security Architecture, Authentication, Session Management und Access Control, und neben weiteren auch Input Validation, Cryptography und HTTP Security. Schließlich legt der ASVS Anforderungen an die zu erstellenden Sicherheitsberichte fest.

Damit steht Entwicklern, Betreibern und Nutzern eine unabhängige Grundlage zur Überprüfung der Sicherheit von (Web-) Anwendungen zur Verfügung. Der Standard wird sich im Zusammenspiel mit weiteren OWASP-Projekten durchsetzen, die sich in der Praxis bewährt haben (wie z. B. dem Testing Guide oder Development Guide). Aber Vorsicht: Auch hier darf der Blick auf das Zertifikat nicht die Beschäftigung mit dem Testbericht ersetzen.

Regenbogenbrecher

Eine Passwort-Mindestlänge von acht Zeichen gilt selbst bei alphanumerischen Passwörtern noch immer als solide Empfehlung, auch in den IT-Grundschutz-Maßnahmenkatalogen des BSI.

Dabei werden die Entwicklung der Rechenleistung aktueller PCs, die Nutzung von Grafikkarten durch moderne Cracking-Tools sowie die Auswirkungen der von Philippe Oechslin (EPFL) bereits auf der Crypto 2003 publizierten Optimierungen für Rainbow Tables offenbar erheblich unterschätzt.

Ein schneller PC berechnet heute 800 Mio. NTLM-Hashwerte pro Sekunde – und hat in knapp 80 Stunden alle möglichen achtstelligen alphanumerischen Passwörter durchprobiert. Mit einer schnellen Grafikkarte (2 Mrd. Hashes/sec.) genügen 30 Stunden – und unter Verwendung von Oechslins Rainbow-Tables vom 12.02.2009 (74 Mrd. Hashes/sec.) sogar 50 Minuten. Wenn sie einem Cracking-Angriff auf die SAM-Datei zumindest einige Tage widerstehen sollen, müssen alphanumerische Passwörter heute eine Mindestlänge von 10 Zeichen aufweisen.

Phishing still alive

Am 12.05.2009 belegte die Anti-Phishing Working Group (APWG) mit Veröffentlichung ihres „Global Phishing Survey", dass Phishing noch lange nicht tot ist. Der 26 Seiten starke Bericht über die Trends im zweiten Halbjahr 2008 dokumentiert knapp 57.000 Phishing-Attacken unter Benutzung von 30.500 Domain-Namen – aus 170 Top Level Domains (TLDs). 81 % der Angriffe wurden von kompromittierten Webservern ausgeführt. Phishing ist weiterhin ein attraktiver Markt – und die Phisher passen sich aktuellen Verteidigungstrends an.

Erfreulich: Die APWG bietet eine Hilfestellung für den Fall, dass eine Webseite einem Hacking-Angriff durch Phisher zum Opfer gefallen ist. Und auch für den Endverbraucher werden gute Ratschläge erteilt – wenn auch nur in Englisch.

Folgt man einem Positionspapier von Microsoft Research vom 01.09.2008, ist Phishing ein „Profitless Endeavour": Danach weisen die hohen Aktivitätszahlen darauf hin, dass – größtenteils erfolglose – Kriminelle verzweifelt versuchen, sich doch noch ein Stück vom vermeintlich großen Kuchen der aus Online-Konten zu phishenden Beträge abzuschneiden. Allerdings geht das Papier nur von „einfachen" Phishing-Mails aus, die Anwender dazu auffordern, ihre Passwörter auf einer betrügerischen Webseite einzugeben. Das mag in den USA ausreichen, um ein Online-Konto zu plündern – in Deutschland gehört die iTAN mittlerweile zum Mindeststandard.

Allerdings ist auch die iTAN für Täter dank Trojanern und Man-in-the-Middle Attacken nicht unüberwindlich, wie ein Beitrag des BKA auf dem BSI Sicherheitskongress am 18.05.2009 belegt. Ob die Microsoft-Autoren bedacht haben, dass vermeintlich leergefegte Phishgründe wieder ergiebig werden, wenn man statt einer Angelrute einen Trawler mit Echolot benutzt?

Secorvo News

Sicherheitsregion Karlsruhe

Das Hightech.Unternehmer.Netzwerk CyberForum, die IHK Karlsruhe und die KA-IT-Si laden zum ersten Karlsruher „Tag der IT-Sicherheit" am **16.07.2009** ein. Im Saal Baden der IHK werden ausgewiesene Experten aus der „Sicherheitsregion Karlsruhe" ab 14 Uhr mit spannenden Vorträgen („Die sieben Todsünden der IT-Sicherheit") und preisgekrönten Beispielen aus der Praxis, u. a. von der Edelstahl Rosswag GmbH und der Fiducia IT AG, Einblicke in ihre Erfahrungen und Anregungen zur Diskussion geben. Beim anschließenden Buffet-Networking ab 18 Uhr bietet sich die Gelegenheit, Fragen zu Haftung, Datenschutz und IT-Sicherheit mit Referenten und Gästen zu vertiefen.

Nähere Informationen und Anmeldung unter www.ka-it-si.de. Teilnahmegebühr: 75 Euro.



Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2009	
06.-07.07.	SANS WhatWorks Summit in Forensics and Incident Response (SANS, Washington/US)
16.07.	Tag der IT-Sicherheit (IHK Karlsruhe/CyberForum e.V./KA-IT-Si, Karlsruhe)
August 2009	
12.-14.08.	USENIX Security '09 (Usenix, Montreal/CA)
16.-20.08.	Crypto 2009 (IACR, Santa Barbara/US)
17.-18.08.	Digital Forensic Research Workshop (DFRWS, Montreal/CA)
31.08.-04.09.	TRUSTBUS 09: 6th International Conference on Trust, Privacy & Security in Digital Business (University of the Aegean, Linz/AT)
September 2009	
07.-11.09.	TISP-Schulung (Secorvo College)
21.-23.09.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
24.09.	Pacta sunt servanda (KA-IT-Si, Karlsruhe)
29.09.-02.10.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)

Fundsache

Dass die Entwicklung einer modernen Passwort-Policy komplexer ist, als es auf den ersten Blick scheinen mag, belegt der am 21.04.2009 als Draft erschienene „Guide to Enterprise Password Management“ des NIST (Special Publication 800-118).

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Juli 2009



Zenon und die Verfüglichkeit

Die Beispiele sind zahlreich und reichen von der RZ-Blackbox, die im Notfall die gespeicherten Daten via WLAN preisgibt, bis zum Verlust der PKI-Root-Keys bei der gematik: Immer wieder verursacht der Konflikt zwischen den Sicherheitszielen Vertraulichkeit und Verfügbarkeit Sicherheitsvorfälle oder zumindest – wie beim Thema Schlüsselhinterlegung (Key Escrow) – heftige Auseinandersetzungen.

Tatsächlich geraten diese beiden Sicherheitsziele bei fast jeder Sicherheitslösung aneinander. Wer Backups erstellt, um eine hohe Datenverfügbarkeit zu erreichen, schafft unvermeidlich einen neuen Angriffspunkt auf deren Vertraulichkeit. Wer Daten verschlüsselt abspeichert, riskiert mit dem Verlust des Schlüssels auch den der Daten. Und ein Passwortrücksetzungsverfahren kann die Vertraulichkeit bedrohen, wenn Unberechtigte es auslösen können.

Das Spannungsverhältnis ist beiden Zielen immanent – warum aber werden in der Praxis allzu häufig Maßnahmen für das eine Ziel auf Kosten des anderen umgesetzt? Zu vermuten ist, dass bei vielen Konzepten übersehen wird, dass jede Maßnahme zur Erreichung eines der Sicherheitsziele das Schutzobjekt des anderen Ziels verändert: Auch Backups sind bei Vertraulichkeitsmaßnahmen zu berücksichtigen, und für Passworte und Schlüssel müssen Verfügbarkeitsmaßnahmen getroffen werden.

Das klingt verdächtig nach Zenon von Eleas Paradoxie von Achilles und der Schildkröte, deren Vorsprung er trotz höherer Geschwindigkeit nicht einholen kann: Sobald er die Stelle erreicht, auf der die Schildkröte eben noch stand, ist diese bereits weitergekrochen.

Ein Trugschluss – denn auch eine unendliche Reihe (wie die schrumpfenden Abstände zwischen Achilles und der Schildkröte) kann eine endliche Summe besitzen. So müssen auch Vertraulichkeit und Verfügbarkeit nicht ad infinitum konkurrieren – geeignete Schutzkonzepte müssen jedoch immer beide angemessen berücksichtigen.



Inhalt

Zenon und die Verfüglichkeit

Security News

Sicher ist sicher – oder?

BDSG novelliert

Bedrohungsanalysetools

Nmap/Zenmap v5.0

Rechtssicherheit beim § 202c

Urlaubsrätsel

Secorvo News

Secorvo College aktuell

Security News Symposium

Vertrag ist Vertrag

Veranstaltungshinweise

Fundsache

Security News

Sicher ist sicher – oder?

„Sicherheitsmechanismen bei Root-Zertifikaten wirksam“ meldete am 15.07.2009 die gematik, als Projektgesellschaft zuständig für die elektronische Gesundheitskarte (eGK) und die Heilberufsausweise (HBA) für medizinisches Personal. Anfang Juli hatte D-TRUST, Betreiber des Trustcenters für eGK und HBA, ein neues Root-Zertifikat erstellen müssen – übrigens nicht nach X.509, sondern im „card verifiable“ Zertifikatformat gemäß ISO-7816, das u. a. auch beim digitalen Tachographen verwendet wird: Das für den Schutz der Schlüssel eingesetzte Hardware Security Modul (HSM) hatte Probleme in der Stromversorgung als Angriff gewertet und folgerichtig – alle Schlüssel gelöscht.

Nun müssen etliche Hundert „Musterkarten“ ausgetauscht werden. Zwar hätte man für Tests mit fiktiven Daten besser auf die hohe Sicherheit durch HSMs verzichtet und eine Root-CA in Software eingesetzt, oder die geplante Produktivumgebung inklusive Backup und Restore des Root-Schlüssels nachgebildet. Der Entscheidung für ein HSM ohne Backup verdankt die Welt jedoch zwei wichtige Ergebnisse: Erstens einen seltenen, realitätsnahen Test des Worst-Case Szenarios, und zweitens ein geschärftes Bewusstsein dafür, dass Sicherheit nicht nur bedeutet, dass Daten nicht in die falschen Hände fallen, sondern auch, dass sie in den richtigen verbleiben.

Veteranen der PKI-Szene mag bei der Meldung ein Deja-vu-Gefühl beschlichen haben: Vor knapp zehn Jahren verlor eine weltweite Banken-PKI kurz nach Betriebsbeginn auf dieselbe Weise die Root-Schlüssel. Ob es ein schlechtes Omen für die eGK ist, dass besagte Banken-PKI inzwischen als Beispiel für einen überkomplexen, grandiosen Fehlschlag gilt?

BDSG novelliert

In der letzten regulären Sitzung dieser Legislaturperiode hat der Deutsche Bundestag am 03.07.2009 den „Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften“ der Bundesregierung vom 18.02.2009 (BT-Drs. 16/12011) entsprechend den Beschlussempfehlungen des Innenausschusses vom 01.07.2009 (BT-Drs. 16/13657) verabschiedet. Im Hau-Ruck-Verfahren wurde damit in letzter Minute auf die teilweise vernichtende Kritik selbst engagierter Verfechter eines gesetzlich geregelten Datenschutzaudits reagiert und das Datenschutzauditgesetz, seit 2001 in § 9a BDSG angekündigt, erneut vertagt. Das Resultat wäre anderenfalls ein mit heißer Nadel gestricktes Gesetz voller handwerklicher Mängel im Detail gewesen – ohne Aussicht, den Datenschutz wirksam zu verbessern.

Nach der nun beschlossenen „Novelle II“, die am 01.09.2009 in Kraft tritt, ist der betriebliche Datenschutzbeauftragte zukünftig nur noch „aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist“ kündbar, und die verantwortliche Stelle verpflichtet, die Teilnahme an Fort- und Weiterbildungsmaßnahmen zu ermöglichen und zu finanzieren. Die Zulässigkeit der Nutzung listenmäßig zusammengefasster Daten für Zwecke des Adresshandels bleibt erhalten. Konsequenter geregelt wurde die Auftragsdatenverarbeitung in § 11 BDSG – eine Überprüfung der Verarbeitung beim Auftragnehmer hat nun vor Beginn der Verarbeitung und regelmäßig während dessen Verlaufs zu erfolgen; die Ergebnisse sind zu dokumentieren. Als neuer § 32 wurde eine Regelung zum Arbeitnehmerdatenschutz ergänzt – gut gemeint, aber inhaltlich nicht mehr als ohnehin bereits geltendes Recht. Schließlich wurden die Geldbußen auf bis zu 300.000 Euro angehoben und damit unmissverständlich klar gestellt: Die Zeit, in der Datenschutzverstöße als Kavaliersdelikt durchgehen, ist endgültig vorbei.

Bedrohungsanalysetools

Wieder war es ein Softwarefehler in BIND 9 des ISC, der ziemlich genau ein Jahr nach der letzten großen Attacke (SSN 07/2008) am 28.07.2009 das weit verbreitete Softwarepaket BIND 9 erneut in die Knie zwang. Diesmal reichte ein einzelnes „dynamic update message“-Paket, um Master-DNS-Server zum Absturz zu bringen – ein weiterer Beleg für die Dringlichkeit sichererer Softwareentwicklung.

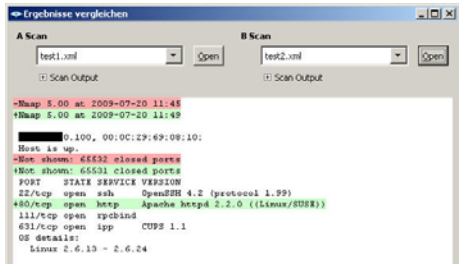
Einen großen Komfortsprung bei der Erstellung von Bedrohungsanalysen für Applikationen verspricht nun Version 3.0 von Microsofts TAM (Threat Analysis and Modelling). An der am 23.07.2009 erschienenen ersten Beta-Version lassen sich, wie erste Tests zeigen, signifikante Fortschritte bei der Bedienbarkeit des Werkzeugs feststellen. Getrübt wird der Eindruck durch Instabilitäten in der Testumgebung: So ließen sich manche Funktionen noch nicht richtig oder gar nicht ausführen. Die Verbesserungen der Visualisierungsmöglichkeiten sind vielversprechend. Bei verbesserter Stabilität wird TAM 3.0 eine sinnvolle Ergänzung des Werkzeugkastens zur sicheren Softwareentwicklung darstellen.

Einen anderen Ansatz verfolgt IBM mit seiner auf die Sicherheit von Web Applikationen zielende Rational AppScan Suite, die in der Enterprise Edition neben dem Application Scanner ein Dashboard mit Reports über die Entwicklung der Zahl und Art der gefundenen Schwachstellen enthält. Dazu erschien am 29.05.2009 in der Serie Redguides das 38seitige

Whitepaper „Improving Your Web Application Software Development Life Cycle's Security Posture“, das auf den ersten 20 Seiten eine sehr anschauliche Einführung in die aktuelle Bedrohungslage und Best Practices zur Entwicklung sicherer Web-Applikationen bietet.

Nmap/Zenmap v5.0

Am 16.07.2009 wurde Version 5.0 des wohl bekanntesten Netzwerk-Portscanners Nmap veröffentlicht. Sie ist sowohl für Linux als auch für Windows verfügbar und bietet über die eigentlichen Scan-Funktionen hinaus die Möglichkeit, grafische Netzwerkübersichten zu erstellen und Scan-Ergebnisse mit früheren Resultaten zu vergleichen.



Auch die Verwaltung der Scan-Profile wurde verbessert, und für alle, die keine Kommandozeilen-Gurus sind, wurde die grafische Oberfläche „Zenmap“ intuitiver und übersichtlicher gestaltet. Schon deswegen lohnt der Wechsel auf die neue Version.

Rechtssicherheit beim § 202c

Mit dem Nichtannahmebeschluss vom 18.05.2009 über drei Verfassungsbeschwerden im Zusammenhang mit dem „Hackerparagraphen“ § 202c StGB hat das Bundesverfassungsgericht Rechtssicherheit geschaffen und klargestellt, dass Programme, die lediglich für Hacking-Angriffe geeignet, nicht aber genau dafür entwickelt wurden (so genannte „Dual Use“-Software) nicht unter die Strafvorschrift fallen. Zur Durchführung von Penetrationstests ist auch die Nutzung von Hacking- und Analyse-Tools wie Nmap zulässig – sollte allerdings nachvollziehbar dokumentiert werden.

Urlaubsrätsel

Wer auch im Urlaub Security-Themen nicht missen und auch am Strand nicht von der Websicherheit lassen will, dem sei das OWASP-Kreuzworträtsel empfohlen. Es gibt auch was zu gewinnen – aber Beeilung, das Rätsel ist seit dem 21.07.2009 online.

Secorvo News

Secorvo College aktuell

Direkt nach der Sommerpause haben Sie wieder Gelegenheit, Ihre Information-Security Kenntnisse zertifizieren zu lassen: Am 07.09.2009 startet die fünftägige TISP-Schulung mit anschließender Prüfung. Auch bei allen weiteren Seminaren, die wir im Herbst anbieten, präsentieren Ihnen unsere Experten gebündeltes Wissen und Expertise aus langjähriger Berufserfahrung und Beratungspraxis. Sichern Sie sich einen der wenigen noch freien Plätze für „IT-Sicherheitsaudits in der Praxis“ vom 21. bis 23.09.2009 oder für „PKI“ vom 03. bis 06.11.2009.

Den „Schwarzen Gürtel“ in sicherer Softwareentwicklung können Sie vom 29.09. bis 02.10.2009 in Gestalt des CPSSE-Zertifikats (Certified Professional for Secure Software Engineering) erwerben oder Ihre IT-Security Grundlagenkenntnisse mit dem Seminar „IT-Sicherheit heute“ vom 13. bis 16.10.2009 auffrischen. Programme und Online-Anmeldung unter www.secorvo.de/college.

Security News Symposium

Mit den Secorvo Security News unterstützen wir Sie seit Juli 2002 Monat für Monat dabei, in der Informationsflut der IT-Sicherheit die wichtigsten Entwicklungen nicht aus den Augen zu verlieren, und lassen Sie an unseren Einschätzungen teilhaben. Aber nicht alle wichtigen Entwicklungen der Informations- und IT-Sicherheit lassen sich in einem wenige Zeilen umfassenden Beitrag angemessen beleuchten. Daher greifen wir in diesem Jahr mit dem ersten „Security News Symposium 2009“ am **06.–07.10.2009** in Ettlingen ausgewählte Themen auf und möchten sie in Vorträgen und Diskussionen mit Ihnen vertiefen. Zusammen mit ausgewählten weiteren Fachexperten bieten wir Ihnen ein spannendes und hoch aktuelles Programm in einem inspirierenden Ambiente – und freuen uns auf den Austausch mit Ihnen (Anmeldung).



Vertrag ist Vertrag

Auf dem Event „Pacta sunt servanda“ weiht Sie die KA-IT-Si am 24.09.2009 in „Design by contract – die hohe Schule der sicheren Softwareentwicklung“ ein. Hagen Buchwald, Vorstandsvorsitzender des Cyber-Forum e.V., gibt Einblick in den Prozess, der Softwareentwicklern helfen soll, das reibungslose und Sicherheitslücken freie Zusammenspiel einzelner Programmmodule von Anfang an zu gewährleisten. Im Anschluss gibt es wie immer die Möglichkeit zum Buffet Networking. Das Event beginnt um 18 Uhr im Schlosshotel Karlsruhe (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2009	
12.-14.08.	USENIX Security '09 (Usenix, Montreal/CA)
16.-20.08.	Crypto 2009 (IACR, Santa Barbara/US)
17.-18.08.	Digital Forensic Research Workshop (DFRWS, Montreal/CA)
September 2009	
06.-09.09.	CHES: Workshop on Cryptographic Hardware and Embedded Systems (IACR, Lausanne/CH)
07.-11.09.	TISP-Schulung (Secorvo College)
15.-17.09.	IMF 2009: 5th International Conference on IT Security Incident Management & IT Forensics (GI, Stuttgart)
17.09.	RZ-Compliance (Lampertz/Secorvo/Kroll Ontrack, Friedrichshafen)
21.-23.09.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
24.09.	Pacta sunt servanda (KA-IT-Si, Karlsruhe)
29.09.-02.10.	ISSECO Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)

Fundsache

Seth Misenar systematisiert in seinem am 13.06.2009 bei SANS publizierten Aufsatz „A Virtually Secure Browser" die aktuellen Bedrohungen beim Surfen im Internet. Als wirksame Schutzmaßnahme empfiehlt er insbesondere den Einsatz einer lokalen Sandbox: Damit lässt sich die Sicherheit beim Surfen ohne signifikanten Komfortverlust erheblich steigern. Ein Ansatz, den auch Microsoft im Projekt Office 2010 verfolgt.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch und Jochen Schlichting.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2009



Gefährliche Gewissheiten

In seinem kürzlich erschienenen lesenswerten Thriller „Der Täuscher“ (2009) schildert Jeffery Deaver, wie leicht überzeugende Tatbeweise konstruiert und so Straftaten Unschuldigen „untergeschoben“ werden können.

Nicht ahnen konnte er beim Verfassen seines Romans (Originaltitel: „The Broken Window“), dass es noch schlimmer kommen würde. Inzwischen wissen wir, dass selbst DNA-Spuren ein zweifelhaftes Beweismittel sind. Nicht nur, dass DNA auch bei der Spurensuche am Tatort und durch Verunreinigung hinterlassen werden kann, wie die monatelange peinliche Suche nach dem „Phantom“ eindrucksvoll bewies. Nun wiesen vier israelische Forscher in dem am 17.07.2009 im Fachorgan der International Society for Forensic Genetics erschienenen Beitrag „Authentication of forensic DNA samples“ nach, dass jeder Biologiestudent im 3. Semester DNA-Spuren fälschen kann.

Auch IT-forensische Beweismittel wackeln. Nach einem Bericht des Daily Telegraph vom 25.08.2009 belegt eine interne Studie der britischen Polizei die geringe Wirkung der aufwändigen Videoüberwachung: Auf je 1.000 Kameras käme gerade eine aufgeklärte Straftat – pro Jahr. Eine Erkenntnis, die sich mit den Ergebnissen einer Studie der Berliner Verkehrsbetriebe aus dem Jahr 2006 deckt: Das Bildmaterial erlaubte selten eine Täteridentifikation, und eine Abschreckungswirkung war nicht nachweisbar. Ein ähnliches Schicksal droht der Vorratsdatenspeicherung, sofern sie kommt: Darf man aus der IP-Adresse eines DSL-Anschlusses tatsächlich auf einen Täter schließen? Was, wenn sich dahinter ein schlecht oder gar nicht geschütztes WLAN verbirgt? Dasselbe gilt für forensische Analysen beschlagnahmter PCs. Was beweist die Entdeckung kinderpornographischer Bilder, wenn das Passwort schlecht gewählt oder bekannt ist?

Rechtfertigt mit dem zweifelhaften Argument gesteigerter innerer Sicherheit dulden wir die Entstehung unkontrolliert wachsender Datensammlungen – mit der voraussehbar fatalen Folge einer kontinuierlichen Verkleinerung des privaten Rückzugsraums.



Inhalt

Gefährliche Gewissheiten

Security News

iSpion

RainbowCrack 1.4

Blitzkekse

Fortschritte bei AES-Analyse

Exploits kein Kinderspiel

Fast alles über Chipkarten

Sommerrätsel

Secorvo News

Secorvo College aktuell

Erstes Security News Symposium

Veranstaltungshinweise

Fundsache

Security News

iSpion

Die kontrollierte Verbreitung mobiler Applikationen, wie von Apple für das iPhone und von Nokia für SymbianOS praktiziert, bietet in der Praxis nur einen unzureichenden Schutz, wie ein Blogeintrag am 31.07.2009 enthüllte: Auf zahlreiche Benutzerdaten, von der ID-Nummer des Geräts über das Geburtsdatum (falls Facebook genutzt wird) bis zum aktuellen Standort als Geokoordinate, greifen beliebige iPhone-Apps zu – um die gesammelten Daten an die Firma Pinchmedia weiter zu leiten, die daraus Statistiken z. B. zur Nutzungshäufigkeit und -dauer erstellt. Um Zustimmung zu dieser Übermittlung werden Nutzer von den wenigsten Apps gebeten – nach Ansicht von Pinchmedia genügt dazu die allgemeine Nutzervereinbarung von Apple.

Um so erfreulicher der Ansatz, den Rich Cannings vom – nicht gerade für Datensparsamkeit bekannten – Konzern Google am 12.08.2009 auf der diesjährigen Usenix in Montreal vorstellte: In das auf Linux und OpenSource basierende Handy-Betriebssystem Android werden Mechanismen integriert, die den Benutzer entscheiden lassen, ob er z. B. einem Spiel den Zugriff auf seinen Adressbestand gestatten möchte. Auch wenn die Gefahr besteht, dass wenig versierte Benutzer einfach „permit all" wählen, erscheint der Ansatz geeignet, das zu Grunde liegende Privacy-Problem durch Transparenz und Benutzerkontrolle zu lösen.

RainbowCrack 1.4

Am 17.08.2009 gab das Projekt RainbowCrack (siehe SSN 6/2009) eine erneut deutlich verbesserte Version 1.4 ihres Passwort-Crackers frei: Auf einem mit der Grafikkarte NVIDIA GForce 9800 GTX+ ausgestatteten PC prüft sie knapp 104 Milliarden NTLM-Hashwerte pro Sekunde – eine 40-prozentige Steigerung. Alpha-numerische 10-Zeichen-Passwörter sind damit nach spätestens 1,5 Monaten gefunden.

Blitzkekse

Am 10.08.2009 veröffentlichten fünf amerikanische Forscher eine Studie über Sicherheits- und Datenschutzimplikationen von Flash-Cookies („Flash Cookies and Privacy"). Dabei handelt es sich wie bei HTTP-Cookies um Mechanismen zur Speicherung von Statusinformationen zwischen Aufrufen von Webseiten.

Die Studie gibt einen guten Überblick über die Technik der immer populäreren Flash-Cookies. So kann ein Flash-Cookie 100 KB an Informationen speichern – gegenüber maximal 4 KB bei traditionellen HTTP-Cookies. Flash-Cookies können browserübergreifend ausgelesen werden, und werden von den Privacy-Mechanismen in aktuellen Browsern nicht erfasst.

Komfortable Werkzeuge zur Benutzerkontrolle von Flash-Cookies sind Mangelware. Adobe bietet zur Steuerung der lokalen Einstellungen den „Settings Manager" als Flash-Applikation an, der – wenn auch unkomfortabel – eine gewisse Kontrolle von Flash-Cookies ermöglicht. Seit Version 2.19.889 (Mai 2009) unterstützt das freie Tool CCleaner die Löschung von Flash-Cookies. Nutzern von Firefox immerhin bietet das Add-on BetterPrivacy eine Flash-Cookie-Kontrolle.

Fortschritte bei AES-Analyse

So sicher wie der Tag der Nacht folgt verbessern sich auch Analysen kryptographischer Verfahren. So hat ein Team um Biryukov und Khovratovich zum zweiten Mal in diesem Jahr einen Angriff auf AES vorgestellt. Dessen Grundlage ist eine Schwäche im Key-Scheduling, das die Rundenschlüssel aus dem eigentlichen Schlüssel ableitet.

Der gegen AES-192 und AES-256 mit reduzierter Rundenzahl gerichtete Angriff ist eine Related-Key-Attacke, d. h. der Angreifer benötigt nicht beliebige Klartext-Schlüsseltext-Paare, sondern solche, die *verschiedene* Schlüssel in einer *dem Angreifer bekannten* Beziehung verwenden. Der Angriff ist wirkungslos, wenn für jede Verschlüsselung ein zufällig gewählter Schlüssel verwendet wird, und betrifft keine AES-Variante mit voller Rundenzahl.

Dennoch ist der Angriff etwas befremdlich: Obgleich man eine stetige Verbesserung der Angriffe erwarten kann, ist der sprunghafte Fortschritt überraschend. AES-256 hat 14 Runden, davon sind bereits 10 mit einem praktikablen Angriff überwunden. Und ausgerechnet AES-256, das mutmaßlich stärkste Mitglied der AES-Familie, weist hier die größten Schwächen auf, während AES-128 praktisch unbehelligt bleibt. Man hüte sich jedoch vor falschen Schlüssen: AES-256 ist nach wie vor erheblich schwerer zu brechen als AES-128, denn für beide Verfahren ist bei voller Rundenzahl weiterhin Brute-Force der beste bekannte Angriff.

Wird den AES nun dasselbe Schicksal ereilen wie den SHA-1, dessen Sicherheit schneller als erwartet erodiert ist (siehe SSN 6/2009)? Die Autoren halten den Angriff für bedenklich, gleichwohl sind sie weit davon entfernt, AES als unsicher zu deklarieren. Auch David Wagner, Koautor von Twofish, meldet sich in Bruce Schneier's Blog in diesem Sinne zu Wort: Der AES ist, spezifikationsgemäß eingesetzt, sicher. Kein Grund zur Panik also.

Exploits kein Kinderspiel

Alexander Sotirov präsentierte am 12.08.2009 auf der Usenix einen historischen Abriss der letzten 10 Jahre Exploit-Entwicklung. Danach schien 2004 die Welt aus Entwicklersicht noch in Ordnung: War eine Schwachstelle entdeckt, ließ sich ein Exploit innerhalb kurzer Zeit entwickeln. Während Schwachstellen seitdem immer leichter zu finden sind, wird die Entwicklung von Exploits hingegen durch neue Sicherheitsmechanismen in Betriebssystemen erschwert. Zwar ist ein Denial-of-Service-Angriff über einen Buffer Overflow immer noch eine vergleichsweise einfache Sache – die Ausführung von eigenem Code wird hingegen schwieriger. Nach Sotirov kann die Entwicklung eines zuverlässigen Exploits heute mehrere Monate erfordern.

Damit verschiebt sich im Wettrennen zwischen Exploits und Patches das Gleichgewicht zu Ungunsten der Angreifer, sofern die Schwachstelle bekannt ist – vorausgesetzt, die Sicherheitsfunktionen des Betriebssystems werden ausreichend genutzt.

Fast alles über Chipkarten

Die fünfte Auflage des „Handbuchs der Chipkarten“ von Wolfgang Rankl und Wolfgang Effing erschien nach zweijähriger Überarbeitung im August 2008. Angesichts von über 1100 Seiten braucht man eine kräftige Hand, um das Buch zu halten. Da ist es einfacher zu sagen, was nicht darin enthalten ist: Kryptologische Grundlagen werden nur so weit behandelt, wie dies für Anwendungen in Chipkarten relevant ist, und auch zur Einbindung in PC-Betriebssysteme finden sich eher überblicksartige Informationen – Details zu Themen wie Windows Smart Card Logon, .NET-Karten oder Kartenmanagement-Systeme sucht man vergeblich.

Aber alles, was an Chipkarten-Basistechnik dazwischen liegt, ist ausführlich beschreiben. Die Liste der Angriffe auf Chipkarten reicht vom Abgreifen der Kommunikation an den Kontakten bis zu den Mifare-Attacken vom vergangenen Jahr. Eine der wichtigsten Überarbeitungen ist die Darstellung kontaktloser Karten. Speziell die ISO 14443 „Proximity“-Kommunikation wird dank Near Field Communication in Handys und dem elektronischen Personalausweis immer wichtiger.

Auch mit dieser Auflage ist die Geschichte der Chipkarten sicher noch nicht zu Ende: Die Kapitel zu elektronischen Gesundheitskarten und Chipkarten als Ausweisdokumenten warten darauf, fortgeschrieben zu werden. Dennoch gehört das aktualisierte Standardwerk in den Bücherschrank.

Sommerrätsel

Amateur- und Profi-Kryptologen, die ein wenig Denksport an heißen Tagen mögen, mögen sich an dem folgenden Kryptogramm versuchen:

```
signaturif+kaoti+aun+lzqimiuaia+sig
eebu+signaturiz+m0+g9
```

Unter allen richtigen Lösungen, die die Redaktion unter redaktion-security-news@secorvo.de bis zum 30.09.2009 erreichen, verlosen wir unter Ausschluss des Rechtswegs drei Exemplare des „Handbuchs der Chipkarten“.

Secorvo News

Secorvo College aktuell

Unsere Herbstseminare erfreuen sich erheblicher Nachfrage – daher sichern Sie sich bei Interesse möglichst bald einen der wenigen noch freien Plätze des Seminars „IT-Sicherheitsaudits in der Praxis“ (21.-23.09.2009) bzw. „PKI“ (03.-06.11.2009).

Vom 29.09. bis 02.10.2009 gibt es den „Schwarzen Gürtel“ in sicherer Softwareentwicklung – in Gestalt des CPSSE-Zertifikats. Eine Auffrischung Ihrer IT-Security Grundlagenkenntnisse bietet das Seminar „IT-Sicherheit heute“ (13.-16.10.2009).

Programme und Online-Anmeldung unter http://www.secorvo.de/college

Erstes Security News Symposium

Die Themengebiete IT-Sicherheit und Datenschutz unterliegen ständiger Weiterentwicklung – das merken wir nicht zuletzt Monat für Monat bei der Zusammenstellung unserer Security News. Aber nicht alle wichtigen Entwicklungen lassen sich in einem kurzen Textbeitrag angemessen beleuchten.

Daher bieten wir Ihnen in diesem Jahr erstmalig mit dem „Security News Symposium 2009“ am 06.-07.10.2009 in Ettlingen die Gelegenheit, ausgewählte Themen – darunter der Umgang mit USB-Sticks, Aktuelles zur Passwortsicherheit und zur Zukunft des Mifare-Chips – in Vorträgen, Demonstrationen und Diskussionen mit uns und weiteren Fachexperten zu vertiefen.

Die Vorträge und Referenten, das können wir versprechen, werden vom Feinsten sein – ein fachliches „Best of“ in einem inspirierenden Ambiente. Wir freuen uns auf Ihr Kommen und den Austausch mit Ihnen (Anmeldung).



Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2009	
06.-09.09.	CHES: Workshop on Cryptographic Hardware and Embedded Systems (IACR, Lausanne/CH)
15.-17.09.	IMF 2009: 5th International Conference on IT Security Incident Management & IT Forensics (GI, Stuttgart)
17.09.	RZ-Compliance (Lampertz, Friedrichshafen)
21.-23.09.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
24.09.	Pacta sunt servanda (KA-IT-Si, Karlsruhe)
29.09.-02.10.	ISSECO Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
Oktober 2009	
06.-07.10.	Security News Symposium 2009 (Secorvo, Ettlingen)
13.-16.10.	IT-Sicherheit heute (Secorvo College)
November 2009	
03.-06.11.	PKI (Secorvo College)
23.-27.11.	TISP-Schulung (Secorvo College)

Fundsache

Am 16.08.2009 veröffentlichte John Gerber in seinem Blog eine hilfreiche Zusammenstellung von 30 „Cheat Sheets" zu diversen Security Themen, darunter auch ausgefallenere wie „Reverse-Engineering Malware Cheat Sheet" und „Troubleshooting Human Communications". Ergänzend verweist er auf weitere „Cheat Sheets" zu Tools, Netzwerktechniken und weiteren Sammlungen.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2009



Profilvertrieb

Die hohe Kunst des Vertriebs beginnt lange vor der Kontaktaufnahme mit potentiellen Kunden. Ein gutes Produkt, gute Argumente und ein überzeugungsstarker Vertrieb allein garantieren keinen Verkaufserfolg: Entscheidend sind die „Streuverluste" bei der Auswahl der Kontakte. Daher ist das Bemühen verständlich, die Selektion durch das Sammeln von Informationen zu schärfen. Besonders viel versprechend sind echte Interessenten – Menschen mit Bedarf, die sich bereits über das Angebot informiert haben.

Da bietet der eigene Internetauftritt gänzlich neue Möglichkeiten. Webseiten-Optimierungstools wie Google Analytics haben den Appetit geweckt: Welche Seiten hat ein Nutzer besucht? Hat er eine Demo-Software, ein Datenblatt oder eine Leistungsbeschreibung heruntergeladen? Wie viel Zeit hat er auf der Seite verbracht?

Wie schön wäre es, aus der IP-Adresse auf die Identität des Besuchers schließen und ihn unmittelbar kontaktieren zu können! Oft ist das nicht schwierig: Hat er einmal ein Kontaktformular ausgefüllt, können Name und Anschrift im CRM mit der IP-Adresse verknüpft werden – und jeder weitere Besuch lässt sich zuordnen. Kostenlose Angebote wie utrace oder infosniper liefern auf Knopfdruck Provider und Domaininhaber, kommerzielle Anbieter ordnen IP-Adressen recherchierte Namen zu. Und wäre es vor einem Anruf nicht gut zu wissen, bei welchem Wettbewerber der Besucher sich vorher informiert hat und welches Bildungsniveau und Interessenprofil aus dem Surfverhalten abgeleitet werden können?

Tatsächlich ist die Erstellung von Surf-Profilen ohne Einwilligung des Betroffenen verboten (§ 12 Telemediengesetz). Ein Passus in der Datenschutzerklärung, der eine implizite Einwilligung bei Nutzung annimmt, genügt § 13 (2) TMG nicht. Verstöße sind jedoch verbreitet, wie das Xamit-Datenschutzbarometer vom 30.06.2009 belegt. Wer sicher gehen will, prüft eine Webseite vorher – vielleicht auch einmal die des eigenen Arbeitgebers...



Inhalt

Profilvertrieb

Security News

Playstation-Cracker

Durchbruch: 15 = 3*5

Soziale Sicherheitsbugs

WLAN-Sicherheit

Top Cyber Security Risks

Open Source Security

Mobilfunk-Knacken für alle

Secorvo News

Secorvo College aktuell

Lesefutter

Security News Symposium 2010

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Playstation-Cracker

Am 08.07.2009 gelang es der Forschungsgruppe um Arjen Lenstra an der École Polytechnique Fédérale de Lausanne, nach knapp sechs Monaten einen diskreten Logarithmus auf einer elliptischen Kurve über einem endlichen Primkörper von 112 bit zu lösen – mit anderen Worten: den privaten Schlüssel eines asymmetrischen Kryptosystems auf einer elliptischen Kurve der Moduluslänge 112 bit zu bestimmen. Ein neuer Rekord. Zuletzt war im Oktober 2002 die Berechnung eines diskreten Logarithmus auf einer elliptischen Kurve über einem 109 bit großen endlichen Körper gelungen (SSN 1/2003).

Nicht nur die verwendeten „Rechenknechte" sind ungewöhnlich – Lenstra parallelisierte die Berechnung in einem Cluster von über 200 Playstations. Auch die Implikationen sind erheblich, wie Lenstra gemeinsam mit Peter Montgomery, einem weiteren Schwergewicht der Faktorisierungsforschung, in einer IACR-Online-Veröffentlichung vom 01.09.2009 darlegt: Anders als in der berühmten Schlüssellängen-Prognose, die Lenstra 1999 mit Verheul publizierte, kommen die Autoren zu dem Schluss, dass mit der Faktorisierung einer 1024 bit langen Zahl kaum vor 2020 zu rechnen sei; die erste Faktorisierung eines 768 bit langen RSA-Modulus erwarten sie für das kommende Jahr. Diese Einschätzung deckt sich mit einer Prognose von Secorvo aus dem Jahr 2001 (SSN 5/2004).

Durchbruch: 15 = 3*5

Bereits im Jahr 1994 entdeckte Peter Shor einen Algorithmus, der es erlaubt, das RSA-Kryptoverfahren in polynomialer Zeit zu brechen, also ebenso schnell, wie man damit verschlüsseln oder signieren kann. Ein Krypto-GAU. Zum Glück läuft sein Algorithmus nur auf einem hypothetischen Quantencomputer.

Am 03.09.2009 wurde bekannt, dass es Physikern der Universität Bristol gelungen ist, einen rudimentären Quantencomputer zu bauen. Damit gelang es, mit Shors Algorithmus die Zahl 15 in die Primfaktoren 3 und 5 zu zerlegen. Das gleiche Kunststück gelang Forschern von IBM schon im Jahr 2001; die Gruppe aus Bristol verkleinerte jedoch den Experimentalaufbau deutlich. Die Kontrolle von mehr Quanten-Bits zur Faktorisierung größerer Zahlen ist allerdings auch ihnen nicht gelungen.

Beruhigend für RSA-Anwender: In der Welt herkömmlicher Computer stockt die Entwicklung besserer Faktorisierungsalgorithmen, in der Welt der Quanten die von größeren Computern.

Soziale Sicherheitsbugs

Nachdem im von Aviv Raff zum „Month of Twitter Bugs" erklärten Juli 2009 insgesamt 31 Schwachstellen in Third-Party-Diensten rund um Twitter veröffentlicht wurden, stand im September das nächste Soziale Netzwerk im Brennpunkt. Pünktlich zum Bergfest des „Month of Facebook Bugs" am 15.09.2009 wurde im „Halfway Report" ein Zwischenstand veröffentlicht. Danach wurde auch diesmal jeden Tag ein „FAXX Hack" (= Facebook Application XSS/XSRF) veröffentlicht.

Wie einige Social Networks haben Facebook und Twitter einen rasanten Aufstieg hinter sich. Der Erfolg bringt aber offensichtlich zahlreiche Sicherheitslücken mit sich. Beide „MoB"s haben zu einer Erhöhung der Sicherheit der Plattformen beigetragen – wohl auch, weil sich die Betreiber und Entwickler bei der Behebung der Schwachstellen sehr kooperativ zeigten. Hoffentlich nehmen sich weitere Social Networks daran ein Beispiel.

WLAN-Sicherheit

Würden Sie mit einem Flugzeug fliegen, das, sagen wir mal, von Straßenbauingenieuren konstruiert wurde? Wohl kaum. In der digitalen Welt passieren Dinge dieser Art jedoch andauernd. Das WEP-Protokoll zur kryptografischen Sicherung von WLAN-Datenübertragungen gehört zu der Sorte von ad-hoc-Kryptografie, die von Laien entworfen wurde. Es überraschte daher nicht, als WEP im Jahr 2001 gebrochen wurde (SSN 3/2002).

Ein zentraler Punkt der Angriffsstrategie war dabei eine Methode mit dem Namen chopchop. Beim Entwurf des WEP-Nachfolgers WPA verfiel man daher auf die Idee, dieser Strategie mit einer anti-chopchop-Funktion zu begegnen - dazu wurde TKIP erfunden. Anstatt einen fundierten Protokollentwurf vorzulegen, wurde mehr oder weniger lediglich der spezielle Angriff abgewehrt, dem WEP zum Opfer gefallen war.

Im November 2008 wurde eine Schwäche von TKIP bekannt, durch die ein chopchop-Angriff auf WPA möglich wurde (SSN 11/2008). Der Angriff dauert strategiebedingt etwa eine Viertelstunde und ermöglicht lediglich das Erreichen von Teilzielen; ein Angreifer kann das WLAN also (noch) nicht übernehmen. Am 15.07.2009 veröffentlichten japanische Forscher einen praktikablen physischen Man-in-the-Middle-Angriff, der den Angriff verbessert und auf unter eine Minute beschleunigt. Auch wenn dieser nur relativ „kleine" Angriffsziele erreicht, zeigt sich einmal mehr: Hat man erst einmal einen guten Ansatzpunkt für das Brecheisen gefunden, ist die Kiste bald offen.

Was sollte man daraus lernen? Erstens, dass der Umstieg auf WPA2 mit AES-CCMP spätestens jetzt fällig ist, und zweitens, dass beweisbare Sicherheit gelegentlich ein sehr praktisches Fundament für langfristige Sicherheit bildet.

Top Cyber Security Risks

Die von SANS im September 2009 veröffentlichten „Top Cyber Security Risks" bestätigen Trends, die uns schon länger am Herzen liegen. Danach sind die beiden Top Sicherheitsthemen ungepatchte Client-Software, über die Schadcode eingeschleust werden kann, sowie Schwachstellen in Web-Applikationen.

Diese Beobachtung deckt sich mit unseren eigenen Erfahrungen, dass einerseits Netzwerk- und Perimetersicherheit in Firmen immer besser werden, es andererseits aber immer schwieriger wird, die eingelassenen Daten zu kontrollieren. Die Stadtmauern sind errichtet – an den Torkontrollen muss jedoch noch gearbeitet werden.

Open Source Security

Am 21.09.2009 hat der Toolhersteller Coverity den „Scan Open Source Report 2009" veröffentlicht. Für den zum ersten Mal 2006 auf Initiative des Department of Homeland Security (DHS) veröffentlichten Bericht wurden 280 auf C/C++ basierende Open Source Projekte mit statischer Code-Analyse auf Schwachstellen untersucht und vergleichend bewertet. Die Ergebnisse, Metriken und Benchmarks präsentiert der Bericht ausführlich auf 35 Seiten.

In erster Linie ist der Bericht eine Hilfestellung für Entscheider, die Sicherheitsaspekte bei der Auswahl von Open-Source-Lösungen berücksichtigen wollen. Aber auch die teilnehmenden Projekte selbst profitierten von der Untersuchung. Die Verbesserung der Qualität und Sicherheit einzelner Projekte wird von Coverity in der „Scan Ladder" gewürdigt. 127 Projekte erklommen die Stufe 1, 36 inzwischen sogar die Stufe 2 – darunter honorige Vertreter wie OpenVPN, OpenLDAP, Perl und Postfix.

Mobilfunk-Knacken für alle

Die Rechenleistung moderner Grafikprozessoren zieht immer mehr Codebreaker an: Bei der Konferenz Hacking at Random präsentierte Karsten Nohl (bekannt durch seine Analyse der Mifare-Chips) am 15.08.2009 ein Projekt zur weltweit verteilten Vorberechnung der Schlüsselsuche für die GSM-Mobilfunk-Chiffre A5.1, die schon lange „angezählt" ist (SSN 9/2003 und SSN 11/2007).

Nach Abschluss dieser Vorberechnung könnten abgehörte GSM-Gespräche unter Rückgriff auf die dabei erzeugte riesige Tabelle in kurzer Zeit entschlüsselt werden. Falls sie überhaupt verschlüsselt waren: Denn ob die Verschlüsselung ein- oder ausgeschaltet wird, entscheidet das GSM-Mobilfunknetz, und macht damit das Abhören via IMSI-Catcher erst möglich – unsichtbar für den Benutzer, denn fast kein Handy zeigt seinem Besitzer an, in welchem Modus es gerade arbeitet.

Secorvo News

Secorvo College aktuell

Zwei Gelegenheiten zur Aktualisierung, Erweiterung und Zertifizierung Ihres Fachwissens bietet Ihnen Secorvo-College noch in diesem Jahr:

Das viertägige Seminar „PKI – Grundlagen, Vertiefung, Realisierung" am **03.–06.11.2009** lässt keine Ihrer Fragen zu Konzeption, Implementierung und Nutzung von PKIs unbeantwortet.

Und vom **23.–27.11.2009** (mit direkt anschließender Prüfung am 28.11.2009) haben Sie Gelegenheit, Ihre Fachkenntnisse mit dem TISP-Zertifikat zu krönen – das inzwischen schon die Visitenkarten von mehr als 300 Absolventen ziert.

Neben detaillierten Seminarprogrammen mit Online-Anmeldung finden Sie auf unseren Webseiten den druckfrischen Seminarkalender 2010 zur Planung Ihrer Seminarbesuche im kommenden Jahr.

Lesefutter

Immer wieder beschäftigt uns die Frage nach der Angemessenheit diverser Anforderungen an eine Passwort-Policy. Das Ergebnis unserer Überlegungen und vieler Diskussionen haben wir nun publiziert – und räumen darin mit einigen liebgewonnenen, aber irreführenden Überzeugungen auf. Wer noch nicht vollständig auf Token-basierte Zwei-Faktor-Authentisierung umgestellt hat, findet in dem Aufsatz „Passwörter – fünf Mythen und fünf Versäumnisse" (Dirk Fox, Frank Schaefer; DuD 7/2009, S. 425-429) möglicherweise den einen oder anderen wertvollen Hinweis.

Auch zum Löschen von Daten kursieren zahlreiche nicht mehr zeitgemäße Vorstellungen (SSN 1/2009), die zu aufwändigen Verfahren führen. Unser schon im Februar erschienene Aufsatz „Sicheres Löschen von Daten auf Festplatten" (DuD 2/2009, S. 110-113) gibt aktuelle Empfehlungen und stellt geeignete Tools vor.

Security News Symposium 2010

Schon jetzt steht er fest – der Termin unseres „Security News Symposiums 2010". Wer das Event am **20.–21.04.2010** nicht verpassen will, kann sich bereits heute online anmelden.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2009	
03.-04.10.	Datenspuren 2009 (CCC, Dresden)
06.-08.10.	ISSE 2009 (eema & enisa, The Hague/NL)
28.-30.10.	Hack.LU (CSRRT-LU, Luxembourg)
November 2009	
03.-06.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
17.-20.11.	In-Depth Security Conference 2009 (DeepSec, Wien/AU)
19.-20.11.	33. Dafta (GDD, Köln)
23.-27.11.	TISP-Schulung (Secorvo College)
Dezember 2009	
27.-30.12.	26th Chaos Communication Congress (CCC, Berlin)
Januar 2010	
19.-21.01.	Omnicard 2010 (inTIME, Berlin)

Fundsache

Derzeit erfreuen sich pointierte Historiendarstellungen großer Beliebtheit. So die Geschichte und Funktionsweise des AES – erzählt von Jeff Moser in knapp 70 Strichmännchen-Bildern. Ebenfalls amüsant ist die knappe History of Hacking. Gleichfalls fokussiert und sehr informativ kommt die mit Unterstützung von Jean-Jacques Quisquater entwickelte interaktive Darstellung der Cryptographic Key Length Recommendations von BlueKrypt daher, zuletzt aktualisiert am 28.09.2009.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2009



EgPh>10S-uks0Mm*

Trotz aller Ermahnungen, Drohungen, Anleitungen und Best-Practice-Tipps zum sicheren Gebrauch von Passwörtern besteht bis heute ein erhebliches Defizit auf diesem Gebiet. Warum ist das so? Nüchtern betrachtet kann man nur eine Antwort darauf geben: Passwörter sind ungeeignet. Denn es liegt nicht in der Natur des Menschen, sich kontextfreie Zeichenfolgen mit hoher Entropie zu merken.

Zwar gibt es Best-Practice-Regeln zur Ableitung von Passwörtern z. B. aus ganzen Sätzen. Daher werden schlechte Passwörter gerne mit falschen Gewohnheiten begründet, in der tröstlichen Hoffnung, dass für die nächste Generation die Wahl guter Passwörter genauso selbstverständlich sein werde wie andere Dinge des täglichen Lebens. Das greift jedoch zu kurz, denn es geht ja nicht um ein oder zwei Passwörter, sondern zumeist um mehr als ein Dutzend, die unterschiedlich sein und regelmäßig gewechselt werden sollen. Nur wenige Menschen sind dazu in der Lage, und noch weniger sind hierzu gewillt – alle anderen stehen Schlange beim Helpdesk. Das ist wenig überraschend, denn die meisten Menschen wollen einfach nur unbehindert ihren Aufgaben nachgehen, und das Ausdenken und Merken kryptischer Passwörter gehört selten dazu. Das Langzeit-Experiment an Millionen IT-Nutzern lässt nur einen Schluss zu: Für durchschnittliche Menschen sind Passwörter ein völlig ungeeigneter Authentifizierungsmechanismus, und keine noch so guten Tipps (die ja auch erst mal gelesen sein wollen) werden daran etwas ändern.

Der entscheidende Grund für die weite Verbreitung von Passwörtern ist, dass sie so billig sind: ihr sicherer Gebrauch kann auf die Benutzer abgewälzt werden. Passwort-Manager und -Diversifizierer können das Leiden mildern, aber lösen das eigentliche Problem nicht. Wenn Authentifizierung wirklich so kritisch für eine Organisation ist, dann sind Passwörter schlicht und einfach nicht die richtige Wahl.

Dr. Safuat Hamdy

* *„Ein gutes Passwort hat mehr als 10 Stellen – und kann sich kein Mensch merken."*



Inhalt

EgPh>10S-uks0Mm*

Security News

Koalitionspläne

Schutz vor Querverweisen

Benchmarking Software Security

Schwarzer-Peter-Spiele

Passwörter im Web

Secorvo News

Secorvo College aktuell

Passwort- und Schlüssellängen

Abrakadabra

Veranstaltungshinweise

Fundsache

Security News

Koalitionspläne

Am 26.10.2009 wurde der zwischen CDU, FDP und CSU ausgehandelte Koalitionsvertrag unterzeichnet. Immerhin knapp 10 der 124 Seiten des Werks beschäftigen sich mit Themen der Inneren Sicherheit, zwei Seiten darunter mit dem Datenschutz.

So sollen zahlreiche Gesetze der Inneren Sicherheit, von der Telekommunikationsüberwachung bis zum BKA-Gesetz, im Hinblick auf die Zielerreichung und den „Schutz des Kernbereichs privater Lebensgestaltung" evaluiert werden – die Ergebnisse früherer Evaluierungen staatlicher Eingriffsbefugnisse geben jedoch wenig Anlass zur Hoffnung auf substanzielle Korrekturen. Der Zugriff der Bundesbehörden auf die Daten der Vorratsdatenspeicherung wird bis zur Entscheidung des Bundesverfassungsgericht ausgesetzt – eine wirksame Stärkung der „Grundsätze der Verhältnismäßigkeit, der (...) Datensparsamkeit, der Zweckbindung" sieht allerdings anders aus.

Die Bürger sollen durch „Aufklärung und Sensibilisierung der Öffentlichkeit zu mehr Selbstschutz und der Nutzung sicherer IT-Produkte" motiviert und es soll eine „Stiftung Datenschutz" errichtet werden, „die den Auftrag hat, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen (...) und ein Datenschutzaudit zu entwickeln". So weit sind wir also schon gekommen: Weil eigene ordnungspolitische Vorstellungen fehlen, wird das Primat der Politik an eine Stiftung delegiert.

Das Bundesdatenschutzgesetz soll dafür „lesbarer und verständlicher" gestaltet und der „Arbeitnehmerdatenschutz in einem eigenen Kapitel (...) ausgestaltet" werden. Auch das De-Mail-Gesetz bleibt auf der Tagesordnung: um „Unternehmen die Möglichkeit (zu) geben, Geschäftsprozesse elektronisch abzuwickeln". Na endlich – darauf haben die deutschen Unternehmen nur gewartet.

Wie von einem unter Zeitdruck und zwischen erfahrenen und unerfahrenen Partnern ausgehandelten Text kaum anders zu erwarten, ist der Koalitionsvertrag eine Mischung aus nebulösen Absichtserklärungen, wenigen konkreten Vereinbarungen und einigen skurrilen Ideen – ein großer Wurf ist er jedenfalls nicht. Immerhin: Die Regierung will zukünftig „die Lebenswirklichkeit der Mehrheit der Menschen in Deutschland (...) berücksichtigen". Offenbar war das bisher nicht üblich.

Schutz vor Querverweisen

Dass Firefox-Anwender mit dem Add-On NoScript die Ausführung von Skripten und anderen potentiell gefährlichen Webseiteninhalten an ihr Einverständnis binden können, hat sich mittlerweile herumgesprochen (siehe auch SSN 10/2008).

Aber auch NoScript stopft nicht alle Bedrohungen auf Webseiten. So ermöglicht es keine Kontrolle von Flash-Cookies (vgl. SSN 08/2009), und bei Cross-Site-Requests – das sind in eine Suite eingebettete Inhalte, die von anderen Websites bezogen werden und oft zur Verfolgung von Benutzer-Aktivitäten dienen – kann NoScript nur die Ausführung von Skripten in diesen Inhalten verhindern, nicht aber den Aufruf selbst. Zumeist hat der Anwender damit schon seine Daten beim Tracking-Server abgeliefert – dazu genügt ein eingebettetes „Null-Pixel"-Bild.

Gegen Flash-Cookies hilft BetterPrivacy und gegen Cross-Site-Requests das zuletzt am 28.07.2009 aktualisierte Add-On RequestPolicy, das ähnlich wie NoScript die komfortable Pflege zulässiger Ausnahmen erlaubt, für unbekannte Websites aber die betreffende Lücke versperrt. Wer darüber hinaus zulässige und verbotene Cookies komfortabler kontrollieren will, als mit Firefox möglich, sollte zu einem Cookie-Manager wie Firecookie greifen.

Benchmarking Software Security

Building Security In Maturity Model (BSIMM) ist eine Sammlung von Best Practices zur sicheren Software-Entwicklung, vergleichbar den Best Practices zur Information Security im Standard ISO/IEC 27002:2005. Das darin beschriebene Software Security Framework (SSF) ist in zwölf Bereiche mit insgesamt 110 empfohlenen Maßnahmen unterteilt. Software-Entwickler können anhand des Abdeckungsgrades der Maßnahmen den Reifegrad der Software-Sicherheit in ihrer eigenen Organisation überprüfen.

Seit dem 24.09.2009 läuft eine von Gary McGraw initiierte Web-Studie, bei der der Umsetzungsgrad eines eingeschränkten Umfangs von Maßnahmen als BSIMM Beginn durch eine Umfrage erfasst wird. Die Ergebnisse dieser Studie sollen den Einstieg in einen geregelten Security-Prozess bei der Softwareentwicklung erleichtern und grundlegende Daten für erste Benchmarks liefern. Die Teilnahme an der Studie ist für alle Interessierten offen und jedem zu empfehlen, der die Qualität dieses Benchmark-Ansatzes zu verbessern helfen möchte.

Schwarzer-Peter-Spiele

Kurz bevor Microsoft am 13.10.2009 – sicher nicht ohne Stolz – auf sechs Jahre Patch Tuesday zurück blicken konnte, erklärte Steve Ballmer am 05.10.2009 in einem Interview den mangelnden wirtschaftlichen Erfolg von Windows Vista mit den verbesserten Sicherheitsfunktionen: Sie seien für

dessen schlechten Ruf verantwortlich. In diese Perspektive passen die häufigen Sicherheitswarnungen und Rückfragen des Vista-Systems, die bestimmt eben so häufig mit routiniertem Klick auf den „Ist mir doch egal!"-Button ignoriert werden.

In die Diskussion, die das Ballmer-Interview losgetreten hatte, mischte sich am 21.10.2009 Bruce Schneier mit einem bemerkenswerten Argument: Für ihn sind viele Sicherheitswarnungen Ausdruck der Ratlosigkeit von Entwicklern, die die Verantwortung für sicherheitsrelevante Entscheidungen, zu denen sie selbst keine vernünftige Antwort wissen, auf diese Weise als Schwarzen Peter an den überforderten Anwender weitergeben.

Merke: Die Vereinbarkeit von Sicherheit und Bedienbarkeit ist ein zentraler Aspekt der sicheren Softwareentwicklung, der im Kampf gegen Buffer Overflows, Cross Site Scripting & Co. oft vergessen wird. „Security and Usability" ist dementsprechend auch eines der vier Schwerpunkt-Themen der Psychology and Security Resource Page, die Ross Anderson vom Computer Laboratory der Universität Cambridge am 23.10.2009 ins Netz gestellt hat.

Passwörter im Web

Das Bekanntwerden eines umfangreichen und erfolgreichen Phishing-Angriffs auf E-Mail-Accounts von Hotmail und anderen Providern am 01.10.2009 hat erneute Diskussionen über Passwörter als Schutzmechanismus ausgelöst. Dass die Wahl und Nutzung von Passwörtern auch heute immer noch weit entfernt von Best-Practice-Ansätzen ist, belegt eine Analyse der veröffentlichten Passwörter des Tool-Herstellers Acunetix vom 06.10.2009.

Hierdurch inspiriert hat Jeremiah Grossman am 07.10.2009 auf seinem Blog den Eintrag "All about Website Password Policies" veröffentlicht. Darin beleuchtet er verschiedene Aspekte der Passwort-Sicherheit (insbesondere) im Web, wie z. B. Längenbetrachtungen, Zeichenauswahl, Komplexität, Speicherung beim Anbieter, Schutz vor Brute-Force-Angriffen und Gültigkeitsfristen.

Viele Überlegungen zur Passwort-Sicherheit konzentrieren sich auf die Auswahl eines guten Passworts. Die aktuellen Attacken zeigen aber, dass Aufbewahrung und Nutzung eine ebenso wichtige Rolle für die Sicherheit von Passwörtern spielen, da bei den Angriffen auf u. a. Hotmail keine Sicherheitslücken ausgenutzt, sondern die Passwörter den betroffenen Opfern entlockt wurden.

Eine Hilfe bietet das Open-Source-Tool pwdHash vom Stanford Security Lab. Es erzeugt für jede Webseite einen individuellen Schlüssel, den es aus einem Master-Passwort und der URL der Webseite ableitet. Dadurch führt ein kompromittiertes Passwort nicht gleich zur Preisgabe aller eigenen Web-Accounts. Außerdem wird im Falle eines Phishing-Angriffs dem Angreifer ein falsches Passwort übermittelt, da für die Erzeugung die URL der Phishing-Seite einfließt. Das Tool steht in aktuellen Versionen für verschiedene Browser auf der Projektseite zum Download zur Verfügung.

Secorvo News

Secorvo College aktuell

Bevor Secorvo College mit neuen Seminaren in das Jahr 2010 startet, haben Sie noch in diesem Jahr Gelegenheit, Ihr Wissen mit dem TISP-Zertifikat zu besiegeln. Sichern Sie sich einen Platz auf der TISP-Schulung vom 23. bis 27.11.2009 mit direkt anschließender Prüfung am 28.11.2009. So starten Sie mit einem Know-How-Update ins neue Jahr. Detaillierte Seminarbeschreibungen des Schulungsangebots für 2010 finden Sie auf unseren Webseiten, darunter die neuen Seminare Datenschutzaudit und Sicherheitsmanagement. Eine Planungserleichterung bietet Ihnen die praktische Jahresübersicht 2010. Wir freuen uns auf Ihre Anmeldung.

Passwort- und Schlüssellängen

Nicht nur Rechenleistung und Speicherkapazität (Verdoppelung alle 1,5 Jahre gemäß Moore's Law), sondern auch Angriffsalgorithmen wie RainbowCrack (siehe SSN 08/2009) entwickeln sich weiter. Daher müssen kryptographische Schlüssel und Passwort-Mindestlängen von Zeit zu Zeit an die technische Entwicklung angepasst werden. Der Frage, welche Längen heute und für die kommenden Jahre zu empfehlen sind, geht der Beitrag „Mindestlängen von Passwörtern und kryptographischen Schlüsseln" von Dirk Fox nach, erschienen in Datenschutz und Datensicherheit (DuD), Heft 10/2009.

Abrakadabra

Das letzte KA-IT-Si-Event in diesem Jahr dreht sich rund um die Datenrettung. In einem Expertenbericht zeigt Margret Horn von Kroll Ontrack, was zu tun ist, wenn eine Datei versehentlich gelöscht wird oder eine Platte plötzlich defekt ist. Was lässt sich überhaupt retten? Wann ist eine Datei unwiederbringlich gelöscht? Was sollte man bei einer unbeabsichtigten Löschung tun, um eine Datenrettung zu erleichtern – ohne noch mehr Schaden anzurichten? Am 26.11.2009 erfahren Sie es – ab 18 Uhr im Schlosshotel Karlsruhe. Im Anschluss gibt es wie immer die Möglichkeit zum Buffet Networking. Um Anmeldung wird gebeten.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2009	
03.-06.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
17.-20.11.	In-Depth Security Conference 2009 (DeepSec, Wien/AU)
19.-20.11.	33. Dafta (GDD, Köln)
23.-27.11.	TISP-Schulung (Secorvo College)
Dezember 2009	
27.-30.12.	26th Chaos Communication Congress (CCC, Berlin)
Januar 2010	
19.-21.01.	Omnicard 2010 (inTIME, Berlin)
Februar 2010	
02.-03.02.	20. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
05.-07.02.	ShmooCon 2010 (Shmoo Group, Washington/USA)
09.-10.02.	17. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)

Fundsache

Am 24.08.2009 ging die Webseite „verbraucher-sicher-online.de“ an den Start. Das vom Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz geförderte und der TU Berlin umgesetzte Projekt bietet eine Sammlung von Hilfestellungen für den Schutz von Rechnern und Daten. Die Hinweise richten sich an Privatnutzer, dürften aber auch in Awareness-Kampagnen hilfreich sein.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

November 2009



Social Engineering 2.0

Für viele Jugendliche ist der eigene Auftritt in SchülerVZ, Wer-kennt-wen oder Facebook inzwischen ein soziales Muss, wie die Nutzerzahlen von Sozialen Netzwerken belegen. Und immer mehr Berufstätige pflegen ihre Kontakte über Business-Netzwerke wie Xing oder publizieren ihre Ein- und Ansichten in Twitter. Diese Entwicklung ist schon allein aus Datenschutzperspektive bedenklich: Neben den gespeicherten Personendaten kennt der Netzwerk-Betreiber alle Kontaktbeziehungen, das Nutzungsverhalten und die Suchanfragen.

Für einen Social Engineer ist ein mächtigeres Auskunftssystem hingegen kaum vorstellbar. Jeder registrierte Nutzer kann die öffentlichen Teile aller Personenprofile einsehen und nach Unternehmen und Personen, in deren persönlichen Daten, Interessen und Kontakten recherchieren – ideales Informationsfutter für einen gezielten Social Engineering Angriff. Da die Identität bei der Registrierung nicht überprüft wird, fällt es leicht, sich mit falschem Namen und CV anzumelden, um sich anschließend in das Kontaktnetz anderer Nutzer hineinzumogeln. Dann sind deren Kontakte, Telefondurchwahl und Mobilfunknummer, Interessen, E-Mail-Adresse und jede Änderung im Kontakt-Netzwerk sichtbar. Und Auswertungstools wie Twitnest liefern die wichtigsten Kontaktknoten frei Haus.

Zum Schutz vor raffinierten Social Engineers hilft da nur ein striktes Nutzungsverbot – oder die Aufklärung über „Dos and Don'ts".



Abb. 1: Twitnest-Grafik



Abb. 2: Nutzungszahlen



Inhalt

Social Engineering 2.0

Security News

Angriff auf SSL/TLS

(Alp)Traum iPhone

Windows 7 Sicherheitsprofile

OWASP Top 10 runderneuert

Vorsicht Falle!

Secorvo News

Secorvo College aktuell

Wunsch und Wirklichkeit

Feiertagslektüre

Veranstaltungshinweise

Fundsache

Security News

Angriff auf SSL/TLS

Marsh Ray und Steve Dispensa deckten am 04.11.2009 eine bislang unbekannte, gravierende Schwäche des SSL- und TLS-Protokolls – seit Januar 1999 IETF-Standard – auf. Sie erlaubt einem Angreifer, beliebigen Text in die Kommunikation zwischen Client und Server einzuschleusen. Im Fall von HTTPS kann das z. B. dazu führen, dass ein Client ein vom Angreifer bestimmtes Formular im Kontext einer neuen Sitzung angezeigt bekommt.

Die Schwäche betrifft das Protokoll zur Neuaushandlung von Sitzungsschlüsseln. Zwar bleibt die Vertraulichkeit gewahrt, aber bei der Aushandlung entsteht eine „Authentizitäts-Lücke", durch die nicht nur der Client oder Server, sondern auch ein Angreifer die (üblicherweise gar nicht benötigte) Neuaushandlung veranlassen kann. Der Angriff wurde zunächst für Client-Zertifikate demonstriert, funktioniert jedoch auch allein mit Server-Zertifikat. Betroffen sind alle Anwendungsprotokolle vom Online-Banking bis POP3S, die SSL/TLS nutzen.

Als schnelle Abhilfe gibt es zumindest für OpenSSL einen Patch, der die Neuaushandlung von Schlüsseln einfach abschaltet.

Ein so wirksamer Angriff auf ein so gut untersuchtes und etabliertes Protokoll wie SSL/TLS kommt sehr überraschend. Er zeigt aber einmal mehr, dass Schwachstellen oft an den „Nähten" auftreten (hier der Kontextwechsel zwischen zwei Sitzungen), und dass daher selten genutzte Features in einem Sicherheitsprotokoll entweder weggelassen oder mindestens ebenso genau analysiert werden sollten wie das Kernprotokoll.

(Alp)Traum iPhone

Dem seit dem 19.06.2009 in Deutschland verfügbaren iPhone 3GS hat Apple neben einer neuen Betriebssystemversion auch eine hardware-basierende Verschlüsselung gegönnt. Dank dieser und weiterer Sicherheitsfunktionen wie IPSec VPN, WPA2 Enterprise Wi-Fi und SSL/TLS erfreut sich das iPhone 3GS auch in Unternehmen wachsender Beliebtheit. Um letzte Zweifler von der Sicherheit des iPhone zu überzeugen, bietet Apple mit dem Dienst „Mobile Me" für 79 €/Jahr die Services „Mein iPhone suchen" und „Remote Wipe" an. Damit sollen sich ein vermisstes iPhone lokalisieren und alle Benutzerdaten aus der Ferne löschen lassen.

Der Sicherheitsgewinn ist jedoch begrenzt, denn zur Deaktivierung beider Dienste genügt es, die SIM-Karte zu wechseln. Auch die Datenverschlüsselung lässt sich umgehen, selbst wenn das iPhone durch einen Passcode gesperrt ist, wie Jonathan Zdziarski am 23.07.2009 in einem Interview mit dem Magazin Wired beschrieben und in einem tags darauf auf Youtube veröffentlichten Video demonstriert hat. Denn wie beim iPhone 2G/3G ist eine „Sicherung" der Benutzerdaten auch beim iPhone 3GS ohne Aufspielen einer modifizierten Firmware und ohne Brechen der Verschlüsselung möglich. Dazu wird das iPhone von einer RAM-Disk gebootet und dann die Partition mit den Benutzerdaten als Raw-Disk-Image gesichert – für die Entschlüsselung der Daten sorgt das iPhone dabei automatisch. Anschließend lässt sich das Raw-Image unter Mac OS mounten oder mit gängigen Forensik-Tools analysieren.

Das Glück des Forensikers ist in diesem Fall zugleich der Alptraum des Sicherheitsverantwortlichen, der seinem Management darlegen muss, warum der sichere Einsatz des iPhones im Unternehmen tatsächlich nicht so einfach ist, wie Apple verspricht.

Windows 7 Sicherheitsprofile

Mit dem am 28.10.2009 von Microsoft veröffentlichten Security Compliance Management Toolkit stehen nun neben einer detaillierten Dokumentation der Sicherheitseinstellungen von Windows 7 auch zwei direkt nutzbare Grundtypen von Sicherheitsprofilen zur Verfügung: Die Profile EC (Enterprise Client) und SSLF (Specialized Security – Limited Functionality), beide schon von ihrer Einführung für Windows XP, Server 2003, Vista und Server 2008 im Februar 2009 bekannt.

SSLF folgt dem Prinzip, Sicherheitseinschränkungen vor Funktionalität zu stellen, und legt damit eine gute Grundlage für die Härtung kritischer Systeme. Spezialisten sei als weiterführende Lektüre das Windows 7 and Windows Server 2008 R2 Application Quality Cookbook empfohlen.

Schade nur, dass der Fehler von vergangenen Windows-Härtungen konsequent fortgesetzt wurde: auch diesmal werden die Sicherheitseinstellungen der Zugriffskontrolllisten (DACL) für u. a Dateisystem, Registrierung und Dienste (Services) sowie die dazugehörigen Auditfunktionen (SACL) nicht weiter gewürdigt. Mit Windows NT4 (SP6a) war Microsoft da schon einmal weiter.

OWASP Top 10 runderneuert

Im Rahmen der OWASP Appsec 2009 in Washington stellte Dave Wichers am 13.11.2009 die Überarbeitung der bekannten OWASP Top 10 vor. Zeitgleich wurde der Release Candidate 1 der Top 10 zum Download veröffentlicht.

Bei der neuen Version handelt es sich um die inzwischen dritte Überarbeitung. Die Änderungen liegen etwas im Verborgenen, prägen aber den Charakter der neuen Top 10 grundlegend. Listeten

die Vorgängerversionen die am meisten auftretenden Schwachstellen bei Web-Anwendungen auf, orientieren sich die Top 10 nun an Risiken, die nach vorgegebenen Kriterien bewertet wurden. Dabei wurden Angreifer, Ausnutzbarkeit der Schwachstelle und mögliche Auswirkungen berücksichtigt.

Auch die Darstellung der Top 10 hat sich verändert. Zielte das Dokument bisher hauptsächlich darauf, die Awareness von Entwicklern für Schwachstellen zu verbessern, wurde die Zielgruppe jetzt auf Entscheider, Tester und Sicherheitsexperten erweitert. Jeder Eintrag besteht aus einer Bewertung des Risikos, der Vorstellung von Schutzmaßnahmen, Beispielen und Referenzen. Die meisten der enthaltenen Verweise zeigen auf hilfreiche OWASP-eigene Dokumente.

In den neuen Top 10 haben die beiden Spitzenreiter der Vorversion „Injection" und „XSS" die Plätze getauscht. Auf Platz 6 und 8 finden sich als Neueinsteiger „Security Misconfiguration" und „Unvalidated Redirects and Forwards". Zur Zeit befinden sich die Top 10 noch in der Review-Phase. Kommentare und Verbesserungsvorschläge an den Autor sind herzlich willkommen.

Vorsicht Falle!

Für einen am 04.09.2009 veröffentlichten Technical Report hat sich Frank Stajano von der Universität Cambridge mit Paul Wilson, einem der Autoren der BBC-Serie „The Real Hustle" (einer Art Mischung aus „Vorsicht Falle!" und „Vorsicht Kamera!") zusammen getan – nicht, um Prinzipien der Informationssicherheit anschaulich zu illustrieren, sondern um die „menschlichen Faktoren" zu verstehen, die Trickbetrüger regelmäßig ausnutzen.

Der Report stellt zunächst zahlreiche typische, in der Sendung gezeigte Betrugsfälle vor. Daraus leiten die Autoren dann sieben Verhaltensprinzipien von Ablenkung über Herdentrieb bis zum gefühlten Zeitdruck ab, die Betrüger ausnutzen – und die es im Umkehrschluss beim Design von sicher nutzbaren Systemen zu vermeiden gilt.

Das Dokument liefert viele lebendige Beispiele zur Illustration von Security-Themen – und könnte als Lehrmaterial für Entwickler von Security-relevanten Benutzerschnittstellen effektiver sein als manches Theorie lastige „Securitiy & Usability"-Papier. Unterhaltsamer ist es allemal.

Secorvo News

Secorvo College aktuell

Der TISP ist etabliert: Seit der Einführung im Jahr 2004 haben 350 Teilnehmer das Zertifikat erworben – Tendenz steigend. Gehören auch Sie zu den ersten 500 und buchen Sie Ihren Platz in einer der TISP Schulungen 2010 bei Secorvo College – zum Beispiel vom 22. bis 26.02.2010. Auch in der Softwareentwicklung beginnt sich erfreulicherweise Sicherheit als Qualifikation durchzusetzen. Das zeigt unter anderem das Interesse am CPSSE, dem ersten Qualifikationszertifikat für sichere Softwareentwicklung. Nächster Termin: 16. bis 19.03.2010.

Details zu allen Seminaren finden Sie auf unseren Webseiten; die Jahresübersicht 2010 erleichtert die Planung. Wir freuen uns auf Ihre Anmeldung.

Wunsch und Wirklichkeit

Gelegentlich werden auch in der IT-Sicherheit Wünsche wahr. Das zeigt die Awareness-Kampagne „SecurityCup 2009", in der es die FIDUCIA zusammen mit der Agentur DauthKaun geschafft hat, ihre Mitarbeiter wirksam zum Schutz von Informationen, Daten und Know-How zu sensibilisieren. Am 18.02.2010 stellen Sven Kaun (DauthKaun) und Lutz Bleyer (FIDUCIA) die Kampagne auf der ersten Veranstaltung der KA-IT-Si im neuen Jahr vor – wir freuen uns auf Ihre Teilnahme (Beginn wie immer um 18 Uhr im Schlosshotel Karlsruhe, mit anschließendem Buffet-Networking).

Übrigens: Die Unterlagen des letzten diesjährigen KA-IT-Si-Events vom 26.11.2009 zum Thema Datenrettung finden Sie zum Download auf den KA-IT-Si-Seiten.

Feiertagslektüre

Seit Online-Banking in den Fokus von Internet-Angriffen gerückt ist und sowohl Phishing-E-Mails als auch spezialisierte Banking-Trojaner die Vermögen deutscher Bankkunden bedrohen, haben Banken neue Protokollvarianten eingeführt – von iTAN über mTAN bis zum TAN-Generator. Nun hat Hans-Joachim Knobloch zwei grundlegende Verfahren einer Sicherheitsanalyse mittels BAN-Logik unterzogen und die Ergebnisse in Ausgabe 12/2009 der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)" veröffentlicht.

Ebenfalls in der DuD erscheint im Januar 2010 in der Rubrik „Best Practice" eine Empfehlung von Kai Jendrian zur Erweiterung des Web-Browsers Firefox um Add-ons, die die Sicherheit und den Schutz der persönlichen Daten beim Surfen signifikant erhöhen. Da ist möglicherweise der eine oder andere wertvolle Tipp dabei, um an den Feiertagen den Schutz des neuen PCs wirksam zu verbessern.

Weitere Publikationen von Secorvo finden Sie in der Übersicht auf unserer Webseite.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2009	
06.-10.12.	15th ASIACRYPT 2009 (IACR, Tokio/JP)
27.-30.12.	26th Chaos Communication Congress (CCC, Berlin)
Januar 2010	
19.-21.01.	Omnicard 2010 (inTIME, Berlin)
Februar 2010	
02.-03.02.	20. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
03.-04.02.	ESSoS (DistriNet Research Group, Pisa/I)
05.-07.02.	ShmooCon 2010 (Shmoo Group, Washington/USA)
09.-10.02.	17. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
22.-26.02.	TISP-Schulung (Secorvo College)
März 2010	
16.-19.03.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)

Fundsache

In einem 123seitigen Report vom 20.11.2009 hat die European Network and Information Security Agency (ENISA) die Nutzung von Cloud-Computing einer Risiko-Analyse unterzogen. Acht von 35 betrachteten Risiken ordnet sie dabei der Risikoklasse „High" zu. Daraus leitet sie zahlreiche Empfehlungen für die Nutzung von Cloud-Computing ab.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Jochen Schlichting, Jörg Völker

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Dezember 2009



Endogene Bedarfsexpansion

Wenn Sie Kinder haben, kennen Sie das Phänomen. Besonders gut ist es jährlich vor dem Weihnachtsbaum zu beobachten: Ganz gleich, wie viele Pakete Ihre Kinder ausgepackt haben – nach dem letzten schweifen die Blicke sehnsüchtig suchend bis zur enttäuschenden Einsicht durch den Raum, dass es tatsächlich das letzte war.

Vielleicht ist diese „Gier nach mehr" ja nicht nur die natürliche Erklärung für die Faszination des österlichen Eiersuchens, sondern der wahre Antrieb hinter dem Streben nach immer mehr Kontrolldaten – wie die Ausweitung der Videoüberwachung im öffentlichen Personenverkehr (Verkehrsministerkonferenz vom 04.12.2009) oder die anlassunabhängige des Individualverkehrs, die erst das Bundesverfassungsgericht stoppen konnte (Beschluss vom 11.08.2009). Auch die Zahl der Telefonüberwachungen, bereits 2007 weltweit auf historisch einmalig hohem Niveau, stieg 2008 erneut – um 11% auf 16.463 Maßnahmen. Dass daher die Vorratsdatenspeicherung von Telekommunikationsdaten, die am 15.12.2009 vom Bundesverfassungsgericht verhandelt wurde, keine gute Idee ist, zeigen auch die Versuche der Strafverfolgungsbehörden, trotz expliziten Verbots im § 7 Autobahnbaumtgesetz („Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig") auf die vom Betreiber Toll Collect an Maut-Kontrollbrücken erhobenen Daten zuzugreifen, Stellungnahmen wie die der Musikindustrie und die Feststellungen des Bundesdatenschutzbeauftragten, dass TK-Unternehmen weit mehr speichern als erlaubt: Einst auf schwere Straftaten beschränkt, droht der Eingriff ins Fernmeldegeheimnis zum Standard-Ermittlungsinstrument zu werden. Fehlen noch die Pflicht zu „intelligenten Stromzählern" und die Abschaffung des Bargelds: Präziser lassen sich Lebensgewohnheiten kaum bestimmen.

„Die Freiheit stirbt scheibchenweise": Worte des Jahres 2001 in „Die ZEIT", von Sabine Leutheusser-Schnarrenberger. Seit dem 28.10. 2009 ist sie Bundesjustizministerin. Die Hoffnung stirbt zuletzt.



Inhalt

Endogene Bedarfsexpansion

Security News

SQL-Firewall

Nichts gelernt ...

Forensik-Folklore

Schöner neuer Personalausweis

ISO 2700x mit x=4

Feiertagslektüre

Secorvo News

Secorvo College aktuell

Wege zum Ruhm

Teamverstärkung

Veranstaltungshinweise

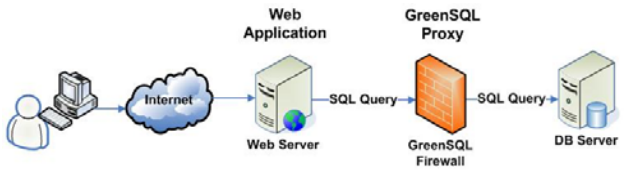
Fundsache

secorvo
security consulting

Security News

SQL-Firewall

Am 02.12.2009 wurde Version 1.2 der OpenSource SQL-Firewall GreenSQL freigegeben. Die Idee hinter diesem speziellen Application Level Gateway ist, Zugriffe von (Web-) Applikationen auf dahinter liegende Datenbanken zentral und unabhängig von der Anwendung filtern zu können.



(Quelle: greensql.net)

Audits von Web-Applikationen zeigen, dass sehr viele Web-Anwendungen keine ausreichende Eingabevalidierung vornehmen und so anfällig für SQL-Injection sind. Zudem besteht immer das Risiko, dass ein Webserver über Schwachstellen der Plattform, des Webservers selbst oder der Anwendung (PHP, .net, J2EE, Ruby etc.) kompromittiert wird. In diesen Fällen kann auf die dahinter liegende Datenbank, selbst wenn sie in einer separaten Netzwerkzone betrieben wird, unberechtigt zugegriffen werden.

Bei einer Kontrolle der Zugriffe mittels GreenSQL ist es beispielsweise möglich zu definieren, auf welche Tabellen und Datenbestände zugegriffen werden darf, oder ob Daten nur gelesen, aber nicht geschrieben werden dürfen. Einen ersten Eindruck zu den Konfigurationsmöglichkeiten kann man sich in einer Live-Demo verschaffen. Derzeit werden MySQL und PostgreSQL unterstützt.

Nichts gelernt ...

... aus den Datenschutzskandalen der jüngsten Zeit hatten offenbar die Verantwortlichen des Sozialen Schülernetzwerks haefft.de. Am 04.12.2009 deckte der Chaos Computer Club (CCC) Scheunentor große Sicherheitslöcher bei dem Portal auf. Erschreckend in diesem konkreten Fall: die schlechten Implementierungen von Sicherheitsmaßnahmen zum Schutz intimer personenbezogener Daten von Kindern.

Nachdem in einer inzwischen gelöschten Pressemitteilung der Fall von den Verantwortlichen herunter gespielt worden war, eskalierte der Vorgang. Nun ist das Portal offline – der Betreiber entschuldigt sich in einer neuen Stellungnahme für die Fehler und erläutert das nun geplante Vorgehen.

Der Vorfall ruft drei Grundregeln ins Gedächtnis:

1. Sorgen Sie *als Entwickler* von Web-Anwendungen, die personenbezogene Daten speichern und verarbeiten, für korrekte Implementierung, sicheren Betrieb und wirksame Schutzmaßahmen.

2. Achten Sie *als Betreiber* bei Sicherheitsvorfällen auf eine angemessene Krisenkommunikation.

3. Bedenken Sie *als Betroffener* genau, welche Daten Sie über sich wo preisgeben – und sprechen Sie mit Ihren Kindern über das Thema.

Forensik-Folklore

Zu dem bereits am 15.04.2009 veröffentlichten 2009 Data Breach Investigations Report des Sicherheitsdienstleisters Verizon Business (vgl. SSN 04/2009) erschien am 09.12.2009 – als Nachschlag – ein Supplemental Report, der die Bedrohung durch die 15 häufigsten Angriffsarten, von Keyloggern über Social Engineering bis hin zum Durchforsten des RAM-Speichers in Kassensystemen und zum „*ishing“, ausführlicher analysiert und jeweils ein anonymisiertes Fallbeispiel schildert.

Bei einigen dieser anekdotischen Schwachstellenbeschreibungen lässt sich ein Schmunzeln kaum unterdrücken (wie beim manuellen Ersetzen von „validUser=0“ durch „...=1“ in einer Web-Anwendung, um die Anmeldung einzusparen), bei anderen beschleicht einen das ungute Gefühl, möglicherweise selbst nicht ausreichend gegen ähnliche Angriffe gefeit zu sein.

Schöner neuer Personalausweis

Nachdem am 10.11.2009 bekannt geworden war, dass das BMI ein Konsortium unter Siemens-Führung mit der Bereitstellung der Middleware für den neuen elektronischen Personalausweis, den „Bürger-Client“ beauftragt hatte, meldete die mtG media transfer AG am 30.11.2009, dass sie den Zuschlag für den Aufbau der Root CAs für die Nutzung und den Zugriff auf die Daten des künftigen Personalausweises erhalten habe.

Bemerkenswert: Diese Root CAs werden beim BSI in Anlehnung an die bestehende Verwaltungs-PKI (die im gleichen Zuge runderneuert wird) aufgebaut. Hingegen bleiben die Zertifizierungsdiensteanbeiter für die elektronische Signatur und deren bei der BNetzA betriebene Root CA ein optionales Anhängsel der Ausweiskarte. Darf das als späte Einsicht in die Erfolglosigkeit überregulierter Signatur-Infrastrukturen gewertet werden?

ISO 2700x mit x=4

Mit Veröffentlichungsdatum vom 15.12.2009 ist ein neuer Standard in der ISO-27000er-Reihe zur Messung der Informationssicherheit erhältlich – ISO/IEC 27004:2009 „Information technology – Security

techniques – Information security management – Measurement".

Darin wird endlich verbindlich geregelt, was unter Messungen und Bewertungen im Rahmen eines Informationssicherheitsmanagements nach ISO 27001 zu verstehen ist. Neben den Erklärungen zu einem sinnvollen Vorgehen bei der Entwicklung von Messungen finden sich auch Hinweise zur Verantwortung des Managements sowie zu Durchführung und Dokumentation von Messungen.

Einen großen Teil der über 50 Seiten des Standards füllen praktische Beispiele und eine Dokumentationsvorlage im Anhang. Damit wird dem Praktiker eine nützliche Arbeitshilfe zur Verfügung gestellt. Der neue Standard ergänzt das Dokument „BIP 0074 – Measuring the effectiveness of your ISMS implementations" nun verbindlich.

Übrigens: Seit etwa sechs Monaten ist das Rahmenwerk – der Standard ISO 27000 – auch Lizenzkosten frei verfügbar.

Feiertagslektüre

Wer schon immer wissen wollte, wie es wäre, wenn Stanley Kubrick eine Anfängervorlesung in IT-Sicherheit gegeben hätte, wird wohl mit Vergnügen den am 15.12.2009 erschienenen Bericht von Matt Blaze über seinen Besuch in einem zum Museum umgewandelten Interkontinentalraketen-Silo lesen. Darin analysiert der bekannte Kryptologe und Autor des Cryptographic Filesystem CFS die Sicherheitsmaßnahmen, mit denen im Kalten Krieg die ins Extrem getriebenen, einander widerstrebenden Anforderungen nach Hochverfügbarkeit bei gleichzeitiger strikter Zugriffskontrolle realisiert wurden, wie Vier-Augen-Prinzip, Physische Zutrittskontrollen oder „Separation of Duties".

Secorvo News

Secorvo College aktuell

Auch im neuen Jahr bieten wir Ihnen im Secorvo College wieder zahlreiche Gelegenheiten, Ihr Wissen zu zertifizieren. Neben der etablierten TISP-Schulung, unter anderem vom 22. bis 26.02.2010, können Sie sich mit dem CPSSE als Experte im Bereich der sicheren Softwareentwicklung zertifizieren. Die erste Schulung im neuen Jahr findet vom 16. bis 18.03.2010 statt. Hintergründe zur Zielsetzung und Entstehung des Zertifikats liefern zwei kürzlich erschienene Aufsätze von Petra Barzin, einer der Initiatorinnen des CPSSE: „A New Qualification to Guarantee Secure Software Engineering Skills" (in: ENISA Quarterly Review, Vol. 5 No. 3, September 2009, S. 18) und „International Secure Software Engineering Council (ISSECO)" (in: SecurityActs No. 1, Oktober 2009, S. 14 f.).

Unsere Grundlagenseminare zu den Themen Sicherheitsmanagement, PKI und IT-Sicherheitsaudit finden Sie ebenfalls im Programm 2010, nicht zuletzt dank der durchweg positiven Rückmeldungen der Teilnehmer. Eine aktuelle Übersicht finden Sie in unserem Seminarkalender 2010. Melden Sie sich an, wir freuen uns auf Sie!

Wege zum Ruhm

Die KA-IT-Si verabschiedet sich nach sechs Events zu spannenden Themen der IT-Sicherheit aus dem Jahr 2009 in eine kurze Verschnaufpause. Am 18.02.2010 stellen Sven Kaun und Lutz Bleyer die Awareness-Kampagne „Security Cup 2009" der FIDUCIA IT AG vor – und sich beim anschließenden Buffet-Net(t)working der Diskussion. Um Anmeldung wird gebeten.

A propos Awareness: Die KA-IT-Si freut sich über jeden weiteren Partner, der die Arbeit der Initiative unterstützt – den Wissenstransfer zur IT-Sicherheit auf den Fachevents, den regen Erfahrungsaustausch unter IT-Sicherheitsverantwortlichen und die Sensibilisierung insbesondere mittelständischer Unternehmen für die Bedeutung der Informationssicherheit. Nähere Informationen zur KA-IT-Si-Partnerschaft finden Sie auf der KA-IT-Si-Webseite.

Teamverstärkung

Seit dem 01.08.2009 verstärkt Dr. Safuat Hamdy das Secorvo-Team – den regelmäßigen und aufmerksamen Lesern bereits vom Editorial der SSN 10/2009 bekannt.

Im kommenden Jahr soll unser Team weiter wachsen: Wir suchen mehrere Beraterinnen oder Berater im Gebiet Datenschutz und IT-Sicherheit mit Berufserfahrung für zahlreiche herausfordernde Projekte – und freuen uns über Empfehlungen und Bewerbungen an personal@secorvo.de.



Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2009	
27.-30.12.	26th Chaos Communication Congress (CCC, Berlin)
Januar 2010	
19.-21.01.	Omnicard 2010 (inTIME, Berlin)
Februar 2010	
02.-03.02.	20. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
03.-04.02.	ESSoS (DistriNet Research Group, Pisa/I)
05.-07.02.	ShmooCon 2010 (Shmoo Group, Washington/USA)
09.-10.02.	17. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
15.-18.02.	SecSE 2010: Fourth International Workshop on Secure Software Engineering (SINTEF, Krakau/PL)
22.-26.02.	TISP-Schulung (Secorvo College)
März 2010	
16.-19.03.	ISSECO Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)

Fundsache

Wer noch ein Weihnachtsgeschenk oder Lesestoff für die Feiertage sucht, dem sei ein Blick in die Bücherliste von Tobias Schrödel empfohlen. Fast 500 Werke rund um das Thema Kryptographie hat er zusammengetragen. Allerdings sind einige nicht mehr käuflich zu erwerben, so wie Giovanni Battista Bellasos „Novi et singolari modi di cifrare" (1555).



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2010



O Elena, O mores...

Noch ist die Entscheidung über die verfassungsrechtliche Zulässigkeit einer Vorratsspeicherung von Telekommunikationsdaten nicht gefallen, da tritt das ELENA-Verfahren aus dem Windschatten in die öffentliche Wahrnehmung. Das überrascht etwas – wurde das Verfahren des „Elektronischen Entgeltnachweises" doch bereits am 22.09.2009 vom Bundestag beschlossen. Tatsächlich weist die Entstehungsgeschichte sogar sieben Jahre weit zurück – und ist ein Lehrstück regulativer Technikgestaltung in Deutschland.

Als Projekt „JobCard" erblickte Elena im August 2002 als ein Vorschlag der Hartz-Kommission das Licht der Welt. Signaturkartenverfechter witterten Morgenluft: War das endlich die „Killer-Applikation" der digitalen Signatur? Mit der Behauptung einer Entlastung der Unternehmen um 85,6 Mio. Euro jährlich – im Schnitt beeindruckende 29 Euro je Unternehmen – wurden die verfassungsrechtlichen Zweifel von Datenschützern an der für das Verfahren erforderlichen zentralen Speicherung von Arbeitnehmerdaten erstickt. Tatsächlich macht die Spezifikation der Datensätze vom 19.10.2009 (inzwischen von der Elena-Webseite gelöscht) sprachlos: Neben Entgeltinformationen werden Fehlzeiten mit Datum und Grund, Urlaubstage, Kündigungsgründe und vorausgegangene Abmahnungen inklusive einer Beschreibung des vertragswidrigen Verhaltens (Freitext) erhoben.

Wir erinnern uns: Datenschutz ist Teil des allgemeinen Persönlichkeitsrechts (Art. 2 GG). Eines der Prinzipien ist der Erforderlichkeitsgrundsatz („Datensparsamkeit") – keine Spur davon bei Elenas Vorratsdatenspeicherung. Aber mit dem Datenschutzrecht nimmt man es bei Elena sowieso nicht so genau: „Eine Auskunft ist vor 2012 (...) nicht realisierbar, da der Abruf durch die abrufenden Stellen erst ab 2012 möglich ist„, heißt es lapidar auf der Webseite. Ein klarer Rechtsverstoß, denn das Auskunftsrecht besteht nach § 34 BDSG uneingeschränkt. Wir empfehlen: Fordern Sie es ein (Vorlage). Und falls Sie keine Auskunft erhalten, wenden Sie sich an den Bundesdatenschutzbeauftragten.



Inhalt

O Elena, O mores...

Security News

768 bit faktorisiert

Legic gebrochen

WASC Threat Classification

Empfohlene Kryptoverfahren

DNSSEC livehaftig

Audit-Wundertüte runderneuert

SOA-Kompendium

Secorvo News

Secorvo College aktuell

SecurityCup 2009

Veranstaltungshinweise

Security News

768 bit faktorisiert

Schon am 12.12.2009 gelang einem internationalen Kryptologen-Team um Bos, Franke, Kleinjung, Lenstra und Montgomery die Lösung der 768-bit-RSA-Challenge – die Zerlegung eines 768-bit-Modulus in seine Primfaktoren. Details der Number Field Sieve-Faktorisierung veröffentlichten die Autoren am 06.01.2010. Danach benötigten sie 2^{37} Operationen (≈ 4,7 Mio. MIPS-Jahre) zur Bestimmung der Primfaktoren – nur ein Zehntel des von Silverman im Jahr 2000 geschätzten Aufwands. Für den aufwändigsten Teil der Berechnung, das „Aussieben", arbeiteten viele hundert Workstations über zwei Jahre – das entspricht etwa 1.500 Rechenjahren eines 2.2 GHz AMD Opteron-Prozessors.

Tatsächlich deckt sich dieser Erfolg fast exakt mit der im Jahr 2002 veröffentlichten Prognose von Secorvo (siehe Abb.): Darin hatten wir die Faktorisierung von 768 bit für Anfang 2010 vorausgesagt.

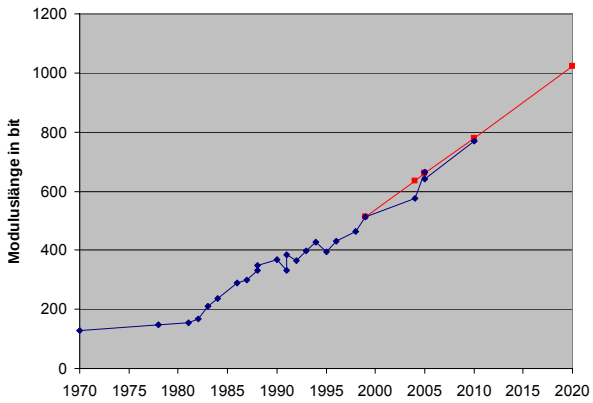


Abb.: Faktorisierungserfolge (blau), Prognose (rot)

Trotz dieses Faktorisierungserfolgs liegt die öffentliche NFS-Faktorisierung eines 1.024-bit-Modulus noch deutlich in der Zukunft – der dafür erforderliche Aufwand ist um den Faktor 1.000 größer. In den kommenden fünf Jahren sei daher auch unter Berücksichtigung des technischen Fortschritts nicht mit einer Faktorisierung zu rechnen. Die Secorvo-Prognose erwartet die Faktorisierung Anfang des Jahres 2020 – spätestens dann sollten 1.024-bit lange RSA-Schlüssel nicht mehr eingesetzt werden.

Legic gebrochen

Fast auf den Tag genau zwei Jahre nach dem spektakulären Brechen der Mifare-Classic-Chipkarten (siehe SSN 03/2008) haben Karsten Nohl und Henryk Plötz am 29.12.2009 auf dem 26. Chaos Computer Congress das Clonen von Legic Prime Chipkarten präsentiert. Da der Hersteller, wie sie feststellen mussten, komplett auf Kryptoverfahren verzichtet und lediglich ein simples 7-bit-Schieberegister für den „Schlüsselstrom" verwendet hatte, konnten sie sich eine aufwändige Chip-Analyse sparen – „Security by Obscurity" bricht man eleganter mit „Trial and Error".

Unternehmen, die vor zwei Jahren schadenfroh mit dem Finger auf die vom Mifare-Hack betroffenen Firmen gezeigt, sich aber bis heute auf ihre Legic Prime Chips verlassen haben, ohne auf das „Legic Advant"-Verfahren zu migrieren, droht nun ein böses Erwachen – den Passepartout in ihr Unternehmen gibt es jetzt zum Preis einer Taxifahrt.

WASC Threat Classification

Zum Jahresbeginn wurde am 01.01.2010 vom Web Application Security Consortium (WASC) die Version v2.0 der „WASC Threat Classification" veröffentlicht. Die Darstellung von 34 verschiedenen Angriffen (z. B. Buffer Overflow, XSS, SQL Injection) auf Web-Anwendungen und 15 Schwachstellen (z. B. Directory Indexing, Insufficient Authorization, Server Misconfiguration) ist sowohl online als auch als 171 Seiten starkes PDF-Dokument verfügbar. Sie gibt einen guten Überblick über aktuelle mögliche Probleme von Web-Anwendungen.

Jeremiah Grossman nimmt in seinem Blog eine Zuordnung zwischen der WASC Threat Classification und den OWASP Top Ten 2010 RC1 (siehe SSN 11/2009) vor – wobei sich der Eindruck aufdrängt, dass durch eine engere Zusammenarbeit und Abstimmung zwischen WASC und OWASP doppelte Arbeit vermieden werden könnte.

Empfohlene Kryptoverfahren

Das US-amerikanische National Institute of Standards and Technology (NIST) veröffentlichte am 14.01.2010 die jüngsten Empfehlung zu Krypto-Algorithmen und Schlüssellängen als Draft Special Publication 800-131. Danach steigt das vorgeschriebene Sicherheitsniveau ab 2011 auf mindestens 112 bit – nur noch Triple-DES mit drei Schlüsseln und AES-128, -192 und -256 dürfen dann noch von Bundesbehörden eingesetzt werden. Auch der SHA-1 darf ab 2011 nicht mehr für die Signaturerzeugung genutzt werden, DSA und RSA müssen Moduluslängen von mindestens 2.048 bit verwenden und Verfahren auf Elliptischen Kurven wie ECDSA Endliche Körper der Ordnung 224. Ab dem Jahr 2031 soll das Sicherheitsniveau auf mindestens 128 bit steigen – eine Anforderung, die die NSA bereits heute an „secret" klassifizierte Daten stellt.

Dem Entwurf des BSI zu Folge wird sich auch die Empfehlung geeigneter Algorithmen der BNetzA, die in Kürze im Bundesanzeiger publiziert werden wird, an die NIST-Empfehlung annähern: RIPEMD-

160 und SHA-1 dürfen danach nur noch bis Ende 2010 zur Signaturerzeugung eingesetzt werden, die Mindestlänge von RSA-Moduli steigt auf 1.976 bit.

DNSSEC livehaftig

Seit dem 05.01.2010 stellt die DENIC eG im DNSSEC Testbed für Deutschland auf zwei speziell eingerichteten Nameserverclustern einen Name Service für die Top Level Domain .de bereit, bei dem die autoritativen Auskünfte per DNSSEC signiert sind. Dies ist zwar noch kein regulärer DNSSEC Betrieb für .de, aber doch genau wie im richtigen Leben: Die DNS-Auskünfte des Testbeds sind ebenso vollständig und aktuell wie die der offiziellen Nameserver von a.nic.de bis z.nic.de.

Wer selbst schon DNSSEC für seine .de-domain einsetzt, muss sich noch bis zum März 2010 gedulden - ab dann wird die DENIC auch Key Signing Keys untergeordneter Domains registrieren und per DNSSEC zertifizieren.

Audit-Wundertüte runderneuert

Die am 11.01.2010 erschiene Auditing-Distribution Backtrack 4 Final wurde gegenüber Version 3 auf Ubuntu umgestellt, um ein zeitnahes Patchmanagement zu ermöglichen. Der revisionssicher nachvollziehbare Change der ca. 500 Prüfwerkzeuge – sowie zukünftiger Ergänzungen – kann anhand der Loginformationen der Installationsumgebung nachgewiesen werden. Wichtige Ergänzungen – neben der deutlich erweiterten Treiberunterstützung für Hardware – sind bekannte Programmpakete, wie OpenVAS 3.0, Nmap 5.2 und Metasploit 3.3.3. Die Sniffersuite lässt nun auch bei Bluetooth, RFID und Voice over IP kaum noch einen Wunsch offen.

Der Scanner OpenVAS wurde als freier Nessusersatz integriert und läuft stabil mit ca. 15.500 Prüfungen. Zeitsparend ist die integrierte Versionierung von bisherigen Scans und Scanergebnissen für deren Wiederholbarkeit. Für Prüfungen, die einen Proof-of-Concept erfordern, ist die Weiterführung von milw0rm in der exploit-db (mehr als 10.000 technische Schwachstellen) eine erfreuliche Ergänzung. Spannend wird es – die richtige Grafikkarte(n) vorausgesetzt – bei der Nutzung von Werkzeugen, die auf CUDA basieren. Hier sind u. a. Multiforcer (Passwort-Bruteforcer für MD5, FASTMD5, MD4, FASTMD4, NTLM, FASTNTLM, SHA1, FASTSHA1), der RAR-Archivbrecher cRARk und Pyrit (für WPA2-PSK) treue Helfer.

Insgesamt also ein unverzichtbares Werkzeug für den (technischen) Auditor mit zahlreichen sinnvollen „Aufrüstungen".

SOA-Kompendium

Am 05.01.2010 hat das BSI Version 2.0 des in erster Fassung vor zwei Jahren veröffentlichten „SOA-Security-Kompendium Sicherheit in Service-orientierten Architekturen" herausgegeben. In dem 371seitigen PDF-Dokument werden verschiedene Sicherheitsaspekte von SOA-Umgebungen ausführlich dargestellt. Aufgrund der Komplexität des Themas ist die Verfügbarkeit eines umfassenden Referenzwerks, das neben einer Einführung besonders die Themen Technologien (96 Seiten), Security Management (46 Seiten) und spezielle Sicherheitskonzepte (72 Seiten) behandelt, eine echte Arbeitshilfe.

Secorvo News

Secorvo College aktuell

Die Nachfrage nach einer TISP-Zertifizierung ist ungebrochen - seit 2004 haben 350 Sicherheitsexperten das Zertifikat erworben. Lassen auch Sie Ihre Qualifikation bei der nächsten TISP-Schulung mit anschließender Prüfung vom **22.–27.02.2010** zertifizieren. Dass Sicherheit auch in der Software Entwicklung eine immer wichtigere Rolle spielt, zeigt das wachsende Interesse am Certified Professional for Secure Software Engineering (CPSSE). Das Zertifikat können Sie vom **16.–19.03.2010** erwerben. Im März steht außerdem erstmals das neue Seminar „Sicherheitsmanagement heute" auf dem Programm. Verschaffen Sie sich vom **23.–25.03.2010** einen Überblick über die Grundlagen des Information Security Managements. Das gesamte Seminarangebot 2010 sowie die Möglichkeit zur Online-Anmeldung finden Sie hier.

SecurityCup 2009

Die Karlsruher IT-Sicherheitsinitiative beginnt ihre diesjährige Veranstaltungsreihe mit einem spannenden Thema: Die FIDUCIA IT AG führte 2009 ihre dritte Security-Awareness-Kampagne durch – auf höchstem konzeptionellen Niveau und mit einer aktiven Mitarbeiterbeteiligung von über 50 Prozent. Am 18.02.2010 stellen Lutz Bleyer, Leiter der Zentrale Security bei der FIDUCIA IT AG Karlsruhe, und Sven Kaun, Geschäftsführer der Dauth.Kaun Communication Group GmbH sowohl die Highlights des „SecurityCup 2009" als auch ihre „Lessons Learned" und „Do's and Dont's" vor. Anschließend gibt es Gelegenheit zum Networking am Buffet. Um Anmeldung wird gebeten.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2010	
02.-03.02.	20. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
03.-04.02.	ESSoS (DistriNet Research Group, Pisa/I)
04.-05.02.	COSADE 2010 (CASED, Darmstadt)
05.-07.02.	ShmooCon 2010 (Shmoo Group, Washington/USA)
09.-10.02.	17. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
11.02.	Infoveranstaltung Datenschutz (CyberForum/ORGA GmbH, Karlsruhe)
15.-18.02.	SecSE 2010: Fourth International Workshop on Secure Software Engineering (SINTEF, Krakau/PL)
18.02.	Wege zum Ruhm – „SecurityCup 2009“ (KA-IT-Si, Karlsruhe)
22.-26.02.	TISP-Schulung (Secorvo College)
23.02.	CASED-Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
März 2010	
16.-19.03.	ISSECO Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)
April 2010	
13.-16.04.	PKI (Secorvo College)
20.-21.04.	Security News Symposium 2010 (Secorvo, Ettlingen)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2010



Editorial: Gotcha

Mit jedem Klick im Browser geben wir viele Informationen preis, die wir für sich genommen harmlos finden. Bei genauer Betrachtung zeigt sich aber, dass 33 bit Information ausreichen, um einen Menschen weltweit eindeutig zu identifizieren. Jeder Browser übermittelt in der Grundeinstellung zahlreiche Daten, die geeignet sind, einen digitalen Fingerabdruck des Surfers zu erstellen. Durch clevere Ergänzungen verraten Browser weitere Informationen wie die eingesetzten Add-Ons oder das Zeitverhalten bei der Passwort-Eingabe.

Damit nicht genug: Wie seit fast acht Jahren in der Mozilla-Community diskutiert, lassen sich den Browsern durch History-Stealing Informationen über vormals besuchte Seiten entlocken. Diese Technik wird von Internetseiten wie didyouwatchporn.com oder whattheinternetknowsaboutyou.com eindrucksvoll demonstriert. Mag man diese Seiten noch amüsant finden, vergeht einem das Lachen spätestens bei der Lektüre der Studie „A Practical Attack to de-Anonymize Social Network Users“, in der erläutert wird, wie durch History-Stealing die tatsächliche Identität eines Surfers über das Nutzerverhalten in Sozialen Netzwerken ermittelt werden kann – dies lässt sich im Selbstversuch leicht überprüfen.

Diese Techniken sind leider nicht nur von theoretischer Bedeutung, sondern werden teilweise schon zum Tracking von Surfern eingesetzt. Mit etwas Fantasie lässt sich ausmalen, was möglich wäre, wenn Dienste wie Google-Analytics oder etracker damit arbeiten würden. Die Tendenz, die Privatsphäre von Internet-Nutzern einzuschränken, ist – aus unterschiedlichen Motiven – weit verbreitet, das zeigen Initiativen wie die Vorratsdatenspeicherung, der Bundestrojaner oder die zahlreichen Datenschutzskandale in der Wirtschaft.

Kundige Nutzer können durch Selbstschutzmaßnahmen ihre Situation verbessern. Für den Schutz der Privatsphäre aller Internet-Nutzer ist es jedoch erforderlich, dass Browser diesen in der Grundkonfiguration respektieren.



Inhalt

Editorial: Gotcha

Security News

Bitte einbrechen!

25 MDPE

Film-Tipps für Chipkartenfans

Wert von Sicherheitsbeweisen

Learning Websecurity by Doing

Brothers are Listening

Secorvo News

Secorvo College aktuell

Security News Symposium

Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Bitte einbrechen!

Einsichtsfähigkeit zählt im Allgemeinen nicht zu den menschlichen Stärken. Noch seltener gelingt es den meisten Menschen, die Kluft zwischen Einsicht und Umsetzung zu schließen. Ein Paradebeispiel dafür ist die wachsende Begeisterung, mit der Privates auf Portalen wie StudiVZ, Wer-kennt-wen, Facebook oder Xing preisgeben wird – und Hunderttausende ihren Tagesablauf via Twitter herauszwitschern.

Am 17.02.2010 ging die Webseite „Please rob me!“ online – eine Art „Awareness-Service“ für Uneinsichtige, betrieben von forthehack (Rijswijk). Eine automatische Twitter-Suche liefert alle aktuellen Nachrichten, aus denen die Abwesenheit von zu Hause erkennbar ist, und zeigt Namen, Foto und den aktuellen Aufenthaltsort an (via foursquare). Zugegebenermaßen eine drastische Methode – aber vielleicht wirksamer als Predigten. Wie wäre denn eine Webseite „Don't hire me!“ mit den heftigsten StudiVZ-Fotos vom vergangenen Wochenende?

25 MDPE

Am 17.02.2010 wurden die von Mitre und SANS zusammengestellten „2010 CWE/SANS Top 25 Most Dangerous Programming Errors“ als grundlegende Überarbeitung der vorjährigen Liste veröffentlicht. Wenig überraschend finden sich unter den schwerwiegendsten Schwachstellen Cross Site Scripting, SQL-Injection und Cross Site Request Forgery wieder auf den Plätzen eins, zwei und vier.

Bahnbrechend neue Erkenntnisse liefert die Liste nicht – Dokumente wie die OWASP Top Ten oder WASC Threat Classification (SSN 01/2010) weisen auf die gleichen Gefahren hin. Im Gegensatz zu diesen beiden Dokumenten adressiert die CWE/SANS-Liste die Probleme aus Entwicklersicht und bietet, auch durch Verweis auf die deutlich umfangreichere „Common Weakness Enumeration“-Datenbank, konkrete Hilfestellung zur Vermeidung oder Behebung der identifizierten Probleme. Softwareentwicklern sind alle drei Dokumente zur regelmäßigen Lektüre zu empfehlen.

Film-Tipps für Chipkartenfans

Im Januar machte ein RBB-Video Furore, das die Umsetzung des Angriffs auf Legic Prime (siehe SSN 01/2010) am Hamburger Flughafen zeigt. Im Februar sind gleich zwei spannende Videos zu empfehlen: Bei der Konferenz Blackhat DC präsentierte Chris Tarnovsky am 02.02.2010 das Ergebnis monatelanger Analysen: Mit einer Laborausstattung zum geschätzten Anschaffungspreis von US$ 200.000 und unter Verschleiß etlicher Testmuster gelang es ihm, geheime Daten aus dem Trusted Platform Module (TPM) einer XBox Spielekonsole auszulesen – einem TPM-Chip der Infineon SLE66 Smartcard-Chipfamilie. In einem Wired-Video vom 23.08.2008 hatte Tarnovsky bereits demonstriert, wie er einen Smartcard-Chip und seine Datenleitungen frei legt. Nun gibt es eine belegte Abschätzung des nötigen Aufwands an Geld und Zeit.

Den Sicherheitsforschern der Universität Cambridge um Ross Anderson gelang es derweil, mit einem am 11.02.2010 als Vorabdruck veröffentlichten Man-in-the-Middle Angriff das EMV-basierte „Chip & PIN“ Verfahren zu brechen, das in Großbritannien für Kartenzahlungen am Point of Sale (POS) eingesetzt wird. Dabei gaukelten sie der Karte vor, dass das Terminal eine Transaktion mit Unterschrift (statt PIN) angefordert hat, während sie dem Terminal signalisierten, dass eine (beliebige) Ziffernkombination von der Karte als gültige PIN akzeptiert wurde. Die zwischen der (gestohlenen) echten Karte und dem ins Terminal eingesteckten Kartenadapter eingeschobene Gerätschaft passt, wie in einem BBC-Video zum Bericht vom 11.02.2010 demonstriert, bequem in einen Rucksack.

Spektakulär an dem Angriff ist, dass er auch im Online-Modus des POS-Terminals funktioniert und der Kundenbeleg „PIN verified“ ausweist. Chip&PIN verstößt offenbar gegen die wichtige Design-Maxime für kryptografische Protokolle, dass in die errechneten Authentisierungs- oder Signaturdaten alle relevanten Statusinformationen eingehen müssen – in diesem Fall auch die Tatsache, ob eine PIN angefordert bzw. verwendet wurde.

Wert von Sicherheitsbeweisen

Quantenkryptografie wurde bisher von seinen Protagonisten als absolut sichere Verschlüsselungsmethode verkauft, da die Grundlagen des Quanten-Schlüsselaustauschs auf den ehernen Gesetzen der Quantenphysik basieren. Der Traum vom praktisch verwendbaren One-Time-Pad war in so greifbare Nähe gerückt, dass es schon erste kommerzielle Produkte dafür gibt. So bestechend der Sicherheitsbeweis für Quantenkryptografie ist – man muss auch auf die äußeren Umstände einer Implementierung achten, denn der Beweis setzt voraus, dass ein Angreifer den Austausch nicht beobachten kann, ohne bemerkt zu werden.

In einem Beitrag auf dem CCC-Kongress führte ein Team aus Singapur am 27.12.2009 vor, wie gängige Implementierungen ausgehebelt werden können, indem sie geblendet werden. Die Quantenphysik beschreibt Phänomene im mikroskopischen Bereich, was jedoch nicht bedeutet, dass es keine Wechsel-

wirkung mit der makroskopischen Welt gibt. Dies zeigt, dass die Quantenkryptografie noch am Anfang steht, und dass noch Jahre bis zur Entwicklung praxistauglicher Verfahren vergehen werden.

Es zeigt darüber hinaus, dass man die Annahmen, die einem Sicherheitsbeweis zugrunde liegen, sehr genau verstehen muss. Nicht umsonst hat die Forschung etwa zwanzig Jahre gebraucht, um ein brauchbares und allgemein anerkanntes Modell für die Sicherheit von Verschlüsselung zu finden. Dabei wurden viele Beweise und Modelle verworfen, weil die Annahmen zu stark oder implizite Annahmen unrealistisch waren. Es bedeutet jedoch nicht, dass man auf Sicherheitsbeweise verzichten kann, denn ad-hoc-Konstruktionen und intuitive Entwürfe taugen erst recht nicht – das immerhin ist gut belegt.

Learning Websecurity by Doing

Ausprobieren ist eine der besten Methoden, um komplexe Sachverhalte zu verstehen. Diesen Ansatz verfolgt das OWASP WebGoat Projekt. Bisher waren allerdings zu Beginn einige Hürden zu nehmen, wie die manuelle Installation der Anwendung. Seit dem 27.01.2010 ist das nicht mehr erforderlich: Das OWASP Broken Web Applications Projectwaspbwa (owaspbwa) bietet eine VMware-kompatible virtuelle Maschine zum Download an, die eine Vielzahl fertig installierter schwachstellenbehafteter Web-Anwendungen enthält. Dem Lernbegierigen stehen neben WebGoat Konzeptanwendungen wie Vicum, Multidae, Damn Vulnerable Web App und andere, auch ältere Versionen mit echten Bugs von phpBB, WordPress und Yazd zur Verfügung. Wir wünschen viel Erfolg beim „Hands on"-Training.

Brothers are Listening

Aufgrund des am 20.02.2010 auf CryptoMe.org veröffentlichten „Microsoft® Online Services Global Criminal Compliance Handbook" ließ Microsoft die Domäne am 25.02.2010 wegen Verstoßes gegen den Digital Millennium Copyright Act (DMCA) kurzzeitig sperren. Das Dokument vom 29.05.2008 zählt auf Seite 22 die im Rahmen von Auskunftsersuchen der US-Behörden zu liefernden Daten auf. Betroffen sind der Freemail-Dienst Hotmail, die Authentifizierung Windows Live ID, das Instant Messaging mit Windows Live Messenger und das Unterhaltungsportal Xbox. Bei anderen amerikanischen Online-Diensten wie Facebook, Skype, Paypal, MySpace oder Yahoo sieht es hinsichtlich der Kooperationsfreude mit Behörden ähnlich aus, wie die ca. 30 „Lawful Spy Guides" auf CryptoMe belegen.

Zwar haben Benutzer dieser Dienste im Rahmen der Registrierung einer solchen Weitergabe ihrer Daten zugestimmt. Vermutlich werden diese Nutzungsbedingungen aber ebenso genau und häufig gelesen wie kleingedruckte AGB – unterliegen nur nicht denselben Verbraucherschutzbestimmungen. Die Gestaltung der Dienste genügt zudem meist nicht den Anforderungen des Telemediengesetzes (TMG) vom 26.02.2007, das in § 13 wichtige datenschutzrechtliche Anforderungen stellt, darunter die Widerrufbarkeit von Einwilligungen, die Erstellung ausschließlich pseudonymer Nutzungsprofile und die Möglichkeit zur anonymen Nutzung.

Durchsetzbar sind diese Anforderungen bei amerikanischen Anbietern nicht. Zu denken gibt allerdings, dass inzwischen deutsche Anbieter den Amerikanern nacheifern. Angesichts der bekannt gewordenen Datenschutz-Skandale lässt diese Entwicklung für die Zukunft Böses befürchten.

Secorvo News

Secorvo College aktuell

Noch immer wartet das Ausführungsgesetz zum Datenschutzaudit auf seine Verabschiedung. Des ungeachtet sind Datenschutzaudits bereits gängige Praxis in vielen Unternehmen. Das Seminar „Datenschutzaudit: Best Practice" am **20.–21.05.2010** stellt vor, welche Vorgehensweisen sich in der Praxis bewährt haben.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Security News Symposium

Am **20.–21.04.2010** ist es so weit – wir laden Sie herzlich ein zum ersten „Security News Symposium". Zahlreiche aktuelle Themen, die uns immer wieder in den Security News beschäftigen, werden im Zentrum intensiver Diskussionen stehen: Von neuen Bedrohungen durch und Empfehlungen zum Umgang mit USB-Sticks über Erfahrungen mit Krisenmanagement-Übungen, die Herausforderung iPhone, die Zukunft von Mifare und digitalen Signaturen bis zu verwurzelten Passwort-Mythen. Wir freuen uns auf Ihre Teilnahme.

Tag der IT-Sicherheit

Den 15.07.2010 sollten Sie sich vormerken: Dann findet der zweite Karlsruher „Tag der IT-Sicherheit", eine Kooperationsveranstaltung der KA-IT-Si mit der IHK Karlsruhe und dem Cyberforum e.V., im Saal Baden der IHK Karlsruhe statt. Es erwarten Sie Praxisberichte u. a. zu den Themen Wirtschaftsspionage, PDA-Sicherheit und Awareness.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2010	
08.-11.03.	Audit Challenge 2010 (Frankfurt School of Finance & Management, Frankfurt/Main)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)
April 2010	
13.-16.04.	PKI (Secorvo College)
20.-21.04.	Security News Symposium 2010 (Secorvo, Ettlingen)
20.-22.04.	Datenschutztage 2010 (FFD Forum für Datenschutz, Frankfurt)
27.-28.04.	a-i3/BSI-Symposium 2010 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
27.-29.04.	Forensik – Verfahren, Tools, Praxis (Secorvo College)
Mai 2010	
04.-05.05.	11. Datenschutzkongress 2010 (EUROFORUM, Berlin)
17.-19.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
20.-21.05.	Datenschutzaudit – Best Practice (Secorvo College)
25.-28.05.	3rd Int. Workshop on Post Quantum Cryptography PQCrypto 2010 (Cased, Darmstadt)

Fundsache

Der bewährte Mustervertrag des Bitkom zur Auftragsdatenverarbeitung liegt seit dem 04.12.2009 in einer neuen, an die Änderungen des BDSG angepassten Fassung 3.0 (inkl. Erläuterungen in Englisch) vor.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2010



Innovationsklima

Erfolgreiche Innovationen sind das Lebenselixier eines an Rohstoffen armes Landes. Kein Wunder, dass mit Initiativen wie „Land der Ideen“ oder „Partner für Innovation“ der Erfindergeist beschworen und mit Innovationsindikatoren die Innovationsfähigkeit gemessen wird. Viel wichtiger als die Höhe der Investitionen in Bildung, Forschung und Entwicklung oder die Zahl der Patentanmeldungen ist in der Praxis aber eine andere Frage: Woran lässt sich erkennen, dass aus einer Innovation ein erfolgreiches Produkt wird? Diese Frage stellen sich täglich unzählige Manager, Unternehmer, Analysten und Investoren. Meist liegen sie mit ihren Einschätzungen daneben: Obwohl nur ein Bruchteil aller Ideen Produktreife erlangt, liegt deren „Floprate“ bei 70-90%.

Viel Geld ließe sich sparen, gelänge es, die Trefferquote zu erhöhen. Die Geschichte zeigt jedoch, dass das nicht so einfach ist. „Das Telefon hat zu viele ernsthaft zu bedenkende Mängel für ein Kommunikationsmittel. Das Gerät ist von Natur aus von keinem Wert für uns“, hieß es 1876 in einer internen Meldung von Western Union. „Ich denke, es gibt weltweit einen Markt für vielleicht fünf Computer“, prognostizierte 1943 Thomas Watson, Vorsitzender von IBM. Und Ken Olson, Präsident von DEC, stellte 1977 fest: „Es gibt keinen Grund, warum irgend jemand einen Computer in seinem Haus wollen würde.“ Selbst Bill Gates lag daneben, als er 1981 konstatierte: „640 Kilobyte sind genug für jeden.“

Einfacher ist es, mit der Prognose bis zum kommerziellen Durchbruch der Innovation zu warten. So muss wohl auch Spam, Bot-Netzen, Zero Day Exploits und neuerdings Banking Trojanern wie insbesondere ZeuS der Status einer erfolgreichen Innovation zugebilligt werden. Offenbar herrscht im Bereich der Internetkriminalität ein äußerst fruchtbares Innovationsklima – ganz ohne F&E-Förderung und Innovationsindikatoren. Das sollte zu denken geben. Hoffen wir, dass es Auszeichnungen wie dem Deutschen IT-Sicherheitspreis gelingt, den Tüftlergeist der „White Hats“ zu beleben.



Inhalt

Innovationsklima

Security News

Fog Computing

ISMS-Hilfe

Ladegerät mit Trojaner

Digitale Wahlen

Ach wie gut, dass niemand ...

SSL am Ende?

Samurai gegen Web-Apps

Secorvo News

Security News Symposium 2010

Teamverstärkung

Die guten ins Töpfchen

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Fog Computing

Cloud Computing ist derzeit in aller Munde. Google, Amazon und Co. vermieten überschüssige Kapazität kostengünstig oder gar umsonst als virtualisierte Dienste. Mit der Frage, was dabei aus Sicherheitssicht zu beachten ist, beschäftigen sich u. a. der Report „Cloud Computing Security Risk Assessment“ der ENISA (Fundsache in SSN 11/09), die am 01.03.2010 erschienenen „Top Threats to Cloud Computing“ der gerade einmal ein Jahr alten Cloud Security Alliance und der seit 14.03.2010 elektronisch verfügbare Forschungsartikel „A 'cloud-free' security model for cloud computing“ von Manal Yunis.

Beim genaueren Hinschauen bestehen die Handlungsempfehlungen überwiegend darin, dass der Wolkenmieter seine Hausaufgaben machen sollte: Risikobewertung, Security Management und insbesondere umfangreiche Überwachung und Revision dessen, was da in der Cloud vor sich geht. Und wie immer beim Outsourcing sollte man sich vergegenwärtigen, dass die Verantwortung zur Kontrolle - ernst genommen - den eingesparten Betriebsaufwand zumindest relativiert.

Allerdings wird der Kunde beim standardisierten Angebot eines großen Cloud Computing Providers im Gegensatz zum herkömmlichen Outsourcing deutlich schlechtere Karten haben, ein individuelles Service Level Agreement mit weitreichenden Einblicks- und Kontrollmöglichkeiten auszuhandeln – Cloud Computing wird damit zum Fog Computing.

Werden in der Wolke personenbezogene Daten verarbeitet, entstehen damit auch Risiken für Dritte – schön zusammengefasst in dem Bericht „Privacy in the Cloud“ von Robert Gellmann vom 23.02.2009.

In Deutschland ist eine solche Verarbeitung schnell rechtswidrig, denn die erst im vergangenen Jahr präzisierten Anforderungen des § 11 BDSG zur Auftragsdatenverarbeitung stellen strikte Bedingungen an die Zulässigkeit einer Verarbeitung durch Dritte. Vor Vertragsabschluss ist daher besondere Sorgfalt geboten, denn die Verantwortung für den Schutz der durch Dritte verarbeiteten personenbezogenen Daten verbleibt nach BDSG beim Auftraggeber.

ISMS-Hilfe

Mit dem am 01.02.2010 veröffentlichten und nun auch erhältlichen Standard ISO/IEC 27003: 2010 „Informations technology - Security techniques – Information security management system implementation guidance" hat das JTC 1/SC 27 eine konkrete Implementierungshilfe für ein Informationssicherheitsmanagement nach ISO/IEC 27001: 2005 entwickelt.

Auf 68 Seiten werden in dem Standard Empfehlungen zur Anwendung des ISO/IEC 27001:2005 und zum Aufbau eines ISMS gegeben sowie einige unklare Anforderungen präzisiert. Wer einen einfach zu befolgenden Fahrplan zum ISMS-Aufbau erwartet hat, wird von dem Dokument enttäuscht. Einem erfahrenen Sicherheitsverantwortlichen wird das Dokument in der Praxis allerdings für das eine oder andere Detail eine echte Arbeitshilfe sein.

Ladegerät mit Trojaner

Nachrichten über Trojaner sind leider inzwischen nichts Besonderes mehr. Die Meldung des US CERT vom 02.03.2010, dass ein USB-Batterieladegerät mit einem Trojaner ausgeliefert wurde, zeigt jedoch, dass immer kreativere Wege zur Verbreitung schädlicher Software gewählt werden.

Daher sollte grundsätzlich auch Software aus vermeintlich vertrauenswürdiger Quelle mit gesunder Skepsis begegnet und diese vor einer Installation überprüft werden.

Digitale Wahlen

Im März 2010 führte die International Association for Cryptologic Research (IACR) einen Probelauf für digitale Wahlen durch. Lange Zeit gab es Vorbehalte gegen diese Form der Wahl, nicht zuletzt, weil dies als Werbung für ein bestimmtes Produkt missverstanden werden könnte. Aus Gründen der Benutzerbequemlichkeit entschloss man sich jedoch, digitale Wahlen auszuprobieren – in einer nicht bindenden Probeabstimmung fand das Verfahren große Zustimmung.

Da mittlerweile immer öfter digitale Wahlen zu allen denkbaren Anlässen durchgeführt werden, scheint die Zeit möglicherweise reif dafür zu sein. Die von der IACR genutzte Technologie Helios beruht auf einem Konzept, das von Ben Adida als Dissertation am MIT unter der Betreuung von Ron Rivest entwickelt wurde. Es handelt sich um ein Wahlsystem, bei dem die Stimme anonym abgegeben wird (die Wähler selbst sind nicht anonym und müssen aber zuvor registriert sein), und bei dem jeder Wähler im Nachhinein (wie bei Bingo Voting, SSN 3/2009) verifizieren kann, ob seine Stimme gezählt wurde. Die HeliosSoftware ist quelloffen. Wem Download und Installation zu kompliziert sind, kann seine Wahl auch im Web organisieren: Heliosvoting bietet dazu eine virtuelle Wahlkabine mit virtuellen Stimmzetteln. Sobald alle Wahlberechtigten registriert sind, steht einer Abstimmung nichts mehr im Wege.

Ach wie gut, dass niemand ...

Dass Kontrollfragen wie die nach dem Mädchennamen der Mutter nicht nur im spanischen Sprachraum eine einfache Hintertür für gut gesicherte Zugänge sind, sollte sich herumgesprochen haben, als im US-Wahlkampf persönliche E-Mails von Sarah Palin publiziert wurden. Das Problem: Durch persönliche Kontakte oder sogar Internet-Recherchen sind die richtigen Antworten auf derartige Fragen oft leicht herauszufinden.

Forscher aus Cambridge und Edinburgh haben nun den Blickwinkel gewechselt: Ein Angreifer könnte im Stil der Rasterfahndung bei allen Anwendern z. B. auf die Frage nach dem Vornamen des Lieblingslehrers einfach eine Handvoll der geläufigsten Namen ausprobieren. Ihrer am 04.03.2010 veröffentlichten Studie zufolge ist die zu erwartende Trefferquote erschreckend hoch. Neben Tabellen, denen man u. a. den beliebtesten weiblichen Vornamen in den USA der 60er Jahre (Lisa) entnehmen kann, enthält das Papier einen Vorschlag für ein passendes Komplexitätsmaß und eine Literaturliste, die gute Argumente für den sicheren Einsatz resp. Verzicht bestimmter Kontrollfragen liefert.

SSL am Ende?

Die Sicherheit einer SSL/TLS-Verbindung steht und fällt mit der Vertrauenswürdigkeit des Server-Zertifikats. Soweit die Theorie. In der Praxis ist die jedoch gar nicht so einfach zu überprüfen: Viele der mehr als 250 von verbreiteten Browsern anerkannten Zertifizierungsstellen wurden inzwischen übernommen oder haben umfirmiert: Aus Baltimore wurde Cybertrust wurde Verizon, aus SecureTrust und XRamp wurde TrustWave – die alten Zertifikate haben jedoch noch bis zu 30 Jahre Gültigkeit. Wie vertrauenswürdig ist da das zugehörige CA-Zertifikat? Ist auf die Identitätsverifikation der Zertifizierungsstelle noch Verlass? Warnt der Browser, wenn eine oft besuchte Webseite ein neues Zertifikat von einer anderen Zertifizierungsstelle erhält?

Am 24.03.2010 stellten Christopher Soghoian und Sid Stamm in ihrem Papier „Certified Lies“ eine neue Angriffsklasse vor: Stellt eine CA z. B. einer Strafverfolgungsbehörde oder einem Nachrichtendienst ein „Intermediate CA“-Zertifikat aus, lassen sich gefälschte Zertifikate erzeugen und damit „man-in-the-middle“-Abhörangriffe durchführen. Die Firma Packet Forensics bietet dafür sogar eine fertige Appliance namens „5 Series“ mit einem Durchsatz von mehreren Gb/s an.

Als Gegenmaßnahme entwickeln sie ein Firefox-PlugIn namens CertLock, das in Kürze verfügbar sein soll. Es folgt einem „Trust-On-First-Use“-Prinzip und warnt, wenn der Zertifikatsaussteller wechselt oder die Länderkennungen von CA, besuchter Webseite oder Besucher sich unterscheiden.

Das ursächliche Problem – die Schwierigkeit, die Vertrauenswürdigkeit von SSL-Zertifikaten zu beurteilen – ist damit nicht gelöst. Folgt man Matt Blaze, so brauchen wir ein gänzlich neues Konzept.

Samurai gegen Web-Apps

Der Umfang der Tool-Sammlung „Samurai“ zur Analyse der Sicherheit von Web-Anwendungen hat sich mit Veröffentlichung der Version 0.8 vom 15.03.2010 auf ca. 1,7 GB mehr als verdoppelt. Die Installation der herunterladbaren ISO-Datei basiert immer noch auf der Ubuntu-Version 9.04, bietet aber einen zur Vorgängerversion deutlich erweiterten Werkzeugumfang. Sehr hilfreich ist die Möglichkeit, diese einfach aus den Code-Repositories der Entwickler zu aktualisieren.

Secorvo News

Security News Symposium 2010

Wie übt man einen Krisenfall? Sollte man iPhones verbieten? Welche verborgenen Risiken schlummern in USB-Sticks? Was kommt nach dem Mifare-Hack? Hängen wir an Passwort-Mythen? Diesen und weiteren aktuellen Fragen werden wir am **20.-21.04.2010** auf dem ersten „Security News Symposium“ in Karlsruhe/Ettlingen auf den Grund gehen. Wir freuen uns auf Ihre Teilnahme.

Teamverstärkung

Ab dem 01.04.2010 wird Michael Knopp das Secorvo-Team mit juristischer Kompetenz verstärken. Als Mitarbeiter der „Projektgruppe Verfassungsverträgliche Technikgestaltung“ (provet) und des „Instituts für Europäisches Medienrecht“ (EMR) hat er sich unter anderem mit rechtlichen Fragen der Langzeitarchivierung elektronischer Dokumente, mit Bürgerportalen und eGovernment-Lösungen auseinander gesetzt und sich als „Mittler zwischen den Welten“ von Recht und Technik bewegt.

Die guten ins Töpfchen

IT-Grundschutz-Zertifikate sind nach wie vor rar: Wenige Unternehmen schafften bisher eine Zertifizierung ihres Sicherheitsmanagements und der Umsetzung der in den Grundschutzkatalogen definierten Maßnahmen. Auf dem KA-IT-Si-Event am **29.04.2010** wird der DE-CIX, dem größten europäischen Internet-Knoten, im Panoramasaal der IHK Karlsruhe das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz verliehen. Begleitet wird die Prämierung von einem Erfahrungsbericht - und einem Sektempfang zum Büfett-Networken (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2010	
19.-20.04.	Datenschutz kompakt (Gesellschaft für Datenschutz und Datensicherung e.V., Köln)
20.-21.04.	Security News Symposium 2010 (Secorvo, Ettlingen)
20.-22.04.	Datenschutztage 2010 (FFD Forum für Datenschutz, Frankfurt)
23.04.	Verbandstagung des Berufsverbandes der Datenschutzbeauftragten (BvD e.V., Berlin)
27.-28.04.	a-i3/BSI-Symposium 2010 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
29.04.	Die guten ins Töpfchen... (KA-IT-Si, IHK Karlsruhe)
Mai 2010	
04.-05.05.	11. Datenschutzkongress 2010 (EUROFORUM, Berlin)
17.-19.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
20.-21.05.	Datenschutzaudit – Best Practice (Secorvo College)
25.-28.05.	3rd Int. Workshop on Post Quantum Cryptography PQCrypto 2010 (Cased, Darmstadt)
Juni 2010	
07.-11.06.	TISP-Schulung (Secorvo College)

Fundsache

Am 17.03.2010 wurde die Studie „Know-How-Schutz in Baden-Württemberg 2009/2010" des Sicherheitsforums BW und des Steinbeis-Instituts Stuttgart vorgestellt, für die 239 Unternehmen befragt wurden. Sie gibt ein detailliertes Bild der Einschätzung der Bedrohung durch Wirtschaftsspionage und der ergriffenen Schutzmaßnahmen.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Kobloch, Kai Jendrian

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

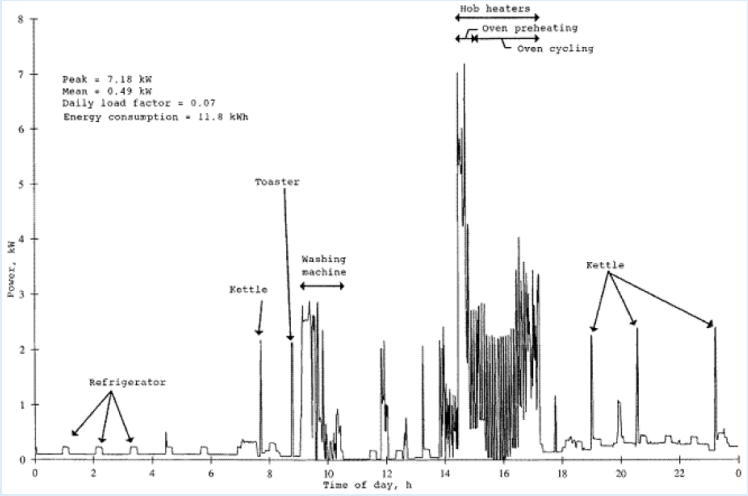
Secorvo Security News

April 2010



Der Feind in meiner Steckdose

Seit Januar müssen in Neubauten und bei Renovierungen „intelligente Stromzähler" verbaut werden, die Verbrauchswerte elektronisch übermitteln und eine Abrechnung nach wechselnden Tarifen erlauben. Damit sollen den Energieversorgungsunternehmen eine verbrauchsabhängige Energiebereitstellung ermöglicht und durch lastabhängige Tarife das Verbraucherverhalten gesteuert werden. Dass die vermeintlich unkritische Erfassung des Stromverbrauchs in 15'-Intervallen einen erheblichen Eingriff in den vom Bundesverfassungsgericht im Urteil zum „Großen Lauschangriff" vom 03.03.2004 definierten „Kernbereich privater Lebensgestaltung" darstellt, wird erst auf den zweiten Blick deutlich. Abgesehen von einem Gutachten des ULD vom 11.09.2009 und Kapitel 4 eines NIST-Drafts vom 02.02.2010 blieb selbst die fachöffentliche Diskussion weitgehend aus. Das ist, wie die Abbildung zeigt, wohl dringend nachzuholen.



Quelle: Elias Leake Quinn, Smart Metering & Privacy: Existing Law and Competing Policies, Frühjahr 2009, S. 3.



Inhalt

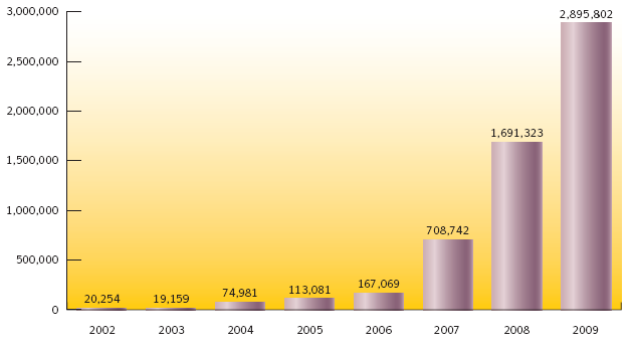
Der Feind in meiner Steckdose
Security News
Symantec Report
Internet zertifiziert
Leitfaden IS-Revision
Diffie + Murphy = Lenin
OWASP Top 10 – 2010,5
Secorvo News
Secorvo College aktuell
Lesestoff
Nachlese
Vorschau
Veranstaltungshinweise
Fundsache

Security News

Symantec Report

Am 14.04.2010 erschien der immer wieder lesenswerte halbjährliche Internet Security Thread Report von Symantec. Einige der Ergebnisse, die Symantec über 240.000 eigene „Sensoren“ gewinnt, sind auch für Experten überraschend: So stürmten Angriffe mit bösartigen PDF-Dateien die Top-Ten; sie waren für 49% aller Web-basierten Attacken verantwortlich. Daher sollte dem Patchen des Acrobat-Readers eine mindestens ebenso hohe Priorität eingeräumt werden wie den Betriebssystem-Updates.

Während das „Window of Exposure“ trotz zahlreicher kritischer Bugs 2009 bei den meisten Browsern auf unter einen Tag schrumpfte, stieg die Zahl der neue Viren, Würmer und Trojaner 2009 auf durchschnittlich fast 8.000 – je Kalendertag.



Neue Viren, Würmer, Trojaner (Symantec)

Auch der Handel mit ergaunerten „Credentials“ floriert, wenn auch die Preise sinken: Kreditkartendaten gibt es schon ab 0,85 US$, E-Mail-Adressen ab 1,70 US$ je MB und Kontendaten bereits ab 15 US$. Offenbar überwiegt hier das Angebot die Nachfrage (bzw. die Zahl der „nützlichen Idioten“, die ihr Bankkonto für die Geldwäsche hergeben).

Internet zertifiziert

Am 29.04.2010 erfolgte im Rahmen eines Events der Karlsruher IT-Sicherheitsinitiative die offizielle Übergabe des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz an den deutschen Internet-Knoten DE-CIX – mit einem Durchsatz von mehr als 600 GBit/s der größte Knoten Europas und der zweitgrößte weltweit. Gute drei Jahre dauerte das von der Karlsruher Connect GmbH begleitete Projekt von der Idee bis zum von Secorvo durchgeführten erfolgreichen Audit. Die Erfahrungsberichte finden sich auf der Webseite der KA-IT-Si.

Der Aufwand hat sich nach Überzeugung von Arnold Nipper (CTO des DE-CIX) gelohnt: Das Projekt habe konsequente Sicherheitsprozesse und ein durchgängiges, hohes Sicherheitsniveau erzwungen – wichtige Voraussetzung für die Vertrauenswürdigkeit eines Internet-Knotens. Bei der Übergabe scherzte Bernd Kowalski, Abteilungsleiter Zertifizierung beim BSI, daher auch: „Jetzt ist das deutsche Internet Grundschutz-zertifiziert.“

Leitfaden IS-Revision

Am 19.03.2010 wurde vom BSI Version 2.0 des Leitfadens IS-Revision auf Basis von IT-Grundschutz veröffentlicht. Die Vorgehensweise wird umfänglich beschrieben und enthält wenig Überraschendes. Interessant sind die Aufwandschätzungen für eine „Querschnitts-Revision“, die mit 30-60 Personentagen bei normaler und bis zu 60-100 Personentagen bei sehr hoher Komplexität angesetzt werden. Für eine „IS-Kurzrevision“ werden 8-10 Tage geschätzt, eine Methode, um einen ersten definierten Eindruck zum Stand der Informationssicherheit zu erhalten.

Ein als Hilfsmittel zur Verfügung gestelltes Dokument Prüfthemen für die IS-Kurzrevision soll diese Kurzrevision unterstützen. Der Titel „verbindliche Prüfthemen“ klingt vielversprechend; bei genauerer Betrachtung werden aber nur Themen aufgelistet. Wie diese konkret zu prüfen sind, ist nicht geregelt. Lediglich stichpunktartig werden Beispiele angeführt, die einen großen Interpretationsspielraum lassen.

Es bleibt zu hoffen, dass im Rahmen der Überarbeitung der IT-Grundschutzkataloge bei den jeweiligen Maßnahmen auch verbindliche Prüffragen definiert werden, die dann als Grundlage für die Erstellung von Informationssicherheitskonzepten bzw. einer ISO 27001-Zertifizierung auf Basis von IT-Grundschutz sowie für die IT-Revision verwendet werden können.

Diffie + Murphy = Lenin

Gut 33 Jahre ist die Epoche machende Veröffentlichung von Whit Diffie und Marty Hellman zur Public Key Kryptographie inzwischen alt. Und selbst die bekannte und oft genutzte PKI-Bibliothek OpenSSL liegt nach mehr als einem Jahrzehnt Anlauf seit dem 29.03.2010 offiziell in Version 1.0 vor.

Eigentlich ist also alles ganz einfach mit einer PKI, sollte man meinen: CAs als vertrauenswürdige Zertifizierungsinstanzen stellen nach eingehender Prüfung der Antragsteller Zertifikate aus und PKI-Anwendungen nutzen diese Zertifikate, um mit den zugehörigen Schlüsseln alle relevanten Daten zu signieren oder für den beabsichtigten Empfänger zu verschlüsseln. In der Praxis scheint aber immer noch eher Murphys Gesetz zu regieren, wie die folgenden aktuellen Ereignisse zeigen.

Am 02.04.2010 wurde bei einer Kontrolle unter den bei der Mozilla Foundation geführten vertrauenswürdigen Stammzertifikaten ein herrenloses Root-CA-Zertifikat entdeckt. Erst vier Tage später konnte geklärt werden, dass der Schlüssel dieser CA zwar nicht kompromittiert ist, aber weder verwendet noch auditiert wird; daraufhin wurde das Zertifikat – für künftig neu installierte Firefox-Browser – aus der vorgegebenen Stammzertifikatsliste entfernt.

Am 01.04.2010 wurde gemeldet (leider kein Aprilscherz), dass es ausreicht, als Kunde eines Free-Mail- oder Web-Mail-Providers die E-Mail-Adresse „ssladministrator@...“ zu belegen, um hochoffizielle SSL-Zertifikate für Server unter der Domäne des jeweiligen Providers zu beziehen.

Am 13.04.2010 erschien ein Microsoft-Patch für Authenticode, der dafür sorgt, dass jetzt tatsächlich der gesamte in einem Cabinet oder Portable Executable Container enthaltene Code in die Prüfung der Code-Signatur einbezogen wird. Bis dato konnte ein Angreifer diesen Containern Code anfügen, ohne dass deshalb die Signatur des ursprünglichen Herausgebers als ungültig gewertet wurde.

Und ebenfalls am 13.04.2010 wurde ein Bug bestätigt, der dazu führt, dass Thunderbird ausgehende E-Mails u. U. nicht mit dem Zertifikat des adressierten Empfängers, sondern mit einem ganz anderen verschlüsselt.

Auch nach 33 Jahren sollte man es bei der PKI-Nutzung also immer noch mit der (fälschlich) Wladimir Iljitsch Uljanow (vulgo: Lenin) zugeschriebenen Maxime halten: Vertrauen ist gut. Kontrolle ist besser.

OWASP Top 10 – 2010,5

In den SSN 11/2009 haben wir bereits auf die Entwurfsversion der überarbeiteten OWASP Top 10 hingewiesen. Seitdem verstrichen fast sechs Monate intensiven Feinschliffs, bevor am 19.04.2010 die endgültige Version veröffentlicht wurde.

Das 22-seitige Dokument, an dem noch die Reihenfolge einiger Risiken im Tabellenkeller verändert wurde, zeigt anschaulich allen Verantwortlichen und an der Entwicklung von Web-Anwendungen Beteiligten die gravierendsten Risiken auf. Zusätzlich wird das notwendige Handwerkszeug zur Risikoreduzierung vorgestellt. Das halbe Jahr bis zur Veröffentlichung hat geholfen, den Entwurf zu einem rundum gelungenen Arbeitswerkzeug reifen zu lassen.

Secorvo News

Secorvo College aktuell

Die Nachfrage nach dem T.I.S.P.-Zertifikat ist ungebrochen: Schon weit über 300 deutsche Security Professionals dürfen sich mit diesem Titel schmücken, und 2010 werden voraussichtlich weitere 100 Absolventen das Zertifikat erwerben. Freie Plätze gibt es noch auf dem T.I.S.P.-Seminar am **07.–11.06.2010** (mit anschließender Prüfung). Die nächste Gelegenheit zur T.I.S.P.-Zertifizierung bietet Secorvo College nach der Sommerpause vom 20.-25.09.2010.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Lesestoff

In der März-Ausgabe der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“ (Schwerpunktthema „Softwaresicherheit“) hat sich Kai Jendrian ausführlich zur Überprüfung von Webanwendungen mit dem „OWASP Application Security Verification Standard 2009“ geäußert (S. 138-142).

Nachlese

Unser erstes „Security News Symposium“ am 20.-21.04.2010, auf dem wir zahlreiche aktuelle Themen der IT-Sicherheit und des Datenschutzes vertieften, wurde von den Teilnehmern überschwänglich gelobt – nicht nur für das hervorragende Essen. Wer es verpasst hat, kann eine CD mit den Vortragsunterlagen zum Preis von 50 Euro per E-Mail an security-news-symposium@secorvo.de bestellen. Das Essen lässt sich allerdings erst auf dem nächsten Symposium nachholen.

Vorschau

Am **07.–08.06.2010** findet die diesjährige 12. Fachkonferenz „DuD 2010“ in Berlin statt – mit einem spannenden und aktuellen Programm (von Cloud Computing über Elena, Auftragsdatenverarbeitung und den neuen Personalausweis bis zum Intelligenten Stromzähler) und Rekordbeteiligung: Schon jetzt gibt es mehr als 100 Anmeldungen. Wer noch dabei sein möchte, sollte sich zügig anmelden.

Ebenfalls vormerken sollten Sie den **15.07.2010** – den zweiten Karlsruher „Tag der IT-Sicherheit“, der in Kooperation von KA-IT-Si, IHK Karlsruhe und dem Cyberforum e.V. veranstaltet wird. Es erwarten Sie Praxisberichte u. a. zu den Themen Wirtschaftsspionage, iPhone-Sicherheit und Security Awareness.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2010	
04.-05.05.	11. Datenschutzkongress 2010 (EUROFORUM, Berlin)
20.-21.05.	Datenschutzaudit – Best Practice (Secorvo College)
20.-21.05.	International Secure Systems Development Conference (Enabled Security Limited, London/UK)
25.-28.05.	3rd Int. Workshop on Post Quantum Cryptography PQCrypto 2010 (Cased, Darmstadt)
30.05.-03.06.	Eurocrypt 2010 (IACR, Nizza/F)
Juni 2010	
07.-08.06.	DuD 2010 (Computas, Berlin)
07.-11.06.	TISP-Schulung (Secorvo College)
22.-25.06.	Certified Professional for Secure Software Engineering (CPSSE) (Secorvo College)
Juli 2010	
15.07.	2. Karlsruher „Tag der IT-Sicherheit“ (KA-IT-Si/IHK/Cyberforum, IHK Karlsruhe)
24.-29.07.	Black Hat (Las Vegas/US)

Fundsache

Eine ausführliche Auseinandersetzung mit Sicherheits- und Datenschutzaspekten von Smart Metern (= „Intelligenten Stromzählern“) im Smart Grid hat das NIST am 02.02.2010 als zweiten Draft zur Kommentierung veröffentlicht: *Smart Grid Cyber Security Strategy and Requirements* (NIST IR 7628, 305 Seiten).



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Mai 2010



Die Vernunft stirbt nie

Wiederholt gerieten in den vergangenen Monaten „Social Networks“ wie Xing, StudiVZ und Facebook aufgrund von Datenschutzvorfällen in die Schlagzeilen. Aber keineswegs allen lagen Gesetzesverstöße zu Grunde.

Die meisten Fälle gründeten auf einem sehr grundsätzlichen Missverständnis. Denn anders als die Betreiber Glauben machen möchten, sind „Social Networks“ keineswegs ein digitales Abbild sozialer Netze. Sie entsprechen nicht den fein gewobenen sozialen Beziehungen, die Menschen knüpfen, und in denen sie in unterschiedlichen Rollen auftreten: als Partner, Geschwister, Gönner, Kumpel, Mitbewerber, Kollegen, Bekannte, Freunde. Selbst ähnliche Rollenbeziehungen unterschieden sich im Detail erheblich: Denn Freund ist nicht gleich Freund, und Kollege nicht gleich Kollege.

In echten sozialen Beziehungen werden Informationen und Gerüchte, Tipps und Erlebnisse sehr selektiv und kontextabhängig getauscht – keine zwei Personen aus dem sozialen Beziehungsgeflecht eines Menschen verfügen über dieselben persönlichen Kenntnisse. Auch Sprache, Stil und Ton der Kommunikation unterscheiden sich.

„Social Networks“ sind hingegen große Verflacher: Jeder „Freund“ („Kontakt“) kann auf dieselben Daten und Informationen zugreifen – jederzeit und fast überall. Jede Person erscheint allen „Freunden“ gegenüber in derselben undifferenzierten Rolle. Und wer „twittert“, spricht im selben Ton und Wortlaut zu allen „Followern“. Im „echten Leben“ käme kein Mensch auf die Idee, jedem, den er kennenlernt, gleich seinen Geburtstag in den Kalender einzutragen, seine bisherige berufliche Laufbahn und alle Qualifikationen lückenlos zu offenbaren, unbegrenzten Zugriff auf sein Fotoalbum einzuräumen und gleich noch die Liste aller Freunde und Bekannten vorzulegen.

Der Irrsinn wird wohl immer mehr Menschen bewusst: Angeblich planen 60 % der deutschen Facebook-Nutzer eine Kontolöschung. Offenbar ist ein Hype doch nicht das Ende aller Vernunft.



Inhalt

Die Vernunft stirbt nie

Security News

DECT-Verschlüsselung gebrochen

Das BDSG ist nicht genug

iPhone der ID-Karten?

Fish and Cheese

Zeitläufte

MoPS 2010

Ein Quentchen Trost

Secorvo News

Alles auf eine Karte

Lizenz zum Prüfen

Best of Consulting

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

DECT-Verschlüsselung gebrochen

Die Liste der gebrochenen proprietären Krypto-Verfahren ist erneut um eines angewachsen: Auf dem diesjährigen Fast Software Encryption Workshop (FSE 2010) vom 07.-10.02.2010 in Korea war das DECT-Verschlüsselungsverfahren an der Reihe.

Karsten Nohl, Erik Tews und Ralf-Philipp Weinmann gelang eine vollständige Rekonstruktion und die Feststellung ernsthafter Schwachstellen der DECT Standard Cipher (DSC). Dabei handelt es sich um eine 64-Bit Stromchiffre, die strukturell der GSM-Chiffre A5/1 ähnelt. Das Design beruht auf irregulär getakteten, linear rückgekoppelten Schieberegistern, einer Konstruktion, die typisch für Umgebungen ist, bei denen es auf eine möglichst einfache Implementierung und hohe Performanz ankommt.

Der Angriff ermöglicht es, den geheimen Schlüssel mit Hilfe leistungsstarker Hardware innerhalb weniger Stunden zu finden. Seit dem 04.04.2010 sind die Ergebnisse der Kryptoanalyse verfügbar.

Der Vorgang zeigt wieder einmal, dass von der Verwendung Hersteller eigener Kryptoverfahren dringend abzuraten ist – insbesondere, wenn das Verfahren (wie DSC) in zig-Millionen Endgeräten implementiert wird. Selbst wenn bald ein sicherer Nachfolger für DSC zur Verfügung stehen sollte, so wird DSC wegen seiner enormen Verbreitung noch auf Jahre in Gebrauch bleiben. Auch wenn es vom Standpunkt der Alcatel aus verständlich erscheint, mit einem geheim gehaltenen Verfahren Patentgebühren einnehmen zu wollen, so rechtfertigt dies nicht den Einsatz minderwertiger Algorithmen auf Kosten der Sicherheit der Verbraucher.

Das BDSG ist nicht genug

Während die Unternehmen noch an der Umsetzung der jüngsten Novellierung des BDSG arbeiten, leitete der Hamburger Senat, veranlasst durch Google Streetview, am 07.05.2010 dem Bundesrat einen Gesetzesentwurf zur Ergänzung des BDSG (BR-Drs. 259/10) zu. Schon am 01.04.2010 hatte das Bundesinnenministerium (BMI) Eckpunkte zum Arbeitnehmerdatenschutz vorgestellt, die ebenfalls auf eine Gesetzesänderung zielen.

Beiden Vorschlägen ist eine überbordende Einzelfallorientierung gemein. Der Hamburger Entwurf sieht zahlreiche Ergänzungen des ohnehin wuchernden § 28 vor, darunter eine eingeschränkte Erlaubnis für georeferenzierte Straßenansichten und ein Widerspruchsrecht, sowie eine Benachrichtigungspflicht in einem neuen § 33a. Die Eckpunkte des BMI greifen insgesamt elf Beispiele auf, wie Videoüberwachung, Datenerhebung im Bewerbungsverfahren und private Kommunikationsmittelnutzung. Sie sollen in einem neuen Kapitel „Arbeitnehmerdatenschutz" zusammengefasst werden.

Aber beide Entwürfe springen zu kurz: Weder lösen sie grundsätzliche Fragen des Datenschutzrechts, noch bieten sie angesichts des zu erwartenden ständigen Anpassungsbedarfs Rechtssicherheit.

iPhone der ID-Karten?

Zum 01.11.2010 wird der elektronische Personalausweis eingeführt. Das Bundesinnenministerium hat den Informationsbedarf angesichts des optionalen Charakters vieler Neuerungen erkannt und präsentiert nun eine eigene Website. Dort wird der ePersonalausweis als multifunktionaler Problemlöser angepriesen – quasi als iPhone der ID-Karten.

Die Informationen insbesondere über den elektronischen Identitätsnachweis sind sehr einfach gehalten. Es stehen eine Reihe von zum Teil fehlerhaften Formularen bereit. Vergeblich sucht man überzeugende Argumente für die Nutzung der neuen Funktionen, Hinweise zu dem für den elektronischen Identitätsnachweis erforderlichen Lesegerät oder die zu erwartenden Kosten. Auch über die benötigte Software schweigt sich das Portal aus.

Auf dem versteckt verlinkten Informationsangebot des BSI zu elektronischen Ausweisen finden sich die technischen und organisatorischen Einzelheiten – in Gestalt von fast 20 Technischen Richtlinien. Die schiere Menge und das Ausblenden kritischer Aspekte dürfte selbst dem professionell interessierten Publikum den Zugang erschweren. Dass der ePersonalausweis so zum Kultobjekt wird, darf bezweifelt werden.

Fish and Cheese

Am 04.05.2010 erweiterte Google seine Sammlung von Tools zur Sicherheit von Web-Anwendungen um Jarlsberg – eine Microblogging-Anwendung, löchrig wie dänischer Käse. Sie soll wie z. B. auch OWASP WebGoat (siehe SSN 2/2010) zum Experimentieren mit Web-Schwachstellen einladen. Erst kurz zuvor hatte Google am 19.03.2010 als Pendant den Application-Scanner skipfish veröffentlicht. Nun vergnügen sich Fisch und Käse in unserem Labor miteinander ...

Zeitläufte

Seit dem 08.04.2010 ist die stark überarbeitete Version 2 des SANS Investigative Forensics Toolkit (SIFT) als VMware mit über 350 Werkzeugen verfügbar. Wesentliche Neuerung ist der Logparser log2timeline, der mit Hilfe von timescanner alle Zeitinforma-

tionen aus über 23 Logformaten in 13 Artefaktklassen (u. a. EXIF, PCAP, Flash Cookies) automatisiert extrahiert. Nutzt man weitere in SIFT enthaltene Werkzeuge wie TSK (aktualisierte V 3.12 vom 23.05.2010) und RegRipper (modifizierte Windows-Version vom 10.05.2010), lässt sich die Menge korrelierbarer Zeitquellen vervollständigen. Durch eine abschließende chronologische Sortierung werden Aktivitäten eines untersuchten Systems oder interaktiven Benutzers im Zeitverlauf nachvollziehbar.

Da der überwiegende Teil der auswertbaren Informationen aus Verlaufsdaten besteht, die während der Systemnutzung automatisch anfallen, lässt sich so auf jedem länger genutzten (und unmanipuliertem) Linux- bzw. Windows-System das Nutzungsverhalten im Zeitverlauf rekonstruieren. Nicht nur Google und Facebook machen gläsern – auch das eigene System vergisst nie.

MoPS 2010

Gut drei Jahre nach dem Month of PhP Bugs (MoPB 2007, siehe SSN 3/2007) wurde der Mai 2010 zum Month of PHP Security (MoPS 2010) umgewidmet. Bisher veröffentlichte das vierköpfige Initiatoren-Komitee neun Artikel und vierzig neue Bugs – ein weiterer Beleg, dass eine konzertierte Aktion zur Verbesserung der Sicherheit von Software auch kurzfristig enorme Fortschritte bewirken kann.

Ein Quentchen Trost

„Das kann doch jedem mal passieren…“ – so wirkte die Bewertung des gefühlten Komplettausfalls des deutschen Internets am 12.05.2010 durch den Verursacher, die DENIC eG. Eine sehr knappe Stellungnahme trug zu zahlreichen Spekulationen über mögliche Ausfallursachen bei. Ein wenig gemildert wurde die Verunsicherung durch eine etwas ausführlichere Stellungnahme zu Hintergründen, zwei Tage nach dem Vorfall.

Vorbildlich dagegen der Blog-Eintrag, mit dem die ASF auf einen erfolgreichen Angriff auf das Apache Projekt vom 05.04.2010 reagiert hatte: Darin wurde der Angriff analysiert und sowohl technische als auch organisatorische Maßnahmen als Konsequenzen präsentiert. Auf diesem Niveau hätte man sich die Kommunikation des DENIC gewünscht – das hätte die verunsicherungsbedingten Folgeschäden des Ausfalls begrenzt. Auch Krisenkommunikation will gelernt sein.

Secorvo News

Alles auf eine Karte

Der Traum jedes Sicherheitsbeauftragten ist ein durchgängiges Identitätsmanagement, das Betriebsausweis, Gebäude- und Rechnerzugang integriert. Die KIT-Card, die mit der Gründung des „Karlsruher Instituts für Technologie“ (KIT) entstand, führt an diesen traumhaften Zustand heran – sie organisiert die Wege von über 8.000 Mitarbeitern der im Rahmen der Exzellenzinitiative ausgezeichneten Spitzenforschungseinrichtung.

Wie die technisch-organisatorische Umsetzung erfolgte, welche Klippen dabei zu umschiffen waren und was er aus dem Projekt gelernt hat, stellt Projektleiter Michael Gehle auf dem KA-IT-Si-Event am **24.06.2010** im Schlosshotel vor (Anmeldung).

Lizenz zum Prüfen

Seit dem 01.05.2010 verstärkt Jochen Schlichting als BSI-lizensierter ISO 27001-Auditor auf der Basis von IT-Grundschutz das Secorvo-Grundschutz-Team.

Best of Consulting

Ein leichter Anfall von Hybris, gewürzt mit einer Prise Chuzpe, ließ uns im vergangenen Jahr als kleiner David bei dem von der WirtschaftsWoche ausgelobten Beratungsranking „Best of Consulting 2010“ in der Kategorie „IT-Strategie“ antreten.

Nach drei Qualifikationsrunden, in denen die Qualität der Beratungsleistung aus der Sicht von zehn verschiedenen Kunden und ein ausgewähltes Referenzprojekt von einem wissenschaftlichen Fachbeirat analysiert und bewertet wurden, erreichte Secorvo im Februar 2010 das Finale.



Am 27.05.2010 wurde die Jury-Entscheidung über die Platzierung der Finalisten in Berlin bekannt gegeben – und Secorvo als Zweitplatzierter in der Kategorie IT-Strategie ausgezeichnet. Ein dritter Preis wurde wegen des großen qualitativen Abstands zu den weiteren Kandidaten nicht vergeben.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2010	
30.05.-03.06.	Eurocrypt 2010 (IACR, Nizza/F)
Juni 2010	
07.-08.06.	DuD 2010 (Computas, Berlin)
07.-11.06.	TISP-Schulung (Secorvo College)
Juli 2010	
15.07.	2. Karlsruher „Tag der IT-Sicherheit“ (KA-IT-Si/IHK/Cyberforum, IHK Karlsruhe)
24.-29.07.	Black Hat (Las Vegas/US)
29.07.-01.08.	DEFCON 18 (Las Vegas/US)
August 2010	
02.-04.08.	DFRWS 2010: Digital Forensic Research Workshop (Portland/US)
09.-13.08.	19th USENIX Security Symposium (Washington/US)
15.-09.08.	Crypto 2010 (IACR, Santa Barbara/US)
September 2010	
28.-29.09.	7. Security Awareness Symposium (Secorvo, Ettlingen)

Fundsache

Zahlreiche Datenschutz-Verstöße haben in den vergangenen Jahren die Sensibilität für den Schutzbedarf personenbezogener Daten geschärft. Seit September 2009 sammelt das „Projekt Datenschutz“ Berichte über Datenschutzpannen – gute Munition gegen hartnäckige Verweigerer.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2010



Unqualifiziert qualifiziert

Damit eine elektronische Signatur als „qualifizierte“ gilt, muss sie bekanntlich etliche Voraussetzungen erfüllen. Eine davon ist, dass sie mit technischen Komponenten erstellt wurde, deren Sicherheit durch eine von der Bundesnetzagentur (BNetzA) anerkannte Stelle überprüft und bestätigt wurde.

Seit dem 19.12.2008 besitzt der Chipkartenleser „Kobil KAAN TriB@nk“ eine solche Bestätigung. Am 17.04.2010 veröffentlichte ein Unbekannter unter dem Pseudonym ‚Colibri’ eine Dokumentation, die zeigt, wie eine manipulierte Firmware in diesen Leser geladen werden kann. Damit ließen sich zumindest theoretisch nicht nur die PINs von Karteninhabern abfangen, sondern auch heimlich weitere Signaturen erzeugen.

Der Fehler: Der Leser validierte beim Update zwar die Signatur des Herstellers über die übertragenen Datenblöcke, prüfte jedoch nicht, ob die Blöcke auch in der richtigen Reihenfolge an der beabsichtigten Stelle im Speicher landen. Dass diese (inzwischen gepatchte) Lücke bei der Prüfung des Geräts übersehen wurde, zeigt, wie auch Prof. Dr. Rainer W. Gerling von der Max-Planck-Gesellschaft kommentierte, dass selbst eine standardisierte Zertifizierungsprüfung letztlich auf individuellem Geschick und Erfahrung des Prüfers basiert.

Am 07.06.2010 erklärte die BNetzA die Sicherheitsbestätigung des Geräts für ungültig – mit Wirkung zum Veröffentlichungstag des Angriffs. Damit schuf sie unvermeidlich zwei neue Klassen von elektronischen Signaturen (vgl. SSN 04/2009): Alle zwischen dem 17.04. und 07.06.2010 mit dem TriB@nk-Leser erstellten Signaturen wurden rückwirkend zu „dann doch nicht ganz so qualifizierten Signaturen“, alle zwischen dem 19.12.2008 und dem 17.04.2010 erstellten zu „qualifizierten, die möglicherweise gefälscht sein könnten“.

Bleibt ein profanes Problem: Woran erkennt man, sofern man möchte, bei der Prüfung einer Signatur, mit welchem Chipkartenleser sie erstellt wurde?



Inhalt

Unqualifiziert qualifiziert

Security News

WLAN-Haftung

„Grundschutzscanner“

Sammelwütig

Mythen sterben langsam

Schauen, was läuft

Löchrige Pen-Tests

Secorvo News

iPhone Security

„Tag der IT-Sicherheit"

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

WLAN-Haftung

Anspruch auf Unterlassung, aber kein Schadensersatz – das ist das Ergebnis der mit Spannung erwarteten BGH-Entscheidung vom 12.05.2010 zur Haftung von Anschlussinhabern für von Dritten verübte Schädigungen über unbefugt genutzte WLANs.

Nach der seit dem 07.06.2010 vorliegenden Begründung treffen den Anschlussinhaber Prüfpflichten hinsichtlich der von ihm ergriffenen Sicherheitsmaßnahmen. So sind mindestens die zum Zeitpunkt des Routerkaufs marktüblichen Sicherungen zu ergreifen; ein kontinuierliches Aktualisieren der Maßnahmen sei allerdings nicht zumutbar.

In dem aus dem Jahr 2006 datierenden Fall erwartete der BGH eine aktivierte WPA-Verschlüsselung. Jedoch habe der Beklagte seine Sorgfaltspflicht verletzt, indem er für den Routerzugang kein eigenes, ausreichend langes Passwort vergeben, sondern es bei dem voreingestellten Passwort belassen habe – eine merkwürdige Einschätzung, sofern das Herstellerpasswort individuell und zufällig gewählt war.

Zur Klärung der bestehenden Rechtsunsicherheit wird diese Entscheidung wenig beitragen. Zu lückenhaft waren die weitgehend auf Annahmen und Unterstellungen beruhenden Sachverhaltsfeststellungen der Instanzgerichte; zu viele Fragen waren nicht Gegenstand der Revision. Offen bleibt bspw. die Anwendbarkeit der Deckelung der Abmahnkosten aus § 97a UrhG. Auch hätten dem Urteil Ausführungen zur Handhabung der Beweislastverteilung gut getan. Sowohl unschuldig Abgemahnte als auch Opfer einer Urheberrechtsverletzung werden es weiterhin schwer haben, ihre jeweiligen Rechtsansprüche durchzusetzen.

„Grundschutzscanner“

Seit dem Linuxtag (09.-12.06.2010) ist Version 3.0 der BOSS-Scanner-Live CD des BSI verfügbar. Sie basiert nun auf einer komfortabel startbaren Version des Scannerframeworks OpenVAS 3.0. Damit bleibt das BSI seiner Open-Source-Philosophie treu. Mit der Förderung der Entwicklung von Plugins (ca. 17.000) wurden auch die Anwender in Unternehmen und Behörden nicht vergessen: Aktuelle Plugins sind über den kommerziellen Greenbone Security Feed (GSF) beziehbar.

BOSS 3.0 liefert mit dem GSF bei einigen Plugins genauere und weiter gehendere Ergebnisse als Nessus und OpenVAS. Der GSF wurde sogar mit Scan-Konfigurationen für die 10. und 11. Ergänzungslieferung der IT-Grundschutz-Kataloge ausgestattet. Aber Achtung: Ein „fehlerfreier“ Scan bedeutet nicht, dass ein IT-Verbund IT-Grundschutz-konform ist – naturgemäß werden z. B. organisatorische Maßnahmen nicht geprüft. Schließlich wird die als Open Source verfügbare Security Management Suite OSSIM den GSF unterstützen.

Erfreulich ist, dass mit BOSS 3.0 bewährte und neue Werkzeuge nun wieder „amtlich“ für Auditoren verfügbar sind, darunter amap, nmap, ldapsearch, snmpwalk, strobe, portbunny und w3af – ein wichtiges Signal zur Klärung der immer noch verbreiteten Unsicherheiten im Umgang mit dem „Hackerparagrafen“ § 202c StGB.

Sammelwütig

Nach Mahnungen diverser Gerichte und des Bundesdatenschutzbeauftragten (22. Tb., S. 58) hat das Bundesinnenministerium mit Zustimmung des Bundesrats am 04.06.2010 im Schatten der WM die konstituierende Verordnung zur „Verbunddatei Gewalttäter Sport“ und zahlreichen weiteren zentralen Dateien des Bundeskriminalamts erlassen.

Die Verordnung legt die Art der zu speichernden Daten für ca. 80 präventive Verbunddateien fest, die zwischen 100 und 6 Millionen Datensätze über verdächtige Bürger enthalten.

Für die „Hooligan-Datenbank“ mit 11.245 gespeicherten Personen (Stand 2009) dürfen neben Adress- und Identifizierungsdaten etwa Schulabschluss, frühere Staatsangehörigkeit, Volkszugehörigkeit, Angaben zu Personalausweis oder Reisepass, Angaben zu Kommunikationsmitteln, Konten- und Vermögensinformationen, Beziehungen zu Orten, Gruppen, Ereignissen oder Einzelpersonen sowie Referenzen auf weitere gespeicherte Vorgänge gesammelt und gespeichert werden. Zur Aufnahme in die Datei genügen eingeleitete Ermittlungen; beschränkt auf umfassende Kontaktdaten sogar die bloße Begleitung von Verdächtigen. Gelöscht werden müssen die Daten dagegen nur, wenn bei einer Einstellung des Verfahrens ausdrücklich das Fehlgehen des Verdachts festgestellt wurde.

Mit rekordverdächtiger Reaktionszeit hat das Bundesverwaltungsgericht am folgenden Tag einen anhängigen Löschantrag mit Verweis auf die Verordnung zurückgewiesen.

Ein Lerneffekt aus der gerade erst drei Monate alten Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung ist nicht feststellbar – das betrifft bereits die Rechtsgrundlagen im BKA-Gesetz: Es fehlen konkrete Vorgaben zur Datensicherheit, die Transparenz der Erhebung und Speicherung ist ebenso wie die diesbezüglichen Kriterien zur Zulässigkeit ungenügend – ein weiterer Fall für das Bundesverfassungsgericht?

Mythen sterben langsam

Am 28.06.2010 publizierte der Branchenverband BITKOM die Ergebnisse einer Forsa-Studie – mit vermeintlich erschütternden Ergebnissen: 41 % der Befragten ändern ihre Passworte nie. „Die wichtigsten Passwörter sollten alle drei Monate geändert werden“, fordert Prof. Dieter Kempf vom Präsidium des BITKOM.

Dabei sind erzwungene Passwortwechsel in der Praxis meist nutzlos: Sie verleiten Benutzer dazu, sich „Bildungsregeln“ zu überlegen – und damit den Sinn von Passwortwechseln zu konterkarieren. Denn Wechsel sollen im Falle einer Kompromittierung den Schaden begrenzen – erkennt der Angreifer aber die Bildungsregel, kann er aus jedem geknackten Passwort das nächste ableiten.

Sinnvoller als die Verbreitung von Passwort-Mythen (siehe SSN 6/2009) wäre die Forderung nach längeren Passwörtern. Das Projekt RainbowCrack publizierte am 17.06.2010 Version 1.41 des Software-Crackers, der mit einer schnellen Grafikkarte als Co-Prozessor und einer 576 GB großen Rainbow-Tabelle acht Zeichen lange Passwörter in 30 Minuten findet. Kürzer als 10 Zeichen dürfen Passwörter (zumindest unter Windows) heute nicht mehr sein, wenn sie einem solchen Cracker wenigstens 90 Tage standhalten sollen – zum Schutz vor einer parallelisierten Berechnung sind 12 Zeichen das Minimum.

Nur ein Zeichen mehr, und der Aufwand, ein gutes Passwort zu Cracken, steigt um den Faktor 84 – das sollte für ein halbes Berufsleben reichen.

Schauen, was läuft

Am 15.06.2010 wurde Version 10 von Autoruns veröffentlicht. Ursprünglich von Sysinternals entwickelt und später von Microsoft übernommen zeigt es unter anderem an, welche Programme und Dienste unter Windows gestartet werden. Damit lassen sich nicht nur unnötig gestartete Programme, Dienste und Prozesse erkennen und deaktivieren, sondern auch eingenistete Schadsoftware und Spyware identifizieren.

Ähnliches leistet das Programm Starter; es bietet sogar die Möglichkeit, Dienste direkt zu konfigurieren oder eine Recherche zu den „Fundsachen“ in verschiedenen Internet-Suchmaschinen zu starten.

Allerdings sollten derartige Tools generell vor der produktiven Nutzung in einer Testumgebung überprüft werden – nicht selten wird beliebte Freeware in mit Schadcode infizierten Varianten verbreitet.

Löchrige Pen-Tests

Unter dem Titel “Why Johnny Can't Pentest” veröffentlichten drei Forscher von der University of California am 27.04.2010 einen ausführlichen Vergleich aktueller Schwachstellenscanner für Web-Anwendungen. Dafür analysierten sie die Ergebnisse der Pen-Tests eigens entwickelter Web-Anwendungen mit bekannten Schwachstellen.

Die 21seitige Studie liefert nicht nur ein “Ranking” der getesteten Produkte – besonders interessant sind die Dokumentation der Vorgehensweise und die Erkenntnis, dass sich mit heutiger Technik einige Schwachstellen, wie beispielsweise Fehler in der Anwendungslogik, gar nicht und andere nur sehr schwer automatisiert erkennen lassen.

Das Fazit ist wenig überraschend: Der Einsatz von automatisierten Scannern sollte grundsätzlich durch händische Prüfungen ergänzt werden. Ausführlich werden die Ergebnisse der Studie auf der DIMVA 2010 in Bonn am 08.-09.07.2010 vorgestellt.

Secorvo News

iPhone Security

In nicht wenigen Unternehmen hält derzeit Apples iPhone Einzug. Trotz seiner nach wie vor deutlichen Nachteile bei Business-Anwendungen gegenüber RIMs BlackBerry wiegen „Sex-Appeal“ und Nimbus des Geräts auch bei Führungskräften oft schwerer.

Wie sicher aber sind Unternehmensdaten auf einem iPhone aufgehoben? Was ist von der Hardware-Verschlüsselung und anderen Schutzmechanismen zu halten? Lassen sich iPhones ohne Inkaufnahme zusätzlicher Risiken in die IT-Infrastruktur integrieren? Diesen und weiteren Fragen ist Jörg Völker auf den Grund gegangen – und hat die Ergebnisse seiner Untersuchungen nun in der Fachzeitschrift „Datenschutz und Datensicherheit“ (DuD) veröffentlicht.

„Tag der IT-Sicherheit"

Zum zweiten Mal findet am **15.07.2010** der Karlsruher „Tag der IT-Sicherheit“ statt – eine Kooperationsveranstaltung der IHK Karlsruhe, des Cyber-Forum e. V. und der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si). Die Vorträge behandeln aktuelle Themen der IT-Sicherheit und Best-Practice-Beispiele, darunter ein Lagebericht des Landesamts für Verfassungsschutz Baden-Württemberg zur Wirtschaftsspionage in deutschen Unternehmen, eine kritische Analyse der Sicherheit von iPhones und die erfolgreiche Awareness-Kampagne der EnBW AG.

Die Veranstaltung beginnt um 14 Uhr und richtet sich an Geschäftsführer und IT-Leiter unabhängig von Branche und Unternehmensgröße. Hier finden Sie das vollständige Programm und die Möglichkeit zur Anmeldung.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2010	
08.-09.07.	DIMVA 2010 (Bonn)
15.07.	2. Karlsruher „Tag der IT-Sicherheit“ (KA-IT-Si/IHK/Cyberforum, IHK Karlsruhe)
24.-29.07.	Black Hat (Las Vegas/US)
29.07.-01.08.	DEFCON 18 (DEFCON, Las Vegas/US)
August 2010	
02.-04.08.	DFRWS 2010: Digital Forensic Research Workshop (DFRWS, Portland/US)
09.-13.08.	19th USENIX Security Symposium (Washington/US)
15.-09.08.	Crypto 2010 (IACR, Santa Barbara/US)
September 2010	
20.-23.09.	SEC 2010 (IFIP, Brisbande/AUS)
20.-24.09.	TISP-Schulung (Secorvo College)
28.-30.09.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
28.-29.09.	7. Security Awareness Symposium (Secorvo, Ettlingen)

Fundsache

Die Skulptur „Kryptos“ des Künstlers James Sandborn vor dem Hauptsitz der CIA von 1991 enthält vier Kryptogramme, von denen drei 1998 von einem Mitarbeiter der CIA dechiffriert wurden. Das vierte, 97 Zeichen lange Kryptogramm ist bis heute ungelöst.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2010



Makellose Bürger

Für den Staatsphilosophen Thomas Hobbes (1588-1679), aufgewachsen im von Bürgerkriegen geprägten England des 17. Jahrhunderts, legitimiert sich das Gewaltmonopol des Staates aus einem (fiktiven) Gesellschaftsvertrag, mit dem die Bürger alle Macht uneingeschränkt dem Souverän übertragen. Sie gewinnen damit Sicherheit vor äußeren Feinden und ihrer eigenen „wölfischen" Natur – zum Preis eines weitgehenden Verzichts auf freie Entfaltung.

Nun sind wir in den westlichen Industrieländern heute zum Glück weit von bürgerkriegsähnlichen Verhältnissen entfernt – aller organisierten Kriminalität und terroristischen Bedrohungen zum Trotz. Dennoch erfreut sich der Kerngedanke der Hobbes'schen Lehre auch in repräsentativen Demokratien zahlreicher Anhänger. Bürgerliche Freiheiten, wie sie sich in allen Verfassungen der Aufklärung als Abwehrrecht des souveränen Bürgers gegenüber einem übermächtigen Staat finden, werden in wachsendem Umfang Sicherheitsbedürfnissen geopfert – selbst dann, wenn es sich um nachweislich wirkungslose Symbolik handelt: „Nacktscanner" und Internet-Sperren lassen grüßen.

Nun sind innere und äußere Sicherheit zweifellos von hohem Wert – ohne sie können sich weder Freiheit noch Wohlstand entfalten. Man beachte jedoch die Kausalität: Sicherheit dient dem Schutz der freien Entfaltung. Tastet sie deren Substanz an, gefährdet sie das zu schützende Gut – und verfehlt ihren Zweck. Selbstmord ist eben keine angemessene Reaktion auf die Angst vor dem Tod.

Wie weit dieser Werterahmen bereits aus dem Blick geraten ist, zeigt die schamlos zynische Namenswahl der NSA für ein Überwachungsprojekt kritischer Infrastrukturen im Volumen von 100 Mio. US$, das das Wall Street Journal am 08.07.2010 öffentlich machte: „Perfect Citizen". Von der „Anomalie-Erkennung" ist es dann nicht mehr weit bis zu deren präventiver Beseitigung. Noch einfacher ginge es allerdings gleich ganz ohne Bürger.



Inhalt

Makellose Bürger

Security News

Whitelisting am Ende?

Microsoft is evil, ...

Viel Rauch um Skype

Rückzug von der Signatur?

CC-BS-Schutzprofil

State of the Crypto-Art

Sichere Virtualisierung

Deadlines

Secorvo News

Secorvo College

Security Awareness Symposium

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Whitelisting am Ende?

Der Stoßseufzer „Wem kann man eigentlich noch trauen?“ ist leider eben so abgedroschen wie berechtigt. Anfang Februar 2010 wurde auf der Konferenz Black Hat DC demonstriert, dass sich Malware für iPhones sogar über Apples offiziellen App Store verteilen lässt – wie zuvor schon bei Stores anderer Hersteller. Am 17.06.2010 wies Marissa Vicario (Symantec) in ihrem Blog darauf hin, dass über 90% aller Malware-infizierten Webseiten von seriösen Anbietern stammen. Sie wurde am 28.06.2010 vom tschechischen Antiviren-Hersteller Avast bestätigt: Auf eine „Schmuddelkram“-Webseite kämen mittlerweile 99 seriöse Seiten, über die man sich beim Browsen infizieren kann. Dann wurde im offiziellen Download-Bereich für Firefox-Addons am 13.07.2010 die Schadsoftware „Mozilla-Sniffer“ entdeckt. Und schließlich musste Dell am 20.07.2010 Austausch-Motherboards zurückrufen, die ab Werk mit Malware bestückt waren.

Die Häufung derartiger Meldungen legt nahe, dass man sich immer weniger auf vermeintlich zuverlässige Quellen verlassen kann, von denen man Daten, Anwendungen oder Systeme bezieht. Der Whitelisting-Ansatz „Erlaube seriöse Quellen und behandle alle anderen restriktiv“ dürfte mittelfristig ins Leere laufen. Solange noch Zeit ist, sollten sich Unternehmen, die sich darauf stützen, Gedanken über einen Plan B machen.

Microsoft is evil, ...

... so die allgemeine Wahrnehmung, wenn es um die Sicherheit von PCs geht. Eine der wichtigsten Erkenntnisse im „Secunia Half Year Report 2010“ vom 13.07.2010 zeigt, dass diese Wahrnehmung nicht mehr der Realität entspricht: Von den 50 meist installierten Programmen auf PCs sind 24 Programme nicht von Microsoft – und weisen im Untersuchungszeitraum 3,5-mal so viele entdeckte Schwachstellen auf. Berücksichtigt man, dass die Zahl der „Bug-Searcher“ bei Microsoft deutlich höher sein dürfte, könnte das Verhältnis der tatsächlichen Schwachstellen noch größer sein. Diese Entwicklung sollte Anlass sein, auch für Programme von „Drittherstellern“ ein funktionierendes Patch-Management zu etablieren.

Viel Rauch um Skype

Seit dem 07.07.2010 geistern Meldungen durch die Presse, nach denen Sean O'Neil die Skype-Verschlüsselung „geknackt“ habe (siehe z. B. Spiegel Online oder Chip Online). Tatsächlich wurde ein von Skype verwendetes Verschlüsselungsverfahren *aufgedeckt*, auf dessen Geheimhaltung Skype sehr viel Mühe verwendet hat. So enthält der Code der Skype-Clients verschiedene Reverse-Engineering-Gegenmaßnahmen. Durch die Publikation des Codes sind diese *Gegenmaßnahmen* als gebrochen anzusehen.

Eine erste Begutachtung des Quellcodes hat ergeben, dass Skype als Stromchiffre eine Variante von RC4 nutzt – mit dem Ziel einer beabsichtigten Inkompatibilität. Da der Code nun offenliegt, wird sich bald zeigen, ob das modifizierte Verfahren ebenso sicher ist wie RC4, oder ob demnächst Millionen Nutzer unter den Folgen schlechter Kryptographie zu leiden haben werden.

Rückzug von der Signatur?

Der Rat der Europäischen Gemeinschaft hat am 13.07.2010 Vereinfachungen der Richtlinie über das gemeinsame Mehrwertsteuersystem (2006/112/EG) erlassen. Diese betreffen auch die vereinheitlichten Anforderungen an die elektronische Rechnungsstellung. Entscheidend ist die Änderung des Art. 233 Abs. 1, der bislang die Verwendung einer qualifizierten elektronischen Signatur oder die Nutzung des EDI-Verfahrens vorgab. Nun stellt sie dem einzelnen Steuerpflichtigen frei, mit welchen Mitteln er Authentizität, Integrität und Lesbarkeit der Rechnung vom Ausstellungszeitpunkt bis zum Ende der Aufbewahrungsfrist sicherstellt. Auch der Einsatz organisatorischer Kontrollmittel soll zulässig sein, solange eine verlässliche Buchungskontrolle zwischen dem Waren- oder Dienstleistungsbezug und der Rechnung gewährleistet wird. § 14 Abs. 3 UStG, der das Signaturerfordernis im deutschen Recht festschreibt, wird nun bis zum 31.12.2012 angepasst und gelockert werden müssen.

Unternehmen werden diese Entwicklung vermutlich mit Erleichterung zur Kenntnis nehmen. Die Bundesregierung hat die Signaturpflicht des § 14 Abs. 3 UStG ohnehin auf die Streichliste zum Bürokratieabbau gesetzt (dort lfd. Nr. 14) und plant eine Befassung mit der Thematik noch in diesem Jahr. Allerdings geht die Erleichterung auf Kosten der Rechtssicherheit, denn während sie die Mittel freigibt, bleibt die Verpflichtung zur Sicherung von Authentizität und Integrität erhalten. Ob allein organisatorische Maßnahmen hierfür ausreichen, wird für den Gesetzgeber, die Steuerpflichtigen und die Rechtsprechung schwer bestimmbar sein. So wird der Zwang zur ungeliebten Signatur durch ein erhöhtes Eigenrisiko der Unternehmen ersetzt.

CC-BS-Schutzprofil

Schutzprofile ermöglichen für eine definierte Produktkategorie von IT-Systemen eine standardisierte Beschreibung der Bedrohungen, Sicherheitsziele,

Annahmen über die Betriebsumgebung und daraus resultierenden Sicherheitsanforderungen. Sie legen die Mindeststandards für eine Zertifizierung nach den international vereinheitlichten „Common Criteria for Information Technology Security Evaluation“ fest.

Am 24.06.2010 veröffentlichte das BSI ein neues Schutzprofil für moderne verteilte Betriebssysteme. Das „Operating System Protection Profile (OSPP)“ wurde von einem Konsortium bestehend aus BSI, Vertretern des amerikanischen Zertifizierungsschemas (NIAP) und namhaften Betriebssystemherstellern entwickelt. Die aktuelle Version 2.0 der OSPP definiert die Anforderungen an ein sicheres Betriebssystem und fordert die Evaluierungsstufe EAL 4, die nicht nur formale Anforderungen an die Entwicklung stellt, sondern auch die Analyse von Design und Quellcode verlangt.

Dabei bezieht sich ein Schutzprofil wie auch eine CC-Zertifizierung immer auf eine definierte Einsatzumgebung. OSPP setzt voraus, dass die Plattform (Hardware, Geräte, Firmware), auf der das Betriebssystem ausgeführt wird, gegen physische Angriffe und Manipulationen geschützt ist und alle Managementaktivitäten von vertrauenswürdigen und geschulten Anwendern durchgeführt werden. Immerhin: Eine Abkoppelung des PCs vom Netz ist keine Voraussetzung für den sicheren Betrieb.

State of the Crypto-Art

Als Referenz dafür, welche Kryptoalgorithmen und Schlüssellänge dem Stand der Technik entsprechen, wird – zumindest hierzulande – gerne die vom BSI erarbeitete und von der BNetzA jährlich aktualisierte Übersicht über geeignete Algorithmen heran gezogen. Da sie sich auf das Signaturgesetz bezieht, berücksichtigt sie zwar nur Verfahren, die für Signaturen nötig sind. Allerdings lassen sich daraus die Anforderungen an ein entsprechendes Schutzniveau von Verschlüsselungsverfahren ableiten.

Am 16.07.2010 endete die Kommentarfrist für den Draft der NIST Special Publication 800-131, der Empfehlungen für Algorithmen und Schlüssellängen in allen wichtigen Anwendungsgebieten von Verschlüsselung über Signatur und Schlüsselableitung bis zu Message Authentication Codes geben wird. Er fordert für Verfahren der amerikanischen Bundesbehörden ab 2011 ein Sicherheitsniveau von mindestens 112 bit – das Doppelte dessen, was der (einfache) DES bot, und 32 bit mehr als die bis Ende 2010 verlangten 80 bit. An dieser Empfehlung werden auch nationale Standards künftig nicht vorbei kommen, die für sich reklamieren, kryptografisch „State of the Art“ zu sein.

Sichere Virtualisierung

Ein „Guide to Security for Full Virtualization Technologies“ wurde am 07.07.2010 vom NIST in einer Draft-Version veröffentlicht. Auf 35 Seiten werden anschaulich Begriffe und prinzipielle Sicherheitsmaßnahmen beim Einsatz von Server- und Desktop-Virtualisierung beschrieben. Der Guide eignet sich gut für einen systematischen Einstieg in die Thematik; konkrete technische Empfehlungen für bestimmte Virtualisierungslösungen bleibt er allerdings schuldig.

Deadlines

Zahlreiche Konferenzen zur IT-Sicherheit werfen ihre Schatten voraus – und werben noch um Beiträge. Schnell Entschlossene können bis zum **01.08.2010** einen Vorschlag für den 18. DFN Workshop „Sicherheit in vernetzten Systemen“ (15.-16.02.2011) einreichen.

Ebenfalls bis zum **01.08.2010** werden spannende Vorträge für die OWASP-Konferenz Appsec Germany 2010 (20.10.2010) gesucht. Und das Bundesamt für Sicherheit in der Informationstechnik (BSI) freut sich bis zum **10.10.2010** auf Einreichungen für den 12. Deutschen IT-Sicherheitskongress (10.-12.05.2011).

Secorvo News

Secorvo College

Gleich nach Ende der Sommerferien bietet Secorvo College die nächste Gelegenheit zur Zertifizierung als Information Security Professional mit dem TISP-Seminar am **20.–24.09.2010**. Nähere Informationen zu den Zulassungsvoraussetzungen, den Inhalten und der unabhängigen Zertifikatsprüfung finden Sie unter www.tisp.de (Online-Anmeldung).

Alle weiteren Seminarangebote im Oktober und November mit ausführlichem Programm unter http://www.secorvo.de/college

Security Awareness Symposium

Am **28.–29.09.2010** findet das von Secorvo, dem Berliner eLearning-Spezialisten digital spirit und der Karlsruher Agentur DauthKaun initiierte siebte „Security Awareness Symposium“ in Ettlingen statt. Auch diesmal erwartet Sie ein „Erfahrungsfeuerwerk“ von Projektleitern zahlreicher Awareness-Kampagnen, die ihre Ideen, Erfolge und „Lessons Learned“ präsentieren – ein Treffen, das Sie sich nicht entgehen lassen sollten, wenn die Sensibilisierung Ihrer Kollegen für IT-Sicherheit oder Datenschutz auch auf Ihrer Agenda steht (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2010	
29.07.-01.08.	DEFCON 18 (DEFCON, Las Vegas/US)
August 2010	
02.-04.08.	DFRWS 2010: Digital Forensic Research Workshop (DFRWS, Portland/US)
09.-13.08.	19th USENIX Security Symposium (Washington/US)
15.-19.08.	Crypto 2010 (IACR, Santa Barbara/US)
30.08.	Sommerakademie 2010 (ULD, Kiel)
September 2010	
07.-10.09.	OWASP AppSec US (Irvine/US)
20.-24.09.	TISP-Schulung (Secorvo College)
28.-29.09.	7. Security Awareness Symposium (Secorvo, Ettlingen)
28.-30.09.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
Oktober 2010	
21.10.	it-sa Datenschutztag 2010 (Computas, Nürnberg)

Fundsache

Grundlegende praktische Regeln für die Informations- und IT-Sicherheit in kleinen und mittelständischen Unternehmen wurden im Interagency Report „Small Business Information Security: The Fundamentals“ (NISTIR 76121) der Computer Security Division des NIST vom Oktober 2009 zusammengefasst – prägnant auf 20 Seiten die wichtigsten Sicherheitsaspekte für Mensch und Technik.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Petra Barzin, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2010



Editorial: Todesmut

Urlaube überraschen gelegentlich mit neuen Erfahrungen. So fand ich mich kürzlich unversehens auf einem Baum wieder: unter mir zwölf Meter gähnendes Nichts, vor mir zwei nicht einmal fingerdicke, zehn Meter lange Drahtschnürchen zum nächsten Stamm, und dort, auf einer weniger als 1 qm großen hölzernen Plattform, meine feixenden Söhne. Vor meinem inneren Auge spulten sich, von inbrünstiger Reue begleitet, zwar nicht mein bisheriges Leben, aber doch die Ereignisse des vergangenen Abends ab: In geradezu jugendlichem Leichtsinn hatte ich meinen Söhnen zugesagt, mit ihnen einen nahen Hochseilgarten zu besuchen. Nun ja, welcher Vater mag sich schon von seinen Halbwüchsigen als Hasenfuß verlachen lassen... Jetzt aber gab es kein zurück mehr, und mit zittrigen Fingern klinkte ich meine beiden Karabiner ins Seil.

Als ich nach langen 60 Minuten endlich wieder festen Boden unter den Füßen hatte und mein Hirn wieder an etwas anderes als „Todesmut“ denken konnte, machte ich eine überraschende Beobachtung: Kein einziger Besucher rutschte von einem der an Seilen baumelnden Balken, federnden Feuerwehrschläuche oder schaukelnden Saftkisten, über die man sich von Baum zu Baum hangeln musste. Und schon beim zweiten Parcours, auf den mich meine Söhne zwangen, wuchs meine Zuversicht, die andere Seite wohlbehalten zu erreichen, und gewann schließlich sogar die Oberhand.

Bei nüchterner Betrachtung war das kein Wunder, denn die soliden Sicherungen begrenzen das tatsächliche Risiko auf eine Falltiefe von 20 cm (und lachende Söhne).

Kaum zurück aus dem Urlaub konfrontierte mich das echte Leben mit einem völligen Kontrasterlebnis: ein CIO, der die Risiken unverschlüsselter mobiler Geräte mit einem „Bei uns ist noch nie etwas passiert“ beiseite wischte. Da beschlich mich die ketzerische Idee, ihn in den Hochseilgarten einzuladen. Ob er sich dort oben wohl auch ausklinken würde?



Inhalt

Editorial: Todesmut

Security News

Rechtswidrige Webseitenanalyse

iPhone Jailbreak via Safari

RainbowCrack 1.5

I Can Stalk You...

Cryptool 1.4.30

EU-Verfahrensverzeichnis

Secorvo News

Secorvo College aktuell

Xdr3$gFa*9z

Security Awareness 7.0

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Rechtswidrige Webseitenanalyse

Die Aufsichtsbehörde Baden-Württembergs für den Datenschutz im nicht-öffentlichen Bereich hat auf der Grundlage des Entschlusses des Düsseldorfer Kreises vom 26./27.11.2009 am 01.07.2010 eigene Hinweise zum Einsatz von Web-Analysediensten veröffentlicht. Insbesondere der Einsatz von Google Analytics wird als rechtswidrig eingestuft.

Die Datenschutzaufsichtbehörden betrachten IP-Adressen als grundsätzlich personenbezogene Daten. Daher erfordert ihre Erhebung und Verarbeitung zu Analysezwecken gemäß §§ 12, 15 TMG eine (praktisch nicht realisierbare) Einwilligung des Website-Nutzers. Weitere Gründe für die Einstufung liegen in der Datenübertragung in das außereuropäische Ausland, den Nutzungsbedingungen, in denen sich Google die Verarbeitung der Daten auch zu eigenen Zwecken vorbehält, die unzureichende Widerspruchsmöglichkeit und die ungewisse Löschsituation bei Vertragsende.

Fehl geht das Innenministerium allerdings, wenn es eine Auftragsdatenverarbeitung annimmt: Hierzu fehlen Kontrollmöglichkeiten und Weisungsrechte der Verwender sowie ein entsprechender Vertrag nach § 11 BDSG. Vor allem aber beschränkt sich Google nicht auf ein auftragsgebundenes Verarbeiten, sondern handelt eigenständig.

Damit riskieren die Nutzer von Google Analytics, die sich über Webseiten wie OnTraxx leicht identifizieren lassen, Bußgelder nach § 16 TMG. Zwar bietet Google in Reaktion auf den Düsseldorfer Kreis bereits Zusatzcode zur Verkürzung von IP-Adressen. Aber auch damit werden die Probleme des Widerspruchs gegen eine Profilbildung und der Auslandsübertragung nicht gelöst. Die Widerspruchslösung von Google – Sperrung von Cockies – ist unzureichend. In Baden-Württemberg sind nun verstärkte Kontrollen angekündigt; weitere Bundesländer dürften dem Beispiel folgen.

iPhone Jailbreak via Safari

Seit längerem ist bekannt, dass auch für das iPhone 4 und iOS 4.0.1 sowohl ein Jailbreak als auch ein Unlock möglich sein sollen (siehe SSN 11/2009). Dennoch war die Überraschung groß, als am 02.08.2010 das Dev Team den Jailbreak für das iPhone 4 veröffentlichte. So stand der Jailbreak nun nicht nur für alle iOS-Geräte von Apple (iPod, iPad, iPhone) und alle iOS-Versionen zur Verfügung, sondern nutzte eine Lücke im PDF-Reader des mobilen Safari-Browsers aus, der es PDF-Dateien erlaubt, unsignierten Code auf dem iPhone auszuführen.

Diese Lücke kann natürlich auch durch andere Angreifer ausgenutzt werden, um beliebige Anwendungen auf dem Gerät zu installieren. Einen wirksamen Schutz gegen diese Schwachstelle bietet derzeit nur das Update für iOS 4.0.2 vom 11.08.2010. Auf Geräten, die bereits einen Jailbreak durchgeführt haben, lässt sich ein Tool installieren, dass vor dem Öffnen von PDFs warnt. Ansonsten bleibt nur die Empfehlung, auf dem iPhone vorläufig lieber keine PDF-Dateien unbekannter oder zweifelhafter Herkunft zu öffnen.

RainbowCrack 1.5

Fast exakt ein Jahr nach Veröffentlichung der Version 1.4 (siehe SSN 08/2009) stellte das Projekt RainbowCrack am 26.08.2010 mit Version 1.5 eine für 64bit-Betriebssysteme optimierte Fassung ihres Passwort-Crackers zum Download bereit. Mit über 320 Milliarden (MD5-) Hashwerten pro Sekunde erreicht diese Version auf der Referenzhardware mehr als die vierfache Geschwindigkeit der Vorversion – selbst alpha-numerische 10-Zeichen-Passwörter lassen sich damit auf einem Standard-PC mit schneller Grafikkarte in wenigen Tagen finden.

I Can Stalk You...

Erst Mitte Februar hatte der Dienst „PleaseRobMe" für Aufregung gesorgt, der aktuelle Twitter-Nachrichten anzeigte, in denen die Autoren ihren Aufenthaltsort fern von zu Hause preisgaben (siehe SSN 02/2010). Offenbar genügte das nicht, um Millionen naiver Tweeter die Gefährlichkeit ihrer öffentlichen Mitteilungsfreude vor Augen zu führen. Daher startete Myhemic Labs mit „ICanStalkU" am 05.05.2010 eine Webseite, die den aktuellen Aufenthaltsort aus den Metadaten von auf Twitter veröffentlichten SmartPhone-Fotos gewinnt – die inzwischen häufig Geodaten enthalten.

Dabei ist Abhilfe simpel: Wie man iPhone, Android und Blackberry dazu überredet, keine Geodaten zu speichern, erläutern die Autoren bereitwillig. Wer eine solche Vorsicht pathologisch (oder zumindest übertrieben) findet, dem sei der Aufsatz von Blumberg und Eckersley über Locational Privacy vom August 2009 dringend zur Lektüre empfohlen.

Cryptool 1.4.30

Am 04.08.2010 wurde Version 1.4.30 der Lernsoftware Cryptool veröffentlicht. Wir haben dies zum Anlass genommen, die Software unter didaktischen Gesichtspunkten unter die Lupe zu nehmen. Nach der Installation stellt die Anwendung ein Hauptfenster zur Verfügung, innerhalb dessen allerlei Experimente angestellt werden können, d. h. der Anwender kann eine große Vielfalt von kryptografischen Verfahren auf beliebige Textdateien anwen-

den lassen, etwa zur Verschlüsselung oder zur Signaturerzeugung. Der Punkt, der Cryptool dabei so interessant macht, ist die Visualisierung der Verfahren. Die ist allerdings unterschiedlich gelungen ausgefallen; bei manchen Verfahren werden nur Zwischenergebnisse angezeigt, bei anderen wird der Anwender im Detail durch den Algorithmus geführt. Andere Experimentierfelder ergeben sich bei der Analyse klassischer Kryptoverfahren oder bei der Durchführung zahlentheoretischer Experimente.

Da es viele Mitwirkende an dem Projekt gibt, ist das Erscheinungsbild der Software insgesamt recht inhomogen. Das ist kein Schaden; etwas störend fielen aber unterschiedliche didaktische Herangehensweisen auf. So kommt die Zahlentheorie mit dem Charme einer Vorlesung daher, während etwa die Demonstration des AES-Verfahrens sehr lebendig und greifbar wirkt. Für zukünftige Versionen wäre es schön, wenn der didaktische Ansatz sowie die Visualisierung an verschiedenen Stellen poliert und vereinheitlicht würde. Auch wenn Cryptool aus einem Anwender keinen Kryptologen macht, hat es zweifellos einen hohen Lernwert – mit Spaßfaktor.

EU-Verfahrensverzeichnis

Die EU-Kommission hat am 26.07.2010 einen „Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht“ veröffentlicht. Das Papier soll den EU-Bürgern Transparenz darüber verschaffen, wer auf europäischer Ebene welche Daten zu welchem Zweck speichert und welche Stellen Zugriff erhalten. Erläutert werden 18 bestehende, in Umsetzung befindliche oder geplante Datensammlungen vom Schengener Informationssystem (SIS) über die Vorratsdatenspeicherungsrichtlinie bis zu dem geplanten Passenger Name Records (PNR) System für Europa.

Im Stil eines Verfahrensverzeichnisses werden zu jedem Instrument Hintergrund, Zweck, zentraler oder dezentraler Aufbau, die Art der gespeicherten personenbezogenen Daten, die Zugriffsberechtigungen, Regelungen zum Datenschutz, Speicherdauer, Umsetzungsstand und Überprüfungsverfahren angegeben. Zu einigen Datensammlungen, darunter zur Vorratsdatenspeicherungsrichtlinie, zur schwedischen Initiative zum Austausch von Ermittlungsdaten und zum Prüm-Beschluss (grenzüberschreitender DNA-Abgleich) werden Beispiele erfolgreicher Straftataufklärungen oder Statistiken angeführt. Zur Vorratsdatenspeicherung fehlt eine Erfolgsstatistik; es werden lediglich zwei Beispiele aufgeklärter Tötungsdelikte, eine Einbruchsserie und eine bandenmäßige Raubserie benannt.

Die Mitteilung ist gerade auch im Zusammenhang der Rechtsprechung des Bundesverfassungsgerichts zur TK-Vorratsdatenspeicherung zu begrüßen, die angesichts der sehr umfassenden Speicherung in diesem Bereich zur Zurückhaltung in weiteren Bereichen mahnt. Sie könnte Ausgangspunkt für die überfällige Diskussion sein, wie viel Kontrolle wir uns angesichts der tatsächlichen Aufklärungserfolge leisten wollen.

Secorvo News

Secorvo College aktuell

Sichern Sie sich einen Platz auf einem unserer Herbst-Seminare. Los geht es im September mit der Möglichkeit, Ihr Fachwissen durch das anerkannte T.I.S.P.-Zertifikat belegen zu lassen: Vom 20. bis 24.09.2010 findet die nächste T.I.S.P.-Schulung mit anschließender Zertifikatsprüfung statt. Für den „Doppelpack Grundlagen“ empfehlen wir eine baldige Anmeldung: Sicherheitsmanagement heute – Prozesse, Steuerung, Organisation vom 05. bis 07.10.2010 und der „Klassiker“ IT-Sicherheit heute vom 26. bis 28.10.2010 beleuchten neben den aktuellen Standards die wichtigsten Trends im IT-Sicherheitsbereich.

Xdr3$gFa*9z

Eine zentrale Verschlüsselungslösung für die größte Bank im Südwesten Deutschlands – diese Aufgabe haben die IT-Security-Experten Joachim Seeger und Volker Kölz von der Landesbank Baden-Württemberg (LBBW) gemeistert. Die Anforderungen umfassten nicht nur technische Herausforderungen: So sollte die Lösung für den Anwender so unauffällig wie möglich sein, weitestgehend automatisiert laufen und keinen Einfluss auf die Betriebsführung haben. Schließlich mussten die Daten bei einer Störung einfach wiederherstellbar sein. Wie die Experten der LBBW die Datei- und Ordnerverschlüsselung und die Verschlüsselung der Endgeräte heute organisieren, verraten sie am **23.09.2010** bei der nächsten Veranstaltung der KA-IT-Si im Schlosshotel Karlsruhe (Anmeldung).

Security Awareness 7.0

Auf dem siebten „Security Awareness Symposium“ am **28.–29.09.2010** in Ettlingen, das Secorvo zusammen mit dem Berliner eLearning-Spezialisten digital spirit und der Karlsruher Agentur DauthKaun initiierte, erwarten Sie wieder spannende Erfahrungsberichte von Projektleitern zahlreicher Awareness-Kampagnen, die ihre Ideen, Erfolge und „Lessons Learned“ präsentieren – ein Treffen, das Sie sich nicht entgehen lassen sollten, wenn die Sensibilisierung Ihrer Kollegen für IT-Sicherheit oder Datenschutz auf Ihrer Agenda steht (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2010	
07.-10.09.	OWASP AppSec US (Irvine/US)
20.-24.09.	TISP-Schulung (Secorvo College)
21.-22.09.	D·A·CH Security (GI/OCG/BITKOM/SI/TeleTrusT, Wien)
28.-29.09.	7. Security Awareness Symposium (Secorvo, Ettlingen)
28.-30.09.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
Oktober 2010	
04.-07.10.	ISSE 2010 (Teletrust, Berlin)
04.-07.10.	Sicherheitsmanagement heute (Secorvo College)
19.-21.10.	ISSECO Certified Professional for Secure Software Engineering (Secorvo College)
19.-21.10.	it-sa (SecuMedia Verlag, Nürnberg)
21.10.	it-sa Datenschutztag 2010 (Computas, Nürnberg)
November 2010	
18.-19.11.	34. DAFTA (GDD e.V., Köln)

Fundsache

Der jüngste IBM X-Force-Halbjahresbericht vom 24.08.2010 belegt einige beunruhigende Tendenzen: Ein deutlicher Anstieg von pdf-Angriffen, die Zunahme von mit Schadsoftware „versetzten" Webseiten und die meisten innerhalb von sechs Monaten gezählten Sicherheitsschwachstellen. Für Interessierte bietet der 112seitige Bericht zahlreiche wertvolle Detailanalysen aktueller Bedrohungen.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Michael Knopp, Jörg Völker

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2010



Laufzeitverlängerung

In Deutschland wurde im vergangen Jahrhundert eine Technologie eingeführt, die man für so sicherheitskritisch hielt, dass ihre Rahmenbedingungen gesetzlich geregelt wurden und der Bund eine Aufsichtsbehörde etablierte, um die Unternehmen zu überwachen, die die kritischen Anlagen zur Nutzung dieser Technologie betreiben. Die Begeisterung der Bürger über diese Technologie hielt sich stark in Grenzen – nun aber wird aus Gründen der Wirtschaftlichkeit diskutiert, ob die Bundesregierung nicht deren Laufzeit verlängern sollte.

Nein, die Rede ist nicht von der Nutzung der Kernenergie – sondern von der „qualifizierten elektronischen Signatur“ (QES).

In einem Gutachten zu den Auswirkungen des ELENA-Verfahrens auf Wirtschaft, Bürger und Verwaltung vom 13.09.2010 stellte der Nationale Normenkontrollrat kürzlich fest, dass der mit Abstand größte Kostenfaktor auf Verwaltungsseite die Erstattung für die QES an die Antragsteller ist, die damit ihr Einverständnis zum Abruf ihrer Daten geben müssen – und das, obwohl die Beträge sehr optimistisch geschätzt wurden. Zur Kostensenkung wird nun vorgeschlagen, die Gültigkeit des QES-Zertifikats von fünf auf zehn Jahre zu verdoppeln oder aber gleich einen QES-fähigen Dritten „stellvertretend“ schriftlich (sic!) zur Abruf-Autorisierung zu ermächtigen.

Nun ist aus Sicherheitsgründen die Gültigkeit der QES-Zertifikate per Rechtsverordnung auf fünf Jahre begrenzt, und auch die Sicherheit der Kryptoalgorithmen wird derzeit nur für sieben Jahre prognostiziert. Daraus lässt sich nun zweierlei folgern: Entweder wurden die durch ELENA möglichen Einsparungen deutlich zu optimistisch dargestellt. Oder aber die Nutzung der QES wird seit mehr als einem Jahrzehnt mit übertriebenen Sicherheitsrestriktionen gegängelt – und so unnötig verteuert.

Zum Glück ist es nur die qualifizierte Signatur, über deren Nutzung so munter spekuliert wird. Und nicht die Atomkraft.



Inhalt

Laufzeitverlängerung
Security News
Auslaufmodell Passwort
Smartes Energienetz
Traurige Nachricht
Datenschutz-Informationsquelle
Servergesteuertes NoScript
Schweigendes Orakel
OWASP lebt
Secorvo News
Secorvo College aktuell
Teamverstärkung
Veranstaltungshinweise
Fundsache

Security News

Auslaufmodell Passwort

Seit 2003 ist es dank der von P. Oechslin entwickelten Rainbow-Tables heute für Passwort-Cracker um ein Vielfaches leichter, ein einwegverschlüsseltes Passwort zu rekonstruieren. Besonders betroffen von solchen Angriffen sind die Passwort-Hashes des Windows (LM) und des NT LAN Managers (NTLM), die kein „Salz" beim Hashen verwenden.

Oechslins Unternehmen stellt eine Webseite zur Verfügung, über die sich in Sekundenschnelle praktisch alle bis zu 14-stelligen Windows-Passwörter aus dem LM-Hash rekonstruieren lassen. Und im Projekt RainbowCrack (siehe SSN 8/2010) wurden inzwischen die NTLM-Hashes für fast alle achtstelligen Passwörter aus Großbuchstaben, Kleinbuchstaben und Ziffern tabelliert – auch für alle kürzeren Passwörter mit Sonderzeichen, und für alle neunstelligen aus Kleinbuchstaben und Ziffern.

Wenn irgend möglich sollten Windows XP-Administratoren daher LM-Hashes deaktivieren – bei Windows Vista ist dies ohnehin die Grundeinstellung, und Windows-Passwörter unter neun Zeichen Länge sollten grundsätzlich tabu sein.

Zehnstellige und längere Passwörter, die inzwischen zu fordern sind, sind für Anwender eine Zumutung – es scheint nun endgültig an der Zeit, über Alternativen wie Smartcard Logon nachzudenken.

Smartes Energienetz

Am 22.09.2010 veröffentlichte das amerikanische Marktforschungsunternehmen PikeResearch eine Studie, die für das intelligente Stromnetz (vulgo „Smart Grid") ein Marktwachstum von 75% für die kommenden Jahre vorhersagt – auf einen mehrstelligen Milliardenbetrag in 2015. Kein Wunder, dass sich Unternehmen wie Cisco bereits in Stellung bringen und Miele auf der IFA die ersten Smart-Grid-fähigen Haushaltsgeräte vorgestellt hat. Dass sich aus der Verbindung von Stromnetz, Haushaltsgeräten und Internet neue Schwachstellen ergeben, ist leicht auszumalen: Verhaltensprofile beim Messstellenbetreiber und ferngesteuerte Waschmaschinen bieten viel Stoff für Phantasien.

Auf diese Gefahren reagierte das US-amerikanische NIST am 02.09.2010 mit der Publikation der 600 Seiten starken Richtlinie „Guidelines for Smart Grid Cyber Security". Teil 2 des dreibändigen Werks ist dem Thema Datenschutz gewidmet. An ausgewählten Beispielen wird darin deutlich, welche Begehrlichkeiten der Zugriff auf Stromverbrauchsdaten wecken dürfte: So lokalisierte eine amerikanische Regierungsbehörde anhand des Energieverbrauchs pro Wohnfläche eine Marihuanazucht.

Auch in Deutschland werden datenschutzrechtliche Einwände gegen die Datenerhebung der derzeit ausgerollten Smart Metern laut. Denn aus dem Gebot in § 21b Abs. 3a EnWG, Messeinrichtungen bereitzustellen, die „den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegeln", lässt sich kein Erfordernis zur zeitnahen Übermittlung der Messdaten an den Messstellenbetreiber ableiten – zur Abrechnung reicht die Übermittlung der zeitlich aggregierten Daten.

Auch zur Bereitstellung der in § 40 Abs. 3 EnWG geforderten „lastvariable[n] Tarife" ist eine alternative Gestaltung denkbar: die Daten können z. B. so übertragen werden, dass eine Zuordnung einzelner Datensätze zu einem konkreten Zähler nicht möglich ist – und somit auch keine Erstellung haushaltsbezogener Profile.

Die derzeitigen Implementierungen, bei denen die Verbrauchsdaten im 15-Minuten-Intervall an den Energieversorger übermittelt werden, ist zur Vertragserfüllung nicht erforderlich – und mit dem Prinzip der Datensparsamkeit unvereinbar. Eine datensparsame Realisierung käme hingegen ganz ohne Profile außerhalb des Haushaltes aus.

Traurige Nachricht

Am 23.09.2010 ist im Alter von 52 Jahren überraschend Andreas Pfitzmann verstorben. Mitte der 80er Jahre hatte er mit seinen Arbeiten an der Universität Karlsruhe den „technischen Datenschutz" begründet und war seitdem ein einflussreicher Mahner und Mittler zwischen den Welten des Rechts, der Informatik und gesellschaftlicher Fragestellungen. Andreas Pfitzmann hat nicht nur durch seine mehr als 250 Veröffentlichungen und Stellungnahmen wichtige Weichenstellung der Technikgestaltung beeinflusst, auch als Gutachter des Bundesverfassungsgerichts (Vorratsdatenspeicherung, Online-Durchsuchung) und vieler Bundesbehörden, sondern auch als Hochschullehrer hunderte Studenten für das Thema begeistert. Er wird uns fehlen.

Datenschutz-Informationsquelle

Am 17.09.2010 hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) offiziell ein neues Datenschutz-Wiki als Nachschlagewerk für Datenschutz-Laien und Fachleute eröffnet. Das zum Start verständlicherweise noch recht überschaubare Angebot ist nicht amtlich und offen für jeden Interessierten. Auch die im Internetauftritt des BfDI enthaltenen Materialien sollen übernommen werden, vielleicht auch Texte der Luchterhand-Loseblatt-Sammlung.

Hervorgegangen ist das neue Angebot aus dem Datenschutz-Forum, einem Diskussionsforum zu Datenschutzfragen. Es reiht sich ein in weitere Informationsangebote wie das virtuelle Datenschutzbüro des ULD, das Berichtsarchiv ZAfTDa der FH Gießen-Friedberg, das thematisch engere Wiki des AK-Vorratsdatenspeicherung, die Dokumentation von Datenschutzvorfällen des Projekts Datenschutz und das stärker Material orientierte DuD-Wiki.

Für eine faire Bewertung der Qualität ist es noch zu früh, und verschiedene Bereiche wie die Kategorienbildung, bereitgestellte Artikelvorlagen und die Hilfe bedürfen noch der Entwicklung. Grundsätzlich ist die Initiative jedenfalls zu begrüßen. Es ist zu hoffen, dass durch die Beteiligung vieler Experten eine Wissenssammlung entsteht, die auch Hilfestellung in Zweifelsfällen und Auslegungsfragen bietet.

Servergesteuertes NoScript

In sicherheitsbewussten Kreisen sind die Firefox-Erweiterungen NoScript und RequestPolicy, durch die sich Nutzer vor Cross-Site-Scripting (XSS) schützen können, inzwischen fester Bestandteil des Browsers. Die Freude daran wird jedoch dadurch getrübt, dass ein Nutzer ständig entscheiden muss, welche Webseite er für hinreichend vertrauenswürdig hält, um aktive Elemente zuzulassen.

Mit einem Konzept für serverbasierte Vorgaben, "Content Security Policy" (CSP) genannt, gibt Mozilla nun Anbietern die Möglichkeit festzulegen, welchen Dritt-Anbietern von Inhalten mit aktiven Komponenten vertraut werden soll. Damit wird ein Teil der Funktionalität von NoScript und RequestPolicy fest in der kommenden Version 4 des Firefox-Browsers verankert. Die Gefahr eines XSS-Angriffs wird damit signifikant beschränkt, sofern CSP auch von Web-Anbietern genutzt wird. Bis dahin wird es sicher noch etwas dauern – das Interview mit dem Chefentwickler Brandan Sterne mag die Wartezeit ein wenig verkürzen.

Schweigendes Orakel

Eine spezielle Klasse von kryptologischen Angriffen nutzt das angegriffene System als „Orakel“, indem diese aus unterschiedlichen Reaktionen (sprich: differenzierten Fehlermeldungen) ableiten, bis zu welchem Punkt der Angriff erfolgreich verlaufen ist.

Nach SSL und WPA (vgl. SSN 11/2008) hat ein solcher Orakel-Angriff nun die Cookies und Sitzungsdaten von ASP.NET-Webservern getroffen, wie Microsoft am 17.09.2010 einräumte: Mit einer auf das Jahr 2002 zurückgehenden Technik können diese Daten ohne Kenntnis des Schlüssels Bit für Bit entschlüsselt werden, solange der Server jedes Mal zurückmeldet, ob bei seinem Entschlüsselungsversuch korrekte Padding-Bits entstanden oder nicht.

Der zunächst von Microsoft empfohlene Workaround entbehrte nicht einer gewissen Ironie: Man nutze die „customErrors“ Funktionalität, um die Fehlermeldungen unspezifisch umzugestalten...

OWASP lebt

Am 09. und 10.09.2010 fand die diesjährige weltweite OWASP Konferenz „AppSec 2010“ im kalifornischen Irvine statt. Die von etwa 300 internationalen Experten besuchte und mit herausragenden Referenten besetzte Veranstaltung zeichnete sich durch spannende Fachdiskussionen über den Status und die Entwicklung der Web-Sicherheit aus. Zu den Highlights zählte die Keynote von David Rice, der Parallelen zwischen der Regulierung im Umweltschutz und der Web-Sicherheit aufzeigte. Alle Vorträge sollen in Kürze online verfügbar sein.

Interessierte sollten sich den 20.10.2010 vormerken – an diesem Tag findet in Nürnberg die OWASP AppSec Germany 2010 mit einem ähnlich spannenden Programm statt.

Secorvo News

Secorvo College aktuell

Experten unter sich: Die kommenden Seminare von Secorvo College bieten dank der sehr guten Nachfrage eine ganz besondere Gelegenheit für einen intensiven fachlichen Erfahrungsaustausch, sei es über das Thema PKI, Audit, ISM oder Datenschutz.

Wissensvermittlung durch Secorvo gepaart mit fruchtbaren Diskussionen und viel Praxiserfahrung – noch gibt es freie Plätze bei den Oktober- und Novemberveranstaltungen.

Teamverstärkung

Mit Klaus J. Müller hat das Secorvo-Team am 01.09.2010 erneut Zuwachs bekommen – und damit unsere gesammelte Erfahrung im Gebiet Informationssicherheit und Datenschutz um 10 auf exakt 200 Jahre angehoben. Neben „klassischen“ Themen der IT-Sicherheit hat sich Klaus Müller intensiv mit Smart Metern beschäftigt, nachzulesen unter anderem in der Fachzeitschrift DuD („Gewinnung von Verhaltensprofilen am intelligenten Stromzähler“, DuD 6/2010).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2010	
04.-07.10.	ISSE 2010 (Teletrust, Berlin)
04.-07.10.	Sicherheitsmanagement heute (Secorvo College)
09.-15.10.	Hacker Halted 2010 (Hacker Halted USA, Miami/US)
19.-21.10.	it-sa (SecuMedia Verlag, Nürnberg)
21.10.	it-sa Datenschutztag 2010 (Computas, Nürnberg)
26.-28.10.	IT-Sicherheit heute (Secorvo College)
November 2010	
03.-04.11.	#days Workshops: Exploit Laboratory / Protecting from GSM attacks (DEFCON, Luzern/CH)
05.-06.11.	#days Conference (DEFCON, Luzern/CH)
09.-12.11.	PKI (Secorvo College)
15.-17.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
18.-19.11.	34. DAFTA (GDD e.V., Köln)
22.-26.11.	T.I.S.P.-Schulung (Secorvo College)
Dezember 2010	
06.-07.12.	IsSec/ZertiFA 2010 (Computas, Berlin)

Fundsache

Am 20.09.2010 veröffentlichte Chintan Shah in seinem Blog bei McAfee eine lesenswerte Analyse eines der derzeit leistungsfähigsten (und damit gefährlichsten) „Crimeware"-Werkzeuge: Zeus. Über Konfigurationseinträge lässt sich Zeus zu einem individualisierten Banking-Trojaner umgestalten – der inzwischen sogar Angriffsmuster gegen das mTAN-Verfahren beherrscht.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2010



Stuxnet - mythenfrei

Auch wenn dem sich über USB-Sticks und Netze verbreitenden Wurm „Stuxnet“ technische Raffinesse und den Autoren viel Know-how zugestanden werden muss, ist sein Erscheinen wenig erstaunlich. Sowohl USB-Würmer als auch Zero-Day-Exploits (noch nicht veröffentlichte Schwachstellen) gab es bereits. Neu ist, dass industrielle Regelungs- und Steuerungssysteme befallen wurden, hier Siemens PCS 7 und WinCC. Was lässt sich aber, ohne über Auftraggeber und Zielsetzung zu spekulieren, aus dem Vorfall lernen?

Fakt 1: Virenschutz hat Grenzen. Stuxnet verbreitete sich unerkannt über einen Zeitraum von einem Jahr. Verlässlichen Schutz vor neuartigen Viren und Trojanern können Scanner nicht bieten. Ein wirksamer Schutz kritischer Systeme benötigt umfassendere Konzepte.

Fakt 2: Datenträger sind Gefahrenquellen. Die verbreitete Nutzung von USB-Sticks über Systemgrenzen (privat/dienstlich, intern/extern, Office/Produktionssystem) hinweg ist leichtsinnig – und Bequemlichkeit keine Rechtfertigung. Hier sollte im Detail geregelt werden.

Fakt 3: Vertrauen ist gut, Kontrolle besser. Sie trauen Ihrem Dienstleister oder Lieferanten. Aber haben Sie sich auch davon überzeugt, dass er ebenso auf Sicherheit achtet wie Ihr Unternehmen?

Fakt 4: Netzsegmentierung und Firewalls helfen. Viel zu häufig werden kritische Systeme nicht von weniger kritischen entkoppelt und Verbindungswünsche von innen ins Internet großzügig zugelassen. Einmal eingedrungen, haben Trojaner so leichtes Spiel.

Fakt 5: Schutzbedarfsanalysen identifizieren das Wesentliche. Erst anhand einer Klassifikation kritischer und weniger kritischer Systeme ist es möglich, geeignete Maßnahmen zur Vorsorge auszuwählen – und bei einem Vorfall angemessen und zeitnah zu reagieren.

Unsere Empfehlung: Rechnen Sie mit weiteren derartigen „Neuheiten“ bei Schadsoftware. Beugen Sie möglichen Schäden wirksam vor – durch Schutzmaßnahmen und definierte Sicherheitsprozesse.



Inhalt

Stuxnet - mythenfrei

Security News

Autoritätsfrage

Firefox als Vorratsdatenspeicher

Cyber Security Month

De-Mail ... zum Zweiten

Perlen sicherer Softwareentwicklung

HTTPS soll HTTPS bleiben

Neue Jagdreviere

Secorvo News

Unser Seminarangebot 2011

Kronjuwelen-Hacking

Secorvo hören und sehen

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Autoritätsfrage

Im Jahr 1906 schlüpfte der Schuster Wilhelm Voigt in die Uniform eines preußischen Hauptmanns. Die verlieh ihm so viel Autorität, dass er ohne Rückfrage die Stadtkasse von Köpenick ausgehändigt bekam. Heutige Betrüger nutzen ausgefeilte Trojaner, um in den Browser ihrer Opfer zu schlüpfen und deren Online-Konten zu übernehmen. Gegen derartige „Man-in-the-Browser"-Angriffe bietet es sich an, zusätzlich zum möglicherweise infizierten PC ein weiteres, vertrauenswürdiges Gerät einzusetzen – so etwa bei der mobileTAN das eigene Handy.

Allein: Mit der Autorität der angezeigten Original-Webseite der Bank oder des Online-Anbieters kann der (Haupt-)Mann im Browser dem Anwender nahe legen, die Warnungen seines externen Geräts zu ignorieren – oder sogar es selbst zu manipulieren. Dass dies nicht bloße Theorie ist, wurde am 25.09. 2010 bekannt: Eine Variante des Trojaners ZeuS drängt ihren Opfern ein Update des Sicherheits-Zertifikats (sic!) für ihr Handy auf – und installiert tatsächlich einen Trojaner, der zusammen mit seinem „Partner" auf dem PC die mobileTAN aushebelt.

Hosentaschenforensik

Mit dem FTK-Imager ist seit dem 08.10.2010 die grundlegend überarbeitete Windows-Version 3.0 des bewährten und kostenfreien forensischen Werkzeugs verfügbar. Neu ist die Unterstützung für Images mit den Dateisystemen VxFS, exFAT und Ext4 sowie des forensischen Festplattenabbildformats AFF. Damit ist eine Einbindung der Formate AFF, DD, RAW, E01 und S01 als schreibgeschützte physische Laufwerke unter Windows möglich. Für FAT und NTFS kann bei Bedarf auch eine Schreibemulation genutzt werden, ohne dass die Integrität der Abbilddatei beeinträchtigt wird. Besonders die unkomplizierte Einbindung der Dateisysteme unter Ext3, Ext4 und HFS+ (iPhone) spart Zeit. Ein kleiner Wermutstropfen bleibt: verschlüsselte Abbildformate sind derzeit nicht nutzbar.

Firefox als Vorratsdatenspeicher

Eines der Argumente gegen insbesondere staatliche Vorratsdatenspeicherung ist, dass niemand sicher sein kann, dass nicht eines Tages die angehäuften Daten von weniger wohlmeinender Seite missbraucht werden. Wie einfach das geht, führt gerade der Trojaner Trojan-PWS-Nslog vor: Wie am 06.10. 2010 gemeldet schaltet er kurzerhand in der Firefox-Konfiguration das Speichern eingegebener Passwörter ein und die Rückfrage dazu ab, um sich später der kompletten Sammlung zu bemächtigen.

Cyber Security Month

Den Oktober 2010 erklärte das Internet Storm Center ISC am 01.10.2010 zum "Cyber Security Month". Täglich erschien seitdem ein Tagebucheintrag mit praktischen Hinweisen zur IT-Sicherheit. Die Einträge der ersten Woche wendeten sich an Familien, die der nächsten an Kinder, danach wurden im Bereich "Bosses" Führungskräfte angesprochen und im letzten Teil die Mitarbeiter von Unternehmen. Die Einträge (sowie die zahlreichen Kommentare) enthalten viele hilfreiche Empfehlungen.

De-Mail ... zum Zweiten

Das Bundeskabinett hat am 13.10.2010 den zweiten Gesetzentwurf für De-Mail-Dienste beschlossen – eingestuft als „besonders eilbedürftig", denn Umsetzungsziel ist das Jahr 2011. Das schon im April 2009 von der Großen Koalition initiierte Gesetzgebungsverfahren wurde Ende der Legislaturperiode mit einem Appell des Bundestages an die neue Regierung zur Weiterführung des Projekts abgebrochen.

In dem neuen Entwurf sind weitere Regelungen enthalten. So ist die Verpflichtung des Anbieters, die Verbindung des Nutzers zu seinem Konto zu verschlüsseln, jetzt ausdrücklich geregelt, dafür ist die Verpflichtung zur Bereitstellung pseudonymer Adressen für natürliche Personen entfallen. Neu ist auch die Abholbestätigung einer E-Mail durch den Dienstanbieter des Empfängers gegenüber öffentlichen Stellen und die Verpflichtung der Anbieter, eine automatische Weiterleitung zu ermöglichen.

Zu besserer Verständlichkeit haben die Überarbeitungen nicht geführt. Einige Regelungen, wie die automatische Weiterleitung oder das Streichen der Verpflichtung zum Pseudonymangebot, konterkarieren gar den ursprünglichen Gesetzeszweck.

Perlen sicherer Softwareentwicklung

Sicherheit genießt meist nicht höchste Priorität bei Softwareentwicklern. Dabei gibt es praktikable Vorgehensweisen, die – nach Absolvieren der Lernkurve – nachweislich zu signifikant sichererem Code führen, wie z. B. Design by Contract, ein Ansatz, für den mittlerweile Unterstützung für viele gängige Programmiersprachen existiert.

Ein anderer, vom NIST am 06.10.2010 als SP 800-142 veröffentlichter Ansatz beschäftigt sich mit dem Problem, wie man der Masse an Testfällen effektiv Herr werden kann. Bekanntlich explodiert die Zahl der Testfälle mit der Anzahl der zu testenden Parameter und der Zahl der Werte, die diese annehmen können. Die Autoren präsentieren

Untersuchungsergebnisse, nach denen Programmierfehler selbst in komplexen Systemen sehr oft durch die Interaktion von nur drei bis vier Parametern ausgelöst wird, aber praktisch nie von mehr als sechs. Es ist daher nicht nötig, alle Kombinationen von Parametern durchzuprobieren, um alle Fehler aufzuspüren.

Erfreulicherweise haben die Autoren auch gleich ein frei verfügbares Werkzeug geschrieben, welches einen (fast) minimalen Satz an Kombinationen von Parametern erzeugt, dessen Umfang ganz erheblich geringer ist, als die Zahl sämtlicher Kombinationen. Weder das Werkzeug noch die Vorgehensweise wird Sicherheits-Wunder bewirken, jedoch gibt es nun - bei angemessener Anwendung - ein gutes Argument mehr gegen Ausflüchte, Systeme nicht sicher zu entwerfen und zu implementieren.

HTTPS soll HTTPS bleiben

Die Veröffentlichung des Firefox-Add-On Firesheep am 24.10.2010 auf der Toorcon in San Diego hat einem altbekannten Problem, der unsicheren Übertragung von Cookies als Session-IDs, neue Aufmerksamkeit zu teil werden lassen.

Mit dem Add-On ist es möglich, Netzwerkverkehr mitzuschneiden und automatisiert unverschlüsselt übertragene Session-IDs zu sammeln. Die durch diese IDs authentifizierten Accounts werden direkt in Firesheep angezeigt; ein Anmelden unter fremdem Account ist durch Doppelklick möglich.

Da viele populäre Seiten, u. a. auch Facebook, nach der Anmeldung über eine mit SSL geschützte Seite wieder auf unverschlüsseltes HTTP zurückschalten, geben sie die im Cookie gespeicherte Session-ID jedem preis, der den Netzverkehr mitlesen kann.

So lange dieses Problem nicht von Anwendungsseite durch konsequente Verschlüsselung, beispielsweise durch die Verwendung von HSTS, aus der Welt geschafft ist, bleibt nur, sich mit Werkzeugen wie Force TLS oder NoScript zu behelfen.

Neue Jagdreviere

Die Entfernung von SIM-Locks bei Mobiltelefonen ruft die Strafverfolgungsbehörden inzwischen nicht mehr nur bei gewerblichem Handeln auf den Plan. Nach Auskunft der Polizeiinspektion Göttingen vom 12.10.2010 sind im Zusammenhang mit solchen Entsperrungen nun auch Ermittlungsverfahren gegen 600 Kunden eingeleitet worden.

Zwar ist die Verletzung von Markenrechten durch die gewerbliche Entsperrung schon vor sechs Jahren höchstrichterlich festgestellt worden; ob es sich für die Endanwender dabei um einen Straftatbestand handelt, ist jedoch bislang ungeklärt. Daher ist eine Anklageerhebung in diesen Verfahren eher unwahrscheinlich, zumal die Einschlägigkeit der meisten geprüften Straf-, Urheber- und Wettbewerbsrechtsvorschriften gegenüber privaten Endkunden zweifelhaft ist.

Sollte aus dieser Initiative jedoch eine generelle Strafverfolgung resultieren, könnte sich dies schnell auf weitere Bereiche auswirken, in denen die Funktionsfähigkeit von Software oder Hardware durch das Entfernen von Sperren erweitert werden kann. Dabei wird es für private Nutzer auch auf die Haltung der Hersteller und Rechteinhaber ankommen, denn die Verfolgung vieler der in Erwägung gezogenen Straftatbestände, wie etwa Computerbetrug, setzt einen Strafantrag des Geschädigten voraus.

Secorvo News

Unser Seminarangebot 2011

Zum Jahresende geben wir Ihnen mit der TISP-Schulung vom 22.-26.11.2010 noch einmal die Gelegenheit, Ihr Wissen im Bereich IT-Sicherheit zu zertifizieren. Auch 2011 bietet unser Seminarangebot (jetzt mit Teilnehmer-Rating) Rahmen, Referenten und Teilnehmer für einen intensiven Erfahrungsaustausch unter Experten. Wir freuen uns auf Sie!

Kronjuwelen-Hacking

SAP-Systeme sind das Rückgrat unserer hochautomatisierten Wirtschaft. In den meisten größeren Unternehmen steuern SAP-Anwendungen die kritischen Unternehmensprozesse: Fertigung, CRM, Lieferantenmanagement, Personalplanung, Finanzen, Controlling. Sie verarbeiten sensitivste Daten – die Kronjuwelen des Unternehmens. Auf der nächsten Veranstaltung der Karlsruher IT-Sicherheitsinitiative beleuchtet Dr. Markus Schumacher (Virtual Forge) in seinem Vortrag „SAP Anwendungen im Visier von Hackern“ am **11.11.2010** (18 Uhr im Schlosshotel Karlsruhe) typische Angriffsmöglichkeiten, erläutert deren Ursachen und gibt Handlungsempfehlungen zum Schutz (Anmeldung).

Secorvo hören und sehen

Auf dem kommenden 18. DFN-Workshop „Sicherheit in vernetzten Systemen“ vom 15.-16.02.2011 in Hamburg wird Secorvo gleich mit zwei Vorträgen zu aktuellen Themen der IT-Sicherheit zu hören sein: Klaus J. Müller wird zu „Datenschutz und Datensicherheit in Smart Grids“ vortragen, und Jörg Völker aktuelle Erkenntnisse zur „Sicherheit von iPhones“ vorstellen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2010	
03.-04.11.	#days Workshops: Exploit Laboratory / Protecting from GSM attacks (DEFCON, Luzern/CH)
05.-06.11.	#days Conference (DEFCON, Luzern/CH)
09.-12.11.	PKI (Secorvo College)
15.-17.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
18.-19.11.	Datenschutzsaudit: Best Practice (Secorvo College)
18.-19.11.	34. DAFTA (GDD e.V., Köln)
22.-26.11.	T.I.S.P.-Schulung (Secorvo College)
23.-26.11.	ISDC 2010 Europe (DeepSec GmbH, Wien/AT)
Dezember 2010	
05.-09.12.	AsiaCrypt 2010 (IACR, Singapur/SGP)
06.-07.12.	IsSec/ZertiFA 2010 (Computas, Berlin)
27.-30.12.	27th Chaos Communication Congress (27C3) (Chaos Computer Club, Berlin)
Januar 2011	
18.-20.01.	Omnicard 2011 (inTIME, Berlin)

Fundsache

Eine technisch tiefer gehende Analyse des Stuxnet-Wurms bietet ein am 12.10.2010 erschienenes 50seitiges Dossier der Firma Symantec, verfasst von Nicolas Falliere, Liam O Murchu und Eric Chien. Unter anderem zeigt es die wahrscheinliche Verbreitung – die mindestens von Juni 2009 bis Juni 2010 unbemerkt blieb.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

November 2010



Hybris kommt vor dem Fall

Seit dem 01.11.2010 gibt es den neuen „elektronischen" Personalausweis, der mit seinem kontaktlosen (Krypto-) Chip nicht nur die Speicherung zweier Fingerabdrücke sondern auch die Nutzung als Online-Ausweis und Signaturkarte ermöglichen soll. Dazu werden ein Kartenlesegerät sowie eine „AusweisApp" benötigt, die unter dem sperrigen Arbeitstitel „Bürger-Client" im Auftrag des BMI durch ein von Siemens geführtes Konsortium entwickelt wurde (SSN 12/2009).

Bereits am 21.09.2010 hatte der Chaos Computer Club medienwirksam demonstriert, dass die PIN durch einen Trojaner ausgespäht werden kann, sofern ein Kartenleser ohne eigene PIN-Tastatur verwendet wird. Das war in der Sache wenig überraschend; beim Online-Banking ist dieser Trojaner-Angriff lange bekannt. Der PC ist schließlich immer das schwache Glied in der Kette. Überraschend war allerdings die Reaktion der Bundesregierung: In einem Interview der FAZ versicherte die IT-Beauftragte der Bundesregierung Cornelia Rogall-Grothe („Bundes-CIO") am 01.11.2010: „Es gibt keine Sicherheitslücke. Vor Schadsoftware am PC kann sich jeder wirksam schützen, indem er Virenschutzprogramme benutzt und eine Firewall installiert. (...) Es ist die sicherste Technik, die es gibt."

Acht Tage später stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die AusweisApp zum Download bereit. Und keine 24 Stunden später publizierte Jan Schejbal in seinem Blog ein fatales Sicherheitsleck: Die Update-Funktion der AusweisApp prüft nicht, ob das SSL-Zertifikat auch zu dem Server gehört, von dem das Update geladen wird, und entpackt es, ohne zuvor die Signatur zu prüfen. Seit dem 10.11.2010 findet man auf der AusweisApp-Seite nun einen Verweis auf eine Pressemitteilung des BSI, in der es heißt, dass in Kürze eine neue Version der AusweisApp verfügbar sein wird – nach „umfangreichen Tests".

Etwas spät für „die sicherste Technik, die es gibt".



Inhalt

Hybris kommt vor dem Fall

Security News

Deep links am Ende?

Rundum sorgenreich

Geschütztes Smart Metering

Märchen von Übermorgen

Safe Harbor am Ende?

Happy Birthday Phrack!

Bundesrat zum Datenschutz

Secorvo News

100 mal Security News

Smart Grid Symposium

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Deep links am Ende?

Bereits am 29.04.2010 hat der Bundesgerichtshof ein wichtiges Urteil zur Frage der Verlinkung von Website-Inhalten unter Umgehung der Startseite (*deep link*) verkündet. Danach liegt ein Urheberrechtsverstoß vor, wenn Schutzmaßnahmen der verlinkten Seite den Willen erkennen lassen, keine Direktverlinkung gestatten zu wollen. Auf die Wirksamkeit der Maßnahmen kommt es dabei nicht an. Seit dem 10.11.2010 liegt nun die Urteilsbegründung vor. Mit der „Session-ID" genannten Entscheidung fällt der BGH hinter die sieben Jahre alte Paperboy-Entscheidung zurück, die *deep links* auf ungeschützte Inhalte für zulässig erklärt hatte.

In dem zu entscheidenden Sachverhalt bot die Klägerin im Internet Stadtpläne an. Einmalige Zugriffe über die Startseite waren kostenlos, die Nutzung durch Einbindung der Karte jedoch lizenzpflichtig. Zum Schutz wurden Session-IDs verwendet, die als Teil der weiterführenden URL beim Besuch der Startseite vergeben wurden. Die Beklagte überwand diese Maßnahme, indem sie via Skript eine Session-ID abholte und diese in die URL einband. Trotz der offensichtlichen Unwirksamkeit dieser Schutzmaßnahme sah der BGH hierin eine urheberrechtswidrige Umgehung.

Das Urteil wirft jedoch Fragen auf. Da nach der Begründung des BGH allein die Erkennbarkeit des Urheberwillens (unabhängig von der Wirksamkeit des Schutzmechanismus und der Umgehungsabsicht des „Verlinkers") für den Urheberrechtsverstoß wesentlich ist, bleibt offen, wie mit *deep links* rechtssicher umgegangen werden kann. Schließlich kann ein Urheber auch seinen Willen ändern und zunächst frei zugängliche Dokumente nur noch nach gebührenpflichtiger Anmeldung preisgeben – ist daher vom Verlinker zu fordern, dass er regelmäßig prüft, ob der Urheber seinen Willen geändert hat? Sollte er vor Einrichtung eines *deep link* zu Nachweiszwecken einen Snapshot der Startseite speichern, oder sich lieber gleich vertraglich mit dem Urheber einigen? Oder vielleicht sogar mit Blick auf mögliche Abmahn-Wellen ganz auf *deep links* verzichten? Letzteres wäre zweifellos nicht nur das Ende der Links in den SSN, sondern das Ende des Internet, wie wir es heute kennen.

Rundum sorgenreich

Am 15.11.2010 kündigte Facebook einen Unified-Messaging-Dienst für alle Benutzer an, der E-Mail, Chat und SMS vereinen soll. Keine ganz neue Idee – vor allem aber eine Kriegserklärung an die Freemailer Gmail, Yahoo, Hotmail, GMX und Web.de. Immerhin signalisierten über 28 Mio. Facebook-Nutzer, dass ihnen diese Ankündigung gefällt. Darunter dürften auch zahlreiche Deutsche User sein, deren Zahl sich im Jahresverlauf von etwa vier auf über acht Mio. täglich mehr als verdoppelt hat – jeder zehnte hierzulande verbringt im Schnitt 18 Minuten am Tag bei Facebook.

Dabei ist Vorsicht angeraten: Wie Google analysiert auch Facebook alle Nutzerdaten zur Erstellung von Profilen, um zielgruppenscharfe Werbung schalten zu können. Zudem kann bei einem Webmailer nicht ausgeschlossen werden, dass es der eine oder andere Administrator mit der Privatsphäre nicht so genau nimmt: Erst am 14.09.2010 hatte ein Blogger bekannt gemacht, dass ein (inzwischen ehemaliger) Google-Mitarbeiter offenbar mehrfach Gmail-Accounts von Teenagern mitgelesen und sich in deren Kommunikation eingeschaltet hatte.

Vor allem die Vielzahl der Dienste (Maps, News, Kalender, Textverarbeitung und Tabellenkalkulation, Fotoalbum, Kontaktnetzwerk und Messaging) versorgt den Anbieter mit einem präzisen Bild der Interessen, Neigungen, Vorlieben und sozialen Beziehungen seiner Nutzer, sowie inzwischen sogar deren Standort – besonders interessant, wenn die Dienste auf Smartphones genutzt werden. Die Informationen zu Facebooks neuem Messaging-Dienst, zum Datenschutz, zur Konfiguration der Privatsphäre und zur Sicherheit sollte man sich daher genau anschauen – vor der Anmeldung.

Geschütztes Smart Metering

Auf ihrer 80. Konferenz am 03./04.11.2010 forderten die Datenschutzbeauftragten des Bundes und der Länder Verbesserungen beim Datenschutz der Smart Meter (SSN 09/2010). So sollen bei der Messung des Stromverbrauchs anfallende Daten „unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit [...] Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren" – denn technisch ist eine Übermittlung der Zählerstände dafür nicht erforderlich.

Gängige Praxis ist hingegen eine Übermittlung des Zählerstandes in 15-min-Intervallen mit schriftlicher Einwilligung des Kunden. Diese setzt jedoch Freiwilligkeit und Widerruflichkeit voraus – er kann sich also weigern oder die Einwilligung später zurückziehen. Aus Sicht des Investitionsschutzes sind EVUs also gut beraten, auf datenschutzfreundliche statt einwilligungsbasierte Lösungen zu setzen. Zur Verbrauchsminimierung sind „Vor-Ort-Analysen" ohnehin kostengünstiger realisierbar.

Märchen von Übermorgen

Während sich die Praktiker freuen, dass mit der zunehmenden Verbreitung von Windows Vista/7 der Umstieg vom suspekt gewordenen SHA-1 auf den SHA-2 endlich in greifbare Nähe rückt, läuft bereits der Wettbewerb um den Ende 2012 zu kürenden SHA-3 (SSN 06/2009). Zwei der beteiligten Forscher gingen nun in Aufsätzen vom 04.10. und 12.11.2010 der Frage nach, wie sicher die SHA-3-Kandidaten vor Quanten-Computern sind, da sich dort mit dem Algorithmus von Grover der Brute-Force-Aufwand bei vielen Verschlüsselungs- und Einwegfunktionen von 2^n auf $2^{n/2}$ Operationen senken lässt.

Für Kryptologen ist das ein gewaltiger Unterschied – für die praktische Anwendung des künftigen SHA-3 allerdings etwa so relevant wie die Frage, ob ein neuer Sattel auch für das Reiten toter Pferde taugt: Falls es eines Tages Quanten-Computer gibt, sind dank Shors Algorithmus auch RSA und fast alle anderen Signaturverfahren sofort zu brechen.

Safe Harbor am Ende?

Der Düsseldorfer Kreis, die informelle Zusammenkunft der Datenschutzaufsichtsbehörden im nichtöffentlichen Bereich, hat sich am 28./29.04.2010 auf eine Prüfungspflicht für übermittelnde Stellen gegenüber Safe Harbor-Unternehmen in den USA geeinigt und dies am 23.08.2010 bestätigt. Da sich diese Unternehmen gegenüber der Federal Trade Commission (FTC) und europäischen Behörden lediglich selbst zertifizieren, findet eine Prüfung, ob die Safe Harbor-Grundsätze und ein angemessenes Datenschutzniveau eingehalten werden, nicht statt. Daher hat nach Auffassung des Düsseldorfer Kreises das übermittelnde Unternehmen die Pflicht, z.B. die Aktualität der Zertifizierung, die Erfüllung von Informationspflichten gegenüber Betroffenen und die ergriffenen Maßnahmen zur Einhaltung der Safe Harbor-Grundsätze selbst zu prüfen. Dies ist zu dokumentieren und auf Nachfrage den Aufsichtsbehörden nachzuweisen. Bestehen Zweifel an der Einhaltung der Grundsätze, wird die Verwendung der EU-Standardvertragsklauseln empfohlen.

Für deutsche Unternehmen gehen damit der Nutzen des Safe Harbor-Abkommens und die Rechtssicherheit bei der Übermittlung verloren. Die Forderung der Aufsichtsbehörden nach einer institutionellen Kontrolle der Selbstverpflichtungen ist berechtigt, sollte aber besser in eine Änderung des Abkommens statt in neue Prüfpflichten münden.

Happy Birthday Phrack!

Das Hacker-Magazin Phrack, nach Fyodor (Autor von Nmap) "the best, and by far the longest running hacker zine", feierte am 17.11.2010 seinen 25. Geburtstag. Pünktlich zum Termin erschien Heft Nr. 67 – knapp 1,5 Jahre nach Heft 66. Es enthält gewohnt unterhaltsames Material und technisch fundierte Artikel wie "Dynamic Program Analysis and Software Exploitation" oder eine detaillierte Schwachstellenanalyse im ProFTP-Server. Wir freuen uns auf die nächsten 25 Jahre – Thank you, Phrack Staff, and keep up the good work!

Bundesrat zum Datenschutz

Mit seinen umfassenden Änderungsvorschlägen zum Entwurf eines Gesetzes zum Beschäftigtendatenschutz hat der Bundesrat am 05.11.2010 eine erneute Überarbeitung des Gesetzesentwurfs eingefordert. So sollen Beschäftigtendaten enger definiert, auf europäischer Ebene Regelungen zum Konzerndatenschutz angestrebt, durch Verzicht auf ein Übermaß an Verweisen die Lesbarkeit verbessert, eine Löschfrist für die Daten abgelehnter Bewerber eingeführt und ein allgemeines Beschäftigten-Screening nur bei Vorliegen tatsächlicher Anhaltspunkte für das Vorliegen von Straftaten gestattet werden. Eine Änderung der Definition von Dritten soll die Auftragsdatenverarbeitung in EG-Drittstaaten ermöglichen. Die von Datenschützern und den Bundesratsausschüssen geforderte grundsätzliche Einschränkung der dauerhaften Videoüberwachung und der Möglichkeiten zur Abweichung in Tarifverträgen oder Betriebsvereinbarungen zu Ungunsten der Beschäftigten fanden zwar keine Mehrheit. Dennoch wird deutlich, dass der Gesetzentwurf noch einen weiten Weg vor sich hat.

Secorvo News

100 mal Security News

Sie lesen gerade die 100. Ausgabe der Secorvo Security News: 400 Seiten mit fast 1.000 Nachrichten, für Sie selektiert, recherchiert und formuliert, liegen damit hinter uns. Über 6.500 Abonnenten haben die News bis heute gewonnen – mehr als die meisten deutschsprachigen Fachzeitschriften im Gebiet Informationssicherheit und Datenschutz.

Wir würden uns freuen, wenn Sie das Jubiläum zum Anlass nähmen und uns in einem kurzen Kommentar verraten, was Sie uns schon immer einmal sagen wollten. Unter allen Einsendern verlosen wir am 31.01.2011 einen Teilnahme-Gutschein für ein Secorvo-College-Seminar nach Wahl.

Smart Grid Symposium

Am 01.-02.02.2011 sind wir mit einem Symposium zu Datenschutz- und Datensicherheit rund um das „Intelligente Stromnetz“ wieder in der Buhlschen Mühle zu Gast. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2010	
05.-09.12.	AsiaCrypt 2010 (IACR, Singapur/SGP)
06.-07.12.	IsSec/ZertiFA 2010 (Computas, Berlin)
27.-30.12.	27th Chaos Communication Congress (27C3) (Chaos Computer Club, Berlin)
Januar 2011	
18.-20.01.	Omnicard 2011 (inTIME, Berlin)
Februar 2011	
01.-02.02.	Smart Grid Symposium (Secorvo, Ettlingen/KA)
02.-03.02.	21. SIT-SmartCard Workshop (SIT, Darmstadt)
08.-10.02.	CPSSE-Schulung (Secorvo College)
15.-16.02.	18. DFN-Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
März 2011	
01.-05.03.	CeBIT (Deutsche Messe, Hannover)
22.-24.03.	Sicherheitsmanagement heute (Secorvo College)
28.03.-01.04.	T.I.S.P.-Schulung (Secorvo College)

Fundsache

Am 05.02.2010 hat die EU-Kommission eine überarbeitete Fassung der Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (gemäß der EU-Datenschutzrichtlinie) verabschiedet (Amtsblatt der EU L 39/5 vom 12.02.2010), die seit dem 15.05.2010 in Neuverträgen sowie bei Vertragsänderungen zu berücksichtigen sind.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Dezember 2010



Lehren aus Wikigate

Was ist WikiLeaks? Ein Ventil der Entrechteten? Eine Klagemauer der Gutmenschen? Das Fünkchen Hoffnung im universellen Wahnsinn? Oder ein Racheportal für Wichtigtuer? WikiLeaks mag als der Beweisversuch durchgehen, dass sich im Zeitalter des Internet nur wenig auf Dauer vertuschen lässt. Der Zorn des „Establishments“ jedenfalls lässt sich kaum mit der Veröffentlichung der Botschaftsdepeschen erklären, sondern eher durch Publikationen wie der Videoaufnahme aus einem US-Hubschrauber am 05.04.2010, die das Niedermähen von 12 offensichtlich unbewaffneten Zivilisten, darunter zwei Mitarbeiter der Nachrichtenagentur Reuter, am 12.07.2007 in Bagdad zeigt. Unstreitig ist, dass Publikationen dieser Art einseitige Darstellungen korrigieren, dabei aber selbst Gefahr laufen, eine einseitige Sicht hervorzubringen – schließlich kommen diejenigen (Staaten) am besten davon, die besonders gut vertuschen. Dennoch sind solche Internet-Enthüllungen das demokratische Prinzip der „öffentlichen Kontrolle“ in Reinkultur: Müssen Unternehmen und Behörden damit rechnen, dass Fehlverhalten publik wird, werden sie sich konsequenter um die Einhaltung ethischer Standards und rechtlicher Rahmenbedingungen kümmern.

Das eigentliche Wikigate hinter der öffentlichen Aufregung betrifft jedoch einen anderen Punkt: Offenbar hatten mehr als eine Million Personen regulär Zugriff auf die 250.000 Depeschen – sie waren damit schon vorher semi-öffentlich. Sehr viele WikiLeaks-Dokumente wurden von Zugriffsberechtigten enthüllt – die keine Entdeckung fürchten mussten, weil es so viele davon gab. Das ist der wahre Skandal: Wer das „need-to-know“-Prinzip derart großzügig auslegt, sollte sich besser vor (Wirtschafts-) Spionage ängstigen, als nach Whistleblowern zu fahnden. Denn, wie der Politikwissenschaftler Herfried Münkler so treffend in einem Spiegel Essay formulierte: „In der sozialen Welt ist Vertrauen an die Möglichkeit des Geheimnisses gebunden.“ Bevor das Vertrauen weg (und die Kontrolle total) ist, sollten wir wohl lieber erstmal die Zugriffsrechte begrenzen...



Inhalt

Lehren aus Wikigate

Security News

RossLeaks

Nach dem Ende des Internet

Nicht in Wittenberg

SSLiversum – (Un)bekannte Welten

Another one bites the dust

Aufschub für die Bilanzübermittlung

Hintertüren überall

Secorvo News

T.I.S.P. wird Standard

Smart Grid Symposium

Last Call for Feedback

Veranstaltungshinweise

Fundsache

Security News

RossLeaks

Während sich die Welt mit der Sichtung und Sortierung von 250.000 überwiegend irrelevanten Diplomaten-Äußerungen beschäftigt, sucht sich die Wahrheit andere Kanäle. So publizierte Ross Anderson am 24.12.2010 sein Antwortschreiben an die UK Cards Association, die versucht hatte, unliebsame Veröffentlichungen über Schwachstellen des EMV-Verfahrens von der Webseite der Universität Cambridge entfernen zu lassen.

Mit akademischer Eloquenz klärt er in seinem Schreiben zunächst einmal über das Verständnis der Freiheit der Wissenschaft an der „Universität von Erasmus, Newton und Darwin“ auf – und schließt mit dem Hinweis, dass das Vertrauen in Kreditkarten wohl weniger durch die Veröffentlichung, als vielmehr durch die Vertuschung bekannter Schwachstellen unterminiert werde. Eine erquickliche Lektüre zum Jahreswechsel.

Nach dem Ende des Internet

Nicht nur wegen inhaltlicher Regulierungsbestrebungen wie dem Jugendmedienschutz-Staatsvertrag, sondern auch aus technischen Gründen naht das Ende des Internet: Am 30.11.2010 vergab das Internet-Koordinationsgremium IANA vier der letzten elf /8-Blöcke mit je gut 16 Mio. IPv4-Adressen zur Unterverteilung an regionale Adressverwaltungen. Hochrechnungen zufolge werden die restlichen Blöcke bis März 2011 vergeben sein. Dann ist das Internet „voll“.

Es wird also Zeit, den Umstieg auf IP Version 6 vorzubereiten, deren 128-Bit-Adressraum das Internet für die absehbare Zukunft am Leben erhalten dürfte. Eine am 01.12.2010 veröffentlichte Studie von RIPE NCC zeigt jedoch, dass die Übertragung von IPv6 über IPv4-Netze schon rein funktional noch mit erheblichen Kinderkrankheiten zu kämpfen hat. Das lässt Schlimmes für die Sicherheitseigenschaften von IPv6 befürchten. Am 27.12.2010 stellte der Autor des IPv6-Sicherheitstest-Toolkits thc-ipv6 beim CCC-Kongress 27C3 neue Erkenntnisse zu Sicherheitsproblemen von IPv6 vor – trotz der Neuerungen in den Bereichen Multicasts und Source Routing keine guten Nachrichten.

Nicht in Wittenberg

Auf ihrer Webseite hat die Gesellschaft für Informatik (GI) am 01.12.2010 ihre Zehn Thesen zu Sicherheit und Datenschutz im Cloud Computing angeschlagen. Darin werden die Hauptrisiken bei der Nutzung von Cloud Computing kompakt auf den Punkt gebracht. In knapper Form werden viele Baustellen angerissen, die vor einem Einsatz von Cloud Computing sorgfältig bearbeitet werden sollten. Denn die Ausrichtung der IT auf die Cloud erfordert auch in Sicherheitsfragen ein radikales Umdenken. Ergänzt werden die zehn Thesen der GI durch eine umfangreiche Literaturliste zum Thema Sicherheit und Datenschutz beim Cloud Computing.

Umfangreicher werden die relevanten Fragestellungen im 34seitigen Leitfaden für sicheres Cloud Computing des Verbands der deutschen Internetwirtschaft (eco) behandelt, der fast zeitgleich am 02.12.2010 veröffentlicht wurde. Dieser Leitfaden ist auf Anfrage erhältlich. Lediglich der Bitkom schwächelt: Der bereits am 18.09.2009 veröffentlichte, 84seitige Leitfaden Cloud Computing behandelt Datenschutzaspekte auf drei und Sicherheitsfragen auf einer halben Seite – kein rühmliches Bild.

SSLiversum – (Un)bekannte Welten

Nicht erst seit dem Erscheinen von Tools wie Firesheep (SSN 10/2010) ist es empfehlenswert, für den Zugriff auf Internet-Dienste soweit möglich HTTPS zu verwenden. Aber wie vertrauenswürdig sind „blaue“ und „grüne“ TLS-Zertifikate (SSN 06/2007) in den Weiten des Internet wirklich?

Dieser Frage widmet sich das SSL-Observatorium der EFF. Dessen Mitarbeiter stellten am 30.07.2010 auf der Defcon 18 einen Überblick ihrer Beobachtungen vor, den sie am 28.12.2010 beim CCC-Kongress 27C3 aktualisieren werden. Neben dem einer Protonen-Kollision nicht unähnlichen Graphen der ca. 650 (!) CAs, denen gängige Browser vertrauen, findet man im „SSLiversum“ einige Perlen für PKI-Spötter, so etwa CAs in Manchester und New Jersey, die sich ein Schlüsselpaar teilen, Tausende von offiziellen Zertifikaten für „localhost“ oder das Generalschlüssel-Zertifikat für vier Dutzend verschiedene Hosts.

Another one bites the dust

Alle Welt redet bei passender Gelegenheit gern und viel über Sicherheit. Den Worten folgen allerdings oft keine Taten; wenn doch, dann oft solche, auf die man besser verzichtet hätte. Das lässt sich regelmäßig nicht nur beim Gesetzgeber beobachten, sondern auch in der Industrie.

Was die Sache erstaunlich macht, ist, dass dies auch für die Großen gilt – die es eigentlich besser können oder wissen müssten. Unlängst war Canon an der Reihe: Bekanntermaßen lassen sich Digitalbilder heute mittels moderner Bildbearbeitungswerkzeuge so manipulieren, dass gute Collagen kaum noch als solche zu erkennen sind. Canon hatte daher die – an sich gute – Idee, Bilder so zu

authentifizieren, dass ein Fotograf die Echtheit einer Aufnahme nachweisen kann. Die Authentifizierung übernimmt ein (teures) Security-Kit (OSK-E3), das man an die Kamera anschließen kann. Die Funktionsweise des Kits hält Canon geheim – zur Erhöhung der Sicherheit.

Es kam, wie es kommen musste (Mifair lässt grüßen, SSN 3/2008): Das Verfahren wurde analysiert – und am 28.11.2010 von Dmitry Sklyarov öffentlich gebrochen. Die Details sind peinlich: Der Authentifizierungsmechanismus ist keine Signatur, sondern ein „keyed hash", der HMAC-Key ist für alle Kameras eines Modells identisch und in der Kamera gespeichert, und der Hashwert verwendet kein „Salz" – da hält sich das Mitleid in Grenzen. Wie formulierte Bruce Schneier einmal so schön: Geheime Verfahren sind meist solche, deren sich die Hersteller eigentlich schämen müssten… Dmitry Sklyarow meinte launig, Canon sollte vielleicht Leute einstellen, die etwas von Sicherheit verstehen. Kein schlechter Vorschlag – auch für zahlreiche andere Unternehmen (und gelegentlich den Gesetzgeber).

Aufschub für die Bilanzübermittlung

Mit dem Steuerbürokratieabbaugesetz wurde am 20.12.2008 in Gestalt des § 5b EStG eine Verpflichtung buchführender Unternehmen zur elektronischen Übermittlung ihrer Bilanzen und Gewinn- und Verlustrechnungen eingeführt, die bereits für das kommende Wirtschaftsjahr gegolten hätte. Mit Schreiben vom 16.12.2010 hat das Bundesfinanzministerium nun die Pflicht zur elektronischen Bilanz- sowie Gewinn- und Verlustrechnungsübermittlung um ein Jahr auf die ab dem 01.01.2012 beginnenden Wirtschaftsjahre verschoben.

Zunächst sollen ausgewählte Unternehmen freiwillig an einer Pilotphase zum Test des Verfahrens und des amtlich vorgeschriebenen Datensatzes (Taxonomie) teilnehmen.

Die Übermittlung sollte ursprünglich durch einen den Unternehmen zur Verfügung gestellten Client erfolgen, an den diese ihre Schnittstellen anzupassen hätten. Da weder der auf eXtensible Business Reporting Language beruhende Datensatz noch die Client-Spezifikationen bisher abgeschlossen vorliegen und die Entwürfe umfassender Kritik begegneten, wurde nun die Reißleine gezogen. Auch für den um ein Jahr verschobenen Start ist zu befürchten, dass er in großer Eile erfolgen muss; darunter dürfte auch die Sicherheit des Verfahrens leiden.

Vielleicht aber ist von dem Verfahren bis dahin ähnlich wenig übrig, wie heute von der 2002 eingeführten „Elektronischen Steuererklärung mit digitaler Signatur" – im Wesentlichen der Name „Elster".

Hintertüren überall

Gleich drei schwer wiegende Bugs und Hintertüren wurden Mitte Dezember aufgedeckt: Am 14.12. 2010 wurde öffentlich, dass eine Netzwerkspeicherlösung von Hewlett Packard ein nicht dokumentiertes Benutzerkonto mit vollen Zugriffsrechten und Standardpasswort („!admin") besitzt. Am 13.12. 2010 wurde bekannt, dass in der freien SmartCard-Bibliothek OpenSC über einen Pufferüberlauf im Treiber durch bestimmte Seriennummern Code auf dem Zielsystem ausgeführt werden kann.

Schließlich beschuldigte der Gründer des OpenBSD-Projektes, Theo de Raadt, am 14.12.2010 in einer E-Mail ehemalige OpenBSD-Entwickler, im Auftrag des FBI Hintertüren in die VPN-Komponente eingebaut zu haben – vor etwa 10 Jahren. Man könnte sich nun fragen, ob eine Hintertür in einem Open-Source-Projekt tatsächlich so lange unentdeckt bleiben kann – genau das aber hat das Debian-OpenSSL-Debakel (SSN 5/2008) schon vor über zwei Jahren gezeigt. Vor Hintertüren kann man nie sicher sein – weder bei kommerziellen Produkten noch bei freien Projekten.

Secorvo News

T.I.S.P. wird Standard

Seit der Entwicklung des T.I.S.P.-Zertifikats (TeleTrusT Information Security Professional) wurden über 400 Security-Experten mit diesem Qualifikationsnachweis ausgezeichnet. Immer häufiger wird der T.I.S.P. in Unternehmen zum Qualifikationsstandard für alle Mitarbeiter, die mit Aufgaben der Informationssicherheit betraut sind. Mehr als 50 T.I.S.P.-Absolventen, die sich Anfang November in Köln zum diesjährigen T.I.S.P. Community Meeting trafen, bestätigten diesen Trend. Auch 2011 bietet Secorvo College wieder mehrere Gelegenheiten zur Schulung und unabhängigen T.I.S.P.-Zertifizierung.

Smart Grid Symposium

Am 01.-02.02.2011 sind wir mit einem spannenden Symposium zu Datenschutz- und Datensicherheit rund um das „Intelligente Stromnetz" wieder in der Buhlschen Mühle zu Gast. Werfen Sie einen Blick in das Programm – wir freuen uns auf Ihre Teilnahme!

Last Call for Feedback

Noch bis zum 31.01.2011 nehmen Sie anlässlich der 100. Ausgabe der Secorvo Security News mit Ihrem Kommentar zu unseren News automatisch an der Verlosung einer Teilnahme an einem Secorvo College-Seminar Ihrer Wahl teil. Wir freuen uns auf Ihr Feedback – und drücken die Daumen!

Veranstaltungshinweise

Januar 2011	
18.-20.01.	Omnicard 2011 (inTIME, Berlin)
Februar 2011	
01.-02.02.	Smart Grid Symposium (Secorvo, Ettlingen/KA)
02.-03.02.	21. SIT-SmartCard Workshop (SIT, Darmstadt)
08.-10.02.	CPSSE-Schulung (Secorvo College)
15.-16.02.	18. DFN-Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
März 2011	
01.-05.03.	CeBIT (Deutsche Messe, Hannover)
22.-24.03.	Sicherheitsmanagement heute (Secorvo College)
28.03.-01.04.	T.I.S.P.-Schulung (Secorvo College)
April 2011	
04.-06.04.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
07.-08.04.	Datenschutzaudit: Best Practice (Secorvo College)

Fundsache

Erstmals haben sich die Datenschutz-Aufsichtsbehörden mit einem Beschluss des Düsseldorfer Kreises (vom 24./25.11.2010) auf Mindestanforderungen an den Datenschutzbeauftragten festgelegt. Darin werden schon bei Bestellung „umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung“ des relevanten Datenschutzrechts erwartet, dazu „Kenntnisse der Informations- und Kommunikationstechnologie und der Datensicherheit“. Bei externen DSB wird eine Mindestvertragslaufzeit von vier Jahren, bei Erstverträgen von 1-2 Jahren empfohlen.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2011



Hornberger Schießen

Die Reaktionen sind vorhersagbar: CEOs bekommen beim Thema „Cloud Computing“ glänzende Augen, Datenschützer Bauchgrimmen. Hier die erwarteten Einsparungen durch Bedarfsabrechnung statt pauschaler Lizenzkosten, günstige Thin Clients und vorkonfigurierte Software mit zentraler Pflege, dort die Ungewissheit, welche Daten eigentlich wo, wie und von wem verarbeitet werden – unvorstellbar, dass unter solchen Bedingungen eine rechtskonforme Auftragsdatenverarbeitung (schriftlicher Vertrag, Anweisung der Schutzmaßnahmen, Kontrolle des Auftragnehmers) möglich ist.

Tatsächlich sind die Auswirkungen des Cloud Computing-Konzepts schon heute sichtbar. Wer eine Suchmaschine für sich arbeiten lässt, einen Online-Routenplaner nutzt oder seine Kontakte in einem „Social Network“ pflegt, zahlt mit der Preisgabe personenbezogener Informationen. Auch Angreifer dürften sich nicht lumpen lassen und nutzen wahrscheinlich bereits verteilte Rechenpower, wie das Beispiel von Thomas Roth (siehe „Security News“) zeigt.

Bei genauerer Betrachtung werden die Fronten jedoch unscharf. So dürften viele Schutzmechanismen wie Virenschutz, Spam-Abwehr oder Patch-Services bei zentralen Diensten deutlich aktueller und wirksamer sein als in vielen heutigen IT-Infrastrukturen. Umgekehrt würden interne Informationen ungefiltert die Unternehmen verlassen – eine gruselige Vorstellung für die meisten Mittelständler. Dafür stiege der Schutz vor anderen Informationsabflüssen wie dem Verlust mobiler Geräte, wenn Unternehmensdaten nicht mehr lokal gespeichert sondern nur „in der Wolke“ zugänglich wären.

Voraussichtlich wird auch dieser Hype enden wie das Hornberger Schießen: Nach viel aufgewirbeltem Staub werden die Unternehmen versuchen, durch den Aufbau von Private Clouds die Vorteile zentraler Services mit einer kontrollierten Datenverarbeitung zu verknüpfen – nicht zur Freude der Service-Anbieter, die bereits neue Geschäfte wittern.



Inhalt

Hornberger Schießen

Security News

Sandkastenleck

Krypto-Umbruch vertagt

Simples Foto-Tagging

Im Glashaus

Undurchsichtige Wolke

Secorvo News

Smart, smarter, am smartesten

Lesestoff

Neue Seminare

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Sandkastenleck

Gleich am 04.01.1010 hat Billy Riot in seinem Blog zwei Schwachstellen in einer der Sandboxes von Adobes Flash-Player veröffentlicht. Wenngleich die Dokumentation anderes verspricht, ist damit ein Zugriff auf eine lokale URL und so die Übermittlung von Informationen möglich. Bei der Analyse der zweiten Schwachstelle zeigt sich, dass Adobe sich zur Filterung der Protokolle für eine Blacklist entschieden hat. Damit sind alle Protokolle, die für ungefährlich gehalten werden, auch für Zugriffe auf beliebige Systeme im Internet zugelassen. Auf diese Weise lassen sich aus der Flash-Sandbox heraus beliebige Daten an einen Server im Internet übermitteln.

Beunruhigend, dass Adobe auf die von Julia Wolf am 30.12. 2010 in Ihrem Vortrag auf dem Chaos Computer Congress 2010 (27C3) beschriebenen prinzipiellen Schwächen des Dateiformats PDF mit dem Hinweis auf ein Sicherheitsfeature in der aktuellen Version ihres PDF-Readers reagierte: einer Sandbox. Damit hat Adobe schon Erfahrung ...

Krypto-Umbruch vertagt

Der 2005 erschienenen und zuletzt 2007 überarbeiteten NIST SP 800-57 zufolge hätte der 31.12.2010 das Ende aller Kryptoalgorithmen und Schlüssellängen der „80-Bit-Äquivalent"-Klasse markieren sollen: 1024-Bit-RSA und SHA-1 für digitale Signaturen sowie 2-Key-Triple-DES für die Verschlüsselung.

Die damaligen Abschätzungen waren jedoch sehr konservativ - und seither waren keine spektakulären Erfolge bei der Kryptoanalyse zu verzeichnen. So erteilt die am 13.01.2011 erschienene NIST SP 800-131A diesen Algorithmen nochmals drei bzw. fünf Jahre Gnadenfrist. Dazu wurde zwischen „acceptable" und „disallowed" die Kategorie „deprecated" eingeführt – frei übersetzt: „eigentlich sollst Du nicht, aber wenn es partout nicht anders geht und Du Dir über die Risiken im klaren bist ...". Und bei Verwendung des 2-Key-Triple-DES muss nach maximal 8 MByte Daten der Schlüssel gewechselt werden - wie praktikabel das in der Praxis ist, wenn eine Dateilänge dieses Limit übersteigt, sei einmal dahin gestellt.

Zwar richten sich die NIST-Empfehlungen formal nur an US-Bundesbehörden; sie gelten aber gemeinsam mit dem am 22.12.2010 in der Fassung für 2011 erschienenen SigG-Algorithmenkatalog der BNetzA als Referenz für den Stand der Technik bei Kryptoalgorithmen und Schlüssellängen.

Simples Foto-Tagging

... ist das Thema eines auf den ersten Blick unscheinbaren Eintrags vom 16.12.2010 im Facebook-Blog. Als erstes „Soziales Netzwerk" beginnt Facebook damit, im großen Stil biometrische Informationen über seine Mitglieder (und darüber hinaus) zu sammeln: Die Kombination von automatischer Gesichtserkennung und vereinfachter Markierung von Personen in Fotos wird Facebook dank der Beliebtheit des Fotodienstes absehbar mit einer der größten personenbezogenen Bilddatenbanken ausstatten.

Die Datenbank wird allen europäischen Datenschutzbestimmungen zum Trotz auch Aufnahmen von Personen enthalten, die weder der Bereitstellung eines Bildes in Facebook noch der Markierung zugestimmt haben – möglicherweise nicht einmal Nutzer des „Sozialen Netzwerks" sind. Das wird zweifellos Begehrlichkeiten wecken – sofern diese Begehrlichkeiten nicht bereits eins der Motive für diesen Datenbankaufbau darstellen.

Für die Facebook-Nutzer ist dies ein Danaergeschenk, das Erziehungsberechtigte an die Warnung Laokoons in Vergils Aeneis erinnern sollte: „Quidquid id est, timeo Danaos et dona ferentes."[1] Die Geschichte hat ihm Recht (und Schadsoftware einen illustren Namen) gegeben.

Im Glashaus

... sitzend warf der Hamburger Datenschutzbeauftragte Prof. Johannes Caspar am 10.01.2011 mutig mit Steinen: Bei seiner für Google Deutschland zuständigen Datenschutzaufsichtsbehörde stand nach einer Reihe von Beschränkungsforderungen an Street View und dem Entwurf eines auf Google zugeschnittenen neuen BDSG-Paragrafen 4a (SSN 5/2010) nun Google Analytics auf der Agenda.

Bereits am 26./27.11.2009 hatte der Düsseldorfer Kreis einen Entschluss über Zulässigkeitsbedingungen für Trackingdienste (SSN 8/2010) gefasst. Im Wesentlichen wurden darin die verkürzte, anonyme Verarbeitung von IP-Adressen beim Tracking, die Möglichkeit zum Widerspruch und eine ausreichende Information in den Datenschutzerklärungen gefordert.

Da Google dem eher verhalten nachgekommen war, hatte Caspar angekündigt, nun mit Bußgeldern gegen Nutzer von Google Analytics vorgehen zu wollen. Entgangen war ihm jedoch, dass seine eigene Website sowie die der Stadt Hamburg gleich

[1] *Was auch immer es ist, ich fürchte die Danaer und ihre überbrachten Geschenke.*

mehrere nicht gesetzeskonforme Trackingdienste – darunter Google Analytics – verwendete. Nach seiner eher unglücklichen Verteidigung auf der Blogseite des Rechtsanwaltes Stadler ging die Webseite der Aufsichtsbehörde dann „trackerfrei“ offline.

Dem Datenschutz wird diese Komödie nicht gedient haben. Obwohl die Nutzung von Google Analytics weiterhin gegen geltendes Datenschutzrecht verstößt, dürfte glaubwürdigen Maßnahmen der Aufsichtsbehörden damit bis auf weiteres der Boden entzogen sein.

Undurchsichtige Wolke

Das Verlagern von Rechenaufgaben in die Cloud ist nicht nur für Unternehmen ein Thema. Am 10.01.2011 beschrieb Thomas Roth, wie diese „Demokratisierung von Rechenleistung“ genutzt werden kann, um für wenige Euro per Wörterbuchangriff in der Cloud das WLAN-Passwort (WPA-PSK) des Nachbarn zu knacken, und präsentierte auf der Black Hat DC am 19.01.2011 seine „Cloud Cracking Suite“, mit der die Wolke zum Hacker-Tool mutiert.

Zwar verdankte er den schnellen Erfolg beim Nachbarn einem schlecht gewählten Passwort – dennoch wirft der Fall eine wichtige Frage auf: Muss ein Cloud-Anbieter prüfen, zu welchem Zweck sein Kunde die Rechenleistung nutzt? Und falls ja: Wie kann er das beurteilen? Eine ähnliche Frage stellte sich beim SETI@Home und dem inzwischen eingestellten RC5-Wettbewerb. Zwar dürfte jede „missbräuchliche“ Verwendung der Ressourcen in den AGB der meisten Cloud-Anbieter untersagt sein – in der Praxis ist jedoch eine tatsächliche Bewertung der Nutzung unmöglich.

Mit Cloud-unterstützten Angriffen muss daher zukünftig verstärkt gerechnet werden. Das könnte die eine oder andere Annahme über die einem Angreifer typischerweise zur Verfügung stehende Rechenleistung Makulatur werden lassen.

Secorvo News

Smart, smarter, am smartesten

Das „intelligente Stromnetz“ (vulgo: „Smart Grid“) verspricht in vielerlei Hinsicht Vorteile: So sollen sich Spitzen in Stromerzeugung und -abnahme verringern lassen, wodurch wiederum eine gleichmäßigere Bereitstellung von Energie und der Verzicht auf Kraftwerke ermöglicht werden soll.

Doch eine Beeinflussung von Geräten birgt auch enormes Missbrauchspotenzial, wie die Analyse von Lastprofilen, die detaillierte Einblicke in die Vorgänge in einem Haushalt erlauben, bis zur unautorisierten Fernsteuerung elektrischer Geräte.

In seinem Vortrag über Sicherheits- und Datenschutzaspekte des Smart Grid auf dem nächsten KA-IT-Si-Event am 24.02.2011 im Schlosshotel Karlsruhe beleuchtet Klaus J. Müller beide Seiten. Um Anmeldung wird gebeten.

Lesestoff

Nicht nur in den Security News, sondern auch in einschlägigen Fachzeitschriften meldet sich Secorvo regelmäßig zu Wort. So hat sich in den vergangenen Monaten Michael Knopp zu WLAN-Haftung (DuD 9/2010) und der Datenschutzherausforderung Webtracking (DuD 11/2010) geäußert, Dirk Fox zur betriebswirtschaftlichen Bewertung von Security Investments in der Praxis (DuD 1/2011) Stellung genommen und Kai Jendrian und Klaus J. Müller Features und Maßnahmen gegen Browser-Angriffe beleuchtet (iX 2/2011).

In Kürze wird ein Beitrag zu Herausforderungen bei IPv6 von Dr. Safuat Hamdy und Hans-Joachim Knobloch in der <kes> (Ausgabe 1/2011) erscheinen.

Eine Übersicht der mehr als 350 Publikationen von Secorvo finden Sie auf unserer Webseite.

Neue Seminare

Mit dem Thema Web-Anwendungs-Sicherheit erweitern wir ab Frühjahr 2011 unser Seminarangebot. Jedem, der Web-Anwendungen entwirft, entwickelt, spezifiziert, oder prüft bietet das Seminar alles Wichtige über die Bedrohungen, denen Web-Awendungen ausgeliefert sind, sowie Lösungen, die einen verlässlichen Schutz bieten.

Zudem werden relevante rechtliche Rahmenbedingungen und insbesondere Datenschutzaspekte beleuchtet. Am 12. und 13.04.2011 startet das Seminar „Verlässliche Web-Anwendungs-Sicherheit“.

Ab diesem Jahr werden die unabhängige Prüfung und Zertifizierung zum T.I.S.P. (TeleTrusT Information Security Professional) vom TÜV PersCert durchgeführt, einem Tochterunternehmen des TÜV Rheinland. Die nächste T.I.S.P.-Schulung und -Prüfung bieten wir vom 23.03. bis 02.04.2011 an.

Programme und Online-Anmeldung aller Seminare unter http://www.secorvo.de/college.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2011	
01.-02.02.	Smart Grid Symposium (Secorvo, Ettlingen/KA)
02.-03.02.	21. SIT-SmartCard Workshop (SIT, Darmstadt)
08.-10.02.	CPSSE-Schulung (Secorvo College)
15.-16.02.	18. DFN-Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
März 2011	
01.-05.03.	CeBIT (Deutsche Messe, Hannover)
22.-24.03.	Sicherheitsmanagement heute (Secorvo College)
28.03.-01.04.	T.I.S.P.-Schulung (Secorvo College)
April 2011	
04.-06.04.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
07.-08.04.	Datenschutzaudit: Best Practice (Secorvo College)
12.-13.04.	Datenschutztage 2011 (FFD Forum für Datenschutz, Frankfurt)
Mai 2011	
10.-13.05.	Public Key Infrastrukturen (PKI) (Secorvo College)

Fundsache

Das US-amerikanische NIST hat dem Thema Datenschutz und Datensicherheit beim Cloud Computing ein 60seitiges Dokument gewidment: „Guidelines on Security and Privacy in Public Cloud Computing“, erschienen am 28.01.2011 als SP 800-144 (Draft) zur Kommentierung.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2011



Falsche Freunde

Im Englischen nennt man sie „false friends“. Wörter einer Fremdsprache, die einem Wort der Muttersprache phonetisch oder orthografisch ähneln, aber eine gänzlich andere Bedeutung besitzen, und so zu falschen Übersetzungen verleiten. So z. B. *become* (nicht bekommen, sondern werden), *sensible* (nicht sensibel, sondern fühlbar) oder *pathetic* (nicht pathetisch, sondern erbärmlich).

Ein ähnliches Phänomen lässt sich in der Informationssicherheit beobachten. Damit sind weniger die verbreiteten begrifflichen Unschärfen („persönliche Daten“) oder unterschiedlichen Definitionen von Sicherheit (*safety* versus *security*) gemeint, die gelegentlich zu Missverständnissen führen. Weit schlimmer sind Schutzmaßnahmen, die manchmal sogar Profis ein „Sicherheitsgefühl“ vermitteln – aber im Kern teure potemkinsche Dörfer sind.

So ist es heute in größeren Unternehmen üblich, den Gebäudezugang durch Betriebsausweise mit Foto zu kontrollieren. Tatsächlich werden die Fotos jedoch selten aktualisiert und oft sogar bei der Neuausgabe von Ausweisen wieder verwendet. Konsequenterweise überprüft das Sicherheitspersonal Ausweisfotos gar nicht erst auf Übereinstimmung mit dem Gesicht des Trägers. Zumeist genügt daher ein selbst gebastelter Pappausweis mit beliebigem Passfoto, um Zugang zu erhalten. Verhindert eine elektronische Schranke den unberechtigten Zugang, hilft ein großer Trolley (oder Rollstuhl), damit der „barrierefreie Zugang“ bereitwillig entriegelt wird.

Am Rechnerarbeitsplatz finden sich dann weitere Angriffserleichterungen: Die (ohnehin oft mickrige) Passwortlänge wird durch die Erzwingung regelmäßiger Wechsel effektiv weiter verringert – schließlich werden die letzten Stellen als Folgezähler benötigt (was den Zweck des Passwortwechsels konterkariert). Nicht selten gelingt eine Passwortrücksetzung durch Anruf beim Helpdesk – häufig wird dies durch keine wirksame Anruferauthentisierung verhindert.

Es wäre nicht nur billiger, auf derartigen Schein-Schutz zu verzichten. Denn die Illusion von Sicherheit reduziert die Wachsamkeit.



Inhalt

Falsche Freunde
Security News
Vorgedacht
Nachgedacht
Zu kurz gedacht
Umgedacht
Kompliziert gedacht
Neu gedacht
Speziell gedacht
Zu Ende gedacht
Secorvo News
Grundlagenseminare ...
... und der T.I.S.P.
Sicherheit von IPv6
Veranstaltungshinweise
Fundsache

secorvo
security consulting

Security News

Vorgedacht

Im vergangenen Jahr war es der Datenschutz, der Bewegung in das Thema Smart Metering brachte - nun rückt auch die Datensicherheit in den Fokus. Am 28.01.2011 stellte das BSI einen ersten Entwurf eines Schutzprofils für die Kommunikationseinheit des Messsystems vor, das auch auf dem Smart Grid Symposium in Ettlingen diskutiert wurde. Die Planung sieht vor, das Schutzprofil noch im Jahr 2011 fertig zu stellen.

Da Smart Grids in den USA vor allem eine höhere Robustheit und Netzverfügbarkeit bewirken sollen, genießen Sicherheitsfragen in der amerikanischen Diskussion einen sehr hohen Stellenwert. So hat das NIST bereits im September 2010 600seitige „Guidelines for Smart Grid Cyber Security" (aktuelle Fassung vom 25.10.2010) veröffentlicht. Es wäre zu begrüßen, wenn sich die darin enthaltenen Überlegungen und Erkenntnisse auch im deutschen Schutzprofil wiederfänden.

Nachgedacht

Der Bundesgerichtshof hat am 13.01.2011 über die derzeitige Praxis der Access-Provider zur ca. einwöchigen benutzerbezogenen Speicherung der IP-Adresszuordnung (Urteilsbegründung vom 08.02.2011) entschieden. Nach dem Telekommunikationsgesetz (TKG) bestehen zwei Rechtfertigungsmöglichkeiten: die Speicherung zu Abrechnungszwecken (§ 97 Abs. 1 S. 1, Abs. 2 Nr. 1 TKG) und die Speicherung zur Störungsanalyse und -beseitigung (§ 100 Abs. 1 TKG). Der BGH hat nun deutlich gemacht, dass die Geeignetheit und Erforderlichkeit der Speicherung zu beiden Zwecken detailliert unter Beweis zu stellen ist. Die Instanzgerichte hatten die Erforderlichkeit und mögliche Alternativen gar nicht erst geprüft und eine diesbezügliche Beweislast des beklagten Telekommunikationsunternehmens verneint.

Tatsächlich bestehen begründete Zweifel, denn auch einzeln abzurechnende Dienste innerhalb einer Flatrate rechtfertigen keine generelle Speicherung zu Abrechnungszwecken. Die Begründungen für eine Speicherung zur Störungsbeseitigung beziehen sich bislang überwiegend auf die Störerermittlung bei SPAM- oder DoS-Attacken – dabei ist eine Speicherung jedoch nur für eine anschließende Rechtsverfolgung erforderlich. Ob diese von § 100 Abs. 1 TKG erfasst wird, ist äußerst fraglich. Nun ist das OLG Frankfurt am Zug. Die Prüfanforderungen zur Begründung von IP-Adressspeicherungen sind mit dem Urteil jedoch deutlich schärfer geworden.

Zu kurz gedacht

Die am 26.01.2011 von Alex Rice im Facebook-Blog vorgestellte Reaktion auf Session-Hijacking-Angriffe, die mit Tools wie Firesheep (SSN 10/2010) einfach durchzuführen sind, erweitert das Benutzerprofil um die Option „Facebook mit einer sicheren Verbindung (https) durchstöbern, wenn möglich". Nach Aktivierung werden dann nicht nur die Login-Daten mit SSL geschützt an Facebook übertragen, sondern alle Daten, inklusive des Session-Cookie.

So weit, so gut. Was is aber mit „wenn möglich" gemeint? Da nicht alle Facebook-Apps den Umgang mit gesicherten Verbindungen beherrschen, erhält ein Benutzer beim Zugriff auf eine solche App den Warnhinweis: „Es tut uns leid, aber wir können diese Inhalte nicht anzeigen, während du Facebook über eine sichere Verbindung (https) benutzt. Um diese Anwendung nutzen zu können, musst du zu einer regulären Verbindung (http) wechseln." Das wäre verschmerzbar – wenn das Wechseln auf eine ungeschützte Verbindung temporär erfolgen würde. Tatsächlich schaltet Facebook in diesem Fall die Option zum sicheren Surfen dauerhaft ab.

Umgedacht

Mit der verantwortungsvollen Veröffentlichung von Schwachstellen (Stichwort „responsible disclosure") beschäftigt sich die vom Intrusion Detection Hersteller Tipping Point (HP) betriebene Zero Day Initiative (ZDI) seit ihrer Gründung. Die Kernidee ist, dass festgestellte Schwachstellen zuerst dem Hersteller gemeldet werden, um diesem Zeit zu geben, Gegenmaßnahmen zu ergreifen oder einen Patch bereit zu stellen. Danach erst wird die Schwachstelle öffentlich gemacht. Vorausgesetzt wird dabei, dass die betroffenen Hersteller ein Interesse daran haben, gefundene Schwachstellen umgehend zu beheben. Dass dies nicht immer der Fall ist, zeigt eine am 06.02.2011 von Sami Koivu veröffentlichte Schwachstelle, die er bereits 2008 an Sun gemeldet hatte – und die bis heute nicht behoben wurde.

Die Zero Day Initiative verfolgt daher nun ein „responsible disclosure mit Ultimatum": Festgestellte Schwachstellen werden nach 180 Tagen veröffentlicht, unabhängig davon, ob ein Patch verfügbar ist – zum einen, um betroffene Nutzer möglichst frühzeitig über vorhandene Schwachstellen zu informieren, und zum anderen, um den Druck auf die Hersteller zu erhöhen. Von den aktuellen Veröffentlichungen sind unter anderem Adobe (Acrobat Reader, Flashplayer), Microsoft (Visio, Powerpoint, Excel), EMC, CA, Hewlett-Packard und IBM (Lotus Notes) betroffen. Betroffenen Nutzern empfehlen wir bis zur Bereitstellung von Updates temporär zusätzliche Schutzmaßnahmen.

secorvo
security consulting

Kompliziert gedacht

Die SHA-2 Familie bekommt Zuwachs: Neben den beiden unterschiedlichen Algorithmen SHA-256 und SHA-512 definiert FIPS 180-3 vom 17.10.2008 (SSN 10/2008) den SHA-224 als SHA-256 mit unterschiedlichem Initialwert, dessen Ausgabe auf 224 bit gestutzt wird, und SHA-384 als auf 384 Ausgabebits zurechtgestutzten SHA-512, auch diesen mit abweichendem Initialwert.

Der am 11.02.2011 vom NIST veröffentlichte Draft FIPS 180-4 ergänzt nun entsprechend zurechtgestutzte Versionen des SHA-512 als SHA-512/224 und SHA-512/256. Interessanterweise wird als Begründung für die neuen Familienmitglieder nicht die höhere Sicherheit angeführt, sondern die Tatsache, dass SHA-512 mit 80 Runden auf 64-Bit-Prozessoren schneller ist als der für 32-Bit-Architekturen entworfene SHA-256 mit 64 Runden. Einfach ist anders.

Neu gedacht

Dass Linux-Systeme nicht „per se" sicherer sind als Windows-Systeme zeigen die inzwischen zahlreichen Sicherheitswarnungen und Patches zu den verschiedenen Distributionen. Allerdings hält sich hartnäckig die Überzeugung, dass Windows-Systeme der Ergonomie Vorzug vor der Sicherheit geben und daher – wie bei der Autorun-Funktion von DVD und USB-Sticks – mehr Einfallstore bieten. Tatsächlich wurden solche Einfallswege durch Softwareupdates inzwischen weitgehend dicht gemacht.

Für Linux-Systeme gilt das offenbar nicht, wie Jon Larimer auf der Shmoocon am 30.01.2011 nachwies. Das Einstecken eines USB-Sticks genügt, um beispielsweise über Schwachstellen im Dateisystemtreiber oder (wie im konkreten Fall) des GNOME Filemanagers „Nautilus" Schaden zu stiften – sogar bei aktivierter Bildschirmsperre. Dagegen hilft nur, das automatische Mounten von Wechseldatenträgern manuell zu deaktivieren.

Speziell gedacht

Am 14.02.2011 erschienen gleich drei neue (Web)-Application-Firewalls: OpenWAF, IronBee und Oracle Database Firewall. Bei OpenWAF und IronBee handelt es sich um Open-Source-Lösungen von Herstellern mit Erfahrung – OpenWAF ist aus dem kommerziellen Hyperguard entstanden, IronBee entstammt der Feder von Ivan Ristic, dem Autor von mod_security. Oracles Lösung soll SQL-Datenbanken aller Art vor Angriffen schützen.

So schön die Verfügbarkeit dieser Schutzlösungen ist, drängt sich die Frage auf, wie viele Produkte eigentlich noch hintereinander geschaltet werden müssen, um einen ausreichenden Schutz von Anwendungen zu erreichen? Viel wichtiger wäre es wohl, Hersteller und Entwickler in die Lage zu versetzen, sichere Anwendungen auszuliefern, die nicht auf zusätzlichen Schutz angewiesen sind.

Zu Ende gedacht

Aufgrund der positiven Erfahrungen beim Betrieb des DNSSEC Testbeds (SSN 01/2010) kündigte DENIC am 08.02.2011 an, dass ab dem 31.05.2011 auch für die produktive .de-Zone DNSSEC eingeführt werden wird. Passend dazu gaben bei einer am 18.02.2011 präsentierten Studie von eco e.V. und VeriSign 61 % der befragten deutschen Domain-Anbieter an, DNSSEC bereits anzubieten oder innerhalb der kommenden zwölf Monaten anbieten zu wollen.

Viele Domaininhaber dürften in Bälde zur sichereren Version von DNS übergehen. Unternehmen und Organisationen können also demnächst ihre DNS-Resolver am Übergang zum Internet DNSSEC-Signaturen prüfen lassen.

Secorvo News

Grundlagenseminare ...

Am 22.03.2011 startet die zweiteilige Seminarreihe „Grundlagen" mit dem dreitägigen Seminar Sicherheitsmanagement heute, einer Einführung in alle wesentlichen Bereiche des Informationssicherheitsmanagements. Mitte Mai folgt Teil zwei mit dem ebenfalls dreitägigen Seminar IT-Sicherheit heute.

... und der T.I.S.P.

Experten in Sachen Informationssicherheit bietet das einwöchige T.I.S.P.-Seminar ab 28.03.2011 mit einer Kombination aus Schulung und zertifizierter TÜV-Prüfung einen aussagekräftigen und weithin anerkannten Kompetenznachweis.

Die Programme aller Seminare und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Sicherheit von IPv6

Anlässlich der bevorstehenden Ausschöpfung des Adressraums von IPv4 haben sich Dr. Safuat Hamdy und Hans-Joachim Knobloch mit den Herausforderungen und Sicherheitsrisiken von IPv6 auseinander gesetzt. Die Ergebnisse ihrer Überlegungen sind nachzulesen in der aktuellen Ausgabe der Zeitschrift <kes> (Seiten 11-16).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2011	
01.-05.03.	CeBIT (Deutsche Messe, Hannover)
22.-24.03.	Sicherheitsmanagement heute (Secorvo College)
28.03.-01.04.	T.I.S.P.-Schulung (Secorvo College)
April 2011	
04.-06.04.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
07.-08.04.	Datenschutzaudit: Best Practice (Secorvo College)
12.-13.04.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College)
Mai 2011	
10.-13.05.	Public Key Infrastrukturen (PKI) (Secorvo College)
10.-12.05.	12. Deutscher IT-Sicherheitskongress (BSI, Bonn)
17.-20.05.	12. Datenschutzkongress (Euroforum, Berlin)
24.-27.05.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)

Fundsache

Die internationale SAFECode-Initiative, die sich der Erhöhung der Vertrauenswürdigkeit informationstechnischer Systeme durch die Verbesserung und Verbreitung von Methoden sicherer Sofware-Entwicklung verschrieben hat, und in der sich neben EMC, Juniper und Microsoft insbesondere die SAP AG stark engagiert, veröffentlichte am 08.02.2011 die zweite Auflage der Fundamental Practices for Secure Software Development. Das 56 Seiten starke Dokument enthält praxiserprobte Prinzipien und Empfehlungen für Design, Programmierung und Tests.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

März 2011



Krisenmanagement

Die entsetzliche Naturkatastrophe in Japan hat die Industrienationen dieser Welt in einen Schockzustand versetzt. Mehr noch als die gerne verdrängte Einsicht, dass lange drohende Naturkatastrophen eben doch eines Tages eintreten, erschreckt die Erkenntnis, dass das Krisenmanagement eines so hoch entwickelten und in Qualitätsfragen vorbildlichen Landes wie Japan geradezu hilflos wirkt.

So hielten die Hochhäuser dank präventiver Maßnahmen dem gewaltigen Erdbeben der Stärke 9 stand, nachdem das mit 20 Sekunden deutlich kürzere und schwächere Beben der Stärke 7 vor 16 Jahren in Kobe Häuser und Brücken wie Streichhölzer einknicken ließ.

Die Notfallvorsorge hingegen versagte. Stimmen die Berichte, dann haben Mängel in der Versorgung der Überlebenden des gigantischen Tsunami weitere Todesopfer gekostet. Angesichts der Kritik am Krisenmanagement nach der Kobe-Katastrophe erscheint dies wie ein Déjà-vu. Inzwischen ist zudem bekannt, das der Betreiber des havarierenden Kernkraftwerks zahlreiche Inspektionen versäumt hatte – darunter die des Kühlsystems. Möglicherweise waren die Notstromaggregate also bereits vor dem Tsunami defekt.

Notfallvorsorge bedeutet, sich auf den Umgang mit einem Ereignis vorzubereiten, dessen Eintritt man zugleich durch präventive Maßnahmen zu verhindern sucht. Das ist ein „mentaler Spagat", der oft zu Lasten der Notfallvorsorge ausgeht, da Menschen dazu neigen, die Wirksamkeit ihrer präventiven Maßnahmen zu überschätzen – weil „nicht sein kann, was nicht sein darf".

Dafür gibt es auch in der IT-Sicherheit zahlreiche Beispiele – wie Backup-Bänder, deren Rückspielbarkeit nicht regelmäßig überprüft wird oder Notfallpläne, die auf falschen Annahmen beruhen (wie der Verfügbarkeit von Strom, Telefon oder Internet). Zwar geht es hier meist nicht um „Leib und Leben". Dennoch gilt: Wer die Krisenreaktion nicht übt, wird sie im Ernstfall nicht beherrschen.



Inhalt

Krisenmanagement

Security News

Datenschutzkonformes Webtracking

Legalisierte PIN-Weitergabe?

Desaster I

Desaster II

Schwierige Trennung

Rückkehr der Dialer

Secorvo News

PKI lesen und erleben

Alle IT-Sicherheit geht von Karlsruhe aus

SSN-Symposium

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Datenschutzkonformes Webtracking

Wer die Zugriffsstatistiken seiner Webseitenbesucher datenschutzkonform auswerten wollte, musste sich lange Zeit mühen, eine brauchbare Alternative zu Google Analytics zu finden. Zwar hat Google als Reaktion auf den „Bann" der deutschen Aufsichtsbehörden (SSN 08/2010) im vergangenen Jahr eine Möglichkeit geschaffen, IP-Adressen der Seitennutzer so zu kürzen, dass sie nicht mehr zurückverfolgt werden können. Die Datenverarbeitung in den USA ohne angemessenen Schutz verhinderte jedoch nach wie vor einen rechtskonformen Einsatz in Deutschland. Die Datenschutz-Aufsichtsbehörden nahmen dies zum Anlass, den Einsatz von Google Analytics und anderer Tracking-Tools zunehmend abzumahnen – nicht immer mit glücklicher Hand (SSN 01/2011).

Als Alternative zu Google Analytics wird seit einer Weile das Open-Source-Tool PIWIK diskutiert. Für einen datenschutzkonformen Einsatz muss es allerdings angepasst werden – und genau dafür hat am 15.03.2011 das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) nach einer aufsichtsbehördlichen Analyse eine Arbeitshilfe publiziert. Unternehmen, die weiterhin Google Analytics auf ihren Webseiten nutzen, haben nun nicht einmal mehr eine schlechte Ausrede, wenn sie ein Bußgeldbescheid der Aufsichtsbehörde erreicht.

Legalisierte PIN-Weitergabe?

Am 09.03.2011 hat das Bundeskartellamt nach Auskunft der Payment Network AG eine Stellungnahme zu der am Landesgericht Köln anhängigen Klage der Giropay GmbH abgegeben. Darin wirft Giropay dem Betreiber von sofortüberweisung.de wettbewerbswidriges Verhalten durch die Anstiftung zum Verstoß gegen die Muster AGB der Banken vor. Hintergrund ist das in diesen AGB verankerte Verbot, die Authentifizierungsmittel für das Online-Banking (Login-ID, PIN und TAN) an Dritte weiterzugeben. Genau dies ist jedoch erforderlich, um im Rahmen von Internetgeschäften eine von sofortüberweisung.de unterstützte, in den Kaufprozess eingebundene Überweisung vorzunehmen. Das Bundeskartellamt sieht nach den eingeleiteten Ermittlungen Hinweise darauf, dass durch das Verbot der Weitergabe der Authentisierungsmittel bankenunabhängigen Direktüberweisungsverfahren der Marktzutritt verwehrt wird.

Noch ist offen, wie das LG Köln und die vermutlich folgenden Instanzen den Sachverhalt bewerten werden. Allerdings erscheint fraglich, dass das Bundeskartellamt die Klausel der AGB in ihrer Bedeutung richtig erfasst hat. Für die Sicherheit des Online-Bankings ist die Geheimhaltungsklausel berechtigt, und es darf bezweifelt werden, dass ein Geschäftsmodell, das die Herausgabe der für einen persönlichen Authentisierungsprozess verwendeten Geheimnisse an Dritte erfordert, überhaupt kartellrechtlichen Schutz genießen kann.

Desaster I

Mehrere Security-Unternehmen wurden in den vergangenen Wochen Opfer von viel beachteten Angriffen. Dabei betreffen die Angriffe auf RSA und Comodo auch die Sicherheit der Kunden und weiterer Anwender.

RSA – Hersteller der SecurID Einmalpasswort-Token und inzwischen Teil von EMC – teilte am 17.03.2011 mit, dass das Unternehmen Opfer eines längerfristigen gezielten Angriffs (Neusprech: APT) geworden war. Aus der Mitteilung geht hervor, *dass* ein Schaden für SecurID eingetreten ist – lässt aber offen, *worin* dieser genau besteht und *wie* er sich auswirkt. Dem Vernehmen nach informiert RSA derzeit seine großen Kunden einzeln und unter NDA über Details. Spekulationen zufolge könnte zumindest ein Teil der Datenbank mit den Seed-Werten, aus denen sich alle One-Time-Passwörter aller registrierten Token rekonstruieren lassen, den Angreifern in die Hände gefallen sein. Dann würde nur noch ein Austausch der betroffenen Token helfen.

Desaster II

Am 15.03.2011 wurde eine für die Prüfung von SSL-Zertifikatsanträgen zuständige Registration Authority (RA) der von Comodo (Claim: „Creating Trust Online") betriebenen CA UTN-UserFirst-Hardware kompromittiert. Der vorgeblichlich iranische Angreifer konnte mit deren Zugangsdaten fingierte Zertifikate für Domains wie Google.com und Yahoo.com beziehen – ein Blankoscheck für Phisher. Comodo informierte am 23.03.2011 darüber und veröffentlichte den zugehörigen Incident Report.

Bereits zuvor hatten viele Browserhersteller Patches erstellt, um die falschen Zertifikate unabhängig von den üblichen PKI-Sperrmechanismen zurückzuweisen. Besondere Übung hierin hat Microsoft, das bereits seit 22.03.2001 zwei fingierte „Microsoft Corp." Code-Signing-Zertifikate auf diese Weise aus Windows aussperrt. Falls die Angreifer allerdings wie behauptet noch weitere, nicht identifizierte Zertifikate oder Zugangsdaten erbeutet haben, bliebe letztlich nur, die betroffenen CAs komplett als Vertrauensanker zu entfernen – mit unschönen Konsequenzen auch für alle legitimen Zertifikate.

Beide Fälle belegen, dass selbst in sicherheitskritischen Branchen noch nicht alle Unternehmen ver-

standen haben, dass das langfristige Vertrauen von Kunden und Anwendern in einem solchen Fall nur mit Offenheit, Kulanz und schneller Schadensbegrenzung zurück gewonnen werden kann – und nicht mit vagen Andeutungen, Geheimniskrämerei oder Verharmlosung. Gerade von Anbietern im Bereich der IT-Security sollte man zudem erwarten dürfen, dass sie Notfallpläne für „ihr" Worst-Case-Szenario in der Schublade liegen haben.

Schwierige Trennung

Am 23.03.2011 hat das Bundesarbeitsgericht die vorangegangenen Urteile zum Umfang des Kündigungsschutzes eines betrieblichen Datenschutzbeauftragten bestätigt. Kern des Streits war der gesetzliche Kündigungs- und Widerrufsschutz des betrieblichen Datenschutzbeauftragten aus den §§ 4f Abs. 3 BDSG, 626 BGB einerseits und das Bestreben eines Unternehmens, konzernweit einen einheitlichen externen Datenschutzbeauftragten statt des internen zu etablieren andererseits. Sämtliche Instanzen haben den Wunsch nach einer Neuorganisation des Datenschutzes ebenso wie mögliche Konflikte durch die gleichzeitige Zugehörigkeit zum Betriebsrat nicht als wichtigen Grund gemäß § 626 BGB anerkannt.

Wie das klagende Unternehmen zu Recht vorgetragen hat, hat diese – auch schon zuvor in der einschlägigen Literatur vertretene – Rechtsauffassung zur Folge, dass ein unbefristet bestellter interner Datenschutzbeauftragter ohne sein Mitwirken praktisch nicht mehr abgelöst werden kann.

Rückkehr der Dialer

Bei der Sicherheit von VoIP wird der Fokus gern auf Vertraulichkeit, Integrität und Authentizität gelegt. Diese Sicherheitsziele sind meist jedoch weniger kritisch, solange VoIP nur hausintern betrieben wird. Eine erhebliche Gefahr ist hingegen der Gebührenbetrug. Durch die Vereinigung von Daten- und TK-Netzen werden Angriffe möglich, die die längst totgeglaubten Dialer wieder zum Leben erwecken. Insbesondere Softphones sind stark gefährdet.

So berichtete Mark Collier am 09.03.2011 in seinem VoIP Security Blog von einem Fall, in dem durch die Installation von Dialern acht Millionen US-Dollar „erwirtschaftet" wurden. Der Urheber dieses Betruges wurde ermittelt und zu sieben Jahren Haft verurteilt. Solche Dialer können lange unbemerkt bleiben, wenn der Betrüger nicht zu gierig wird, denn gelegentliche kurze Anrufe an Servicenummern dürften in der Praxis kaum auffallen.

Bei Softphones kommen zudem zwei Angreiferwelten zusammen: Sofern es die Browser-Konfiguration zulässt, wird ein SIP-URI in einem HTML-Dokument an das Softphone weitergereicht – ein Himmelreich für Phisher. Von solchen Angriffen sind auch Smartphones betroffen, wie ein am 28.02.2011 bekannt gewordenes Android-App belegt.

Angesichts der geringen Aufmerksamkeit für diese Bedrohung steht zu befürchten, dass die schmerzlichen Lektionen mit herkömmlichen Endgeräten ignoriert und erneut gelernt werden müssen.

Secorvo News

PKI lesen und erleben

Seit dem 01.03.2011 stehen auf der Secorvo-Webseite zwei neue Whitepaper zum Download bereit: Eine Einführung in „Public Key Infrastrukturen" von Petra Barzin und eine Schritt-für-Schritt-Anleitung zur Realisierung einer „PKI von der Stange" von Hans-Joachim Knobloch. Vom **10.–13.05.2011** können Sie auf dem viertägigen Secorvo College Seminar „PKI – Grundlagen, Vertiefung, Realisierung" beide Autoren persönlich kennen lernen. Sie bieten Ihnen einen detaillierten und praxisorientierten Einblick in Konzeption, Implementierung und Nutzung von PKIs.

Alle IT-Sicherheit geht von Karlsruhe aus

Vor mehr als 25 Jahren wurden an der Universität Karlsruhe – dem heutigen KIT – die ersten Vorlesungen zu Kryptographie, technischem Datenschutz und Informationssicherheit in Deutschland gehalten. Zahlreiche Lehrstühle an deutschen Hochschulen und Unternehmen im Gebiet IT-Sicherheit haben ihre Wurzeln in Karlsruhe, ebenso wie das „Europäische Institut für Systemsicherheit (EISS)".

Am 28.02.2011 wurde das EISS/KIT vom Bundesforschungsministerium zum „**K**ompetenzzentrum für **a**ngewandte **S**icherheits-**Te**chno**l**ogie" ernannt. Was KASTEL in der Zukunft zur IT-Sicherheit in und aus der Region Karlsruhe beitragen wird, stellt Prof. Dr. Jörn Müller-Quade, Leiter des EISS, auf dem kommenden KA-IT-Si-Event am **14.04.2011** vor. Beginn: 18 Uhr im Schlosshotel Karlsruhe, mit anschließendem Buffet-Networking (Anmeldung).

SSN-Symposium

Nach dem überschwänglichen Feedback zu unserem „Security News Symposium" im vergangenen Jahr freuen wir uns, Sie heute zu unserem zweiten SSN-Symposium am **31.05.–01.06.2011** in die Buhlsche Mühle einladen zu können – mit spannenden Vorträgen und Diskussionen zu Security- und Datenschutzfragen rund um VoIP, IPv6, Webtracking, Skimming und Online-Banking. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2011	
12.-13.04.	a-i3/BSI-Symposium 2011 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
Mai 2011	
10.-13.05.	Public Key Infrastrukturen (PKI) (Secorvo College)
10.-12.05.	12. Deutscher IT-Sicherheitskongress (BSI, Bonn)
12.-15.05.	Swiss Cyber Storm 3 Security Conference (Compass Security AG, Rapperswil/CH)
17.-20.05.	12. Datenschutzkongress (Euroforum, Berlin)
24.-27.05.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)
31.05.-01.06.	2. Security News Symposium (Secorvo, Karlsruhe/Ettlingen)
Juni 2011	
06.-07.06.	DuD 2011 (Computas, Berlin)
06.-11.06.	T.I.S.P.-Schulung und -Prüfung (Secorvo College)
06.-11.06.	OWASP Global AppSec Europe (OWASP Foundation, Dublin/IE)
28.-30.06.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)

Fundsache

Anfang März publizierte das US-amerikanische NIST die 88seitige Special Publication 800-39 zum Thema „Managing Information Security Risk“ – ein lesenswerter systematischer und aktueller Überblick.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Karin Schuler

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

April 2011



Anonyme Kontrolle

Der eine oder andere „Datenschutzaufreger" mutet schon etwas skurril an. So wissen wir jetzt, dass der Navigationsgerätehersteller TomTom Daten über Streckendurchschnittsgeschwindigkeiten (die aus den Fahrdaten von TomTom-Kunden errechnet werden, um möglichst realistische Fahrzeiten zu prognostizieren) niederländischen Behörden zugänglich macht, um diesen die Beseitigung von Engpässen und Stauabschnitten zu erleichtern. Die niederländische Polizei nutzte diese Daten unerwartet kreativ: Sie platzierte Radarfallen an Stellen, an denen die von TomTom bestimmten Durchschnittswerte über der örtlichen Geschwindigkeitsbegrenzung lagen. (Vielleicht hatte sie den Datenschutzbericht der Telekom gelesen.)

Aus der Perspektive des Steuerzahlers und Bürgers ist das eine sehr vernünftige Maßnahme: höchste Wirtschaftlichkeit der Geschwindigkeitskontrollen, wirksame Erhöhung der Verkehrssicherheit in kritischen Straßenabschnitten – und datenschutzrechtlich nicht zu beanstanden, da lediglich mit Zustimmung der Nutzer erstellte anonyme Statistiken verwendet wurden. Dennoch ist die Aufregung groß. Das mag daran liegen, dass TomTom-Nutzer den Eindruck gewonnen haben, dass sie mit ihrer Zustimmung zur Datenerhebung der Polizei die Ahndung eigener Verkehrsdelikte erleichtern.

Vielleicht aber versteckt sich hier ein sehr grundsätzliches Datenschutzproblem, das das geltende Recht nur unzureichend erfasst. Denn auch anonyme Statistiken – nach Definition gerade keine personenbezogenen Daten – können die freie Entfaltung beeinträchtigen. So könnten Stadtwerke in Abhängigkeit vom Mietniveau eines Wohnbezirks entscheiden, ob sie bei Zahlungsverzug den Kunden erst anrufen oder lieber gleich zwei kräftige Ableser vorbeischicken. Versandhändler könnten Bestellungen aus Städten mit hoher Arbeitslosigkeit ablehnen, um Zahlungsausfälle zu minimieren. Und Anbieter von Pillen gegen Harndrang könnten die Plakatierung in Gegenden verstärken, in denen die Smart Meter gehäuft nächtliche Toilettengänge registrieren. Schöne neue Welt.



Inhalt

Anonyme Kontrolle

Security News

Ein Goldchip ist keine Silberkugel

Erhöhtes Grundrauschen

Datenschutz zum Anfassen

Virencheck-Check

GPS-Daten in Smartphones

Personalausweis im Test

Smart Meter – mit Sicherheit

Secorvo News

Lizenz zum Entwickeln

Security News Symposium 2011

DuD 2011

College-Seminare

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Ein Goldchip ist keine Silberkugel

Zu Jahresbeginn forderte das BKA, zum Schutz gegen Skimming-Angriffe an Geldautomaten endlich komplett vom Magnetstreifen auf den EC-Karten-Chip umzusteigen. Bereits am 11.02.2010 hatten britische Forscher der BBC demonstriert, wie sich eine Schwäche im dort verwendeten „Chip&PIN" Verfahren am Point-of-Sale-Terminal ausnutzen lässt. Sie benötigten dazu allerdings einen Rucksack voller Elektronik und im Ärmel versteckte Kabel.

Am 10.03.2011 präsentierten amerikanische Wissenschaftler nun bei der CanSecWest Konferenz ein Skimming-Gerät, das vollständig im Schlitz eines Kartenlesers verschwindet und sich als ultraflacher Man-in-the-Middle zwischen die Kontakte des Lesers und der Karte setzt. Ohne starke Krypto-Protokolle schützt auch ein Sicherheitschip nicht vor Missbräuchen an der Automatenschnittstelle.

Erhöhtes Grundrauschen

Am 19.04.2011 veröffentlichte der Sicherheitsdienstleister Verizon Business seinen Data Breach Investigations Report für 2011. Danach hat die große Zahl externer Hacking-Angriffe auf Zufallsopfer den Anteil an Insiderattacken gegenüber dem Vorjahr zurück gedrängt - nicht jedoch deren absolute Zahl.

Diesen Trend bestätigt eine Meldung vom 16.04. 2011, nach der selbst von seriösen Webseiten wie den von Amnesty International aus Drive-By Downloads über die offenbar nicht auszurottenden Schwachstellen des Flash Players verteilt werden.

Die Empfehlung der Autoren des Reports für den Umgang mit dem damit verbundenen Risiko ist Wasser auf die Mühlen von Datenschützern: Man lösche alle nicht benötigten Daten, damit man die verbleibenden besser im Blick behalten kann.

Datenschutz zum Anfassen

Das Projekt „Autobahnmaut" des Betreibers Toll Collect stand vor Beginn des Wirkbetriebs am 01.01. 2005 wegen Startproblemen und der Erhebung der Mautdaten unter starker Kritik. Seither ist es ruhig geworden um Toll Collect - die Mauterhebung läuft reibungslos und der BfDI überzeugte sich 2006 von der Wirksamkeit des Daten-Löschkonzepts.

Am 25.02.2011 ging Toll Collect mit der Eröffnung einer Datenschutz-Ausstellung in die Öffentlichkeit: Spannungsfelder zwischen Techniknutzung und Datenschutz werden in fünf Installationen aufbereitet, z. B. in Form einer Datenspur über einen Tag – mit überraschenden Einsichten. Drei weitere Installationen beschäftigen sich mit der beschlagnahmefesten Zweckbindung der Mautdaten, der Löschkaskade für Kontrolldaten aus den Mautbrücken und den Löschfristen für Daten im Lebenszyklus eines Mautbenutzers. Die Besichtigung der Berliner Ausstellung ist nach Anmeldung möglich.

Bleibt zu wünschen, dass sich solche Best Practice in andere Unternehmen verbreitet – und der Gesetzgeber die strenge Zweckbindung der Mautdaten auch in der Zukunft aufrecht erhält.

Virencheck-Check

Viele IT-Nutzer erleben IT-Sicherheit vor allem beim Viren-Scan – häufig allerdings eher als (vermeintliche) Ursache für Performance- oder Funktionalitätseinschränkungen denn als wirksamen Schutz.

Am 14.04.2011 veröffentlichte nun das renommierte unabhängige Magdeburger AV-Testlabor aktuelle Prüfergebnisse für 22 führende Anti-Virus-Produkte. Seit Mitte 2010 erhalten Produkte, die 11 der maximal 18 zu vergebenden Testpunkte erreichen, von AV-Test ein Zertifikat. Ein zugehöriger Test-Report weist die vom Produkt für die Erkennung und Beseitigung von Viren sowie den Bedienkomfort erreichten Punkte aus.

Zwar kann man geteilter Meinung darüber sein, ob ein umfassender Client-Virenschutz auf rein geschäftlich genutzten Systemen noch zeitgemäß ist – denn eingehende E-Mails und Internet-Downloads lassen sich zentral wirksamer prüfen. Damit bleibt wenig mehr als das Einfallstörchen USB-Stick.

Bei privaten Systemen hingegen, die in der Regel durch keine Firewall und keinen zentralen Virenscanner geschützt sind, sind Anti-Viren-Produkte nach wie vor unverzichtbar – da kann es lohnen, vor der nächsten Verlängerung der Produktlizenz einen Blick auf die Testergebnisse zu werfen.

GPS-Daten in Smartphones

Der am 20.04.2011 publizierte „iPhone Tracker" von Alasdair Allan und Pete Warden, der die im iPhone gespeicherten GPS-Informationen eines Nutzers visualisiert, hat großen Wirbel ausgelöst – dabei ist die Speicherung von GPS-Daten auf dem iPhone lange bekannt. Auch der primäre Zweck der Speicherung ist leicht zu raten: Da präzise GPS-Lokalisierungen zeit- und rechenintensiv (und damit auch energiehungrig) sind, suchen alle Smartphone-Hersteller nach Optimierungen – z. B. durch die Speicherung „bekannter Wege", denn Menschen neigen dazu, bestimmte Wege immer wieder zu nutzen. Nicht auszuschließen allerdings, dass Apple mit den Daten zukünftig auch anderes im Sinn hatte: Erst

im Juni 2010 hatte Apple in seine Datenschutzrichtlinie die Nutzung und Weitergabe (anonymisierter) Standortdaten aufgenommen.

Andere Anbieter haben sich da geschickter angestellt. So erzeugt Vodafone mit seinem Ortungsservice „Vodafone Locate“ zur Handyortung, Routen- und Terminplanung Umsatz – statt eines Datenschutzskandals.

Personalausweis im Test

Am 21.04.2011 hat die Stiftung Warentest die Ergebnisse des Schnelltests der Einsatzmöglichkeiten des neuen Personalausweises veröffentlicht. Ganze 18 Angebote für die Online-Identifikation mit der eID zählten die Tester – davon ist ein Teil nur für registrierte Kunden nutzbar. Die Testseite des „Kompetenzzentrums neuer Personalausweis“ erzeugte z. T. merkwürdige Fehlermeldungen. Und einzig beim Angebot der Schufa erhält man bei deaktivierten Cookies eine aussagekräftige Meldung – alle anderen Angebote stellen sich „tot“.

Das nüchterne Fazit: Der praktische Nutzen der eID-Funktion hält sich (noch) stark in Grenzen, die wenigen Anwendungen gehören zudem zum Teil in die Kategorie „Bananen-Software“: Reift beim Kunden.

Smart Meter – mit Sicherheit

Seit Anfang 2010 ist der Einbau von Smart Metern in Neubauten und bei Renovierungen nach § 21b Abs. 3a/b Energiewirtschaftsgesetz (EnWG) vorgeschrieben. Dass Sicherheitsprobleme in diesen Geräten weit reichende Auswirkungen haben können, ist keine neue Erkenntnis. Daher wird derzeit unter der Federführung des BSI ein passendes Schutzprofil nach Common Criteria für die zugehörige Kommunikationseinheit (auch „Multi Utility Communication Controller“ oder „MUC“ genannt) erarbeitet.

Am 26.04.2011 führte das BSI einen Workshop durch, bei dem die Gerätehersteller den Autoren des Schutzprofils Fragen stellen konnten. Offen blieb dabei, wie im Falle des Bekanntwerdens einer sicherheitsrelevanten Schwachstelle in zertifizierten Geräten vorzugehen ist. Denn bei einem MUC verbietet sich das schnelle Ausbringen einer neuen Version, da die bevorstehende Novelle des EnWG voraussichtlich den Betrieb von nicht-zertifizierten Systemen untersagen wird. Der Einsatz einer fehlerbereinigten, aber noch nicht nachzertifizierten Geräteversion würde also gegen geltendes Recht verstoßen. Denkbar wäre eine definierte Notfallstrategie mit einer Ad-hoc-Freigabe durch das BSI.

Während die für Mitte 2011 angekündigte endgültige Version des Schutzprofils inhaltlich wohl nur marginal von der aktuellen Vorversion abweichen dürfte, bleibt diese Nuss bis zur Markteinführung der Geräte noch zu knacken. Da die Hersteller vorher allerdings noch die Zertifizierung durchlaufen müssen, ist damit allerdings kaum vor Mitte 2012 zu rechnen.

Secorvo News

Lizenz zum Entwickeln

Software ohne Schwachstellen schützt Kunden und Anbieter: Vom 24.-27.05.2011 bieten wir mit dem Seminar „Certified Professional for Secure Software Engineering (CPSSE)“ eine praxisorientierte Einführung in die sichere Softwareentwicklung. Mit der sich anschließenden Prüfung können Sie das international anerkannte Qualifikations-Zertifikat zum CPSSE erwerben.

Security News Symposium 2011

Am 31.05.-01.06.2011 ist es wieder soweit – wir laden Sie herzlich ein zum zweiten „Security News Symposium“ in das Tagungszentrum Buhlsche Mühle in Karlsruhe/Ettlingen. Auch in diesem Jahr werden wir aktuelle Security- und Datenschutzfragen aufgreifen, die uns bereits in den SSN beschäftigt haben, und gemeinsam mit Ihnen in Vortrag und Diskussion vertiefen. Zusammen mit weiteren Fachexperten bieten wir Ihnen ein spannendes Programm rund um VoIP, IPv6, Webtracking, Skimming und Online-Banking - und freuen uns auf Ihre Teilnahme!

DuD 2011

Am 05.-06.06.2011 findet die 13. Fachkonferenz „Datenschutz und Datensicherheit“ (DuD 2011) in Berlin unter der fachlichen Leitung der Herausgeber der Fachzeitschrift DuD statt. Das Programm umfasst eine breite Themenpalette: von der Datenschutzaufsicht über aktuelle Entwicklungen im EU-Datenschutzrecht hin zu aktuellen Datenschutzfragen des Cloud Computing, Smart Metering, Sozialer Netzwerke, forensischer Analysen und der Videoüberwachung – einschließlich einer Führung durch die Datenschutz-Ausstellung von Toll Collect.

College-Seminare

Eine sehr praxis- und anwendungsorientierte Einführung in die Computer-Forensik bieten wir vom 28.-30.06.2011 mit dem Seminar „Forensik – Verfahren, Tools, Praxiserfahrung“.

Die nächste Gelegenheit zur T.I.S.P.-Zertifizierung (TeleTrusT Information Security Professional) bietet Secorvo College vom 06.-11.06.2011.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2011	
10.-12.05.	12. Deutscher IT-Sicherheitskongress (BSI, Bonn)
12.-15.05.	Swiss Cyber Storm 3 Security Conference (Compass Security AG, Rapperswil/CH)
17.-20.05.	12. Datenschutzkongress (Euroforum, Berlin)
24.-27.05.	Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
31.05.-01.06.	2. Security News Symposium (Secorvo, Karlsruhe/Ettlingen)
Juni 2011	
06.-07.06.	DuD 2011 (Computas, Berlin)
06.-11.06.	T.I.S.P.-Schulung und -Prüfung (Secorvo College)
06.-11.06.	OWASP Global AppSec Europe (OWASP Foundation, Dublin/IE)
28.-30.06.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
Juli 2011	
14.07.	3. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum und KA-IT-Si, Karlsruhe)

Fundsache

Satire findet sich bisweilen an Stellen, wo man sie am wenigsten erwartet. So z. B. in Bugzilla, dem Bug-Tracking-System von Firefox & Co. Ähnlichkeiten des dort am 06.04.2011 eingereichten Antrags auf Aufnahme einer weiteren Root-CA mit den Geschäftsmodellen real existierender Trustcenter sind bestimmt rein zufällig.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Mai 2011



So schlau als wie zuvor

Wenn mein Gedächtnis nicht trügt, begann alles in den frühen 90er Jahren mit dem ISO-9000-Hype – einem Qualitätssiegel, das häufig eher das Vorhandensein einer bürokratisch-peniblen Dokumentation belegt als die materielle Qualität des Produkts. Heute sind Zertifikate so allgegenwärtig, dass uns bei einem Produkt ohne Zertifikat schnell das Gefühl beschleicht, dass damit etwas nicht stimmt.

Meist ist es einer von zwei Gründen, der dem Brancheneinzug eines Zertifikats den Weg ebnet: der Wunsch (oft eines neuen „Marktbegleiters“), sich von seinen Mitbewerbern abzusetzen – oder die Hoffnung, nach einem Skandal verlorenes Vertrauen zurückzugewinnen. Wenige Jahre später ist in der Regel die gesamte Branche zertifiziert – und das Gütesiegel zur „conditio sine qua non“ geworden.

Was für die zertifizierende Stelle (und ihren Umsatz) gut ist, ist jedoch nicht notwendig gut für einen Käufer. Denn die Aussagekraft eines Zertifikats hängt von zahlreichen – häufig nicht einmal öffentlich zugänglichen – Kriterien ab: in erster Linie von dem gewählten Prüfschema (was wird geprüft?), dann von der Prüftiefe (wie intensiv wird geprüft?), vom Prüfumfang (welche Aspekte werden geprüft?), dem Prüfzeitpunkt (wurde das fertige Produkt oder bereits in der Konzeptions- und Entwicklungsphase geprüft?), und nicht zuletzt auch von Qualifikation und Sorgfalt der Prüfer. Zwar mag man von der Prüfung eines unabhängigen Dritten grundsätzlich erwarten, dass sich mindestens in der Vorbereitung darauf Qualitätsverbesserungen einstellen – eine Garantie gibt es jedoch nicht dafür.

So bleibt auch nach einem Blick in den Zertifizierungsbericht des TÜV TrustIT Austria zum IE9 eher Ratlosigkeit zurück. Schützt das Zertifikat beim Surfen vor Malware – oder vor Programmierfehlern im IE9? Wem das alles zu unspezifisch ist, sollte den Browser lieber anhand objektiver Kriterien wählen – zum Beispiel nach ihrem Stromverbrauch: das ist zeitgemäß, politisch korrekt und jederzeit überprüfbar. Zum Beispiel mit einem neuen Smart Meter.



Inhalt

So schlau als wie zuvor

Security News

BGH zum Accountmissbrauch

3544, 3653, 5072

EnWG-Novelle

Man-in-the-Middle XXS

Zensus 2011 – aber sicher!

Secorvo News

Einblick in die Forensik

Was nix koscht, isch au nix

3. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

BGH zum Accountmissbrauch

Am 11.05.2011 hat sich der BGH in einem Grundsatzurteil zur Haftung von ebay-Nutzern geäußert. Der Ehemann der Beklagten hatte ein Niedrigpreisangebot unter dem Account seiner Frau auf der Auktionsplattform ebay eingestellt, das diese vor Auktionsablauf zurückzog. Der zuletzt Höchstbietende hatte sie daraufhin auf Schadensersatz wegen entgangenen Gewinns verklagt.

Der BGH hat auf diese Konstellation das herkömmliche Stellvertreterrecht angewendet und eine Anscheinsvollmacht verneint: Danach kommt es ohne nachträgliche Billigung durch die Accountinhaberin nicht zum Vertragsschluss. Aus den bislang nur als Pressemitteilung verfügbaren Ausführungen zur Bindungswirkung der ebay-AGBs, die die Haftung des Account-Anbieters für Handlungen Dritter festschreiben, geht hervor, dass der BGH eine Geltung für Rechtsverhältnisse zwischen den Plattformnutzern verneint. Das hat Konsequenzen für Plattformbetreiber. Wenn sie sich weiterhin – wie ebay – aus den auf ihrer Plattform geschlossenen Geschäften heraushalten wollen, wird es für sie schwierig, Vertragsbedingungen zwischen ihren Nutzern wie den Umgang mit dem Account-Passwort durchzusetzen. Damit steht für Käufer und Verkäufer gegebenenfalls die Rechtsverbindlichkeit der Kaufverträge in Frage.

3544, 3653, 5072

Falls am 08.06.2011 Internetanbieter wie Google, Facebook & Co. nicht wie gewohnt erreichbar sein sollten, dann ist das vermutlich keinem DoS-Angriff geschuldet, sondern dem von der ISOC ausgerufenen World IPv6 Day. An diesem Tag wird getestet, zu welchen Effekten es führt, wenn das Internet im Parallelbetrieb von IPv4 und IPv6 läuft. Auch Anwender, die nur das herkömmliche IPv4 einsetzen, könnten durch die IPv6-Adressauflösung in die Irre geführt werden, wenn Netzwerkfunktionen ungenügend oder fehlerhaft implementiert sind. Testen kann man das vorab über Webseiten wie z. B. test-ipv6.com – leider meist mit viel JavaScript.

Der Test ist ein guter Anlass, zu überprüfen, wieviel unbeabsichtigte IPv6-Konnektivität im eigenen Netz besteht: In den meisten neueren Betriebssystemen ist IPv6 standardmäßig aktiviert. Zudem kann IPv6-Datenverkehr in IPv4-Paketen getunnelt u. U. Firewalls (auch eingehend!) aushebeln, die ausgehende Verbindungen nicht rigide kontrollieren. Man achte auf die drei im Titel genannten Zahlen: Das sind die UDP/TCP-Ports, die die Tunneling-Verfahren Teredo, TSP bzw. AYIYA nutzen.

EnWG-Novelle

Am 11.05.2011 hat die Bundesregierung einen Entwurf zur Novellierung des Energiewirtschaftsgesetzes (EnWGÄndG) vorgelegt. Er enthält u. a. umfassende Ergänzungen zu Smart Metern sowie diesbezügliche Datenschutzregelungen.

In § 21 Abs. 1 werden ausschließliche Zwecke für die Nutzung der durch Smart Meter gewonnenen Daten und in Abs. 2 die zum Datenumgang berechtigten Stellen festgelegt. Dabei wird der Terminus „Datenumgang“ eingeführt, der zukünftig die „Erhebung, Verarbeitung und Nutzung“ personenbezogener Daten bereichern soll. Ein überflüssiger Abs. 3 ermöglicht explizit die Auftragsdatenverarbeitung.

In § 21e werden umfassender als bisher die Anforderungen an Smart Meter aufgegriffen. Im Wesentlichen beschränkt sich der Entwurf jedoch auf einen Verweis auf eine zu erlassende Rechtsverordnung nach § 21i, die Forderung nach Verschlüsselung bei Versendung über offene Netze und den Hinweis auf den Stand der Technik.

Nach Abs. 5 dürfen Messsysteme, die vor Inkrafttreten der Neuerungen verbaut wurden, bis zum Ablauf der Eichgültigkeit (mindestens bis 31.12. 2013) verwendet werden: Damit liegt die Höchstgrenze für „Alt“-Geräte bei acht Jahren. Die Pflicht zum Einbau von Smart Metern nach § 21c Abs. 1, beschränkt auf Neubauten und größere Renovierungen, kann bei Feststellung der wirtschaftlichen Vertretbarkeit durch das Bundeswirtschaftministerium allgemein vorgeschrieben werden.

Substantielle Änderungen wie die von den Datenschutzbeauftragten der Länder geforderte Gestaltungsvorgabe, die Daten so weit wie möglich lokal und unter Kontrolle des Endnutzers zu verarbeiten, wurden jedoch nicht umgesetzt. Mit § 14a werden zudem von außen unterbrech- und steuerbare Verbrauchseinrichtungen eingeführt. Insgesamt gehen die Neuregelungen nicht weit über das bereits im BDSG Geregelte hinaus und verlieren sich teilweise in Details. Hinsichtlich der Sicherheitsanforderungen an Smart Meter werden nun mit Spannung die Endfassung des Protection Profiles des BSI sowie die zugehörige Rechtsverordnung erwartet.

Man-in-the-Middle XXS

Schon am 08.12.2010 präsentierte Vasco einen Chip in einer Folie, der über die „echten“ Kontaktflächen einer SIM-Karte geklebt wird, um unabhängig vom jeweiligen Netzbetreiber Sicherheitsfunktionen für das Online-Banking per Handy zu ergänzen.

Genau wie viele andere Sicherheitslösungen ist das Konzept eine Dual Use-Technologie: Man stelle sich vor, dass eine derartige Folie über den Kontakten eines Geldautomaten klebt, um diesen mit „Zusatzfunktionen“ anzureichern. Das wäre noch eleganter als das in der vorigen Ausgabe der SSN vorgestellte Chipkarten-Skimming-Gerät, das in den Schlitz des Kartenlesers passt. Es wird daher immer wichtiger, dass Chipkarten-Anwendungen auch gegen einen Man-between-Card-and-Reader-Angriff gefeit sind.

Zensus 2011 – aber sicher!

Derzeit wird zum Stichtag 09.05.2011 in Deutschland wieder gezählt. Im Rahmen des Zensus 2011 werden in Form einer repräsentativen Stichprobe Informationen über die Bevölkerung in Deutschland erhoben. Dem Schutz der erhobenen Daten widmet das Statistische Bundesamt auf der Zensus-Webseite einen ganzen Abschnitt. Darin bleiben allerdings Fragen offen: Wie steht es insbesondere um die Transportsicherheit bei der Befragung?

In der öffentlichen Berichterstattung entsteht der Eindruck, die Beantwortung der Fragen müsse in Form eines Interviews durchgeführt werden – in diesem Fall hinge die Sicherheit der persönlichen Daten stark vom Erhebungsbeauftragten ab. Dubiose Aufrufe zur Meldung als Erhebungsbeauftragte, wie der der sächsischen NPD, geben Anlass, die Vertrauenswürdigkeit der Interviewer zumindest kritisch zu hinterfragen.

Etwas versteckt findet sich auf der offiziellen Webseite zum Zensus ein Hinweis auf alternative Möglichkeiten zur Meldung der Daten: Online oder durch Postversand an die Meldestelle. Aber auch dabei ist Vorsicht geboten: In drei Bundesländern wurden externe Dienstleister mit der Beleglesung beauftragt. Bei Versand empfiehlt sich daher eine Prüfung der Rücksendeadresse auf dem Fragebogen.

Auch die Online-Meldung ist nicht ohne Risiken. Im Blog von Jan Schejbal finden sich Angriffsbeschreibungen, und auch das Statistische Bundesamt und das Bundesamt für Sicherheit in der Informationstechnik halten Sicherheitshinweise zur Online-Meldung für erforderlich.

Die deutliche Fokussierung auf die Interview-Erhebung könnte sich mit den Aufwandsentschädigungen für Erhebungsbeauftragte erklären: Jeder analog ausgefüllte Fragebogen wird zusätzlich mit 7,50 Euro entlohnt.

Bei der Meldung der Daten ist also Sorgfalt angeraten. Dann sollten auch Erfahrungen ausbleiben, die Volkszähler der TAZ Berlinern und clevere Betrüger auf der Suche nach Kontodaten Münchner Bürgern bescherten.

Secorvo News

Einblick in die Forensik

Kurz vor der Sommerpause bietet Ihnen Secorvo College mit dem Seminar Forensik – Verfahren, Tools, Praxiserfahrung vom 28.-30.06.2011 einen praxisorientierten Einblick in die Computer-Forensik. Hier erleben Sie in realitätsnahen Übungen, worauf es bei IT-forensicher Arbeit ankommt.

Im September startet Secorvo College mit dem Seminar **Sicherheitsmanagement heute** vom 27.-29.09.2011 in den Herbst. Es folgen die Seminare **Verlässliche Web-Anwendungs-Sicherheit** (05.-06.10.2011), **IT-Sicherheitsaudit in der Praxis** (10.-12.10.2011) und **Datenschutzaudit: Best Practice** (13.-14.10.2011). Zudem bieten wir Ihnen vom 17.-22.10.2011 die nächste Gelegenheit zur T.I.S.P.-Zertifizierung. Alle Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Was nix koscht, isch au nix

„Sicherheit für umsonst“ lautet der Titel des kommenden Events der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 09.06.2011, bei dem Astaro-Technikvorstand Markus Hennig seine Erfahrungen und Einschätzungen zur Frage "Sicherheit durch OpenSource?!" vorstellen wird. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Im Anschluss an den Vortrag gibt es wie gewohnt die Gelegenheit zum „Buffet-Networking“. Wir freuen uns auf Ihre Anmeldung.

3. Tag der IT-Sicherheit

Am 14.07.2011 findet zum dritten Mal der von der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) gemeinsam mit der IHK Karlsruhe und dem CyberForum e.V. veranstaltete „Tag der IT-Sicherheit“ statt.

Der Präsident des Bundesamtes fuer Sicherheit in der Informationstechnik (BSI), Michael Hange, wird in einer Keynote einen Ausblick auf die Bedrohungslage und die Arbeit des BSI in Deutschland geben. Außerdem erwarten Sie Praxisbeiträge zum elektronischen Personalausweis, De-Mail, Web-Angriffen und der Sicherheit im Online-Banking. Die Veranstaltung beginnt um 14 Uhr im Saal Baden der IHK.

Direkt im Anschluss lädt die KA-IT-Si zum Jubiläumsempfang anlässlich ihres 10jährigen Bestehens. Das vollständige Programm und die Online-Anmeldung finden Sie unter www.karlsruhe.ihk.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2011	
06.-07.06.	DuD 2011 (Computas, Berlin)
06.-11.06.	OWASP Global AppSec Europe (OWASP, Dublin/IE)
09.06.	Sicherheit für umsonst (KA-IT-Si, Karlsrsuhe)
28.-30.06.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
Juli 2011	
14.07.	3. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum und KA-IT-Si, Karlsruhe)
30.07.-02.08.	Blackhat USA 2011 (Blackhat, Las Vegas/US)
August 2011	
04.-07.08.	DEFCON 19 (DEFCON, Las Vegas/US)
14.-18.08.	Crypto 2011 (IACR, Santa Barbara/US)
September 2011	
20.-21.09.	8. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)

Fundsache

Am 27.04.2011 veröffentlichte das BSI ein Eckpunktepapier zu Sicherheitsempfehlungen für Cloud-Computing-Anbieter. Das 76seitige Dokument ist übersichtlich strukturiert und enthält – von einzelnen Skurrilitäten wie der Liste von Vorfällen im Kapitel Notfallmanagement abgesehen – viele wertvolle Hinweise. Eine Antwort auf die wichtige Frage, wie eine datenschutzkonforme Auftragsdatenverarbeitung in der Cloud funktionieren kann, bleibt es allerdings schuldig.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2011



Editorial: Sieg der Vernunft

Das Schlimmste ist, dass wir die einfachsten Fragen mit Tricks zu lösen versuchen, darum machen wir sie auch so kompliziert. *Anton Tschechow (1860-1904)*

Manchmal kommt die Vernunft auf ganz leisen Sohlen. Diesmal versteckt sie sich im Steuervereinfachungsgesetz 2011, das am 09.06.2011 vom Bundestag verabschiedet wurde. Darin wird § 14 Abs. 1 des Umsatzsteuergesetzes geändert – und damit GDPdU und deutsches Signaturgesetz (SigG) zugleich „geschleift".

Aber der Reihe nach. Seit dem Inkrafttreten des „Gesetzes über Rahmenbedingungen für elektronische Signaturen" im Jahr 2001 mangelte es nicht an Versuchen, der qualifizierten Signatur zum Durchbruch zu verhelfen. So führte der Gesetzgeber nicht nur die „elektronische Form" im Bürgerlichen Gesetzbuch (BGB) ein, sondern schob auf der Suche nach einer „Killer-Applikation" zahlreiche Initiativen an, darunter – um die prominentesten zu nennen – die elektronische Steuererklärung mit Signatur (ELSTER), das ELENA-Verfahren, den neuen Personalausweis (nPA) mit Signierfunktion und zuletzt das am 03.05.2011 in Kraft getretene De-Mail-Gesetz.

Jedoch signierte nur eine verschwindend geringe Zahl an Bürgern die elektronische Steuererklärung, ELENA wurde gestoppt und für die Signierfunktion des nPA gibt es auch acht Monate nach Einführung kein Trustcenter, das die Nachladefunktion für Signaturzertifikate unterstützt. Daher waren die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen" (GDPdU) vom 16.07.2001 die letzte Bastion: Milliarden elektronischer Rechnungen von TK-Unternehmen, Fluggesellschaften und Online-Shops mussten qualifiziert signiert und vom Empfänger geprüft und protokolliert werden.

Ab dem 01.07.2011 ist das Geschichte. Zwar darf weiterhin signiert werden. Eine Übermittlung per E-Mail ohne Signatur genügt jedoch für den Vorsteuerabzug. Trauern dürften darüber nur externe „GDPdU-Prozessdesigner" – Unternehmer und Steuerberater hingegen werden die FAQ des Finanzministeriums mit ungläubigem Staunen lesen: So viel Bürokratieabbau war selten.



Inhalt

Editorial: Sieg der Vernunft

Security News

Key Escrow 2.0

Web 2.0

Alchemie 2.0

EnWG 2.0

Forensik 2.0

C++ 2.0

Secorvo News

TISP und mehr

3. Tag der IT-Sicherheit

Leseprobe

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Key Escrow 2.0

Nachdem im März 2011 unbekannten Hackern ein Einbruch bei RSA gelang (siehe SSN 03/2011), hat der SecurID-Hersteller am 06.06.2011 seinen Kunden angeboten, alle One-Time-Password-Token auszutauschen. Dieser Schritt wird allgemein als ein Eingeständnis interpretiert, dass bei dem Einbruch tatsächlich die Seed-Werte vieler oder aller Token entwendet wurden – die Masterkeys, die es erlauben, alle von den Token angezeigten Einmalpasswörter nachzuberechnen.

Auch die Seed-Werte der neuen Token wird RSA archivieren, wenn auch vermutlich besser abgesichert. Da stellt sich die Frage, warum Anwender diese Art von Schlüsselhinterlegung („Seed Escrow") so ohne weiteres akzeptieren sollten. Schließlich käme auch niemand auf die Idee, beim Ausstellen eines SSL-Zertifikats den privaten Schlüssel des betreffenden Webservers dem Trustcenter zum Archivieren zu überlassen, nur für den Fall, dass er dem Besitzer verloren ginge – oder eine Kopie des Fahrzeugschlüssels dem Autohändler oder des Haustürschlüssels dem Makler. Die Hinterlegung großer Mengen sensibler Schlüssel war noch nie ein gutes Konzept, sondern ein meist unnötiger „Single Point of Failure".

Web 2.0

Das KG Berlin hat am 29.4.2011 über die Beschwerde wegen der Ablehnung einer einstweiligen Verfügung gegen einen Wettbewerber entschieden, der den „Gefällt-mir-Button" von Facebook nutzt. Einen abmahnungsfähigen Verstoß gegen eine Marktverhaltensvorschrift nach § 4 Nr. 11 UWG wegen fehlender Information über die Datenübermittlung (§ 13 Abs. 1 TMG) lehnte das Gericht ab.

Für Telemedienanbieter, die Social Plugins nutzen, stellt das Urteil dennoch keine Entwarnung dar: Es klammert die datenschutzrechtliche Bewertung der Fragen, wer verantwortliche Stelle beim Einsatz von Social Plugins ist, ob der Verwender ohne diesbezügliche Datenschutzerklärung seine Informationspflicht verletzt oder ob eine unerlaubte Datenübermittlung ohne Einwilligung vorliegt, gänzlich aus. Eine diesbezügliche Stellungnahme des „Düsseldorfer Kreises" dürfte nicht lange auf sich warten lassen – vom Vorliegen einer bußgeldbewehrten Ordnungswidrigkeit ist weiterhin auszugehen.

Alchemie 2.0

In den letzten Wochen überschlagen sich die Meldungen über Bitcoin, eine elektronische Währung, die ohne eine zentrale Ausgabestelle auskommt – jeder Teilnehmer kann als „Miner" neue „Münzen" erschaffen, wenn er Rechenzeit investiert, um bestimmte Krypto-Aufgaben zu lösen. Bitcoins können wie Bargeld anonym übertragen werden, da alle Teilnehmer nur unter Pseudonym bekannt sind. Dabei kontrollieren und beglaubigen in einem Peer-to-Peer-Verfahren andere Teilnehmer die Weitergabe und verhindern, dass digitale Münzen mehrfach ausgegeben werden.

Das Verfahren ist umstritten – die Bewertungen reichen von einem faszinierenden Stück Kryptographie oder einer finanztechnischen Revolution über Geldwäschemechanismus bis zur Unterstellung eines Ponzi-Schneeball-Systems. Jedenfalls werden Bitcoins bereits in Dollar oder Euro gewechselt, es wurden schon Razzien (23.05.2011) und echte oder vorgebliche Diebstähle (13.06.2011) gemeldet und erste Trojaner stehlen entweder Rechenzeit zum „Mining" oder gleich die ganze Bitcoin-Brieftasche. Seit dem 20.05.2011 gibt es überdies eine Javascript-Version, mit der Webseitenbetreiber ihre Besucher als Bitcoin-Miner für sich arbeiten lassen können.

Zwar sind Zweifel am Erfolg dieser Goldsuche des 21. Jahrhunderts angebracht – allerdings könnte Bitcoin das eine oder andere rätselhafte Verschwinden von Rechenleistung plausibel erklären.

EnWG 2.0

Am 06.06.2011 legte die Bundesregierung einen Entwurf zur Novellierung des Energiewirtschaftsgesetzes (EnWG) vor. Eine wesentliche Neuerung ist die Präzisierung des „Smart Meter"-Begriffs als „eine in ein Kommunikationsnetz eingebundene Messeinrichtung". Während es bislang laut EnWG ausschließlich um die Verbrauchsanzeige ging, werden die Kommunikationsschnittstelle und deren Nutzung nun Standard. Über die tatsächlich übertragenen Daten sagt das noch nichts aus – jedoch ist zu befürchten, dass dies zu Stromprodukten führen wird, die mit der Übertragung personenbeziehbarer Verbrauchswerte im 15-Minuten-Takt einhergehen.

In ihren Stellungnahmen plädieren sowohl der BfDI (zum Schutzprofil) als auch das ULD (zur EnWG-Novelle) für eine Lösung, die Datensparsamkeit bereits im Entwurf berücksichtigt. Die Tarifierung sollte im Haushalt vorgenommen und auch bei lastabhängigen Tarifen sollten nur aggregierte Daten übermittelt werden.

Immerhin ist in § 40 (5) verankert, dass „Lieferanten [...] stets mindestens einen Tarif anzubieten [haben], für den die Datenaufzeichnung und –übermittlung auf die Mitteilung der [...] verbrauchten

Gesamtstrommenge begrenzt bleibt". Wenigstens könnte sich Datensparsamkeit als Unterscheidungsmerkmal etablieren – dann würde möglicherweise schon ein Anbieter mit einem attraktiven Stromprodukt („Datenschutztarif") genügen, um datensparsame Tarifmodelle durchzusetzen.

Forensik 2.0

Die seit Anfang Juni 2011 im Betatest befindliche Public Preview 2 von EnCase Forensic Version 7 weist lange erwartete Verbesserungen auf. Neben einer klareren Strukturierung der Oberfläche sticht besonders der neue „Evidence Processor" hervor, der nun vor dem Beginn der inhaltlichen Analyse eine Reihe von derzeit neun Standardaufgaben (darunter eine Dateisignatur-Analyse und die Indexierung) konfigurierbar abarbeitet – für eine beliebige Anzahl forensischer Images. Erste Tests haben gezeigt, dass die Arbeitsabläufe deutlich komfortabler und schneller werden, solange man über ausreichend dimensionierte Hardware für den Evidence Processor verfügt.

In einer zehnten Standardaufgabe (Kategorie „Modules") kann z. B. der File Carver für bestimmte Datentypen eingestellt werden. Noch ist offen, ob dieser Bereich durch Endkunden selbst erweitert werden kann, wie dies z. B. bei EnScript der Fall ist. Falls Erweiterungen bspw. für CAD-Daten benötigt werden, wird man sonst wohl auf EnCase 8 warten oder auf ein forensisches „Schweizer Offiziersmesser" wie X-Ways Forensics ausweichen müssen.

Einen Schritt weiter geht Simson L. Garfinkel mit seinem bulk_extractor V 1.0.0 vom 15.06.2011, der als Stream-basierter Ansatz mit Named Entity Recognition fast in Echtzeit große Datenmengen unterschiedlicher Formate (wie Bilder, Diskimages oder Dateien) nach Zielbegriffen wie z. B. Kreditkartendaten durchsucht. Solche Carving-Ansätze dürften zukünftig maßgeblich die Erfolgschancen einer IT-Forensik-Software bestimmen.

C++ 2.0

Im Juni 2011 hat Michael Howard (Microsoft) eine Übersicht über gefährliche C und C++ Funktionen im Microsoft Developer Network (MSDN) veröffentlicht. Dieser Auszug aus Kapitel 11 seines mit Steve Lipner verfassten und bereits am 31.05.2006 erschienenen Buch The Security Development Lifecyle ist als konkrete Handreichung für Software-Entwickler gedacht. In dem kurzen Artikel findet sich eine Übersicht über potenziell gefährliche Funktionen – und Empfehlungen für sichere Alternativen. Diese Übersicht sollte über jedem Entwicklerschreibtisch hängen.

Secorvo News

TISP und mehr

Mit Blick auf die steigenden Anmeldezahlen möchten wir Sie schon jetzt auf die nächste T.I.S.P.-Schulung vom 17.-22.10.2011 (einschließlich Prüfung) hinweisen. Nutzen Sie die Gelegenheit, Ihre Kenntnisse zu erweitern, und lassen Sie sich Ihr Wissen zertifizieren.

Nach den Sommerferien startet Secorvo College zunächst mit dem Seminar „Sicherheitsmanagement heute" vom 27.-29.09.2011. Es folgen die Seminare „Verlässliche Web-Anwendungs-Sicherheit" (05.-06.10.2011), „IT-Sicherheitsaudit in der Praxis" (10.-12.10.2011) und „Datenschutzaudit: Best Practice" (13.-14.10.2011). Alle Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

3. Tag der IT-Sicherheit

Gemeinsam mit dem CyberForum e.V. und der IHK Karlsruhe veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 14.07.2011 den „3. Tag der IT-Sicherheit" im Saal Baden der IHK Karlsruhe (Beginn: 14 Uhr, Teilnahmebeitrag 75 Euro).

Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Michael Hange, wird in seiner Keynote einen Ausblick auf die Bedrohungslage und die Arbeit des BSI in Deutschland geben. Außerdem erwarten Sie praxisnahe Beiträge zum elektronischen Personalausweis, De-Mail, Web-Angriffen und der Sicherheit im Online-Banking.

Im Anschluss lädt die KA-IT-Si anlässlich ihres 10-jährigen Bestehens zum Jubiläumsempfang. Bitte melden Sie sich rechtzeitig an, damit wir ausreichende Mengen Sekt kalt stellen... Nähere Informationen zum Programm und zur Online-Anmeldung finden Sie unter www.ka-it-si.de.

Leseprobe

Die Fachzeitschrift „Datenschutz und Datensicherheit" (DuD) erscheint bereits im 35. Jahr und seit knapp 15 Jahren unter der Mitwirkung von Dirk Fox als Herausgeber. Dank des wachsenden Interesses am Thema und der Erweiterung des Herausgeberteams um die Juristen Prof. Dr. Benedikt Buchner und Dr. Britta Alexandra Mester im Jahr 2009 wuchs der Umfang des Jahrgangs 2010 auf über 860 Seiten.

Von der Ausgabe 6/2011 ist nun eine digitale Leseprobe verfügbar. Auch ein kostenloses Probeabonnement wird angeboten – wer schnell ordert, erhält noch die Ausgabe 8/2011 mit dem Schwerpunkt „Smart Grids".

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2011	
14.07.	3. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum und KA-IT-Si, Karlsruhe)
30.07.-02.08.	Blackhat USA 2011 (Blackhat, Las Vegas/US)
August 2011	
01.-03.08.	DFRWS 2011 (DFRWS, New Orleans/US)
04.-07.08.	DEFCON 19 (DEFCON, Las Vegas/US)
10.-12.08.	20th USENIX Security Symposium (Usenix, San Francisco/US)
14.-18.08.	Crypto 2011 (IACR, Santa Barbara/US)
September 2011	
19.-23.09.	OWASP Global AppSec North America (OWASP Foundation, Minneapolis/US)
27.-29.09.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Oktober 2011	
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)

Fundsache

Am 14.06.2011 hat das PCI Security Standards Council als Ergänzung zum PCI Data Security Standard das Dokument PCI DSS Virtualization Guidelines in der Version 2.0 veröffentlicht. In der 39seitigen Übersicht werden auf einem recht hohen Abstraktionsniveau Sicherheitsaspekte von Virtualisierung und Cloud Computing vorgestellt – für Nicht-Techniker ein lesenswerter Leitfaden.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

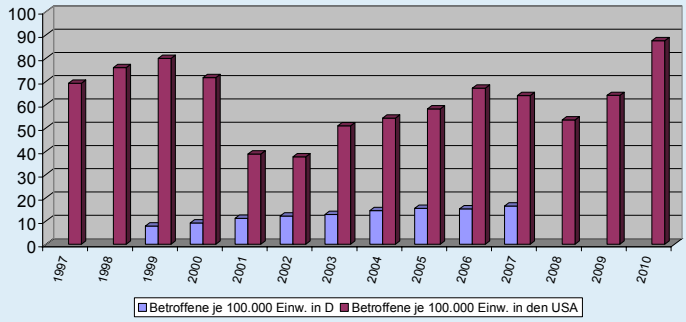
Secorvo Security News

Juli 2011



TK-Überwachung im Vergleich

Die heimliche Überwachung von Telekommunikationseinrichtungen ist ein Eingriff in das Fernmeldegeheimnis (Art. 10 GG) – und den Strafverfolgungsbehörden nur bei begründetem Tatverdacht, schweren Straftaten und als „ultima ratio“ (§ 100a StPO) erlaubt. Sie erfordert zudem eine richterliche Anordnung (§ 100b StPO). Anders als in den USA, die die Richter verpflichten, das Ergebnis der Überwachung in einem „Wiretap Report“ (Umfang, Anklagen und Verurteilungen) zu dokumentieren, unterliegt die TK-Überwachung in Deutschland keiner Erfolgskontrolle. Den tatsächlichen Umfang der Überwachung geben aber auch die amerikanischen Wiretap Reports nicht auf den ersten Blick preis. Im direkten Vergleich zeigt sich, dass die Zahl der von einer Überwachung Betroffenen je Einwohner und Jahr in den USA erheblich schwankt, während sie in Deutschland - auf niedrigerem Niveau - kontinuierlich wächst. Leider ist der deutschen Statistik die Zahl der Betroffenen nur bis 2007 zu entnehmen.



Bedenklicher stimmen die Ergebnisse empirischer Analysen, wie die von Dr. Jens Eckhardt (2009). Sein Fazit: „Die Erfolge stehen in keinem angemessen Verhältnis zu den damit verbundene Eingriffen.“ Und: „Eine substantiierte Begründung der Überwachung war nur in einem geringen Maß festzustellen.“



Inhalt

TK-Überwachung im Vergleich

Security News

Böse Schnittstelle

IMSI-Catcher für jedermann

Mit der Schrotflinte...

Hase ./. Igel

Same procedure ...

ShellBag Forensik

Secorvo News

TISP und mehr

Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Böse Schnittstelle

USB-Sticks haben nicht erst seit Stuxnet (SSN 10/2010) anderen Speichermedien den Rang als verbreitetste „Gefährder“ abgelaufen. Nach Dumper, HackSaw und SwitchBlade hat nun die Firma Netragard dies im Rahmen eines Penetrationstests in besonders kreativer Weise unter Beweis gestellt: Sie verschickte eine „trojanisierte“ USB-Maus als Werbegeschenk getarnt an einen Mitarbeiter des Unternehmens.

Darin befanden sich zusätzlich ein USB-Hub, ein USB-Flash-Drive sowie ein Mikrocontroller, der nach dem Anstecken eine Tastatur emulieren und Tastatureingaben an den PC senden konnte – die Herstellung dieser Spezialmaus wurde detailliert beschrieben. Mit einer Standard-Remote-Shell aus dem Metasploit-Framework konnte damit der PC übernommen und in das Netzwerk eingedrungen werden.

Ein ähnlich kreativer Ansatz, per USB und einem Teensy Controller Systeme anzugreifen, wurde am 13.07.2011 von Didier Stevens vorgestellt: Mit vorprogrammierten Tastatureingaben wird ein Editor geöffnet, binärer Code eingetippt und dieser als PDF gespeichert. Wird das PDF geöffnet, führt das befallene System den Code aus.

In beiden Fällen rettet kein Virenschutz – höchstens eine Kontrollsoftware für angeschlossene USB-Geräte, die die Maus als Datenspeicher entlarvt hätte. Aber es geht auch nicht ohne Benutzersensibilisierung, denn bei allen unbekannten USB-Geräten ist Vorsicht geboten – auch Lautsprecher, Tassenwärmer oder Spaß-Geräte aus externer Quelle können solche Erweiterungen in sich bergen.

IMSI-Catcher für jedermann

In Großbritannien verkauft Vodafone als Femtozelle ein Gerät, das für UMTS eine ähnliche Funktion wie ein WLAN Access Point bietet: Das Handy des Kunden funkt zur Femtozelle, die über den heimischen Internet-Anschluss an das Vodafone Mobilfunknetz angebunden ist. Am 13.07.2011 publizierte nun die Gruppe THC Untersuchungen aus 2009/10, denen zufolge es gelang, dank eines schwachen Root-Passworts mittels Reverse-Engineering die Kontrolle über die Linux-basierten Zellen zu übernehmen. Nach Ausbau bzw. Deaktivieren einiger Sicherheitseinrichtungen konnten die Forscher dann – wie auch von anderen Experten erwartet – Gespräche abhören und auf fremde Kosten telefonieren.

Das gelang, weil die Femtozelle große Teile der Funktion eines UMTS Radio Network Controllers (RNC) wahrnimmt, darunter die Verschlüsselung der Funkstrecke, und die erforderlichen Schlüssel über die Internet-Anbindung aus dem Kern-Netz des Providers bezieht. In der ursprünglichen UMTS-Architektur ist der RNC eine Komponente des Providernetzes – nur autorisiertem Personal zugänglich und kein kleines Gerät im Kunststoffgehäuse, an das der zahlende Kunde Anschlüsse anlöten und „Man-in-the-Middle“ spielen kann.

Auch hier zeigt sich wieder wie wichtig es ist, zuerst die zu Grunde liegenden Sicherheitsannahmen zu hinterfragen, ehe man ein bewährtes Verfahren auf neue Szenarien überträgt.

Mit der Schrotflinte...

Auf Initiative Hessens hat der Bundesrat am 17.06. 2011 einen Entwurf zur Überarbeitung des Telemediengesetzes (TMG-E) vorgelegt. Darin findet sich in § 13 Abs. 8 – entsprechend Art. 2 Abs. 5 der Richtlinie 2009/136/EG, die eine entsprechende Regelung in die Datenschutzrichtlinie für elektronische Kommunikation einfügte und bis Mai 2011 umzusetzen war – die Festlegung, dass die Speicherung und der Abruf von Daten im Endgerät des Nutzers künftig nur mit Unterrichtung und vorheriger Einwilligung zulässig sein werden.

Betroffen hiervon sind sämtliche Cookies und automatischen Abfragen, bspw. durch Apps. Praktisch würde damit der Einsatz von Cookies unhandlich bis unmöglich. Die Ausnahme der „unbedingten Erforderlichkeit zur Dienstnutzung“ ist ungeeignet, diese Wirkung zu entschärfen, denn wie viel Bequemlichkeit ist unbedingt erforderlich?

In § 13a TMG-E werden Anbieter von Foren, Blogs, Social Networks und ähnlichen Diensten verpflichtet ihre – nicht näher definierten – höchsten Sicherheitseinstellungen als Default anzubieten. Einzige materielle Vorgabe ist die Unauffindbarkeit durch Suchmaschinen. Eine Herabsetzung der Einstellungen soll nur Nutzern über 16 Jahren möglich sein.

In beiden Fällen ist die Absicht zu begrüßen, Transparenz, Nutzerkontrolle und Nutzerschutz im Internet zu stärken - die derzeitige Fassung des Gesetzentwurfs erscheint jedoch wenig durchdacht und praxisuntauglich.

Hase ./. Igel

Der Wettlauf zwischen IT-Sicherheit und organisierter IT-Kriminalität geht in die nächste Runde. Da Nutzer der DHL Packstation als potentielle Zieladresse für online ergaunerte Waren ein beliebtes Phishing-Ziel darstellen, ist seit März 2011 eine Kunden-Magnetkarte erforderlich, um eine Sendung abzuholen. Am 25.06.2011 wurde nun gezeigt, wie

man sich zu jeder Packstation-Adresse eine passende Magnetstreifenkarte selbst kodieren kann.

Magnetstreifenkarten haben auch am Geldautomaten bald ausgedient. Die Schadensfälle durch Skimming nehmen dermaßen überhand, dass viele Banken, wie am 05.07.2011 bekannt wurde, die außereuropäische Nutzung der EC-Karte drastisch einschränken. Und beim Online-Banking schließlich wechseln viele Institute mittlerweile von der iTAN zu Verfahren mit Handheld-Kartenlesern (chipTAN oder SmartTAN genannt). Derweil warnte das BKA am 15.07.2011 vor Trojanern, die ihre Opfer ganz offen zu einer Überweisung auffordern – unter dem Vorwand, eine versehentliche Gutschrift rückgängig zu machen. Da hilft leichtgläubigen Kontoinhabern auch kein chipTAN-Verfahren mehr.

Es sieht also so aus, als ob uns dieser Wettlauf noch eine Weile erhalten bleibt. Noch ist allerdings unentschieden, welche Seite im Ziel der Igel ist.

Same procedure …

Bei der Durchsicht der am 27.06.2011 veröffentlichten CWE/SANS TOP 25 Most Dangerous Software Errors – ermittelt anhand des CWSS-Bewertungssystems, reduziert auf Tragweite, Verbreitung und Ausnutzbarkeit der Schwachstellen – fühlt man sich wie Miss Sophie an Sylvester: Seit Jahren finden sich dieselben Schwachstellen auf den Top-Positionen der Liste, darunter SQL-Injection, Command Injection und Cross-Site Scripting, obwohl seit längerem wirksame Ansätze zu deren Bekämpfung bekannt sind.

Die Liste findet ihre praktische Bestätigung in aktuellen Schwachstellenübersichten und Berichten über erfolgreiche Hacks (Citibank, MySQL, Barracuda, REWE, Schufa, …) und deckt sich größtenteils mit den weithin bekannten OWASP Top 10.

Sofern die Entwicklung sicherer Software nicht bald durchgängig ernster genommen wird, müssen wir uns wohl auch im nächsten Jahr auf eine ganz ähnliche Übersicht einstellen. „Cheerio, Sophie, mee girl!“

ShellBag Forensik

Seit dem 29.05.2011 liegt der Windows ShellBag Parser von TZ Works als stabile und skriptfähige 64-bit-Version vor, die auch mit den ShellBags von Windows 7 problemlos arbeitet – anders als etwa kommerzielle, forensische Suiten, bei denen die Auswertung von ShellBags z. T. noch in den Kinderschuhen steckt.

Damit kann aus vorliegenden benutzerspezifischen Profil-Dateien von Windows (NTUSER.DAT, UsrClass.DAT) eine Vielzahl von Informationen über das Laufzeitverhalten eines Windows-Benutzerkontos gewonnen werden. Mit diesen Informationen wird die Erstellung von aussagefähigen Zeitlinien und Nutzungsabfolgen aus Metadaten des NTFS-Dateisystems, gecarvten Dateifragmenten und Benutzerkonteninteraktionen deutlich besser interpretierbar.

Da die Aufrufreihenfolge der jeweils letzten Aktionen in den ShellBags von Windows automatisch festgehalten wird, können so z. B. auch Malwareaktivitäten identifiziert werden, die im Benutzerkontext gestartet wurden – oder auch versehentlich gelöschte Verlaufshistorien zurück gewonnen werden.

Secorvo News

TISP und mehr

Nach der Sommerpause startet Secorvo College zunächst mit dem Seminar „Sicherheitsmanagement heute“ vom 27.-29.09.2011. Es folgen die Seminare „Verlässliche Web-Anwendungs-Sicherheit“ (05.-06.10.2011), „IT-Sicherheitsaudit in der Praxis“ (10.-12.10.2011) und „Datenschutzaudit: Best Practice“ (13.-14.10.2011).

Die nächste Gelegenheit zur TISP-Zertifizierung bietet Secorvo College mit der T.I.S.P.-Schulung vom 17.-22.10.2011 (einschließlich Prüfung).

Die Programme aller Seminare und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Tag der IT-Sicherheit

Wer am 14.07.2011 den mit ca. 100 Besuchern hervorragend besuchten 3. Tag der IT-Sicherheit in der IHK Karlsruhe verpasst hat, findet die Unterlagen der Referenten auf den Webseiten der IHK unter der Dokumentennummer 83415 und eine Pressemitteilung der KA-IT-Si zum Download.

Zum Vormerken: Das nächste KA-IT-Si-Event findet am 22.09.2011 im Panoramasaal der IHK-Karlsruhe statt (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2011	
04.-07.08.	DEFCON 19 (DEFCON, Las Vegas/US)
10.-12.08.	20th USENIX Security Symposium (Usenix, San Francisco/US)
14.-18.08.	Crypto 2011 (IACR, Santa Barbara/US)
September 2011	
13.-14.09.	Cybersecurity 2011 (Handelsblatt, EUROFORUM, Berlin)
19.-23.09.	OWASP Global AppSec North America (OWASP Foundation, Minneapolis/US)
27.-29.09.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Oktober 2011	
05.-06.10.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
24.-27.10.	it-sa (SecuMedia Verlag, Nürnberg)
26.-29.10.	hashdays security & risk conference 2011 (DEFCON Switzerland, Luzern/CH)

Fundsache

Das German Chapter des Berufsverbands ISACA hat am 17.05.2011 einen Prüfleitfaden zur Auftragsdatenverarbeitung (§ 11 BDSG) publiziert. Der knapp 40seitige Leitfaden enthält Prüffragen zu den acht in der Anlage zu § 9 BDSG geforderten Maßnahmenbereichen mit Bezügen zu COBIT (4.1), ISO 27xxx und BSI IT-Grundschutz.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2011



Risiko-Awareness

Bruce Schneier – ein verlässlicher Garant für originelle und scharfsinnige Einschätzungen – veröffentlichte im Februar 2007 ein bemerkenswertes Essay zur „Psychologie der Sicherheit“ (aktualisiert im Januar 2008). Darin fasst er zahlreiche Erkenntnisse der Psychologie zur Risiko-Wahrnehmung zusammen, die vor allem eines deutlich machen: Menschen schätzen Risiken immer wieder falsch ein – selbst dann, wenn sie über genügend Informationen verfügen.

Zwar geben wir vor (und bemühen uns bisweilen), Risiken nüchtern zu analysieren. Tatsächlich aber dominieren intuitive Bewertungen unser Handeln. So neigen wir dazu, spektakuläre, plötzliche und extern verursachte Risiken – wie die Gefahr einer Atomkatastrophe nach den Ereignissen in Fukushima – überzubewerten, während wir unerwünschte Risiken, die zudem nicht uns, sondern andere betreffen, unterschätzen (wie die Gefahr einer Massenpanik bei der Loveparade durch die Verantwortlichen in Duisburg).

Auch „gewohnte“ Risiken (wie die ca. 4.000 Verkehrstoten pro Jahr) werden meist unterbewertet – niemand lässt deshalb sein Auto stehen –, während bei neuen Risiken, über die gesprochen wird und die uns oder unsere Kinder direkt bedrohen – wie die EHEC/HUS-Infektion mit 50 Toten – gleich die halbe Nation den Verzehr von Gemüse einstellt.

So ergeht es uns auch mit Unternehmensrisiken. Weder ein Mehr an Information noch die Etablierung von Risikoanalyseverfahren wird daran etwas ändern – denn, wie Bruce Schneier zutreffend folgert, werden wir nur dann zu zutreffenden Risikobewertungen und angemessenen Reaktionen kommen, wenn „unser Sicherheitsgefühl mit der Sicherheitswirklichkeit übereinstimmt“.

Um das zu erreichen helfen intensive Risikodiskussionen wohl eher als trockene Analysen – und Awareness-Maßnahmen, die diffuse, anonyme, schleichende, verschwiegene und unerwünschte Risiken in unsere und die Wahrnehmung der Verantwortlichen rücken.



Inhalt

Risiko-Awareness

Security News

Mobile Keylogger

Kai su teknon, Facebook

Siemens S7 Hack

HTML 5 Security

Tracking-Tool der IVW

SIFT 2.1

Secorvo News

T.I.S.P. - Das Buch

Budenzauber

Security-Update 2011

2. Smart Grid Symposium

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Mobile Keylogger

Keylogger, die Tastatureingaben protokollieren, wären auch auf Smartphones keine Überraschung – ließen sich aber auch dort recht leicht erkennen. Am 09.08.2011 zeigten jedoch zwei Forscher der University of California auf dem 6. USENIX Workshop HotSec, wie man in Android-Handys aus den Bewegungssensoren einen Keylogger macht.

Zwar verfügt Android über eine Instanz, die den Zugriff auf bestimmte Ressourcen (Adressbuch, Telefon, Netzwerk ...) regelt. Möchte ein Programm eine dieser Ressourcen nutzen, muss der Entwickler dies „anmelden". Bei der Installation der „App" erhält der Benutzer eine Liste der Ressourcen, die das Programm nutzen möchte. Erscheint die Liste dem Nutzer nicht angemessen – etwa weil ein Kartenspiel Zugriff auf das Netzwerk, das Adressbuch usw. haben möchte – kann er sich gegen eine Installation entscheiden. Die Nutzung des Bewegungssensors dürfte allerdings den meisten Nutzern unverdächtig erscheinen.

Auch bei Smartphones ist spätestens jetzt die Zeit der „erkennbar harmlosen Anwendungen" vorbei. Ohne Personal Firewalls mit cleveren Heuristiken kann man nicht davon ausgehen, dass nur der Nutzer auf Daten und Anwendungen zugreifen kann.

Kai su teknon, Facebook

Trackingdienste zur Reichweitenmessung von Websites beschäftigen bereits seit geraumer Weile die Datenschutzaufsichtsbehörden (SSN 08/2010). Nach einer nun veröffentlichten eigenen Untersuchung hat das ULD Schleswig-Holstein am 19.08.2011 eine Aufforderung an sämtliche verantwortlichen Stellen des Landes gerichtet, die Verwendung der von Facebook angebotenen Social Plugins zu unterlassen.

Grund sind die von Facebook verwendeten Cookies sowie die nachweislich erfassten Daten und vorgenommenen Verknüpfungen: Beim Aufruf von Webseiten, die z. B. den Facebook „Like-me"-Button nutzen, werden sowohl angemeldete als auch nicht angemeldete Nutzer von Facebook erfasst. Das Zusammenführen dieser Nutzungsdaten mit Facebookprofilen ist dank der Cookies über die Dauer von zwei Jahren möglich. Eine solche Verknüpfung stellt einen Verstoß gegen § 15 Abs. 3 TMG dar.

Weder die Webseiten-Anbieter noch Facebook halten hierfür ausreichende Erklärungen zum Zweck und Umfang dieser Datenerhebungen bzw. –übermittlungen vor; ein klarer Verstoß gegen § 13 Abs. 1 TMG. Nach der seit dem 25.05.2011 direkt anwendbaren Änderung von Art. 5 Abs. 3 der europäischen Datenschutzrichtlinie für elektronische Kommunikation (RL 2009/136/EG) ist zudem die Einwilligung des Nutzers vor dem Setzen solcher Cookies erforderlich, was bislang allgemein missachtet wird.

Für den Fall der Zuwiderhandlung hat das ULD ab Oktober 2011 Untersagungsverfügungen nach § 38 Abs. 5 BDSG angekündigt. Vielleicht wird so die Beachtung des Datenschutzrechts zum Wettbewerbsfaktor zwischen Social Networks. Ein erster Schritt wäre eine ausreichende Transparenz der Anbieter über ihre Datenverarbeitung.

Siemens S7 Hack

Das ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) warnte am 03.08.2011 vor Schwachstellen in S7-300 SPS-Systemen: Mit auf der diesjährigen Black Hat vorgestellten Exploits von Dillon Beresford können über einen Remote-Zugang Abläufe in der Steuerung verändert werden. Auch wenn andere SPS-Systeme wie die S7-400 von dieser Schwachstelle nicht betroffen sind, ist sehr zu empfehlen, Steuerungssysteme grundsätzlich in eigenen Netz-Segmenten zu betreiben – und schon gar nicht mit dem Internet zu verbinden.

HTML 5 Security

Noch immer sorgen viele alte Sicherheitsprobleme mit Web-Anwendungen für Probleme (siehe SSN 07/2011), da kommt mit HTML 5 neues Ungemach.

Viele der neuen Features von HTML 5 bringen gänzlich neue Angriffsvektoren ins Spiel. Mit Veröffentlichung der Studie „A Security Analysis of Next Generation Web Standards" vom 01.08.2011 sorgt die ENISA hier auf 60 Seiten für eine gute Übersicht. Neue Funktionen von HTML 5 und damit verbundene Sicherheitsprobleme werden ausführlich erläutert – eine Leseempfehlung für alle, die verstehen wollen, welchen Sicherheitsherausforderungen die Entwickler von Web-Applikationen zukünftig gegenüber stehen werden.

Tracking-Tool der IVW

Mit dem Skalierbaren Zentralen Messsystem (SZM) der Fa. INFOnline misst die Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) seit Ende 2008 die Reichweite von Online-Medien. Der Hamburger Datenschutzbeauftragte Prof. Dr. Caspar hat in einer Presseerklärung vom 08.08.2011 die Bereitschaft der Beteiligten gewürdigt, das SZM, das auch von www.hamburg.de genutzt wurde (SSN 01/2011), hinsichtlich des Datenschutzes anzupassen. Das SZM orientiert sich nun an den Vorgaben des Düsseldorfer Kreises zur

Reichweitenmessung und kürzt das letzte Oktett der IP-Adresse. Außerdem wird ein Opt-Out für die Nutzer angeboten. Die Musterdatenschutzerklärung klärt umfassend über das IVW-Verfahren auf, bleibt allerdings bezüglich der eingesetzten Cookies vage.

Es darf jedoch bezweifelt werden, dass in dieser Sache bereits das letzte Wort gesprochen ist. Auch das SZM verwendet Cookies, die eine längerfristige Wiedererkennung ermöglichen. Es ist wahrscheinlich, dass diese durch das in Art. 5 Abs. 3 der EU-Datenschutzrichtlinie für elektronische Kommunikation (RL 2009/136/EG) geforderte Opt-In erfasst werden, da mindestens ein Identifikator dauerhaft auf dem Endgerät gespeichert wird. Zudem bleiben bislang sämtliche Lösungen der mit dem Nutzertracking verbundenen Probleme unbefriedigend, da sie entweder die meisten Nutzer nicht erreichen (Opt-Out-Cookie), zu Nutzerunfreundlichkeit führen (vorherige Einwilligung) oder die Personenbeziehbarkeit weiterer Daten neben der IP-Adresse außer acht lassen.

SIFT 2.1

Seit dem 04.08.2011 ist das generalüberholte SANS Investigative Forensic Toolkit (SIFT) für registrierte Nutzer verfügbar: ein sehr umfangreicher, hochaktueller forensischer Werkzeugkasten für Gegner einer „one click forensic", der die wichtigsten forensischen Entwicklungen der vergangenen zwölf Monate vereint.

Hervorzuheben sind die weitere Automatisierung der Zeitlinienerstellung mit log2timeline, die Vervollständigung der umfangreichen Sammlung von RegRipper-Plugins sowie die Aktualisierung des Speicheranalysewerkzeugs Volatility 2.0. Bei letzterem ist zu beachten, dass ältere Volatility-Scripts noch zu portieren sind. Thematisch wurde der Bereich Smartphones für die Analyse von iPhone, Blackberry und Android ergänzt. Allerdings genügt SIFT hier nicht allein – gerade bei iPhones ist viel Know-How für die erste Sicherung erforderlich.

SIFT sollte in keinem forensischen Arsenal fehlen; es liegt als verlässliches VMware-Image vor.

Secorvo News

T.I.S.P. – Das Buch

Mitte September wird es endlich verfügbar sein: das Begleitbuch zum T.I.S.P. Es führt, strukturiert in Anlehnung an das T.I.S.P.-Seminar, in die „Zentralen Bausteine der Informationssicherheit" ein. Neun der elf an der Erstellung beteiligten Autoren sind zugleich Referenten der nächsten T.I.S.P.-Schulung vom **17.–22.10.2011** (mit Prüfung) bei Secorvo College; alle Teilnehmer erhalten das Buch zur Vorbereitung vorab zugesandt. Es sind noch wenige Plätze verfügbar – bis zum **12.09.2011** sogar zum Frühbucherpreis.

Die Programme weiterer Seminare und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Budenzauber

Ein wirkungsvoller Informationsschutz steht und fällt mit dem sicherheitsbewussten Verhalten aller Mitarbeiter eines Unternehmens. Doch wie sensibilisiert man die Mitarbeiter nachhaltig für Informationssicherheit? Dieser Frage geht Dirk Fox auf dem kommenden KA-IT-Si-Event am **22.09.2011** im Panoramasaal der IHK Karlsruhe nach. In seinem Vortrag „Security Awareness in der Praxis" fasst er Erfahrungen aus zahlreichen Security Awareness Kampagnen großer und mittelgroßer Unternehmen der vergangenen Jahre zusammen und gibt Empfehlungen für ein wirkungsvolles Vorgehen. Die Veranstaltung beginnt um 18:00 Uhr. Um Anmeldung wird gebeten.

Security-Update 2011

„Für Hacker gibt es kaum noch Grenzen", titelte die WirtschaftsWoche am 01.08.2011. Tatsächlich kann sich heute kein erfolgreiches Unternehmen – und sei es noch so klein – vor Angriffen auf seine Infrastruktur sicher wähnen. In einem Land, das seinen wirtschaftlichen Erfolg Ideenreichtum und Wissen verdankt, setzt ein nachlässiger Umgang mit Daten jedoch die eigene Zukunft aufs Spiel.

Geschäftsführer und Vorstände wissen um diese Risiken – allerdings ändern sich Bedrohungs- und Gesetzeslage ständig. Mit dem „Sicherheits-Update 2011„ am 05.10.2011 wollen LEITWERK, Secorvo und Securiton Abhilfe schaffen: Drei Expertenvorträge geben Einblick in die wesentlichen Fragestellungen – und das anschließende Come Together die Gelegenheit zum Erfahrungsaustausch.

2. Smart Grid Symposium

Nach dem großen Erfolg des „Smart Grid Symposiums" im Februar dieses Jahres freuen wir uns, Sie zu unserem 2. Smart Grid Symposium am **29.–30.11.2011** in der Buhlschen Mühle in Ettlingen einladen zu können. Es erwarten Sie spannende Vorträge rund um den Datenschutz und die Datensicherheit im Smart Grid, u. a. vom Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundesverband der Energie- und Wasserwirtschaft (BDEW) und der EnBW. Werfen Sie einen Blick auf das Programm – wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2011	
13.-14.09.	Cybersecurity 2011 (Handelsblatt, EUROFORUM, Berlin)
19.-23.09.	OWASP Global AppSec North America (OWASP Foundation, Minneapolis/US)
27.-29.09.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Oktober 2011	
05.10.	Security-Update 2011 (Leitwerk/Secorvo/Securiton, Appenweier)
05.-06.10.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
11.-13.10.	it-sa (SecuMedia Verlag, Nürnberg)
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
26.-29.10.	hashdays security & risk conference 2011 (DEFCON Switzerland, Luzern/CH)
November 2011	
11.-13.11.	FIfF Jahrestagung 2011 zur Dialektik der Informationssicherheit (FIfF e.V., München)
29.-30.11.	2. Smart Grid Symposium (Secorvo, KA-Ettlingen)

Fundsache

Die Darstellung von Herausforderungen der Web-Anwendungssicherheit muss nicht trocken daher kommen. Die zur Zeit aus drei Videos bestehende OWASP Appsec Tutorial Series informiert verständlich und unterhaltsam über aktuelle Fragestellungen.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Michael Knopp, Klaus J. Müller, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2011



Wem ist noch zu trauen?

Kürzlich ließ sich eine Zertifizierung beobachten, die heftige Zweifel an der Praxis der Vergabe von Zertifikaten aufkommen lässt. Dabei handelte es sich nicht um den Commodo- oder DigiNotar-Hack, sondern um eine irreführende TÜV-Zertifizierung einer Billig-Wetterstation.

Der Vorfall wäre wenig mehr als eine amüsante Anekdote, wären nicht zahlreiche deutsche Webseiten und IT-Produkte mit ähnlichen TÜV-Siegeln verziert – so auch Version 9 des Internet Explorers (SSN 05/2011).

Zweifelhaft daran ist weniger die der Zertifizierung vorausgegangene Prüfung, denn diese ließe sich nur beurteilen, wenn bekannt wäre, *wofür genau* (IE9) oder *nach welchen Kriterien* (Wetterstation) die Prüfung erfolgte. In beiden Fällen schweigt der TÜV sich darüber jedoch aus: Betriebsgeheimnis. Und wie ist das mit den TÜV-Siegeln zahlreicher Webseiten? Welche Zusicherung ist mit einem solchen Siegel verbunden?

Transparenz ist gerade bei Prüfverfahren, die nicht nach internationalen Standards erfolgen, besonders wichtig, da ein Siegel andernfalls zu missbräuchlicher Verwendung einlädt – erst recht, wenn der Zertifizierer eigentlich im Ruf steht, sein Handwerk zu verstehen. Geheimniskrämerei oder Selbstgefälligkeit sind hier fehl am Platz – sie leisten nur Nachlässigkeit oder gar Betrug Vorschub.

Der Wert von Zertifikaten – ob vom TÜV oder von einer CA – beruht darauf, dass dem Aussteller vertraut wird, und dazu gehört, dass die Prüfung nach höchsten Maßstäben der Sorgfalt erfolgt. Fragwürdige oder gar irreführende Zertifizierungen können das Fundament jeder Vertrauensinfrastruktur ins Wanken bringen. Die TÜVs sind seit Jahrzehnten eine Institution, deren Name für Verlässlichkeit steht. Umso schlimmer ist es, wenn sich ausgerechnet der TÜV für zweifelhafte Siegel und Gutachten hergibt.

Wem soll man dann noch vertrauen?



Inhalt

Wem ist noch zu trauen?

Security News

Haftung bei Phishing

*Dis*Trust-Center

Konformes Google Analytics?

Datenschutzkritik

Verkehr der Zukunft – eCall

Secorvo News

Secorvo College aktuell

Security-Update 2011

Zweites Smart Grid Symposium

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Haftung bei Phishing

Das Landgericht Landshut hat am 14.07.2011 über die Haftung einer Bank nach einem erfolgreichen Phishing-Angriff auf das iTAN-Verfahren entschieden. Das Verhalten des Klägers, der gegenüber den Angreifern 100 TAN-Nummern durch Eingabe auf deren Seite preisgegeben hatte, wurde als fahrlässig, nicht aber als grob fahrlässig gewertet.

Nach § 675v Abs. 2 BGB haftet die Bank bei einem unautorisierten Zahlungsvorgang nur dann nicht, wenn der Kunde diesen betrügerisch, absichtlich oder grob fahrlässig ermöglicht hat. Grobe Fahrlässigkeit liegt bei einer Missachtung allgemein einleuchtender Überlegungen und einem damit einher gehenden diesbezüglichen schweren Verschulden vor. Die Unerfahrenheit des Klägers im Umgang mit Computern und seine sprachlichen Defizite mussten im vorliegenden Fall berücksichtigt werden.

Die Bank hatte ihre Kunden darauf hingewiesen, TANs nur zu verwenden, wenn zuvor *z. B.* eine Überweisung erfasst worden sei. Das Landgericht sah diesen Hinweis vor allem durch das „z. B." als zu unpräzise an, zumal der Trojaner SpyEye den Kläger auf eine Website lenkte, die äußerlich der Originalseite entsprach und die die nach dem Login geforderte TAN-Eingabe ausdrücklich als besondere Ausnahme darstellte. Erst recht könne die Bank dem Kläger nicht die Wahl des unsicheren von mehreren angebotenen Authentisierungsverfahren vorwerfen.

Für die Konstruktion von Trojanern stehen schon lange Baukästen wie Zeus bereit. Auch Smartphone-Betriebssysteme sind längst im Visier. Die Frage, ab welcher Grenze der Nutzer eine gestellte Falle erkennen muss, bleibt von den Umständen des Einzelfalls abhängig, doch mit steigender Qualität der Attacken wird die Chance der Banken schwinden, dem Kunden grobe Fahrlässigkeit vorzuwerfen. Sowohl Rechtsprechung als auch Gesetzgebung sind offenbar geneigt, dem Kunden ein hohes Maß an Unbesonnenheit zuzugestehen.

*Dis*Trust-Center

Über den Einbruch beim Trust-Center DigiNotar vom 17.06.-22.07.2011 (der ja nicht der erste Trust-Center-Einbruch war), den folgenden Lizenzentzug durch die niederländische Regierung am 14.09.2011 und die letztliche Liquidation des Unternehmens am 20.09.2011 wurde in verschiedenen Medien ausführlich berichtet. Was lehrt uns dieser Fall?

- Die Trust-Center-Branche betreibt nicht annäherungsweise ein Fraud-Management, wie es bei Finanz- und Zahlungsdienstleistern üblich ist. Ein Zertifikatsantrag für eine der weltweiten Top-Websites darf einfach nicht automatisiert ohne manuelle Prüfung zu einem Zertifikat führen.
- Das Krisenmanagement von GlobalSign, die angeblich ebenfalls kompromittiert wurden, war – Im Vergleich etwa zu RSA Security – geradezu vorbildlich und Vertrauen erweckend: Der Betrieb wurde gestoppt und häufige Updates zu den sofort eingeleiteten Sicherheitsuntersuchungen veröffentlicht. Eine seltene Ausnahme.
- Viele Trustcenter verschweigen schamhaft, wie viele ihrer qualifizierten Signaturzertifikate in Umlauf sind. In diesem Fall wurde es für DigiNotar öffentlich: 4.200.
- Der eigentliche Vertrauensanker für SSL/TLS sind nicht die Trust-Center, sondern die Browser-Hersteller, die deren Root-Zertifikate installieren oder löschen und jetzt schärfere Kontrollen fordern. Kaum ein Anwender kann sich die Mühe machen, etliche Dutzend vorinstallierter Roots (von denen viele noch nicht einmal mehr dem Unternehmen gehören, das sich vor Jahren im Root-Zertifikat „verewigt" hat) zu durchforsten.

Der letztgenannte Punkt könnte sich in den nächsten Jahren ändern, wenn TLS-Zertifikate per DANE über DNS verteilt werden. Dann würden die DNSSEC-Schlüssel der DNS-Root Zone zum Vertrauensanker für TLS – die Single Internet Root 2.0.

Konformes Google Analytics?

Kurz nachdem Prof. Dr. Caspar, Landesdatenschutzbeauftragter Hamburgs, das Verfahren des Reichweitenmessdienstleisters INFOnline (SSN 08/2011) als rechtskonform anerkannt hat, ist einer Pressemeldung vom 16.09.2011 nun auch seine Anerkennung der Anpassungen von Google Analytics zu entnehmen. Danach habe Google die Forderungen des Düsseldorfer Kreises vom 26./27.11.2009 durch die Verkürzung der IP-Adresse, das Bereitstellen eines Opt-Out-Verfahrens und seine Datenschutzhinweise erfüllt. Auf die Notwendigkeit späterer Anpassungen, sollte das Erfordernis eines Opt-In für die verwendeten Cookies eingeführt werden, wird am Rande hingewiesen.

Dennoch dürfen diese Aussagen nicht als Freifahrtschein für Webseitenanbieter verstanden werden. Jene werden zunächst die nach § 13 TMG geforderte Transparenz auf den Datenschutzerklärungen ihrer Webseiten herstellen müssen. Vor der Nutzung ist ein Auftragsdatenverarbeitungsvertrag abzuschließen und durch Löschung des alten Accounts für die Löschung der Altdaten zu sorgen.

Auch bei einer – vom Seitenanbieter zu veranlassenden – Kürzung der IP-Adressen bleibt die Datenverarbeitung im EG-Ausland ein Problem, das der Rechtskonformität durch Auftragsdatenverarbeitung im Weg steht. Selbst wenn der Webseitenbetreiber also seine Pflichten erfüllt (was sich der Überprüfung durch den Nutzer entzieht), bleibt die Rechtskonformität zweifelhaft, daher ist von einer Nutzung von Google Analytics weiterhin abzuraten.

Datenschutzkritik

Mit ihrem Einschreiten gegen eine Reihe von Diensten der Branchenriesen Google und Facebook haben Datenschutzbehörden in jüngster Zeit Schlagzeilen gemacht. In der Blogger-Szene werden die zweifelhaften Erfolge bereits als „Datenschutztheater" bezeichnet.

So sind das Verpixeln von einzelnen Häusern in Straßenzügen mit gleichartigen Reihenhäusern, die durchgesetzte Verkürzung von IP-Adressen unter gleichzeitiger Nutzung von mindestens gleichwertigen weiteren Identifikationsmerkmalen (Cookies) bei Tracking-Diensten oder die eher halbherzige Auseinandersetzung mit Facebooks Gesichtserkennung in der Tat Beispiele für „Datenschutzerfolge", die bestenfalls einzelne Symptome behandeln, das dahinter stehende Problem jedoch ungelöst lassen. Gleichzeitige Bestrebungen des Staates, eigene Datenbanken oder Überwachungsmittel wie die Vorratsdatenspeicherung neu oder wieder einzuführen, schwächen die Glaubwürdigkeit weiter.

Die Ziele des Datenschutzes angesichts immer vielfältigerer Mittel zur Verknüpfung von Informationen und einer Zunahme von verfolgbarem Kommunikationsverhalten umzusetzen wird nicht leichter, weder für den Gesetzgeber noch für die Exekutivorgane und Anwender. Es ist jedoch – und darin ist den Kritikern recht zu geben – dringend erforderlich, die vorhandenen Regeln konsequent umzusetzen. Auf der anderen Seite sind der Schutzbedarf und die angeordneten Mittel auf allen Ebenen zu überprüfen. Ansonsten droht eine substantielle Schwächung des Schutzumfangs der informationellen Selbstbestimmung.

Verkehr der Zukunft – eCall

In einer Empfehlung vom 08.09.2011 hat die EU-Kommission gefordert, anschließend an die europaweite Einführung der Notrufnummer 112 einen eCall als automatisierten Notruf aus Fahrzeugen einzuführen. Dieser Notruf mit einem standardisierten Minimaldatensatz soll von den Fahrzeugsystemen selbst erzeugt und genau wie ein 112-Notruf behandelt werden. Die Empfehlung gibt Definitionen und Standards vor, die eine europaweite Einheitlichkeit der Systeme sicherstellen sollen.

Eine Kommissionsempfehlung ist rechtlich unverbindlich, d. h. es ergibt sich hieraus keine Umsetzungsverpflichtung für die Mitgliedstaaten. Wird ein entsprechendes System eingeführt, sind die Maßgaben jedoch zu berücksichtigen. Die Einführung eines eCalls wird zur Einführung von eigenen Mobilkommunikationswegen in Fahrzeugen führen. Es ist absehbar, dass diese Entwicklung nicht beim eCall-Dienst stehen bleiben wird. Die entstehenden Datenschutz und Sicherheitsfragen werden daher künftig im Auge zu behalten sein.

Secorvo News

Secorvo College aktuell

Für die nächste T.I.S.P.-Schulung vom 17.-22.10. 2011 (einschließlich Prüfung) bei Secorvo College sind noch vier Plätze frei. Schnellentscheider erhalten unmittelbar nach Eingang der Anmeldung das Begleitbuch zum T.I.S.P. zur Prüfungsvorbereitung zugesandt (im Seminarpreis inbegriffen).

Im November folgen die Seminare PKI – Grundlagen, Vertiefung, Realisierung (08.-11.11.2011), IT-Sicherheit heute (15.-17.11.2011) und Certified Professional for Secure Software Engineering (CPSSE) mit anschließender Zertifikatsprüfung (22.-25.11. 2011). Die Programme aller Seminare, die Bewertungen unserer Teilnehmer und die Möglichkeit zur Online-Anmeldung finden Sie hier.

Security-Update 2011

Kein erfolgreiches Unternehmen kann sich mehr vor Angriffen auf seine Infrastruktur sicher wähnen. In einem Land, das seinen Erfolg Ideenreichtum und Wissen verdankt, setzt ein nachlässiger Umgang mit Daten jedoch die Zukunft aufs Spiel. Zwar wissen Unternehmen von diesen Risiken – allerdings ändern sich Bedrohungs- und Gesetzeslage ständig. Mit dem „Sicherheits-Update 2011„ am 05.10.2011 wollen LEITWERK, Secorvo und Securiton Abhilfe schaffen: Drei Expertenvorträge beleuchten die wesentlichen Fragestellungen – mit anschließender Gelegenheit zum Gedankenaustausch am Buffet.

Zweites Smart Grid Symposium

Vom 29. bis 30.11.2011 findet das "2. Smart Grid Symposium" in der Buhlschen Mühle in Ettlingen statt. Es erwarten Sie spannende Vorträge rund um Datenschutz und Datensicherheit im „intelligenten Stromnetz", u. a. vom Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundesverband der Energie- und Wasserwirtschaft (BDEW) sowie der EnBW. Werfen Sie einen Blick in das Programm – wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2011	
05.10.	Security-Update 2011 (Leitwerk/Secorvo/Securiton, Appenweier)
11.-13.10.	it-sa (SecuMedia Verlag, Nürnberg)
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
26.-29.10.	hashdays security & risk conference 2011 (DEFCON Switzerland, Luzern/CH)
November 2011	
08.-11.11.	PKI (Secorvo College, Karlsruhe)
11.11.	Outsourcing und Vendor Security (Gesellschaft für Informatik/Fachgruppe SECMGT, Frankfurt)
11.-13.11.	FIfF Jahrestagung 2011 zur Dialektik der Informationssicherheit (FIfF e.V., München)
15.-17.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
22.-23.11.	ISSE 2011 (TeleTrusT, Prag/CZ)
22.-25.11.	CPSSE (Secorvo College, Karlsruhe)
29.-30.11.	2. Smart Grid Symposium (Secorvo, KA-Ettlingen)
Dezember 2011	
05.-06.12.	IsSec/ZertiFA 2011 (Computas., Berlin)

Fundsache

Am 26.09.2011 hat das US-amerikanische NIST den Draft der Special Publication SP 800-153 "Guideline for Securing Wireless Local Area Networks (WLAN)" publiziert. Auf kompakten 12 Seiten gibt sie konkrete Empfehlungen zur Absicherung von WLANs – auch wertvoll für den privaten Router. Die Kommentierungsfrist endet am 28.10.2011.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2011



Untragbar unerträglich

Gelegentlich ist es unerfreulich, mit einer Prognose richtig gelegen zu haben. Die Erkenntnisse um die vom Chaos Computer Club mit der am 08.10.2011 publizierten Analyse eines „Staatstrojaners“ ausgelösten Recherchen übertreffen jedoch die schlimmsten Befürchtungen. Da ist zunächst das Unternehmen, das die Überwachungssoftware im Auftrag von LKAs und BND entwickelte: Dessen früherer Geschäftsführer wurde nach Erkenntnissen des Handelsblatts 2002 wegen Bestechung zu 1,5 Mio. € Geldbuße und 21 Monaten auf Bewährung verurteilt, und zumindest von Web-Sicherheit versteht es nicht allzu viel. Dann ist da die Software: Sie verschlüsselt die zu übermittelnden Daten mit einem immer gleichen AES-Schlüssel und kann über nachladbare Module sowohl zur Quellen-TKÜ als auch zur Online-Durchsuchung eingesetzt werden. Für letztere hat das BVerfG in seinem Urteil vom 27.02.2008 sehr hohe materielle Zulässigkeitsvoraussetzungen formuliert: „*Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.*“ Anders als bei einer (Quellen-) TKÜ genügen z. B. Verstöße gegen das Betäubungsmittelgesetz diesem Kriterium nicht.

Dass es keine gute Idee ist, die Entscheidung über den Funktionsumfang in die Hand der Strafverfolgung zu legen, zeigt das Urteil des LG Landshut vom 20.01.2011: Bei der Umsetzung eines Quellen-TKÜ-Beschlusses des Amtsgerichts wurden von den bayerischen Strafverfolgungsbehörden mit der Software im 30-Sek.-Takt rechtswidrig 66.000 Screenshots erzeugt. Möglicherweise kein Einzelfall.

In einem Rechtsstaat ist auch die Exekutive an Gesetz und Verfassung gebunden – vor allem das unterscheidet ihn von einer Willkürherrschaft. Ein Landesinnenminister, der einen solchen Rechtsbruch verteidigt, ist daher nicht nur unerträglich, sondern untragbar.



Inhalt

Untragbar unerträglich

Security News

Bepper-Trojaner

Grundschutz EL 12

CAINE erneuert

Risiken der Überwachung

Immer wieder Facebook

Security Theatre in der Cloud

Secorvo News

Kaminlektüre

Seminare

Durch die Hintertür

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Bepper-Trojaner

Immer häufiger werden QR-Codes (zweidimensionale Barcodes) als Link zu weiterführenden Informationen in Zeitschriften, auf Plakaten, Webseiten oder Eintrittskarten angegeben. Diese Grafik kann mit einem Handy oder Smartphone abfotografiert und weiterverarbeitet werden, so dass der interessierte Nutzer auf der darin angegebenen Website landet, ohne eine URL eintippen zu müssen.

Am 30.09.2011 berichtete Denis Maslennikov von Kaspersky Labs über einen Angriff, bei dem auf über QR-Codes referenzierten Webseiten dem Smartphone-Benutzer – ähnlich wie bei einem SMS-Trojaner – eine mit Schadsoftware angereicherte Version eines mobilen ICQ-Clients untergeschoben wird. Theoretisch war ein solcher „Bepper-Trojaner" (umgangssprachlich für „Aufkleber") bereits einige Wochen zuvor beschrieben worden.

Ein gutes Beispiel dafür, wie aus einem ergonomischen Feature eine Angriffsmöglichkeit wird. Wer QR-Codes nutzt, sollte auf keinen Fall Software oder Apps auf diesem Weg beziehen.

Grundschutz EL 12

Seit dem 11.10.2011 steht die aktualisierte und erweiterte Version der BSI-Grundschutzkataloge in der 12. Ergänzungslieferung (EL) im PDF-Format mit dokumenteninternen Sprungmarken online zur Verfügung. Die HTML-Version, die von freien Werkzeugen wie z. B. verinice genutzt wird, bleibt vorerst jedoch auf dem Stand der 11. EL. Für das GSTOOL 4.7 wurde indes bereits eine Aktualisierung (Servicepack 3 und zugehörige Metadaten) für November und Dezember 2011 angekündigt, Version 5.0 soll im 2. Quartal 2012 verfügbar sein.

Zeitgleich mit der Ergänzungslieferung wurden auch eine aktualisierte „Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz" sowie die Formblätter und Kreuzreferenztabellen, die viele Unternehmen als Grundlage für eigene Arbeitswerkzeuge nutzen, vom BSI bereitgestellt. Neben neuen Bausteinen wie „Virtualisierung" (B 3.304) und „Terminalserver" (B 3.305) wird für ein produktunabhängiges Vorgehen bei Webservern in der 12. EL nur noch der generische Baustein „Webserver" (B 5.4) genutzt. Ein richtiger Schritt angesichts der sich schnell ändernden Technologie. Ein Hinweis auf die OWASP-Top 10 wäre dort allerdings sinnvoll gewesen.

CAINE erneuert

Seit dem 19.09.2011 ist die frei nutzbare Live-CD-Forensikdistribution CAINE (Computer Aided INvestigative Environment), die auf Ubuntu basiert, in der überarbeiteten Version 2.5 verfügbar. Auch gibt es eine spezielle USB-Stick-Version.

Besonders hilfreich sind die stark erweiterten NAUTILUS-Scripts für das direkte Einsehen von Dateiinformationen von z. B. gelöschten Dateien und Bilddaten. Ein besonderes Schmankerl ist das unscheinbare Script „FileInfo", welches über die Option „Metadatenextraktion" die Inhalte von SQLite-Datenbanken ausliest, die z. B. von Firefox, Nokia OVI, Skype und Apples iPhones genutzt werden. Abgerundet wird der positive Eindruck durch das Werkzeug frag_find, mit dem z. B. Dokumententeile über identische Sektoren-Hashwerte gefunden und nachgewiesen werden können, vorausgesetzt, dass bei einer Untersuchung das nachzuweisende Dokument digital vorliegt.

Risiken der Überwachung

Das Landgericht Lüneburg hatte am 28.3.2011 über die Rechtmäßigkeit der Beschlagnahme der GPS-Überwachungsanlage eines Privatdetektivs zu entscheiden. Die Anlage wurde zur lückenlosen Verfolgung des Aufenthaltsortes u. a. von Arbeitnehmern beim Verdacht missbräuchlicher Krankschreibungen eingesetzt. Zu diesem Zweck wurde sie an den Fahrzeugen der Zielpersonen angebracht. Dagegen hatte der niedersächsische Landesdatenschutzbeauftragte Strafanzeige gestellt.

Das Landgericht sah darin den Anfangsverdacht einer entgeltlichen unbefugten Erhebung und Verarbeitung personenbezogener Daten (§ 44 i.V.m. § 43 Abs. 2 Nr. 1 BDSG). Sollte die Entscheidung eines anschließenden Strafverfahrens der des Landgerichts folgen, die nicht die erste mit ähnlicher Tendenz ist, dürfte dies sowohl dem Auskunfteigewerbe als auch Auftraggebern privater Überwachungsmaßnahmen deutliche Grenzen setzen.

Immer wieder Facebook

Auf der Entwicklerkonferenz f8 am 22.09.2011 stellte Facebook neue Funktionen vor. So ermöglicht Facebook Timeline dem Nutzer nun, zurückliegende Erlebnisse oder Ereignisse an einer übersichtlichen Zeitleiste – wie eine persönliche „Chronik" – einzustellen. Und unter der Bezeichnung „frictionless sharing" kann man durch einmalige Einverständniserklärung gegenüber Facebook Webdiensteanbietern und Smartphone-Apps erlauben, alle eigenen Aktivitäten an Facebook zu melden. Dieses „Tracking" des gesamten digitalen Lebens (Welche Musik kaufe ich gerade? Auf welcher Seite surfe ich? Welches Online-Spiel habe ich eben gestartet?) kann dann mit Freunden geteilt werden.

In Europa sind mit diesen Diensten die nächsten Rechtsstreitigkeiten vorprogrammiert. Wie bislang wird es auch dabei nicht darum gehen, ob der Nutzer seine Daten in dieser Form der Welt oder Facebook preisgeben darf, sondern dass nach deutschem Datenschutzrecht die Diensteanbieter verantwortliche Stelle für die Übermittlung der Nutzungsdaten sind. Daher benötigen sie als Folge von § 15 TMG jeweils separate Einwilligungen, bei denen sie – deutlich weitergehend als in den Datenverwendungsregeln von Facebook – über Zweck und Art der Nutzung dieser Daten werden aufklären müssen. Dies gilt zumindest für alle europäischen Diensteanbieter und solche, die gezielt in Deutschland anbieten.

Solange sich Facebook außerdem Zweckänderungen und umfangreiche eigene Verarbeitungen vorbehält, selbst nicht umfassend aufklärt und keine ausreichende Einwilligung einholt, ist zudem Facebooks eigene Verarbeitung der Nutzerdaten rechtswidrig. Der Aktivist Max Schrems hat daher gegen Facebooks europäische Niederlassung in Irland wegen 22 Verstößen gegen europäisches Datenschutzrecht Anzeige erstattet.

Der Streit um und mit Facebook steht exemplarisch für die zahlreichen grundsätzlichen Missachtungen der Persönlichkeitsrechte im Internet – und des geltenden deutschen und europäischen Rechts.

Security Theatre in der Cloud

Am 04.10.2011 kündigte Amazon an, dass ab sofort Daten im Amazon Web Service (AWS) S3 durch eine serverseitige Verschlüsselung (SSE) geschützt werden können - eine Meldung, die in der deutschen Presse viel Resonanz gefunden hat. Diese Verschlüsselung erlaubt die „transparente Absicherung" von Daten in der Cloud – durch Amazon, inklusive der Erzeugung, Verwaltung und Vernichtung von Schlüsseln. Da stellt sich die Frage: Was genau wird hier eigentlich geschützt? SSE bewahrt die auf Amazon-Rechnern gespeicherten Daten vor Preisgabe bei einem Diebstahl der Datenträger aus dem Rechenzentrum. Damit schützt Amazon mit viel Wirbel gegen ein eher kleines Risiko.

Einen deutlich besseren Schutz bietet die Client-seitige Verschlüsselung mit dem AWS JDK for Java. Vielleicht möchte Amazon diesen Mechanismus aber gar nicht so gerne bewerben – schließlich macht er die Anwendungsentwicklung aufwändiger. Und die amerikanischen Sicherheitsbehörden sind dabei auch ausgesperrt.

Secorvo News

Kaminlektüre

Über vier Jahre haben wir daran geschrieben, und nach nur sechs Wochen war es so weit: Die erste Auflage des Secorvo-Buchs „Zentrale Bausteine der Informationssicherheit", auch als Begleitbuch zum T.I.S.P. geeignet, ist ausverkauft. Auflage zwei ist bereits im Druck und voraussichtlich ab der ersten Novemberwoche verfügbar. Wem also noch eine Kaminlektüre für die langen Winterabende fehlt, dem sei das Werk ans Herz gelegt. Bei einer Anmeldung zum T.I.S.P.-Seminar (nächster Termin: 07.-11.05.2012) ist das Buch inklusive und wird vorab zugesandt.

Seminare

Für alle Kurzentschlossenen bietet Secorvo noch drei Weiterbildungschancen (mit garantierter Durchführung) im Jahr 2011:

- Das Seminar PKI – Grundlagen, Vertiefung, Realisierung vom 08.-11.11.2011 bietet Ihnen einen Einblick in die Konzeption, Implementierung und Nutzung von PKIs.
- Ihre IT-Security-Grundlagenkenntnisse können Sie beim Seminar IT-Sicherheit heute vom 15.-17.11. 2011 auffrischen.
- Eine praxisorientierte Einführung in die sichere Softwareentwicklung bekommen Sie beim Seminar ISECCO Certified Professional for Secure Software Engineering (CPSSE) vom 22.-24.11.2011 mit anschließender Zertifikatsprüfung.

Sichern Sie sich jetzt einen der noch freien Plätze. Die Programme aller Seminare, die Möglichkeit zur Online-Anmeldung und das Jahresprogramm 2012 finden Sie unter http://www.secorvo.de/college. Wir freuen uns auf Ihre Anmeldung!

Durch die Hintertür

Die Erbringung von IT-Dienstleistungen erfordert in wachsendem Umfang den Fernzugriff auf IT-Systeme. Wie kann man sich dabei aber gegen Zugriffe unberechtigter Dritter und einen unkontrollierten Datenabfluss schützen? Was ist bei der Fernwartung heute „state-of-the-art" – und von welchen Techniken sollte man besser die Finger lassen?

Diese und weitere Fragen rund um die Absicherung von Wartungszugriffen beantwortet Dr. Böttger (Leiter CONNECT-SupportCenter) in seinem Vortrag auf dem kommenden Event „Wer kommt da durch die Hintertür?" der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 17.11.2011 um 18 Uhr im Schlosshotel Karlsruhe. Um Anmeldung wird gebeten.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2011	
08.-11.11.	PKI (Secorvo College, Karlsruhe)
11.11.	Outsourcing und Vendor Security (Gesellschaft für Informatik/Fachgruppe SECMGT, Frankfurt)
15.-17.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
17.11.	Wer kommt da durch die Hintertür? (KA-IT-Si)
22.-25.11.	CPSSE (Secorvo College, Karlsruhe)
Dezember 2011	
05.-06.12.	IsSec/ZertiFA 2011 (Computas, Berlin)
Januar 2012	
17.-19.01.	OMNICARD 2012 (in TIME berlin, Berlin)
24.-26.01.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Februar 2012	
08.-09.02.	22. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	19. DFN Workshop „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)

Fundsache

Das NIST veröffentlichte am 27.09.2011 den Draft einer überarbeiteten Fassung der Special Publication SP 800-121 „Bluetooth Security“, die nun auch die Bluetooth-Standards 3.0 und 4.0 (Low Energy) berücksichtigt. Die Security-Checkliste ist auf 34 Empfehlungen angewachsen und ersetzt die Listen für Headsets und Smart Card Reader der Vorfassung.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

November 2011



Lest Märchen!

Kennen Sie Grimms Märchen? Nein, das ist *keine* iPhone-App. Es war einmal vor vielen, vielen Jahren, da las man den Kindern abends vor dem Kamin Märchen vor – bevorzugt die der Gebrüder Grimm von 1812. Mancher macht das noch heute – sei es aus Tradition, aus Nostalgie oder in Ermangelung anderer Kinderbücher. Oder auch, weil der Fernseher kaputt und der iPhone-Akku leer sind. Wie dem auch sei: Beim Lesen werden Sie feststellen, dass jedes Märchen zahlreiche Lehren enthält – und nicht nur die, die ins Auge springen. Einige davon helfen sogar der Informationssicherheit.

Nehmen wir beispielsweise das Märchen vom Wolf und den sieben Geißlein. Zur Erinnerung: Der Wolf will in Abwesenheit der Geiß deren Kinder zum Öffnen der Haustüre überreden – die aber erkennen ihn erst an der Stimme, dann an der Pfote. Als er beides tarnt, öffnen sie ihm – und er verschlingt alle bis auf das siebte, das sich im Uhrkasten versteckt hat. Weil er sich in der Nähe zum Schlafen legt, wird er später von der Geiß aufgeschlitzt – und die Geißlein befreit.

Was können wir daraus lernen?

1. Plausibilitäts-Checks sind kein wirksamer Schutzmechanismus. (Auch wer redet wie eine Geiß, kann ein Wolf sein.)
2. Die erfolgreiche Abwehr von Angriffen sollte ein Alarmsignal sein. (Der nächste Angriff ist sicher besser als der abgewehrte.)
3. Security Policies sind ohne Sensibilisierung und gesunde Skepsis wertlos. (Angreifer sind erfindungsreicher als Policy-Autoren.)
4. Das Fehlen interner Schutzwälle gibt dem erfolgreichen Eindringling alles preis. (Interne Schotts begrenzen den Angriffserfolg.)
5. Nur bei tierisch dummen Angreifern gibt es eine Chance, die erbeuteten Daten zurück zu erhalten.

Vielleicht darf man wenigstens hoffen, dass bei einem erfolgreichen Angriff 14,3 % der Informationen verschont bleiben. Verstecken Sie daher sicherheitshalber schon mal das Wichtigste im Uhrkasten.



Inhalt

Lest Märchen!

Security News

Ertappt

c = m

No, map!

OWASP.de gibt Gas

Europäischer Treibsand

Secorvo News

Secorvo College aktuell

Für den Weihnachtsmann

Krypto zum Anfassen

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Ertappt

Am 02.11.2011 hat der Hamburgische Datenschutzbeauftragte einen Bericht vorgelegt, der der Nutzung von Cookies durch Facebook nachgeht. Die dem Bericht zugrunde liegende Prüfung orientiert sich an den Zweckangaben, die Facebook unter anderem gegenüber dem ULD Schleswig-Holstein angeführt hat. Zu den einzelnen Zweckangaben wurden für die Prüfung Szenarien gebildet, die dann in einer sicheren Umgebung dokumentiert durchgespielt wurden. Ziel war, festzustellen, ob die verschiedenen Cookies die angegebene Wirkung zeigen würden.

So soll etwa der „datr"-Cookie gemäß Facebook Hinweise auf Missbrauch liefern, indem er feststellt, ob über denselben Browser viele verschiedene Accounts genutzt werden. Bei den durchgeführten Versuchen konnte eine solche Wirkung nicht bestätigt werden. Ähnliches gilt für zahlreiche andere Zweckangaben.

Daraus kann zwar nicht geschlossen werden, dass die Cookies, wie vielfach vermutet, domainübergreifend für das Nutzertracking genutzt werden. Es indiziert jedoch, dass Facebook für einen Teil seiner Cookies keinen zulässigen Verwendungszweck angeben kann. So lassen sich jedenfalls nicht in rechtskonformer Weise Nutzertransparenz herstellen und die Erforderlichkeit der Datenerhebung nachweisen.

Zu Recht stellt der Bericht mindestens einen Verstoß gegen die jeweiligen nationalen Umsetzungen von Art. 5 Abs. 3 der E-Privacy-Richtlinie fest. Bei den Aufsichtsbehörden dürfte Facebook damit weiteres Vertrauen verspielt haben.

c = m

Kryptografie kann so einfach sein. Das dachen wohl auch die Programmierer der Entwicklerversion von Ruby bei der Implementierung des RSA-Verfahrens:

Wenn $c = m^e \bmod n$ zu berechnen ist – dann geht das mit $e := 1$ am schnellsten. Damit folgt:

$$c = m \bmod n,\ m < n \Rightarrow c = m$$

Sollten Sie mit dieser Ruby-Version zwischen dem 01.09.2011 und dem 04.11.2011 RSA-Schlüssel erzeugt haben, dann ersetzen Sie diese besser schnellstmöglich. Denn wenn man bei DES schon Schlüssel als schwache Schlüssel bezeichnet, die bei zweimaliger Verschlüsselung den Klartext liefern,

$$DES(k, DES(k, m)) = m$$

muss man hier wohl von einem überschwachen Schlüssel mit RSA(k, m) = m reden.

No, map!

Um ein erneutes Marketing-Desaster wie die Diskussion um die Abbildung deutscher Hausfassaden in Street View zu vermeiden, geht Google bei der Lokalisierungsfunktion in die Offensive: Wie viele Standort-basierenden Dienste (*location-based services*) verfügt auch Google Maps seit einer Weile über einen Standortbestimmungsdienst, aktivierbar über den „Knopf" oberhalb der Zoom-Einstellung.

Da Google – anders als ein Smartphone – keinen direkten Zugriff auf Dienste des Netzbetreibers zur Standortbestimmung hat, wertet Google u. a. die SSIDs erreichbarer WLANs aus. Deren Standort-Daten wurden beim Fotografieren der Hausfassaden gleich mit erhoben oder von Nachbarn gemeldet – und werden in einer zentralen Datenbank (*Google Location Server, GLS*) vorgehalten.

Am 15.11.2011 machte Google publik, dass jeder, der mit seinem SSID (*service set identifier*) nicht im GLS aufgenommen werden möchte, die Löschung mit einem ungewöhnlichen „Opt-Out"-Mechanismus veranlassen soll: durch die Ergänzung der eigenen SSID um die Endung „_nomap".

Sieht man einmal von der Frage ab, wie vielen privaten WLAN-Nutzern wohl eine entsprechende Umkonfiguration des eigenen WLAN-Routers gelingt, ohne Schaden anzurichten, bleibt die Gefahr, dass das Beispiel Schule machen könnte: Weitere Endungen wie z. B. „_noiphone" oder „_noandroid" dürften die verfügbaren 32 Byte maximaler SSID-Länge schnell abschmelzen. Vielleicht sollten die Standardisierungsgremien besser schon mal mit Anpassungsarbeiten am IEEE 802.11 beginnen...

OWASP.de gibt Gas

Beim deutschen Chapter von OWASP hat sich im November viel getan. Am 16.11.2011 wurde die deutsche Übersetzung der OWASP Top 10 unter der Projektleitung von Kai Jendrian fertig gestellt und publiziert. Damit steht der anerkannte Branchenstandard nun auch in Deutsch zur Verfügung, um das Sicherheitsbewusstsein bei der Entwicklung von Webanwendungen zu verbessern – besonders bei Entwicklern in mittelständischen Unternehmen.

Am 17.11.2011 folgte in München der 4. German OWASP Day, bei dem sich mehr als 160 Experten über Sicherheitsfragen von Webanwendungen diskutierten. Zwei parallele Vortrags-Tracks deckten ein breites Spektrum an Themen ab – von Secure Software Development Life Cycle, Statischer Code Analyse über Web-Service-Security, Mobile Security und Browser-Sicherheit hin zu aktuellen Cyber-Bedrohungen. Ein Highlight war der Ausblick auf

bevorstehende Entwicklungen von Thomas Roessler (W3C).

Schließlich wurde am 19.11.2011 das Portal hacking-lab.com der OWASP Academy freigeschaltet, mit dem sich Entwickler und Sicherheitsfachleute an praktischen Anwendungen zur Sicherheit von Anwendungen fortbilden sollen.

Europäischer Treibsand

Der Europäische Gerichtshof hat am 24.11.2011 in einer Vorabentscheidung über die Auslegung von Art. 7 der Europäischen Datenschutzrichtlinie entschieden. Anlass war ein Rechtsstreit zwischen dem Verband spanischer Kreditinstitute (ASNEF), dem Verband für E-Commerce und Direkmarketing (FECEMD) und dem spanischen Staat. Nach der Entscheidung sind die nationalen Gesetzgeber auf die in Art. 7 aufgezählten Zulässigkeitstatbestände festgelegt und dürfen diese nicht weiter einschränken oder weitere Tatbestände einführen.

Nach Ansicht der Kläger geht Spanien in seinem Datenschutzgesetz über Art. 7 hinaus, indem es die Verarbeitung personenbezogener Daten für berechtigte Interessen des Verarbeiters ohne Einwilligung des Betroffenen nur für veröffentlichte Daten eröffnet. Dem hat der EuGH zugestimmt.

Den Mitgliedstaaten steht zwar offen, Leitlinien für die Abwägung zwischen dem Grundrechtsschutz der Betroffenen und den berechtigten Interessen aufzustellen, die den Unterschied zwischen veröffentlichten und unveröffentlichten personenbezogenen Daten berücksichtigen, er darf jedoch nicht durch den völligen Ausschluss unveröffentlichter Daten Art. 7 überschreiten. Dieser Grundsatz gelte allgemein für die Auslegung von Art. 7, der gleichzeitig für direkt anwendbar erklärt wurde.

Das deutsche Datenschutzrecht ist von der Entscheidung nicht direkt betroffen, da es in § 28 Abs. 1 Nr. 2 und 3 BDSG getrennte Tatbestände für die Wahrnehmung berechtigter Interessen und allgemein zugängliche Daten enthält. Die Entscheidung wirft jedoch die Frage auf, ob die zahlreichen Detailregelungen des Bundesdatenschutzgesetzes lediglich erlaubte Leitlinien innerhalb der Grenzen des Art. 7 darstellen oder Datenkategorien ausschließende neue Tatbestände außerhalb von Art. 7 sind. Die Diskussion um die Zukunft des Datenschutzrechts ist damit um eine europäische Dimension reicher geworden.

Secorvo News

Secorvo College aktuell

Das Jahr neigt sich langsam dem Ende zu und für die Planung Ihrer Weiterbildung im kommenden Jahr lohnt sich bereits jetzt ein Blick in unseren Seminarkalender 2012. Auch im neuen Jahr bietet Secorvo College wieder zahlreiche Weiterbildungsgelegenheiten.

Los geht es gleich im Januar mit dem Grundlagenseminar Sicherheitsmanagement heute (24.-26.01.2012). Im März folgen dann IT-Sicherheit heute (13.-15.03.2012) und Verlässliche Web-Anwendungs-Sicherheit (21.-22.03.2012). Die erste Gelegenheit zur Zertifizierung Ihrer persönlichen Qualifikation im Bereich sichere Softwareentwicklung bieten wir Ihnen am 26.-30.03.2012 beim Seminar Certified Professional for Secure Software Engineering (CPSSE). Das nächste T.I.S.P.-Seminar führen wir vom 07.-11.05.2012 durch – Ihr Exemplar des T.I.S.P.-Buchs erhalten Sie bei frühzeitiger Anmeldung vorab zugesandt.

Das vollständige Jahresprogramm 2012, die detaillierten Programme aller Seminare und die Möglichkeit zur Online-Anmeldung und finden Sie unter http://www.secorvo.de/college. Wir freuen uns auf Ihre Anmeldung!

Für den Weihnachtsmann

Sollten Sie noch Platz unterm Tannenbaum haben und Ihr Weihnachtsmann noch keine durchschlagende Geschenkidee, dann lohnt ein Hinweis auf das T.I.S.P.-Buch: Kann man sich etwas Schöneres vorstellen, als bei Kaffee und Keksen im Kerzenschein vor dem knisternden Kamin zu sitzen und genussvoll in den „Zentralen Bausteinen der Informationssicherheit“ zu schmökern? Wer sich das nicht entgehen lassen möchte, möge hier klicken – oder den Bestellwunsch gleich an den Weihnachtsmann weiterleiten.

Krypto zum Anfassen

Die Karlsruher IT-Sicherheitsinitiative (kurz: KA-IT-Si) erfreute sich in diesem Jahr erneut wachsender Teilnehmerzahlen – zuletzt konnten wir auf der Veranstaltung im November über 50 Teilnehmer begrüßen. Ab 2012 wird eine Kooperation mit dem Karlsruher Institute of Technology (KIT) und dem am 17.10.2011 feierlich eröffneten Kompetenzzentrum für angewandte Sicherheits-Technologie (KASTEL) die KA-IT-Si inhaltlich bereichern.

Am 26.01.2012 startet die Zusammenarbeit mit einem Highlight: Mit Vorträgen und Vorführungen werden wir einen Blick in die Geschichte der Kryptografie werfen – unterstützt durch historische Verschlüsselungsmaschinen u. a. aus der Sammlung des Instituts für Kryptografie und Sicherheit (IKS). Eine frühzeitige Anmeldung wird empfohlen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2011	
05.-06.12.	IsSec/ZertiFA 2011 (Computas, Berlin)
Januar 2012	
17.-19.01.	OMNICARD 2012 (in TIME berlin, Berlin)
24.-26.01.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
26.01.	Krypto zum Anfassen (KA-IT-Si, Karlsruhe)
Februar 2012	
08.-09.02.	22. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	19. DFN Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2012	
13.-15.03.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-16.03.	Black Hat Europe 2012 (Blackhat, Amsterdam/NL)
21.-22.03.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
26.-30.03.	CPSSE (Secorvo College, Karlsruhe)

Fundsache

Seit August 2010 findet sich auf der Webseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) eine Handreichung zu § 11 des Bundesdatenschutzgesetzes. Darin bezieht der BfDI auf drei Seiten zu wichtigen Fragen Stellung, wie der Anpassung von Altverträgen oder dem Verständnis von „sich überzeugen".



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Dezember 2011



Macht verpflichtet

Jede Führungskraft und jedes Staatsoberhaupt sollte es wissen: Mit Macht und Einfluss wachsen nicht nur die Rechte, sondern vor allem die Pflichten.

Die stehen aber oft auf keinem Papier, sondern sind Teil eines „ethischen Codex", wurden durch Kollegen oder Vorgänger vorgelebt oder gehören zur allgemeinen Erwartungshaltung an die jeweilige Position. Das macht es den Betroffenen nicht leicht: Was gestern noch zulässig, unanstößig oder tolerabel war, kann in einer neuen Rolle ein absolutes „No-Go" sein. Ohne eine mentale Umstellung geht das schnell schief – enge, langjährige Freundschaften geraten in den Verdacht der Vorteilsnahme, und die „unbürokratische" Durchsetzung von Entscheidungen riecht schnell nach Amtsmissbrauch. Der souveräne Umgang mit Macht erfordert Selbstdisziplin und vorbildliches Verhalten ebenso wie die Beachtung von Regeln und Kontrollen, und manchmal auch Verzicht.

Das gilt auch für Administratoren. Denn die für den IT-Betrieb Zuständigen sind mit großer Machtfülle ausgestattet: Sie besitzen weit gehende Zugriffsberechtigungen, haben Einblick in detaillierte Log-Protokolle und verfügen über mächtige Analyse-Tools. Mit der Selbstdisziplin ist es allerdings oft nicht weit her: Immer wieder existieren gemeinsame Admin-Passworte, werden aus unsicherer Quelle Programme geladen und ungeprüft installiert oder aus Neugierde Logdaten ausgewertet. Selbst vor dem Lesen vertraulicher Dokumente oder der E-Mails von Kollegen schrecken einige Administratoren nicht zurück. In dieselbe Richtung weist eine Studie der Fa. Balabit vom 15.11.2011: Danach gaben 74 % der anonym Befragten Administratoren zu, ihre Rechte bereits missbraucht zu haben.

Dabei sollten die Passwörter von Admins besonders lang, Logfiles und Daten im Normalbetrieb tabu, die Rechte auf das Erforderliche beschränkt und auf allen Rechnern nur lizenzierte und freigegebene Software installiert sein. Nicht nur Führungskräfte und Staatsoberhäupter, sondern auch „Admins" haben eine Vorbildfunktion.



Inhalt

Macht verpflichtet

Security News

Advent, Advent, der Drucker brennt...

Und sie ist doch personenbezogen...

Content Security Standard

Datenschutz per Verordnung

Weihnachtsgeld

Bin schon da!

Secorvo News

Auf die letzte Minute...

Krypto live

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Advent, Advent, der Drucker brennt...

Am 29.11.2011 wurden Forschungsergebnisse publik, nach denen HP-Druckern mittels eines manipulierten Druckauftrags ein Firmware-Update untergeschoben werden kann. Das von den Medien begierig aufgegriffene Detail, dass damit durch Überhitzung der Fixiereinheit möglicherweise ein Druckerbrand ausgelöst werden könnte, erwies sich jedoch als Falschmeldung: Laut HP verfügen die Drucker über einen Überhitzungsschutzschalter, der nicht per Firmware beeinflusst werden kann.

Ebenso als Falschmeldung erwies sich die Nachricht vom 18.11.2011, wonach Hacker eine Pumpe in einem amerikanischen Wasserwerk zerstört hätten: Am 30.11.2011 erklärte ein Techniker, dass er aus seinem Russland-Urlaub versucht hatte, die defekte Pumpe per Remote-Wartung wieder in Gang zu bekommen.

Trotz dieser spektakulären Advents-Enten sollte man sich nicht in falscher Sicherheit wiegen, denn in beiden steckt ein wahrer Kern: Die (Un-)Sicherheit von digitalen Prozessteueranlagen ist bekannt, und spätestens seit Woz' trickreicher Apple-II-Floppy weiß man, dass es ein Wettbewerbsvorteil sein kann, Funktionen aus teurer Hardware in billige Firmware zu verlagern. Wenn das allerdings kritische Funktionalität betrifft, muss sich der Hersteller intensiv um die Firmware-Integrität kümmern.

Und sie ist doch personenbezogen...

Der EuGH hat am 24.11.2011 auch den Versuch einer belgischen Urheberrechtsverwertungsgesellschaft (SABAM) abgewiesen, einen Internet-Provider (Scarlet Extended SA) zur Implementierung eines P2P-Inhaltsfilters zu verpflichten.

Danach schränkt der Zwang, ein Filtersystem über sämtliche Inhalte auf eigene Kosten zu betreiben, die Provider in ihrem Recht auf unternehmerische Freiheit (Art. 16 der Charta der Grundrechte der EU) ein und schafft keinen angemessenen Ausgleich zwischen den betroffenen Grundrechten. Hierbei sei auch Art. 15 der Richtlinie 2000/31/EG (Richtlinie über den elektronischen Geschäftsverkehr) zu beachten, der es untersagt, Diensteanbietern eine allgemeine Überwachungspflicht aufzuerlegen. Zudem würden das Recht der Nutzer auf den Schutz personenbezogener Daten und auf Informationsfreiheit (Art. 8 und 11 der Charta) unzulässig eingeschränkt.

Bemerkenswert ist die uneingeschränkte Einstufung der IP-Adressen als personenbezogene Daten durch den EuGH – ein großer Schritt zur Klärung dieser wichtigen datenschutzrechtlichen Streitfrage.

Content Security Standard

Bereits in den SSN 09/2010 hatten wir über das Mozilla-Konzept einer Content-Security-Policy (CSP) zur Server-gesteuerten Kontrolle aktiver Inhalte in Webseiten berichtet, das seit Version 4 von Firefox unterstützt wird.

Inzwischen wurde auch bei Google Chrome und dem Internet Explorer mit der Integration begonnen. Bei den Konkurrenzbrowsern dürfte wesentlich zur Motivation beigetragen haben, dass der Ansatz inzwischen durch das W3C gesteuert wird: Seit dem 12.12.2011 liegt ein überarbeiteter CSP-Entwurf für einen W3C-Standard vor. Es darf also erwartet werden, dass sich dieser wirksame Ansatz zum Schutz vor Cross-Site Scripting durchsetzen wird.

Datenschutz per Verordnung

Die Europäische Kommission hat am 29.11.2011 einen länger erwarteten Entwurf einer Datenschutzverordnung vorgelegt. Eine EU-Verordnung ist, anders als eine Richtlinie, unmittelbar geltendes Recht – kein unbedeutendes Dokument also.

In großen Teilen entspricht der knapp 80seitige Verordnungsentwurf bereits geltendem deutschem Datenschutzrecht oder greift Rechtsmeinungen der Aufsichtsbehörden auf. Allerdings schließt er auch Regelungslücken und verschärft die eine oder andere Bestimmung. So zählt die Verordnung alle Personen, die mit vernünftigerweise zu erwartenden Mitteln durch einen beliebigen Dritten identifiziert werden können, zu den Betroffenen (Art. 3). Zudem wird der Anwendungsbereich ausdrücklich auf das Veröffentlichen an einen unbestimmten Personenkreis erweitert (Art. 2).

Die Verschärfungen betreffen u. a. die Vorabkontrolle, die zu einer Risiko- und Folgenabschätzung ausgebaut wird (Art. 30). Die bisherigen Prinzipien (Verbot mit Erlaubnisvorbehalt, Erforderlichkeit, Zweckbindung und Transparenz) werden um das Recht auf Löschung und Vergessen ergänzt (Art. 15) – ein Prinzip, dass ebenso wie die neue Forderung nach Datenschutz durch Technikgestaltung und datensparsame Grundeinstellungen (Art. 20) insbesondere auf Social Networks abzielt. Enttäuschend ist der Empfehlungscharakter der Bestimmung zu Datenschutz-Siegeln und Zertifikaten (Art. 36).

Gleichzeitig wird die geteilte Verantwortlichkeit für Datenverarbeitungen anerkannt (Art. 21). Die Pflicht zur Bestellung eines Datenschutzbeauftragten wird auf Unternehmen mit mehr als 250 Beschäftigten oder besonderen Verarbeitungen beschränkt (Art. 32-34). Eingeführt werden auch

verbindliche Unternehmensrichtlinien als Grundlage des Datenexports in Drittstatten (Art. 40).

Die Durchsetzung wird durch ausführliche Vorgaben und erweiterte Befugnisse für die zu schaffende Aufsicht (Art. 43 ff) und Strafvorschriften (Art. 78 f) sowie Haftungsregeln (Art. 77) gestärkt.

Zwar ist zu erwarten, dass der Entwurf noch eine Reihe von Änderungen erfahren wird. Dennoch dürfte er endlich wieder Leben in die festgefahrene deutsche Diskussion um ein modernes Datenschutzrecht bringen.

Weihnachtsgeld

Weihnachtszeit ist Shopping-Zeit: Die Wochen vor Weihnachten sind nicht nur für Einzelhändler, sondern auch für Online-Shops die umsatzstärkste Jahreszeit. Dass wissen auch Black Hats – und drohen vermehrt mit DDoS-Attacken, die sie erst nach Zahlung eines Schutzgelds via Western Union aussetzen oder einstellen.

Am 20.12. erwischte es Conrad Electronic, am 21.12. den Webhoster Mittwald CMS, und am 22.12.2011 war der Werbemittelversand schneider nicht erreichbar. Nach Auskunft des Bundesverbands des deutschen Versandhandels (bvh) ergab eine Umfrage des britischen e-retailing-Verbands imrg, dass bereits 20 % der E-Commerce-Unternehmen von dieser modernen Form der Schutzgelderpressung betroffen sind.

Kein Wunder, dass Analysten technischen Schutzmaßnahmen gegen gezielte DDoS-Angriffe ein erhebliches Marktwachstum prophezeihen – nach über 50% in 2011. Aber auch mit Bordmitteln kann man vielen DDoS-Angriffen etwas entgegensetzen – eine schöne Übersicht solcher Maßnahmen hat Moritz Jäger am 27.02.2011 publiziert.

Bin schon da!

Alle Arten von Smartphones sind grundsätzlich durch Apps gefährdet, die Schadfunktionen enthalten – das ist nichts Neues. Neu ist, dass auch von vorinstallierten Tools eine Bedrohung ausgehen kann. Der Android-Entwickler Trevor Eckart veröffentlichte am 28.11.2011 ein Youtube-Video, in dem er die von US-Providern und Herstellern auf über 141 Mio. Smartphones vorinstallierte App "CarrierIQ" analysierte. Die Ergebnisse seiner Untersuchungen publizierte er inzwischen auch auf seiner Webseite. Die Software, die ursprünglich zur Optimierung von Netzen gedacht war, erlaubt es, Benutzereingaben und weitere Informationen wie die aktuellen GPS-Koordinaten abzugreifen. Allerdings lässt sie sich nicht einfach deaktivieren – und ist zudem in der Lage, sich zu tarnen.

Auch können Android-Apps über vorinstallierte Anwendungen die zugewiesenen Berechtigungen (*permissions*) unterlaufen, wie Forscher der North Carolina State University herausfanden. Sie stellten fest, dass viele vorinstallierte Apps von anderen Apps eingespannt werden können und so restriktiv eingestellte Berechtigungen erweitern (*permission leaks*). Wir empfehlen daher auch vorinstallierte Apps daraufhin zu prüfen, ob man sie wirklich benötigt, und – um die Angriffsmöglichkeiten zumindest etwas einzuschränken – nicht genutzte Apps zu deinstallieren. Auch sollte man die Dienste GPS und WLAN nur dann einschalten, wenn man sie benötigt. Das schafft nicht nur mehr Privatsphäre – sondern erhöht auch die Akku-Laufzeit.

Wir wünschen Ihnen erholsame und schöne Weihnachtsfeiertage – und einen guten Start in ein rundum sicheres Jahr 2012!

Secorvo News

Auf die letzte Minute…

Wer noch ein Plätzchen unter dem Baum zu füllen hat: Wenige Mausklicks genügen, und die „Zentralen Bausteine der Informationssicherheit“ gehören Ihnen – das Grundwissen des T.I.S.P. in 22 Kapiteln, als Nachschlagewerk oder zur Vorbereitung auf eine T.I.S.P.-Zertifizierung (79,95 Euro).

Krypto live

Ab 2012 wird eine Kooperation mit dem Karlsruher Institute of Technology (KIT) und dem am 17.10. 2011 feierlich eröffneten Kompetenzzentrum für angewandte Sicherheits-Technologie (KASTEL) die Karlsruher IT-Sicherheitsinitiative (kurz: KA-IT-Si) bereichern.

So startet die KA-IT-Si gleich am 26.01.2012 mit einem Highlight: Verschlüsselungstechnik gestern und heute „zum Anfassen“ am Institut für Kryptographie und Sicherheit (IKS) des KIT. Die Veranstaltung beginnt um 18 Uhr im Informatik-Gebäude (50.34) des KIT-Campus Süd, Karlsruhe. Wir freuen uns auf Ihre Teilnahme!



Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Januar 2012	
17.-19.01.	OMNICARD 2012 (in TIME berlin, Berlin)
24.-26.01.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
26.01.	Krypto zum Anfassen (KA-IT-Si/KIT, Karlsruhe)
Februar 2012	
08.-09.02.	22. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	19. DFN Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2012	
13.-15.03.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-16.03.	Black Hat Europe 2012 (Blackhat, Amsterdam/NL)
21.-22.03.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
26.-30.03.	CPSSE (Secorvo College, Karlsruhe)
April 2012	
23.-26.04.	PKI (Secorvo College, Karlsruhe)
24.-25.04.	Datenschutztage 2012 (Forum für Datenschutz, Wiesbaden)

Fundsache

Der Virenschutzanbieter Kaspersky Lab hat einen „Security-Advents-kalender" herausgebracht – mit 24 kernigen Tipps für eine sichere Weihnachtszeit.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2012



So klug als wie zuvor

Studien sind beliebt. Häufig stützen sie die „Propheten im eigenen Haus“, deren Worte kein Gehör finden. Gelegentlich befreien sie Entscheider von der Last der Verantwortung. Und manchmal versachlichen sie eine Diskussion, indem sie den einen oder anderen Irrglauben widerlegen.

Weniger beliebt sind allerdings Studien, die nicht das vom Auftraggeber erwartete oder erwünschte Ergebnis liefern. Zwar werden die Verfasser vom Auftraggeber bezahlt („Wes' Geld ich nehm', des' Lied ich sing“), mit einer Tendenzstudie setzen sie aber ihre Glaubwürdigkeit aufs Spiel – und riskieren Ruf und künftige Geschäfte.

Bei überraschenden Resultaten ist zumindest in der Politik die Neigung zu beobachten, missliebige Ergebnisse zurückzuhalten – vielleicht in der so trügerischen wie verzweifelten Hoffnung, damit einer unerwünschten öffentlichen Debatte ausweichen zu können.

So geschehen mit dem vom Justizministerium beim Max Planck Institut in Freiburg in Auftrag gegebenen Gutachten zur Frage der Erforderlichkeit der Vorratsdatenspeicherung. Die Existenz der „2., erweiterten Fassung“ einer zwischen Mai und August 2010 (!) durchgeführten und im Juli 2011 abgeschlossenen Untersuchung machte erst eine Veröffentlichung von Auszügen in Spiegel Online am 27.01.2012 bekannt. Danach konnten die Autoren keine Hinweise dafür finden, dass der Wegfall der Vorratsdatenspeicherung negative Folgen für Strafverfolgung und Gefahrenabwehr habe: Wasser auf den Mühlen des Justiz- und Öl im Feuer des Innenministeriums.

Liest man die Schlussfolgerungen genau, so wird hinter dem tobenden öffentlichen Säbelrasseln deutlich, dass die Autoren mit einer „sehr unsichere(n) statistische(n) Datengrundlage“ und „sehr unterschiedlichen Einschätzungen bei den unmittelbar betroffenen Praktikern“ arbeiten mussten – sprich: keine belastbaren Erkenntnisse gewinnen konnten. Eines ist daher sicher: Die nächste Studie kommt bestimmt. Und in diesem Fall wäre das auch sehr zu begrüßen.



Inhalt

So klug als wie zuvor

Security News

Ungemach für Surf-Tracker

Smartphone-Sicherheit

Authentifikation systematisch

Kuck mal, wer da...

Verwirrungs-Taktik

Secorvo News

Neue Seminare

Karlsruher IT-Sicherheitsinitiative

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Ungemach für Surf-Tracker

Am 08.12.2011 hat die Art. 29 Gruppe, der beratende Zusammenschluss der europäischen und nationalen Datenschutzaufsichtsbehörden eine Stellungnahme zur künftigen Anwendung der so genannten Cookie-Richtlinie (RL 2009/136/EG) abgegeben. Sie bezieht sich auf Vorschläge der European Advertising Standards Alliance (EASA) sowie des Internet Advertising Bureau Europe (IAB), die ein Opt-out-Verfahren zum Gegenstand hatten.

Als unzureichend abgelehnt werden sowohl ein selbstregulativ von den Tracking-Netzwerken einzusetzendes Icon zur Information des Nutzers als auch das Angebot, über eine zentrale Seite Sperrcookies zu laden. Der geänderte Art. 5 Abs. 3 der E-Privacy Richtlinie (RL 2002/58/EG in der Fassung der RL 2009/136/EG) fordere eine klare und umfassende Information *vor* dem Setzen eines Cookies und ein Opt-In. Dabei sei unwesentlich, ob der Cookie personenbezogene Daten speichere. Tracking-Dienste setzten eindeutige Identifikatoren ein, die ein Erfassen einzelner Nutzer erlaubten und seien damit selbst ein personenbezogenes Datum.

Als zulässige und geeignete Varianten neben Pop-up Fenstern zur Information und Einwilligung werden vorgeschaltete Seiten, die von Heise vorgeschlagene 2-Klick Lösung, ein statisches Informationsbanner und Tracking verhindernde Browser-Voreinstellungen angesehen. Auch genüge eine einmalige Einwilligung für ein gesamtes Werbenetzwerk.

Damit rücken – aus berechtigten Gründen – statt der IP-Adresse die Tracking-Cookies als Identifizierungsmerkmal ins Zentrum der Regulierung. Mit der überfälligen Umsetzung der „Cookie-Richtlinie“ werden daher die mühsam erreichten Übereinkünfte mit Tracking-Betreibern wie z. B. Google Makulatur: Der Einsatz von Google Analytics verstößt dann – ohne eine informierte Einwilligung des Seitenbesuchers – gegen geltendes europäisches Datenschutzrecht. Bei Verstößen wird mit Abmahnungen der deutschen Datenschutz-Aufsichtsbehörden zu rechnen sein.

Smartphone-Sicherheit

Vor etwa zehn Jahren hat die NSA mit SELinux eine Linux-Variante veröffentlicht, die dank starker Sicherheitsmechanismen erheblich widerstandsfähiger gegen Angriffe ist als ein „normales“ Linux.

Am 06.01.2012 veröffentlichte die NSA die erste Version von SEAndroid, ein Projekt, in dem die SELinux-Architektur auf Android übertragen wurde. Derzeit steht noch keine fertige Firmware zur Verfügung; interessierte Nutzer müssen daher noch selber kräftig Hand anlegen.

Das hinter SELinux und SEAndroid stehende Sicherheitsmodell ist durchaus geeignet, verschiedenen Sicherheitsproblemen wirksam zu begegnen. Ob es sich durchsetzen kann, hängt jedoch stark vom Engagement der Smartphone-Hersteller ab.

Die größte Herausforderung bei der Umsetzung ist die Komplexität der Konfiguration. Dafür müssen die Hersteller einen gut durchdachten Ansatz wählen, bei dem die Sicherheitsmechanismen wirksam werden, ohne dass sich der Nutzer mehr als nur oberflächlich mit dem System beschäftigen muss. Gelingt das nicht, wird auch ein unter SEAndroid betriebenes Smartphone bestenfalls „gefühlt sicherer“ sein.

Authentifikation systematisch

Am 12.12.2011 erschien, fünf Jahre nach der Erstfassung, die erheblich überarbeitete und erweiterte Revision 1 der Electronic Authentication Guideline (SP 800-63) des NIST. Darin wird das Thema Authentifikation über unsichere Netze von der initialen Registrierung der Teilnehmer bis hin zum Weiterreichen der Information über den authentifizierten Benutzer an nachgeordnete Anwendungen systematisch betrachtet. Vier aufeinander aufbauende Sicherheitsniveaus und konsistente Anforderungen an alle Nutzungsphasen eines Authentifikationsverfahrens werden definiert.

Auch wenn das Dokument primär für US-Behörden gedacht ist und daher auf Behördenstandards wie FIPS-140-2 oder PIV-Cards abhebt, so bietet es doch eine sehr gute Grundlage für eine angemessene Präzisierung des oft schwammig verwendeten Begriffs „starke Authentifikation“.

Kuck mal, wer da...

Der am 28.11.2011 publizierte 20. Tätigkeitsbericht (2009-2010) des Landesbeauftragten für den Datenschutz Niedersachsen, Joachim Wahlbrink, legt einen Schwerpunkt auf das Thema Videoüberwachung. So wurden in einer großen Fastfood-Restaurantkette nicht nur ein hoher Anteil unzulässiger Überwachungen, sondern auch zahlreiche Datenschutzmängel bei der Installation, Dokumentation und der Erfüllung allgemeiner Datenschutzanforderungen festgestellt.

Einer Beschwerde folgend wurden vier Restaurants der Kette geprüft, die mit insgesamt 94 Kameras förmlich gespickt waren. Diese überwachten vielfach den Sitzbereich – unzulässig nach einem Urteil des AG Hamburg von 2008, denn in öffentlichen

Bereichen, in denen sich Personen typischerweise länger aufhalten, tritt das Beweis- und Präventionsinteresse des Betreibers hinter das Persönlichkeitsrecht der Betroffenen zurück. Nicht vom Personal einsehbare Bereiche dürfen nur noch für eine Übergangszeit weiter beobachtet werden; finden keine nennenswerten Vandalismus-Vorfälle statt, ist auch diese Überwachung mangels Erforderlichkeit einzustellen.

Das betroffene Unternehmen hat infolge der Prüfung seine gesamten einschlägigen Richtlinien überarbeitet, eine Löschfrist von 72 Stunden eingeführt und von den Franchisenehmern die Bestellung von Datenschutzbeauftragten eingefordert.

Auf die andauernde Ausweitung von Videoüberwachungen in Unternehmen reagieren die Aufsichtsbehörden mit einer Intensivierung der Prüfungen. Eine kritische Überprüfung der eigenen Prozesse und Löschfristen erscheint daher angeraten.

Verwirrungs-Taktik

Man stelle sich vor, für jedes Produkt, das man in einem Kaufhaus erwerben möchte, müsste man einen separaten Eingang zum Gebäude mit eigenem, individuellen Ladenschild nutzen. Bald wüssten viele Kunden nicht mehr, bei wem sie da eigentlich gerade einkaufen.

Vielleicht weil die Türen im Internet billiger sind, reservieren viele Marketing-Experten – zur Betonung der Wichtigkeit einer Aktion oder eines neuen Angebots – bei jeder sich bietenden Gelegenheit eine neue Second-Level-DNS-Domain, anstatt Subdomains des eingeführten Namens zu nutzen. So ist es nicht ungewöhnlich, wenn man bei der Online-Buchung eines Flugtickets von der Suche nach passenden Verbindungen über die Eingabe der Daten bis hin zu Zahlung und Buchungsbestätigung über drei oder vier verschiedene Domains geleitet wird.

Dabei bereitet gerade diese verbreitete Praxis Phishing und ähnlichem Trickbetrug den Boden – denn die Nutzer gewöhnen sich durch die alltägliche Verwirrung an ständige Domain-Wechsel und schöpfen im Angriffsfall keinen Verdacht.

Richtig bedenklich aber stimmt es, wenn auch im Sicherheitsbereich derartigen Unsitten Vorschub geleistet wird. So empfahl das BSI am 11.01.2012 einen durchaus sinnvollen Test auf Befall mit der DNSChanger-Malware. Allerdings nicht auf den eigenen amtlichen Webseiten, sondern unter der Domaine dns-ok.de. Wenig später tauchte unter dem homophonen Namen dns-okay.de eine (glücklicherweise harmlose) Verballhornung der Seite auf. Und auf der Webseite bka-trojaner.de wird unter der Titelzeile botfrei.de und den Logos von BSI und eco Hilfe gegen Ransomware angeboten – eine Webseite, die auf den ersten Blick keinen Deut seriöser wirkt als die Schadsoftware, vor der da gewarnt wird.

Kein Wunder also, wenn – wie am 12.01.2012 berichtet – zahlreiche Internetnutzer fürchten, sich auf derartigen Seiten eher mit einem Staatstrojaner zu infizieren als Hilfe zu finden.

Secorvo News

Neue Seminare

Die stetige Weiterentwicklung auf dem Gebiet der Informationstechnologie bringt auch neue Herausforderungen für die IT-Sicherheit mit sich. Ab dem Frühjahr 2012 erweitern wir daher unser Seminarangebot und bieten mit Aktuelle Herausforderungen der Informatinossicherheit vom 23.-24.05.2012 einen Überblick über neue Angriffsszenarien und Risiken sowie wirksame Schutzstrategien und Sicherheitslösungen.

Ihre IT-Security-Grundlagenkenntnisse können Sie vom 13.-15.03.2012 beim Seminar IT-Sicherheit heute auffrischen. Mehr über den Schutz von Web-Anwendungen erfahren Sie vom 21.-22.03.2012 beim Seminar Verlässliche Web-Anwendungs-Sicherheit. Und vom 26.-30.03.2012 bieten wir mit dem Certified Professional for Secure Software Engineering (CPSSE) eine praxisorientierte Einführung in die sichere Softwareentwicklung. Freie Plätze gibt es auch noch für das T.I.S.P.-Seminar vom 07.-12.05.2012 – bei frühzeitiger Anmeldung bekommen Sie Ihr Exemplar des T.I.S.P.-Buchs rechtzeitig vorab zugesandt (Programme und Online-Anmeldung).

Karlsruher IT-Sicherheitsinitiative

Einen fulminanten Start ins Jahr 2012 hatte die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si), die die Kooperation mit dem Kompetenzzentrum für Angewandte Sicherheits-Technologie (KASTEL) am 26.01.2012 mit einer gemeinsamen Veranstaltung einleitete: „Kryptographie zum Anfassen“ lautetet das Thema des Vortrags, der von einer einzigartigen Ausstellung historischer Kryptomaschinen aus zahlreichen Sammlungen begleitet wurde. Zum ersten Mal in der Geschichte der KA-IT-Si musste die Anmeldeliste zwei Tage vor der Veranstaltung wegen Überbuchung geschlossen werden.

Das nächste KA-IT-Si-Event zum Thema „Sichere Softwareentwicklung“ findet am 01.03.2012 im Schlosshotel Karlsruhe statt. Beginn ist um 18 Uhr. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2012	
08.-09.02.	22. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	19. DFN Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2012	
01.03.	Sichere Software-Entwicklung (KA-IT-Si, Karlsruhe)
13.-15.03.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-16.03.	Black Hat Europe 2012 (Blackhat, Amsterdam/NL)
21.-22.03.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
26.-30.03.	CPSSE (Secorvo College, Karlsruhe)
April 2012	
15.-19.04.	Eurocrypt 2012 (IACR, Cambridge/UK)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
April 2012	
07.-12.05.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
09.-10.05.	BvD Verbandstag 2012 (BvD e.V., Berlin)

Fundsache

Am 20.12.2011 veröffentlichte die amerikanische Electronic Frontier Foundation (EFF) einen 24seitigen Guide for Travelers Carrying Digital Devices zum Grenzübertritt in die USA mit digitalen Daten – mit vielen hilfreichen Empfehlungen für US-Reisende.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2012



Trau, schau, wem?

Nicht erst durch die jüngste Entdeckung identischer Primfaktoren in Public Key Zertifkaten durch die Krypto-Forscher der EPFL (siehe „PKI-Feldstudie“) wissen wir, dass es mit der Vertrauenswürdigkeit von „Trust Centern“ möglicherweise nicht immer so weit her ist, wie wir glaubten. Dabei ist schon der Begriff „Trust Center“ semantischer Nonsens – denn natürlich wird dort weder Vertrauen gesammelt noch erzeugt. Im Kontext von Technik ist „Vertrauen“ ohnehin irreführend. Denn der Begriff bezeichnet „die subjektive Überzeugung (auch Glaube) der Richtigkeit, Wahrheit bzw. Redlichkeit von Handlungen, Einsichten und Aussagen eines anderen oder von sich selbst“, so die Definition in Wikipedia. Vertrauen können wir daher einzig und allein Menschen entgegen bringen, denn Richtigkeit, Wahrheit und Redlichkeit sind keine Eigenschaften technischer Systeme. Wenn wir von „Vertrauen in Technik“ sprechen, meinen wir daher eigentlich etwas anderes: nämlich unser Vertrauen darauf, dass diejenigen, die ein technisches System entwarfen, entwickelten, betreiben und warten unser Vertrauen verdienen.

Menschen vertrauen anderen Menschen vor allem dann, wenn sie gute Erfahrungen damit gemacht haben, wenn ihnen keine Hinweise bekannt sind, die Misstrauen nahe legen, und wenn sie den Eindruck gewinnen, dass dem Gegenüber die Bestätigung des Vertrauens wichtig ist. Genau deshalb sind ein positives Markenimage und Prüf-Zertifkate unabhängiger Dritter vertrauensbildend, und Berichte über Vorfälle Gift für eine Vertrauensbeziehung.

Allerdings darf man Vertrauen nicht mit Sicherheit verwechseln. Vertrauen „überbrückt“ Unsicherheit und (Rest-)Risiken: Es greift da, wo Technik nicht weiterhilft. Denn dass RSA-Schlüssel nicht faktorisiert werden können, dass die Identität des Schlüsselinhabers sorgfältig geprüft wurde und dass die zugehörigen Private Keys Dritten unzugänglich sind, lässt sich durch Technik nicht garantieren. Daran müssen wir glauben. Oder auch nicht, wie Aesop schon wusste.



Inhalt

Trau, schau, wem?

Security News

PKI-Feldstudie

Grenzen staatlicher Auskunftsrechte

Taschendiebstahl 2.0

Bauen am IT-Grundschutz

Multimedialer Overflow

Wer zweimal klaut...

Secorvo News

Bildungszeit

Rolltor für den Online-Shop

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

PKI-Feldstudie

Krypto-Forscher der EPFL Lausanne haben in einer am 17.02.2012 veröffentlichten Studie mehrere Millionen Public Keys untersucht, die u. a. vom SSL-Observatory der EFF gesammelt worden waren. Dabei traten einige Fakten zutage, die bei Fachleuten nur Kopfschütteln ernten können: U. a. wurden zu ein und demselben RSA-Schlüsselpaar über 16.000 verschiedene X.509-Zertifikate entdeckt – unklar bleibt, für wie viele unterschiedliche Inhaber. Und etwa 0,2 % der untersuchten RSA-Moduli haben einen ihrer beiden Primfaktoren mit anderen Public Keys gemeinsam, d. h. sie können trivial per GGT-Berechnung gebrochen werden. Dazu kommen noch vereinzelte RSA-„Schlüssel", bei denen einer der beiden Primfaktoren 2 ist, oder bei denen als öffentlicher Exponent 1 verwendet wird – in beiden Fällen ist auch ein 2048-Bit-RSA-Key nicht sicherer als Doppel-ROT13. Daneben gibt die Studie Aufschluss auf die Verbreitung verschiedener Algorithmen und Schlüssellängen: Nur einer von über 11 Mio. Public Keys nutzte elliptische Kurven (ECDSA).

Um die Betroffenen zu schützen, wurde nicht veröffentlicht, ob die betreffenden Schlüssel in PGP-Keys, in selbstsignierten Zertifikaten von Billig-Routern oder in durch öffentliche Trustcenter erstellten Zertifikaten gefunden wurden. Letzteres würde ein weiteres Schlaglicht auf die unterentwickelte Qualitäts- und Risikomanagement-Kultur der Branche werfen – genau wie der am 04.02.2012 publik gewordene Fall, dass bewusst ein CA-Zertifikat zum „Aufbrechen" von SSL verkauft wurde. Merke: Die Schlüssellänge allein garantiert keine unknackbaren Schlüssel – und ein Zertifikat offenbar auch nicht.

Grenzen staatlicher Auskunftsrechte

Das Bundesverfassungsgericht hat mit Beschluss vom 24.02.2012 die Auskunftsbefugnisse von Geheimdienst-, Ermittlungs- und Polizeibehörden eingeschränkt. Überprüft wurden die Auskunftsverfahren über Telekommunikationsbestandsdaten nach den §§ 111 ff. Telekommunikationsgesetz (TKG). Die Preisgabe von PIN, PUK und weiteren Zugangscodes zu den Endgeräten und die Zuordnung von dynamischen IP-Adressen über diese Auskunftsansprüche sind danach verfassungswidrig.

Zwar wurde das automatisierte Auskunftsverfahren und die grundsätzliche Speicherpflicht der TK-Provider in weiten Teilen bestätigt. Der Grundrechtseingriff sei vergleichsweise gering und gerechtfertigt. Die Auskunftserteilung über die Zuordnung von dynamischen IP-Adressen sei jedoch ein Eingriff in das Telekommunikationsgeheimnis (Art. 10 GG) und von den Auskunftsnormen nicht umfasst. Zudem stellen die Auskunftspflichten keine Erhebungsgrundlage für die abfragenden Behörden dar. Diese benötigen fachspezifische Befugnisnormen. Im Fall von § 113 Abs. 1 S. 2 TKG, der Auskunft über Zugangscodes, fehle der Regelung zudem eine ausreichende Bindung an die Zwecke der Codeverwendung.

Bemerkenswert sind die Ausführungen zur bevorstehenden Einführung von IPv6 mit flächendeckend statischen IP-Adressen. Sollte es hierdurch zu einer umfassenden Deanonymisierung der Internetnutzung kommen, wird dem Gesetzgeber die Pflicht zur Neubetrachtung der Eingriffsbeschränkung aufgegeben. Damit bleibt das Bundesverfassungsgericht seiner Rolle als Bollwerk gegen ausufernde staatliche Überwachung treu.

Taschendiebstahl 2.0

Mit der zunehmenden Verbreitung von Smartcard-Chips, die neben den Kontaktflächen auch eine RFID-Schnittstelle besitzen, sprießen auch deren Anwendungen: Nach dem nPA hat am 11.01.2012 die Deutsche Kreditwirtschaft angekündigt, dass die GeldKarte bald unter dem Namen „girogo" auch berührungslos nutzbar sein wird.

Das weckt Befürchtungen über einen berührungslosen Taschendiebstahl. Prompt wurde auf der Shmoocon am 29.01.2012 demonstriert, wie einfach sich eine RFID-fähige Kreditkarte „im Vorbeigehen" kopieren lässt. Glücklicherweise muss der Cyber-Taschendieb bei sicheren Verfahren als „Händler" auftreten und riskiert so seine Entdeckung. Und gegen eine Weiterleitung als Man-in-the-Middle an einen realen Händler helfen Protokolle, die mittels Kryptographie und Signallaufzeiten den Radius eines möglichen Missbrauchs beschränken. Eher ist jedoch zu erwarten, dass elektromagnetische Abschirmung für Portemonnaies bald genauso üblich sein wird wie eingewebte Metallfäden in Winterhandschuhen.

Bauen am IT-Grundschutz

Am 19.02.2012 hat das BSI auf den Webseiten zum IT-Grundschutz die Entwürfe für drei neue Bausteine (Webanwendungen, MacOSx und OpenLDAP) zur Kommentierung bereitgestellt. Da die Weiterentwicklung der IT-Grundschutz-Kataloge zur Zeit etwas stagniert – die 11. Ergänzungslieferung aus 2009 ist immer noch die aktuelle zertifizierungsrelevante Version – ist die Fortschreibung von Bausteinen zu begrüßen. Eine Kommentierung der Entwürfe legen wir allen Interessierten ans Herz.

Die Bereitstellung der bereits im Juni 2011 zunächst nur als pdf publizierten 12. Ergänzungslieferung mit anderen wichtigen Bausteinen als Meta-Daten für das Grundschutz-Tool sowie als html-Version wird dennoch sehnlich erwartet.

Multimedialer Overflow

Der Titel "Spiel mir das Lied vom Rootkit" im Heise-Newsticker vom 30.01.2012 gefiel auch uns – die darin vorgestellte Angriffsmethode allerdings weniger: Eine präparierte Midi-Datei auf einer Webseite kann via Internet-Explorer und Windows-Media Player über eine Heap Spray Attacke einen Buffer Overflow in der Bibliothek winmm.dll auslösen. Anschließend kann beliebiger Code ausgeführt und das System übernommen werden. Trojaner, die die Schwachstelle ausnutzen, sind bereits im Umlauf. Mit einem Patch von Microsoft wurde die Schwachstelle, von der zahlreiche Windows-Systeme betroffen sind, im Januar behoben.

Soweit so vertraut: Richtig neu sind Buffer Overflows in Multimediaanwendungen nicht. Im Gegenteil: Darüber sollten Softwareentwickler inzwischen hinaus sein. Zu befürchten ist aber wohl, dass auch weiterhin derartige Schwachstellen aufgedeckt werden. Dagegen helfen nur Ansätze wie das Sandboxing von IE9, dedizierte Lösungen wie Bitbox oder Surf-VMs à la c't Surfix. Oder eine komplette Trennung des Internetzugangs vom Client-PC über eine virtuelle Maschine wie ReCoBS. Btw.: Haben Sie auf den ersten Link des Beitrags geklickt?

Wer zweimal klaut...

Zum Schutz gegen Urheberrechtsverletzungen im Internet werden derzeit Warnhinweismodelle diskutiert. Danach sollen Zugangsprovider auf Veranlassung von Rechteinhabern Anschlussinhabern, die eine Urheberrechtsverletzung begehen, eine Warnung zusenden sowie eine Liste der gewarnten Anschlussinhaber führen. Nach einer festzulegenden Zahl von Verstößen sollen die Rechteinhaber informiert werden; sie können dann entscheiden, ob sie eine Auskunft über den Anschlussinhaber zur Rechtsverfolgung einholen möchten.

Das Bundeswirtschaftsministerium (BMWi) hat nun am 01.02.2012 eine 2011 in Auftrag gegebene vergleichende Studie über Warnhinweismodelle und die Umsetzbarkeit eines solchen Modells in Deutschland veröffentlicht. Die knapp 350seitige Studie (zzgl. 50 Seiten Anhang) bewertet die Modelle grundsätzlich positiv, unter der Voraussetzung, dass bei Missachtung der Warnungen eine konsequente Rechtsverfolgung erfolgt.

Voraussetzung für das Modell ist jedoch eine Vorratsdatenspeicherung der Zugangsanbieter. Die Studie geht von der grundsätzlichen Zulässigkeit der Verwendung dieser Daten aus. Das Datenschutzrecht wird jedoch nur oberflächlich und fehlerhaft berücksichtigt: So verwechseln die Autoren bezüglich der zu führenden Liste Anonymität und Pseudonymität; auch wird die Erforderlichkeit außer Acht gelassen, bei der Übermittlung von Mehrfachverstößen nach Rechteinhabern zu differenzieren.

Nebenbei liefert die Studie außer dem Vergleich der verschiedenen europäischen Ansätze einen Einblick in die derzeitigen Planspiele der Bundesregierung.

Secorvo News

Bildungszeit

Vom 13.-15.03.2012 haben Sie die Möglichkeit, Ihre IT-Security-Grundlagenkenntnisse beim Seminar IT-Sicherheit heute aufzufrischen. Sichern Sie sich kurzfristig noch einen der freien Plätze. Wir freuen uns auf Ihre Teilnahme!

Die nächste Schulung mit anschließender Zertifikatsprüfung zum TeleTrusT Information Security Professional (T.I.S.P.) findet vom 07.-11.05.2012 statt. Bei frühzeitiger Anmeldung bekommen Sie Ihr Exemplar des T.I.S.P.-Buchs rechtzeitig vorab zugesandt.

Ebenfalls im Mai, vom 23.-24.05.2012, können Sie sich beim Seminar Aktuelle Herausforderungen der Informationssicherheit einen Überblick über neue Angriffsszenarien und Risiken sowie wirksame Schutzstrategien und Sicherheitstechnologien verschaffen.

Die Programme aller Seminare sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Rolltor für den Online-Shop

Die Entwicklung sicherer Online-Plattformen, die potentiell jedem Angreifer ausgesetzt sind, stellt aus Sicherheitssicht eine ganz besondere Herausforderung dar. Sie stellen gänzlich neue Anforderungen an die Qualifikation der Entwickler, die Sicherheitskultur des Unternehmens und die Qualität und Verfügbarkeit von Sicherheitswerkzeugen.

Matthias Honka (asknet AG) beleuchtet in seinem Vortrag auf dem kommenden KA-IT-Si-Event am **01.03.2012** die Gratwanderung zwischen agiler Softwareentwicklung und schneller Reaktion auf Kundenwünsche einerseits und Kontrollmaßnahmen zum Schutz digitaler Güter andererseits. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2012	
01.03.	Rolltor für den Online-Shop (KA-IT-Si, Karlsruhe)
13.-15.03.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-16.03.	Black Hat Europe 2012 (Blackhat, Amsterdam/NL)
21.-22.03.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
26.-30.03.	CPSSE (Secorvo College, Karlsruhe)
April 2012	
15.-19.04.	Eurocrypt 2012 (IACR, Cambridge/UK)
16.-17.04.	a-i3/BSI-Symposium 2012 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
Mai 2012	
07.-12.05.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
23.-24.05.	Aktuelle Herausforderungen der Informations-sicherheit (Secorvo College, Karlsruhe)

Fundsache

Der Branchenverband BITKOM hat am 03.02.2012 die digitale Fassung einer Broschüre mit Sicherheitstipps für Smartphone-Nutzer publiziert, die für den IT-Gipfel 2011 erstellt worden war. Ein hilfreiches Handout auch für Unternehmen – wenn die wesentliche Nachricht auch ist: Wenn Ihr Sicherheit wollt, müsst Ihr Zeit investieren.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2012



Wer hat Angst vorm Murmeltier?

Wir schreiben das Jahr 1990. Vor wenigen Jahren hat Apple den Macintosh vorgestellt und damit die IT-Landschaft nachhaltig geprägt. Da stellt Microsoft ein ähnliches Betriebssystem für die Geräte anderer Hersteller vor – und rollt damit den Markt auf. Kurz darauf breitet sich Schadsoftware für diese Systeme aus.

Zurück im Jahr 2012. Vor wenigen Jahren hat Apple das iPhone vorgestellt und damit die IT-Landschaft nachhaltig geprägt. Da stellt Google ein ähnliches Betriebssystem für die Geräte anderer Hersteller vor – und rollt damit den Markt auf. Kurz darauf breitet sich Schadsoftware für diese Systeme aus.

Einmal mehr scheint das Murmeltier zu grüßen. Allerdings dieses Mal ein Murmeltier mit Reißzähnen und auf Steroiden: Wir sind „always on" und per Netz angreifbar, Angreifer bewegen sich nicht mehr nur neugierig in fremden Gefilden, sondern haben sich längst ziel- und profitorientiert organisiert und können auf bewährte Angriffsmuster wie Drive-by-Infektionen, Phishing und Trojaner zurück greifen.

Auf Seiten der Verteidiger scheint die Zeit allerdings stehen geblieben zu sein: Anwender nutzen nur selten und widerstrebend ausreichend sichere Passcodes, Hersteller setzen auf die Stabilität ausgelieferter Software und haben die Notwendigkeit eines adäquaten Patch-Managements nicht erkannt, Sicherheitssoftware wird als Komforthindernis und unnützer Kostenfaktor wahrgenommen und nicht selten werden private Geräte an der Unternehmens-IT vorbei genutzt.

Höchste Zeit also, uns klar zu machen, dass das Smartphone von heute eben nicht der Computer von 1990 im Hosentaschenformat ist, auch wenn der Marktinnovator wie vor 28 Jahren noch immer Apple heißt. Sondern genau so sorgfältig geschützt werden muss, wie ein PC (oder Mac) anno 2012. Ehe das Murmeltier schmerzhaft zubeißt.



Inhalt

Wer hat Angst vorm Murmeltier?

Security News

97 % vermeidbare Angriffe

Smartphone-Security-Software

Neues iPad – neuer Crack...

Apple goes Datenschutz

Schwachstellen-Hitliste

Secorvo News

Smartphones. Smartpads. Smartlecks.

Seminare in Q2

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

97 % vermeidbare Angriffe

Am 22.03.2012 hat Verizon mit dem 2012 Data Breach Investigations Report eine spannende Analyse publiziert. Auf 80 Seiten werden die Untersuchungsergebnisse von 855 Sicherheitsvorfällen des Jahres 2011 vorgestellt. Die Erkenntnisse sind erschreckend: So werden 96 % aller Angriffe als „nicht schwierig" eingestuft, und 97 % aller Vorfälle wären durch einfache Schutzmaßnahmen vermeidbar gewesen. Erkannt wurden die meisten der Vorfälle (85 %) erst nach Wochen, und in den seltensten Fällen von den Unternehmen selbst (8 %). In größeren Unternehmen konnte der Einfallsweg häufig nicht mehr rekonstruiert werden (31 %).

In den meisten Fällen gelang es einem Angreifer, Schadsoftware remote zu installieren (95 %). In größeren Unternehmen trugen in signifikantem Umfang *SQL-Injections* (12 %), Malware-Downloads (12 %), angeklickte E-Mail-Attachments (18 %) und *Drive-by-Infections* (18 %) zum Angriffserfolg bei: ein Beleg für unzureichende „Security Awareness" in den betroffenen Unternehmen.

Die Erkenntnisse der Studie erlauben den Schluss, dass isolierte Schutzmaßnahmen heute in der Regel zu kurz greifen und Unternehmen verstärkt auf ein umfassendes Schutzkonzept setzen und dabei vor allem ihre im Internet präsenten Anwendungen im Blick behalten müssen.

Dabei können offenbar Zertifizierungen – oder zumindest externe Auditierungen – helfen: Denn 96 % der von den analysierten Sicherheitsvorfällen betroffenen Unternehmen erfüllten nicht die Anforderungen von PCI DSS.

Smartphone-Security-Software

Android ist eines der Sicherheitsthemen, bei denen momentan viel Bewegung zu beobachten ist – im Guten wie im Schlechten. So präsentierte einerseits die NSA im Februar 2012 ein auf SELinux zurück gehendes, um zusätzliche Sicherheitsfunktionen erweitertes SE Android; in Deutschland wurden auf der CeBIT 2012 abhörsichere Handys auf Android-Basis vorgestellt.

Andererseits belegt eine am 07.02.2012 veröffentlichte Untersuchung der Universität North Carolina, dass ca. 0,02 % der Apps in Googles Market und etwa zehn bis 25mal so viele in unabhängigen Märkten Malware enthalten. Dabei behauptete Google am 02.02.2012, nach der Einführung eines automatisierten „Türstehers" bereits einen vierzigprozentigen Rückgang bösartiger Software im Market beobachtet zu haben.

Eine bösartige App zu laden ist jedoch nicht der einzige Weg, über den Schadsoftware auf ein Smartphone gelangen kann: Bei der RSA Konferenz präsentierten Forscher am 29.02.2012 eine funktionsfähige Drive-by-Infektion für Android-Geräte, deren „Marktwert" sie auf 15.000 US$ schätzten. Derweil berichtete die Intel-Tochter McAfee am 14.03.2012 von einem in Spanien gesichteten Android-Trojaner, der sich als vorgeblicher Generator von Sicherheitscodes tarnt, Online-Banking-PINs abphisht und auch gleich die zugehörigen mTANs umleitet – Online-Diebstahl ganz ohne Infektion des heimischen PC.

Dem am 15.03.2012 veröffentlichten Testbericht des unabhängigen Magdeburger Labors AV-Test zufolge erreichen hingegen nur zehn von 41 getesteten Virenscannern für Android eine Schadsoftware-Erkennungsrate von mehr als 90 %. Und auch für verlorene Geräte sieht die Statistik nicht gut aus: Am 09.03.2012 berichtete Symantec von den Resultaten eines Feldtests, bei dem nur etwa die Hälfte der als Köder „vergessenen" Smartphones zurückgegeben, aber die Daten fast aller Geräte vom Finder eingehend durchsucht wurden.

Derzeit sollten daher die Erwartungen an das bei Smartphones erreichbare Sicherheitsniveau generell nicht zu hoch angesetzt werden.

Neues iPad – neuer Crack...

Am 07.03.2012 hat Apple „The New iPad" samt iOS 5.1 vorgestellt. Es kommt mit neuem Prozessor und überarbeiteter Firmware daher und weckte bei Sicherheitsverantwortlichen in Unternehmen die Hoffnung, bestehende Sicherheitslücken, ob durch die Hard- oder die Software der iDevices bedingt, zu beheben. Doch dieser Traum währte nur kurz: Nach kaum einer Woche wurden erste Hinweise auf einen neuen Jailbreak publiziert und auch an älteren iDevices (iPhone 4S und iPad2) demonstriert.

Nicht nur die Geschwindigkeit war überraschend, mit der die Jailbreak Community agierte, sie stellte darüber hinaus auch noch gleich drei Ansätze vor, wie ein solcher Jailbreak in die Tat umgesetzt werden kann. Erstaunlich ist auch, dass einer dieser Ansätze auf einer bereits seit vier Monaten bekannten Schwachstelle beruht. Hier hat wohl die Qualitätssicherung für iOS 5.1 geschwächelt.

Den Sicherheitsverantwortlichen in den Unternehmen bleibt also auch weiterhin nur zu empfehlen, genau zu prüfen, welche Anwendungen und Informationen auf iDevices verwendet und gespeichert werden dürfen, und gegebenenfalls eine Sicherheitsüberprüfung der dienstlich eingesetzten iDevices durchzuführen.

Apple goes Datenschutz

Jedes iOS-Gerät verfügt über eine 40 Stellen lange Zeichenkette, mit der sich iPhone, iPad und iPod touch eindeutig identifizieren lassen: die so genannte UDID (*Unique Device Identifier*). Viele Apps benutzen diese UDID zur Erstellung detaillierter Nutzerprofile und zur Weitergabe an Werbetreibende. Datenschützern war dies schon lange ein Dorn im Auge und führte dazu, dass Apple bereits Mitte August 2011 ankündigte, dies zu ändern.

Nun ist es offenbar soweit: Apple verweigert zur Zulassung eingereichten Apps die Freigabe, wenn sie von der UDID Gebrauch machen. Entwickler, so Apple, sollen sich in ihren Apps zukünftig eigene Kennnummern erstellen und diese unabhängig voneinander verwalten. Eine Umstellung, die vor allem das Tracking individueller Geräte und ihrer Nutzer über mehrere Apps hinweg verhindern soll.

App-Entwickler müssen sich daher umstellen – für sie gibt es zukünftig keine zuverlässige Möglichkeit mehr, anhand der Hardware-ID festzustellen, dass eine App auf einem bestimmten, registrierten und zugelassenen Gerät läuft.

Schwachstellen-Hitliste

Das Forbes-Magazin hat nach eigenen Recherchen eine „Preisliste" für Schwachstellen einzelner Systeme und Anwendungen veröffentlicht. Sie wird derzeit von Apple angeführt: Für iOS-Schwachstellen werden angeblich bis zu 250.000 US$ bezahlt. Die Nachfrage scheint primär von „regierungsnahen Institutionen" zu kommen. Forbes nennt auch einige Kriterien, die erfüllt sein müssen, damit Höchstpreise bezahlt werden: Die Schwachstelle muss neuartig sein, muss dem Käufer exklusiv überlassen werden und darf auch dem Hersteller nicht mitgeteilt werden.

Dieses Interesse könnte aus den Strafverfolgungsbehörden stammen, die im Falle einer Beschlagnahme auch ohne Mitwirkung des Eigners auf die gespeicherten Daten zugreifen möchten, Oder aber es gibt noch Sicherheitsbehörden, deren Glaube an einen funktionierenden behördlichen „Online Trojaner", der sich in der Szene verbergen lässt, nach wie vor ungebrochen ist. Vielleicht arbeiten die Kollegen vom Nachrichtendienst aber auch schon an Stuxnet Mobile.

Secorvo News

Smartphones. Smartpads. Smartlecks.

Steve Jobs hat eine enorme Flutwelle ausgelöst, die Massen an Smartphones und Tablettcomputern in die Unternehmen schwemmt. Zwar können sich IT-Abteilungen eine Zeit lang „schützen", aber früher oder später muss sich auch der letzte standhafte CIO der Kraft der Mobile Device Welle ergeben – der Druck ist einfach zu hoch.

Doch was treibt die Anwender zum verstärkten Einsatz von Smartphones und Tablettcomputern? Was bedeutet der Einsatz solcher Geräte für die IT-Abteilungen, für die IT-Sicherheit und für das Unternehmen? Und welches Mobile Device Management System ist das Beste?

Diese Fragestellungen erörtert Christian Rückert (Netlution GmbH) in seinem Vortrag „Sicheres Mobile Device Management" auf dem nächsten KA-IT-Si Event am **26.04.2012.** Dabei werden neben den führenden Mobile Device Management Lösungen auch organisatorische Themen diskutiert. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Wir freuen uns auf Ihre Teilnahme!

Seminare in Q2

Das zweite Quartal 2012 startet bei Secorvo College mit dem Seminar PKI – Grundlagen, Vertiefung, Realisierung vom 23.-26.04.2012. Erfahren Sie mehr zu Konzeption, Implementierung und Nutzung von PKIs und sichern Sie sich kurzfristig noch Ihren Seminarplatz. Wir freuen uns auf Ihre Teilnahme.

Wenige freie Plätze gibt es auch noch für die nächste Schulung zum TeleTrusT Information Security Professional (T.I.S.P.) vom 07.-11.05.2012 mit anschließender Zertifikatsprüfung. Als Seminarteilnehmer bekommen Sie Ihr Exemplar des T.I.S.P.-Buchs zur Vorbereitung automatisch vorab zugesandt – Sie können das Buch natürlich auch unabhängig von einer Seminaranmeldung bestellen (ISBN: 978-3-942594-08-0).

Ebenfalls im Mai, vom 23.-24.05.2012, bieten wir mit dem zweitägigen Seminar Aktuelle Herausforderungen der Informationssicherheit einen kompakten Überblick zu wesentlichen Themen rund um die Weiterentwicklung der Informationssicherheit.

Die Programme aller Seminare sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college/.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2012	
15.-19.04.	Eurocrypt 2012 (IACR, Cambridge/UK)
16.-17.04.	a-i3/BSI-Symposium 2012 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
Mai 2012	
07.-12.05.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
09.-10.05.	BvD Verbandstag 2012 (BvD e.V., Berlin)
23.-24.05.	Aktuelle Herausforderungen der Informations-sicherheit (Secorvo College, Karlsruhe)
Juni 2012	
11.-13.06.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
14.-15.06.	Datenschutzaudit (Secorvo College, Karlsruhe)
18.-19.06.	DuD 2012 (Computas, Berlin)

Fundsache

Wer hat nicht schon mal von den Sicherheitsprinzipien „Least privilege“ oder „Fail safe defaults“ gehört. Entgegen weit verbreiteter Annahmen handelt es sich hierbei um lang bekannte Prinzipien, die vor 37 Jahren von Saltzer und Schroeder in ihrem Aufsatz „The Protection of Information in Computer Systems“ vorgestellt wurden. Wem das Originalpapier zu trocken ist, dem könnte die Erklärung der Prinzipien anhand von Szenen aus Star Wars gefallen.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Jörg Völker

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

April 2012



Fluch der Vielfalt

Eigentlich ist es der Kern seines Erfolgs: Das „Multi-Purpose"-Konzept des Personal Computers eröffnete Rechenmaschinen einen Multi-Milliardenmarkt. Unvorstellbar heute, dass ein Computer nur eine spezielle Nutzung erlaubt: ein „Word-Prozessor" als Schreibmaschinenersatz, ein „Adress-Manager" statt des Registers im Kalender oder ein Handy, das nur zum Telefonieren taugt. Überlebende Exemplare solcher „Spezial-PCs" (gleichwohl Traum jedes Herstellers, da sie besseren Kopierschutz und höhere Margen bieten) verlieren stetig Marktanteile – wie derzeit Spielkonsolen und mp3-Player.

Das war in der Frühzeit des Computers anders. Ken Olsen, Präsident der Digital Equipment Corp., meinte noch 1977: „Es gibt keinen Grund, warum irgendjemand einen Computer in seinem Haus wollen würde." Im gleichen Jahr erschien der PET von Commodore, und vier Jahre später der IBM-PC. Damit war der Geist aus der Flasche: Heute erwarten wir, dass ein Computer, und heiße er auch „Smartphone" oder „Tablet", via Apps und Internet-Verbindung ein schier grenzenloses Angebot an Funktionen in sich vereint.

Für diese Funktionsvielfalt zahlen wir jedoch einen Preis. Wenn „alles geht", gehen auch Dinge, die wir uns weniger wünschen. Denn Schadsoftware ist vor allem eines – nämlich Software. Und ein „Multi-Purpose"-Gerät kann nicht entscheiden, ob eine App als Nutz- oder als Schadsoftware einzustufen ist. Auch den Hersteller können wir kaum dafür in Haftung nehmen, dass er auf seinen Geräten (fast) alles zulässt – denn genau das haben wir ja gewollt.

So kommt es spätestens beim Online-Banking zum Schwur. Denn ohne ein „One-Purpose-Device" zur Abwicklung unserer Bank-Transaktionen bleibt immer ein Trojaner-Risiko – das wir streng genommen schwerlich der Bank anlasten können, denn wir sind ja die Betreiber des „Alles-Geht-PC". Auch wenn die Einsicht schwerfällt: Wenn wir Sicherheit wollen, müssen wir auf Vielfalt verzichten. Und wenn wir – aus funktionalen Gründen oder aus Bequemlichkeit – nicht verzichten wollen, akzeptieren wir unvermeidlich das Risiko.



Inhalt

Fluch der Vielfalt

Security News

Zielgerade oder Sackgasse?

Hintertür

Haftung bei Filesharing

Steueridentifikationsnummer

Secorvo News

Cloud kommt von Klauen. Oder?

4. Tag der IT-Sicherheit

Nächste Seminare

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Zielgerade oder Sackgasse?

Auf der Crypto-Konferenz Mitte August 2005 wurde ein Angriff gegen SHA-1 präsentiert, der zwar noch nicht praktikabel aber effizienter als Brute-Force-Angriffe war. Seither wurde dieser Angriff verbessert, MD-5 praktisch gebrochen und auch ein Angriff auf die SHA-2-Familie schien in Reichweite.

In dieser Situation, in der die Welt der Krypto-Hashfunktionen, unverzichtbar für Signaturen, Integritätsschutz oder Schlüsselableitung, in Flammen stand, rief das NIST 2007 – ähnlich wie bei der erfolgreichen Entwicklung des AES – einen Wettbewerb für das Nachfolge-Hashverfahren SHA-3 ins Leben.

Nun biegt der Wettbewerb auf die Zielgerade ein: Fünf Finalisten sind benannt, unter denen noch in diesem Quartal der Sieger gekürt werden soll. Anders als beim AES hält sich das NIST jedoch bedeckt. Denn der vermeintliche Flächenbrand entpuppte sich als Strohfeuer: der SHA-2 erscheint heute sicherer als vor sieben Jahren. Und wie NIST-Vertreter Tim Polk am Rande des 83. IETF-Meetings Ende März 2012 erläuterte, wird SHA-3 in den meisten Anwendungsfällen langsamer sein als SHA-2.

Viele Mitglieder des Standardisierungsgremiums schrecken daher davor zurück, eine Unterstützung von SHA-3 verbindlich zu fordern. Angesichts langer Produktzyklen, die dazu führen, dass selbst SHA-2 heute noch nicht durchgängig genutzt werden kann, könnte dies jedoch ein riskantes Spiel sein: ein anderes „Fall-Back"-Verfahren gibt es nicht. Anwender sollten daher in den kommenden Jahren bei ihren Lieferanten auf eine Unterstützung des SHA-3 drängen.

Hintertür

Nicht auszurotten ist offenbar die Neigung von Herstellern, einen permanenten Remote-Zugang in ihre Geräte oder Programme in Gestalt versteckter „Hintertüren" einzubauen. So warnte das US-CERT am 24.04.2012 vor hard-kodierten Accounts in Produkten der Siemens-Tochter RuggedCom, die auch zwölf Monate nach der ersten Warnung nicht behoben sind, und wurde am 26.04.2012 bekannt, dass Telekom-Router vom Typ Speedport einen trivialen Zugang zu privaten WLAN-Netzen via Backdoor ermöglichen.

Diese Vorfälle reihen sich ein in eine lange Liste ähnlicher Probleme. Prominente Beispiele sind eine Schwachstelle in Siemens S7-Geräten vom August 2011 und eine kritische Lücke in Apple Quicktime vom August 2010.

Die Implementierung undokumentierter Zugänge zu Systemen oder Anwendungen ist, wie der Hausschlüssel unter der Fußmatte, eine Einladung für ungebetene Gäste – und gehört auch zu Testzwecken untersagt. Unternehmen sollten sich zumindest für kritische, von außen erreichbare Systeme die Abwesenheit solcher Hintertüren vom Hersteller zusichern lassen.

Haftung bei Filesharing

Das Bundesverfassungsgericht hat mit Beschluss vom 21.03.2012 gegenüber dem OLG Köln deutlich gemacht, dass es die Frage der Überwachungspflichten der Inhaber eines Internetanschlusses noch nicht für abschließend entschieden hält.

Das OLG Köln hatte unter Berufung auf das sog. WLAN-Urteil des BGH („Sommer unseres Lebens") vom 12.05.2010 Prüfpflichten des Anschlussinhabers auch für den Fall angenommen, dass der wahre Störer bekannt ist. Im entschiedenen Fall handelte es sich um den Sohn der Lebensgefährtin. Trotz entgegenstehender Rechtsprechung bspw. des OLG Frankfurt ließ das OLG Köln die Revision nicht zu. Das Bundesverfassungsgericht bejahte dagegen die Uneinheitlichkeit der Rechtsprechung und hielt die Revision für offensichtlich zulässig.

In einer Nebenerwägung hat das Bundesverfassungsgericht außerdem bewusst die Frage offen gelassen, ob die anwaltlichen Massenabmahnungen überhaupt eine taugliche und zu vergütende anwaltliche Leistung darstellen. Für die Unternehmen der Musikindustrie und ihre anwaltlichen Vertretungen bedeutet diese Entscheidung, dass mit weiteren Beschränkungen der postulierten Sorgfaltspflichten der Anschlussinhaber gerechnet werden muss – und dass Massenabmahnungen vielleicht in naher Zukunft kein funktionierendes Geschäftsmodell mehr darstellen.

Steueridentifikationsnummer

Mit Urteil vom 18.01.2012 hat der Bundesfinanzhof über die Rechtmäßigkeit der Vergabe der steuerlichen Identifikationsnummer entschieden. Schwerpunkt des Urteils bildet die Prüfung eines möglichen Verstoßes gegen das Grundrecht auf informationelle Selbstbestimmung der Betroffenen. Anhand der Gesetzesbegründung werden die hier Zwecke der Einführung sowie die über die Steueridentifikationsnummer abgewickelten Übermittlungen untersucht. Die Nummer gelte der Verfahrensvereinfachung, der Durchsetzung der Belastungsgleichheit der Steuerzahler und dem Bürokratieabbau. Dabei kommt das Gericht zu der Einschätzung, dass der Eingriff in die informationelle Selbstbestimmung durch die überragende Bedeutung der verfolgten Schutzziele gerechtfertigt wird.

Mit den Gefährdungen, die mit dem Eingriff verbunden sind, setzt sich das Gericht jedoch kaum auseinander und kommt so zum Schluss, dass die jeweiligen rechtlich verankerten Zweckbindungen der übermittelten Daten den Eingriff ausreichend beschränken. Die Frage, inwieweit bereits die Nummer als Mittel der Datenzusammenführung einen Eingriff darstellt, bleibt unberücksichtigt. Überhaupt werden als Risiken lediglich die gesetzlich vorgesehenen Einsatzzwecke betrachtet und der Eingriff infolge dessen als gering eingestuft.

Ähnlich kurz verneint das Gericht mit Verweis auf die pauschale Forderung nach technischen und organisatorischen Sicherheitsmaßnahmen in § 5 StIdV das Bestehen von Sicherheitsrisiken durch den Einsatz der Steueridentifikationsnummer.

Tatsächlich stellt das Urteil keine ernsthafte Auseinandersetzung mit den Datenschutzrisiken der Steueridentifikationsnummer dar. Die Rechtfertigung des Grundrechtseingriffs wird allein durch den Nutzen begründet – eine beängstigende Argumentation in einem freiheitlichen Rechtsstaat.

Secorvo News

Cloud kommt von Klauen. Oder?

Die Frage nach Sicherheit und Datenschutz beim Cloud Computing wird derzeit intensiv diskutiert. Wie lassen sich sensible Daten in der Wolke wirksam vor Missbrauch schützen? Und wie kann es gelingen, Anforderungen des Datenschutzrechts an Cloud-Computing-Dienste effektiv umzusetzen? Können diese Anforderungen überhaupt rechtsgestaltend und durch technisch-organisatorische Maßnahmen erfüllt werden, oder sollte man als verantwortungsbewusstes Unternehmen auf Cloud Computing verzichten?

Diesen und weiteren Fragen gehen Dirk Achenbach (Karlsruher Institut für Technologie) und Michael Knopp (Secorvo) beim nächsten KA-IT-Si-Event "Cloud kommt von Klauen. Oder?" am **10.05.2012** im Rahmen der Cloudzone 2012 nach. Die Impuls-Vorträge der beiden Referenten bringen die Herausforderungen auf den Punkt und skizzieren Lösungsansätze – anschließend heißt es „Ring frei" für eine intensive Diskussion.

Das Event beginnt diesmal ausnahmsweise bereits um 17 Uhr – und findet im Konferenzbereich der Messe Karlsruhe statt, wie gewohnt mit anschließendem Buffet-Networking. Als KA-IT-Si-Teilnehmer haben Sie außerdem die Möglichkeit, vorab die Cloudzone 2012 kostenfrei zu besuchen. Wir freuen uns auf Ihre Anmeldung!

4. Tag der IT-Sicherheit

Nach der hervorragenden Resonanz der vergangen Jahre freuen wir uns, Sie auch 2012 wieder zum **Tag der IT-Sicherheit**, einer Gemeinschaftsveranstaltung der KA-IT-Si mit der IHK Karlsruhe, dem CyberForum e.V. und KASTEL, einladen zu können. Die Veranstaltung beginnt am **12.07.2012** um 14.00 Uhr im Saal Baden der IHK Karlsruhe. Auch in diesem Jahr erwarten Sie wieder spannende Vorträge rund um die IT-Sicherheit. Die Möglichkeit zur Online-Anmeldung finden Sie Kürze unter http://www.ka-it-si.de. Wir freuen uns auf Ihre Teilnahme!

Nächste Seminare

Das kommende T.I.S.P.-Seminar vom 7.-11.05.2012 ist ausgebucht – die nächste Gelegenheit zur Zertifizierung bieten wir am 17.-21.09.2012 sowie am 12.-16.11.2012.



Genug Zeit, um sich bis dahin den Sommerurlaub mit dem T.I.S.P.-Buch zu versüßen – oder eines der beiden folgenden Seminare zu besuchen, die Ihre besondere Aufmerksamkeit verdienen: Aktuelle Herausforderungen der Informationssicherheit (23.-24.05.2012) bietet eine kompakte Auseinandersetzung mit wesentlichen aktuellen Technologien und Trends. In zwei Tagen werden sechs Themenfelder und zugehörige Schutzmaßnahmen diskutiert. Das Seminar Datenschutzaudit: Best Practice (14.-15.06.2012) zeigt auf, wie es gelingt, auch ohne gesetzliche Maßgaben, sinnvolle und effiziente Datenschutzaudits zu planen und durchzuführen. Basis hierfür sind die umfassenden Erfahrungen des Referententeams.

Alle weiteren Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2012	
07.-12.05.	T.I.S.P.-Schulung und Prüfung (Secorvo College, Karlsruhe)
09.-10.05.	BvD Verbandstag 2012 (BvD e.V., Berlin)
10.05.	Cloud kommt von Klauen. Oder? (KA-IT-Si, Kalrsuruhe)
23.-24.05.	Aktuelle Herausforderungen der Informationssicherheit (Secorvo College, Karlsruhe)
Juni 2012	
11.-13.06.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
14.-15.06.	Datenschutzaudit (Secorvo College, Karlsruhe)
18.-19.06.	DuD 2012 (Computas, Berlin)
19.-21.06.	Forensik (Secorvo College, Karlsruhe)
Juli 2012	
12.07.	4. Tag der IT-Sicherheit (IHK Kalrsruhe, CyberForum und KA-IT-Si, Karlsruhe)
21.-26.07.	Blackhat USA 2012 (Las Vegas/US)
26.-29.07.	DEFCON 20 (Las Vegas/US)

Fundsache

Am 23.04.2012 erschien die 8. Ausgabe des Magazins „hack in the box“ als pdf. Darin werden unter anderem Angriffsmethoden wie die Nutzung von Browser Exploit Packs und gezielte Angriffe auf den Windows-Kernel anschaulich dargestellt.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

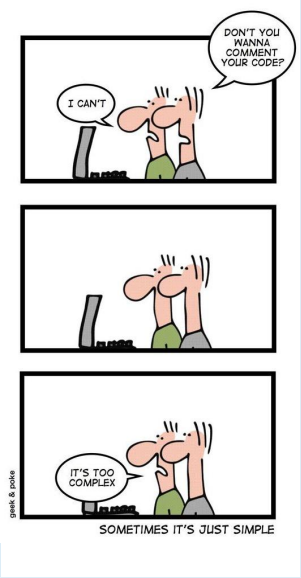
Mai 2012



Die Geister, die ich rief...

Der Umgang mit unkontrollierter Komplexität wurde schon Goethes Zauberlehrling zum Verhängnis. Zunächst verlief alles nach Wunsch des Protagonisten: Er verschaffte sich durch Nutzung eines Reinigungstools eine Arbeitserleichterung. Leider wies dieses einige Schwachstellen auf und ließ sich durch den Lehrling nicht mehr kontrollieren – da wuchs dem Armen die Unbeherrschbarkeit seines Setups über den Kopf: "*Die ich rief, die Geister, werd ich nun nicht los.*"

Moderne Software-Entwicklung weist erschreckend viele Parallelen zu Goethes Lehrling auf. So verlässt sich heute die Mehrheit der Anwendungen auf externe Bibliotheken und Frameworks. Der eigene Code dient häufig nur noch der abstrakten Orchestrierung von wie durch Zauberhand bereit gestellter Funktionalität. Das tiefere Verständnis der genutzten Werkzeuge geht dabei verloren. Gerade die Sicherheit des Endprodukts aber hängt wesentlich von der Sicherheit der verwendeten Bibliotheken ab – und um die ist es nicht besonders gut bestellt: Aspect Security fand im März 2012 in jeder vierten Bibliothek bekannte Sicherheitsbugs. Der geregelte Umgang mit der Komplexität externer Komponenten muss zumindest die Kontrolle der genutzten Werkzeuge und den Überblick über Schwachstellen gewährleisten.



Der Weg zur Meisterschaft ist steinig. Aber nur die erlaubt den erlösenden Ruf: "*In die Ecke, Besen! Besen! Seids gewesen!*"



Inhalt

Die Geister, die ich rief...

Security News

Puls des Internet

Warnung vor Hotspots

Vertrauenswürdiges Internet

Neues TK-Recht

Nmap 6

Neuer Ripper

Secorvo News

Seminare für alle

4. Tag der IT-Sicherheit

Sicher – sicherer – Android?

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Puls des Internet

Das SSL Observatory der Electronic Frontier Foundation (vgl. SSN 12/2010 und 02/2012) widmet sich den SSL-Zertifikaten in „freier Wildbahn" samt den ausstellenden Trust Centern. Eine gute Ergänzung bietet SSL Pulse, eine am 25.04.2012 publizierte Statistik über die Sicherheit von SSL-Websites, bei der unter anderem die Konfiguration der angebotenen SSL/TLS-Protokollversionen und Cipher Suites geprüft wurde. In diese Übersicht flossen die Ergebnisse von ca. 200.000 SSL Server Tests der Qualys SSL Labs ein.

Beunruhigendes Ergebnis: ca. drei Viertel aller Sites sind anfällig gegen die im September 2011 publizierte BEAST Attacke, die es einem Angreifer unter bestimmten Umständen ermöglicht, SSL/TLS-geschützte Passwörter oder Cookies zu ermitteln. Die technische Analyse verrät naturgemäß nicht, ob die betroffenen Serverbetreiber diese Bedrohung als zu gering bewerten, um die mit einem Update oder Einschränkungen verbundenen Gegenmaßnahmen zu ergreifen, oder ob sie die Attacke schlicht nicht kennen. Betreibern öffentlicher SSL/TLS-Server ist jedenfalls sehr zu empfehlen, den eigenen Server dem (kostenfreien) SSL Server Test zu unterziehen – und sei es nur als Rückversicherung, dass die beabsichtigte Konfiguration korrekt umgesetzt ist – bevor andere feststellen, dass der Server doch nicht zum letzten Viertel zählt.

Warnung vor Hotspots

Am 08.05.2012 warnte das Internet Crime Complaint Center (IC3) des FBI, dass Laptops, die sich in öffentliche (Hotel-) WLANs einbuchen, eine Verseuchung durch Malware befürchten müssen. Diese Warnung reiht sich ein in ähnliche Hinweise auf versteckte Manipulationen von Betreibern öffentlicher Hotspots – und kann Techniker erstmal nicht überraschen.

Mit zunehmender Moblilität steigt jedoch die Gefahr, dass Nutzer öffentlichen Hotspots blind vertrauen. Verlässlichen Schutz bietet die Nutzung des VPN-Zugangs der eigenen Firma oder ein vertrauenswürdiges „Personal VPN". Mindestens aber sollte eine „Personal Firewall" Zugriffe von außen abblocken und jeder mobile Nutzer sicher stellen, dass er nicht über ungesicherte Verbindungen auf kritische Dienste zugreift oder vertrauliche Informationen übermittelt.

Vertrauenswürdiges Internet

Am 10.05.2012 kündigte die NCC Group an, das verlorene Vertrauen in das Internet durch die Schaffung einer neuen Top-Level-Domäne (TLD) *.secure* wieder zurück zu gewinnen. Zuteilungen für Domänen unterhalb der neuen TLD sollen nur Betreiber erhalten, die Mindestsicherheitsstandards für ihre Systeme vorweisen können.

Details hierzu werden zur Zeit abgestimmt. Es ist aber bereits bekannt, dass die durchgängige Verwendung von SSL/TLS für Webseiten, die Absicherung von DNS mit DNSSEC und die Verwendung von DKIM für E-Mails gefordert werden. Auf der FAQ-Seite wird angekündigt, dass die Dokumente von Antragstellern durch den Betreiber Artemis überprüft werden.

Aufschlussreich ist der Abschnitt über die Kosten einer *.secure*-Domäne: "*.SECURE domains provide premium value to registrants and their customers an will be priced accordingly.*" Die Erfindung einer Gelddruckmaschine? Auch wenn bereits begründete Zweifel am tatsächlichen Sicherheitsgewinn laut werden, ist eines definitiv sicher: Die indische Regierung wird mit ihrer Domäne kaum glücklich werden: https://in.secure

Neues TK-Recht

Am 04.05.2012 ist das Gesetz zur Änderung telekommunikationsrechtlicher Regelungen in Kraft getreten. Ziel des Gesetzes ist die Stärkung der Verbraucherrechte. Für die Nutzung von Standortdaten der Nutzer wurde in § 98 Abs. 1 TKG eine neue Informationspflicht eingeführt: Der Gerätenutzer – nicht der Anschlussinhaber – muss bei jeder Standortermittlung hierüber per Textmitteilung in Kenntnis gesetzt werden.

Wird der Schutz personenbezogener Daten verletzt, sind neben der BNetzA der Bundesdatenschutzbeauftragte, in schwer wiegenden Fällen die Betroffenen zu informieren. § 109a Abs. 3 TKG verpflichtet die Anbieter ein Verzeichnis über Datenschutzverletzungen zu führen. Die hierdurch entstehende Pflicht zur Selbstanzeige soll durch Verweis auf das Verwertungsverbot in § 42a Satz 6 BDSG rechtsstaatlich entschärft werden.

Die Verpflichtung zur Erstellung und Vorlage eines Sicherheitskonzepts (§ 109 TKG) wurde ausgedehnt auf die Anbieter von Telekommunikationsdiensten. Außerdem wurde entsprechend § 42a BDSG eine Meldepflicht bei Sicherheitsverletzungen in § 109 Abs. 5 und § 109a TKG eingeführt. Die Bundesnetzagentur kann daraufhin den Betreiber oder Dienstanbieter zu einem ausführlichen Bericht verpflichten. Außerdem kann sie nach Abs. 7 dem Betreiber oder Dienstanbieter eine Auditierung auferlegen.

Mit dem Änderungsgesetz zielt der Gesetzgeber darauf, den Datenschutz durch Transparenzpflichten zu stärken. Zwar ist dies zu begrüßen, allerdings muss befürchtet werden, dass gehäufte Transparenz irgendwann zu Abstumpfung der Adressaten führt und damit ihre Wirkung verlieren wird.

Nmap 6

Pünktlich zum nahenden World IPv6 Day hat Gordon „Fyodor" Lion am 21.05.2012 ein neues Release des Portscanners Nmap herausgebracht – passenderweise mit Versionsnummer 6. Eines der Hauptfeatures besteht denn auch in voller IPv6-Unterstützung. Neben den „üblichen" Verbesserungen (schnellere Scan-Engine, mehr und ausgefeiltere Skripte) zeichnet sich ab, dass die Grenzen zwischen Portscanner und Schwachstellenscanner immer mehr verwischen: auch das neue Release von Nmap setzt seinen Vormarsch in Richtung Webanwendungsscanner fort.

Mit dem Einsatz von IPv6 müssen sich Administratoren und Pentester von der beliebten Praxis verabschieden, ein Subnetz nach laufenden Diensten zu durchscannen – das verbietet die schiere Größe des Adressraums von IPv6-Subnetzen. Alternative Ansätze zum Auffinden von Hosts sind beispielsweise in RFC 5157 beschrieben.

Ein Tool, das dabei nützlich werden könnte, ist das neue Nping, das zur Familie der Nmap-Tools hinzugekommen ist; dessen IPv6-Unterstützung ist aber derzeit noch als „experimental" eingestuft.

Einer der Zukunftspläne für Nmap sieht vor, neue NSE-Scripte und OS-Fingerprints über einen Update-Service bereit zu stellen. Aber auch so bleibt Nmap in absehbarer Zukunft eines der wichtigeren Test-Tools für Admins und Pentester.

Neuer Ripper

Seit dem 06.05.2012 steht Version 2.5 des forensischen Werkzeugs RegRipper für Windows zur Verfügung. Bisherige Plugins funktionieren nicht nur weiterhin; mit ihnen können nun die Metadaten einzelner Dateien wie z. B. Benutzerprofilen (NTUSER.DATs) oder Dateigruppen wie Verknüpfungen (*.LNKs) direkt aus den schreibgeschützten Volume Shadow Copies (VSC) abgefragt werden. Dadurch kann auf das fehleranfällige Kopieren von Dateien aus VSCs verzichtet werden. Mit Unterstützung des neuen Dateisystems ReFS ist RegRipper bereits für Windows 8 gerüstet.

Secorvo News

Seminare für alle

Sie haben Verstärkung im Team bekommen? Herzlichen Glückwunsch! Als Steilkurs für die neue Kollegin oder den neuen Kollegen empfehlen wir unser Seminarpaket aus "Sicherheitsmanagement heute" und "IT-Sicherheit heute". Und falls an Ihrer Bürowand noch kein T.I.S.P.-Zertifikat prangen sollte: Das nächste Zertifizierungsseminar bieten wir vom **17.–21.09.2012**. Das T.I.S.P.-Buch erhalten Sie mit der Anmeldung vorab – als erbauliche Urlaubslektüre. Weitere Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

4. Tag der IT-Sicherheit

Gemeinsam mit der IHK Karlsruhe, dem Cyber-Forum e.V. und KASTEL veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **12.07.2012** bereits zum vierten Mal den "Tag der IT-Sicherheit". Die Veranstaltung beginnt um 14.00 Uhr im Saal Baden der IHK Karlsruhe. Auch in diesem Jahr erwartet Sie wieder ein spannendes Vortragsprogramm. Ausgewiesene Experten stellen den Stand der Entwicklung bei Hackerangriffen („Live Hacking") und Schutzstrategien in Theorie und Unternehmenspraxis vor. Gelegenheit zum fachlichen und persönlichen Austausch mit Referenten, Teilnehmern und Ausstellern bietet die „Networking-Pause".

Nach der positiven Ressonanz der vergangenen Jahre rechnen wir mit zahlreichen Teilnehmern und empfehlen daher eine frühzeitige Anmeldung. Wir freuen uns auf Ihre Teilnahme!

Sicher – sicherer – Android?

Besitzern von Smartphones bietet sich eine reiche, ständig größer werdende Auswahl von Apps. Aber wie sicher ist eine Mobile-Banking-App, wenn das neueste Tablet-Spiel "unerwünschte Nebenwirkungen" hat? Wie gut können sensitive Daten in Unternehmens-Apps geschützt werden, wenn die Smartphone-Besitzer daneben so viele Apps eigener Wahl installieren, wie der Speicher hergibt?

Mit diesen und anderen Fragen setzt sich Hans-Joachim Knobloch (Secorvo) beim nächsten KA-IT-Si Event am **21.06.2012** auseinander. Sein Vortrag "Apps - tickende Bomben im Bauch des Androiden?" gibt einen Überblick über die Sicherheitsarchitektur von Android, beleuchtet verschiedene Bedrohungsszenarien und stellt Mechanismen sowie Konzepte zur sicheren Gestaltung von Android-Apps vor.

Beginn der Veranstaltung ist um 18.00 Uhr im Panoramasaal der IHK Karlsruhe. Um Anmeldung wird gebeten.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2012	
18.-19.06.	DuD 2012 (Computas, Berlin)
19.-21.06.	Forensik (Secorvo College, Karlsruhe)
21.06.	Sicher – sicherer – Android? (KA-IT-Si, Karlsruhe)
Juli 2012	
12.07.	4. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
21.-26.07.	Blackhat USA 2012 (Las Vegas/US)
26.-29.07.	DEFCON 20 (Las Vegas/US)
August 2012	
06.-08.08.	DFRWS 2012 (DFRWS, Washington/US)
08.-10.08.	21th USENIX Security Symposium (Usenix, Bellevue/US)
19.-23.08.	Crypto 2012 (IACR, Santa Barbara/US)
20.-24.08.	SecSE 2012 (SINTEF, Prag/CZ)
27.08.	Sommerakademie 2012 (ULD Schleswig-Holstein, Kiel)

Fundsache

Kaum zu glauben: Die schier unausrottbare SQL-Injection – der „Buffer-Overflow der Web-Applikationen" – wird 2012 bereits 14 Jahre alt. Die Erstveröffentlichung erschien 1998 in Heft 54 des Phrack Magazine (Volume 8).



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Safuat Hamdy, Kai Jendrian (Editorial), Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting. Abdruck des Cartoons mit freundlicher Genehmigung von geek & poke.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news"). Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2012



Süßes Gift

Mit Begriffen im schnörkellosen Suchfenster fing es an. Bald ersetzte ‚Googeln' mühsame Bibliotheksrecherchen. Es folgte der Online-Stadtplan: Statt unhandlicher Faltkarten ein Klick auf die Anschrift, und der Routenplaner von Google Maps zeigt uns den Weg. Vor dem nächsten Termin (abgerufen aus dem Google-Kalender) schnell ein Blick in die Nachrichten. Ohne Kleingeld und Kiosk, voluminöse Papierformate und druckschwarze Finger, bequem via Google News und Chrome-Browser auf dem Display des Android-Smartphones. Die Zeit reicht noch für ein Picasa-Upload des Enkel-Fotos für die Oma und eine Youtube-Recherche, da kommt via Gmail ein Vertragsentwurf herein – auf Portugiesisch. Schnell in den Google-Übersetzer geschoben, ein wenig Nachbearbeitung in Google-Docs, und schon liegt eine verständliche Fassung für die Google-Talk-Konferenz vor...

Geräuscharm hat sich Google in unser Leben geschlichen. Betört von der Verlockung unentgeltlicher, benutzerfreundlicher Online-Dienste opfern wir willig Zug um Zug unsere Unabhängigkeit: Nicht mehr lange, und Google wird auch unsere Online-Shops, Zahlungssysteme, Fernsehsender und Webseiten betreiben. Und wir werden uns fragen: Wie ging eigentlich Leben ohne Google?

38 Mrd. US-Dollar Umsatz erwirtschaftete Google 2011, das entspricht etwa 5,5 % des deutschen Steueraufkommens. Damit finanziert Google seine „Gratiskultur". Mitbewerber werden das nicht ewig durchhalten – und aufgeben. Und dann wird, Schritt für Schritt, auch Googles Gratiskultur zu Ende gehen. Aus Mangel an Alternativen werden wir – abhängig und betört – die Zeche zahlen.

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, (...) kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden", konstatierte das BVerfG im Volkszählungsurteil 1983. Der Preis der Bequemlichkeit ist manchmal – die Freiheit.



Inhalt

Süßes Gift

Security News

PKI ist schwierig

Passwörter sind schwierig

Signatur-Harakiri

Safer Browsing

Große Fische

IPv6 World Launch Day

Secorvo News

4. Tag der IT-Sicherheit

Zertifiziertes Wissen

Erfolgreiche KA-IT-Si

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

PKI ist schwierig

Wie Microsoft am 03.06.2012 einräumte, trug der Flame-Trojaner eine gültige Code-Signatur mit einem Zertifikat, das auf die Microsoft Root CA zurück geht und eigentlich von Microsoft für die Lizenzkontrolle von Terminal Servern erstellt wurde.

Kryptologen und Verschwörungstheoretiker wird interessieren, dass von den Flame-Autoren dafür eine MD5-Hashkollision genutzt wurde, die nicht nach dem bisher bekannten Schema konstruiert wurde. Noch frappierender ist das Eingeständnis, dass dies zumindest für Windows XP gar nicht nötig gewesen wäre – weil es auch Zertifikate ohne die Kennzeichnung „für Code-Signing" akzeptiert.

Immerhin ergriff Microsoft die Gelegenheit, im PKI-Bereich durchzugreifen: Künftig wird Windows (einschließlich XP) für die meisten Zwecke Zertifikate für RSA-Schlüssel kleiner 1024 Bit Schlüssellänge zurückweisen. Zudem werden – weil man der Sperrung mittels CRLs nicht recht traut – nicht nur neue CA-Zertifikate über eine Certificate Tust List in Windows nachgepflegt, sondern auch zu sperrende CAs per Windows Update als „nicht vertrauenswürdig" gekennzeichnet. Den Anfang machten die an den Terminal-Server-Lizenzen beteiligten MS-CAs. Der eigentliche Vertrauensanker in der PKI-Praxis sind also nicht die Root-CAs, sondern die Betriebssystem- und Browser-Hersteller.

Passwörter sind schwierig

Immer noch schützen hauptsächlich Passwörter digitale Identitäten im Web. Dabei droht die Gefahr weniger von Brute-Force-Angriffen auf Webanwendungen – denn dagegen helfen schon achtstellige Passwörter, die sich nicht in Wörterbüchern finden. Gravierender sind Sicherheitsvorfälle, bei denen die Passwort(hash)datenbanken von Anbietern kompromittiert werden – wie in diesem Monat bei LinkedIn, eHarmony und Last.fm geschehen. Offenbar wurden in allen Fällen bekannte Mechanismen zum Schutz von Passwortdatenbanken vor Offline-Angriffen nicht eingesetzt. Auch angesichts vereinzelter Kritik an diesen Mechanismen – Sicherheit erfordert immer einen Trade-Off.

Solange Entwickler Passwort-Datenbanken nicht angemessen schützen, sollten Sie für unterschiedliche Dienste auch unterschiedliche Passwörter verwenden. Und „Finger weg" von so genannten Passwort-Checkern: Probieren Sie mal The Passwort Security Checker aus – allerdings besser mit einem fiktiven Passwort...

Signatur-Harakiri

Am 04.06.2012 hat die Europäische Kommission den Entwurf einer Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vorgestellt. Der Entwurf soll die Signaturrichtlinie (RL 1999/93/EG) ersetzen, die als lückenhaft und überarbeitungsbedürftig gilt. Die Verordnung, die in den Mitgliedstaaten direkt anwendbares Gesetz wäre, soll die bislang nicht erreichte Harmonisierung herstellen und nimmt zudem beträchtliche Erweiterungen vor. Ziele sind die Entwicklung eines digitalen Binnenmarktes, die Förderung öffentlicher Dienste, die Anregung des Wettbewerbs und die Verbesserung der Benutzerfreundlichkeit.

Die Verordnung stellt „qualifizierte Siegel" an die Seite qualifizierter elektronischer Signaturen, führt qualifizierte Zertifikate zur Website-Authentifizierung und qualifizierte elektronische Zustelldienste ein und regelt die bereits bekannten Zeitstempel samt den zugehörigen Beweisvermutungen. Die Regelung der Zustellungsdienste fällt deutlich knapper aus als der deutsche De-Mail-Ansatz, ignoriert jedoch mit seiner Beweisvermutung auch eine Vielzahl wichtiger Detailfragen, wie etwa die der Empfangseröffnung. Die Kommission wird ermächtigt, Detailregelungen zu treffen.

Spätestens mit den direkt geltenden Beweisvermutungen greift die Verordnung tief in die nationalen Rechtsordnungen ein, ohne Rücksicht auf jegliche bestehende Systematik. Zu mehr Rechtssicherheit wird ein solches Vorgehen kaum führen.

Die Kommission geht offenbar von einer völlig verkürzten Problemanalyse aus. Während die Stellungnahme der Bundesregierung immerhin fehlende Nutzerakzeptanz und ein Auseinanderfallen von primären Nutznießern und Kostenträgern anspricht, fehlen in den Augen der Kommission lediglich europaweite Interoperabilität und die ergänzten weiteren Dienste für den Durchbruch der Signaturen. Bei dieser Förderung braucht das Konzept der elektronischen Signatur eigentlich keine Feinde mehr.

Safer Browsing

Am 21.05.2012 jährte sich die „Safe Browsing"-Initiative von Google zum fünften Mal. Nach eigenen Angaben identifiziert Google täglich knapp 10.000 Malware-verseuchte Webseiten und warnt deren Betreiber, ISPs und CERTs – sowie bis zu 14 Mio. Suchanfragen. 2012 summierten sich die entdeckten Phishing-Sites auf über 300.000 pro Monat. Das ist mehr als ein Tropfen auf dem heißen Stein – ein wichtiger Beitrag zur Eindämmung der zunehmenden Online-Kriminalität.

Große Fische

Angreifer, die Online-Banking-Nutzer ins Visier nehmen, haben seit Jahren mit heftiger Gegenwehr der Kreditinstitute zu kämpfen. Mit iTANs, mTANs und TAN-Generatoren, Überweisungslimits und hartem Vorgehen gegen „Geldboten", die – oft reichlich naiv – ihre Konten für die betrügerischen Überweisungen zur Verfügung stellen, halten die Banken die Schäden bislang in Grenzen.

Nun stehen offenbar erstmals Firmenkunden im Fokus der Angreifer, wie McAfee in einem am 26.06.2012 publizierten White Paper ausführt. Zwar ist das erfolgreiche Einschleusen von Trojanern in Unternehmen oft ungleich schwieriger; dafür ist der finanzielle Anreiz deutlich größer, schließlich weisen Geschäftskonten in der Regel eine erheblich höhere Liquidität auf. Zudem bleiben gut getarnte Transaktionen mit mittelgroßen Beträgen länger unentdeckt – und erleichtern es einem Angreifer, die Spuren zu verwischen.

Spätestens jetzt ist es an der Zeit, die Führung des Firmen-Online-Kontos, sofern noch nicht geschehen, auf einen separaten Rechner und Token-Nutzung umzustellen – denn iTANs bieten keinen ausreichenden Schutz vor Trojanern, die sich als „Man-in-the-Browser" im System einnisten.

IPv6 World Launch Day

Auf den World IPv6 Day 2011 folgte am 06.06.2012 der World IPv6 Launch Day: Seitdem sind diverse Internet-Sites dauerhaft über IPv6 erreichbar. Der IPv6-Support der Hersteller wird auch im Home-Bereich immer besser, und verschiedene ISPs planen, auch im Consumerbereich IPv6 anzubieten. Diesmal ist die „Drohung" IPv6 wohl ernst gemeint.

Eine übereilte Einführung kann jedoch fatale Folgen für Sicherheit und Betrieb der eigenen Netze haben. So wurde auf dem IPv6-Kongress am 10.-11.05. 2012 der Aufwand einer IPv6-Umstellung mit der Behandlung des Y2K-Problems verglichen. Die größte Gefahr bestehe darin, IPv6 wie IPv4 mit längeren Adressen zu betreiben, da IPv6 eine deutlich andere Architektur aufweist. Ein typischer Stolperstein ist beispielsweise NAT, das bei IPv6 so nicht vorgesehen ist. So langsam sollte die Beschäftigung mit der Umstellung daher auch bei Sicherheitsverantwortlichen oben auf der Agenda stehen.

Secorvo News

4. Tag der IT-Sicherheit

Bereits zum vierten Mal findet am **12.07.2012** der "Tag der IT-Sicherheit" statt - eine Gemeinschaftsveranstaltung der KA-IT-Si mit der IHK Karlsruhe, dem CyberForum e.V. und KASTEL.

Im Rahmen der diesjährigen Keynote „Hacking 2012" werden aktuelle Entwicklungen bei Angriffsmethoden aufgezeigt und einige Bedrohungen live vorgeführt. Anschließend erwarten Sie weitere spannende und praxisnahe Vorträge zu den Themen Hardware- und Softwaresicherheit, Verschlüsselung und Onlinebanking, begleitet von fachlichem und persönlichem Networking mit Referenten, Teilnehmern und Ausstellern. Beginn ist um 14.00 Uhr im Haus der Wirtschaft/Saal Baden der IHK Karlsruhe. Wir freuen uns auf Ihre Anmeldung!

Zertifiziertes Wissen

Wenn Sie planen, noch 2012 das T.I.S.P.-Zertifikat zu erwerben, empfehlen wir Ihnen, den Termin jetzt zu wählen: Für das Seminar vom **17.-21.09.2012** stehen noch wenige freie Plätze zur Verfügung; ein weiteres Seminar bieten wir vom **12.-16.11.2012** an. Die Autoren des T.I.S.P.-Buches (im Seminarpreis enthalten) bereiten Sie persönlich auf die Zertifikatsprüfung vor.

Sicherheitslöcher in Software sind meist die Ursache von Sicherheitsvorfällen. Damit Ihre Webanwendungen und Programme dagegen gefeit sind, sollten Sie Ihren Entwicklern das Seminar „Certified Professional for Secure Software Engineering (CPSSE)" vom **24.-27.09.2012** ans Herz legen. Dort erfahren sie, worauf es bei der Entwicklung sicherer Software ankommt. Das CPSSE-Zertifikat bestätigt ihre persönliche Qualifikation – und belegt den Qualitätsanspruch Ihres Unternehmens.

Alle weiteren Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Erfolgreiche KA-IT-Si

Die Events der KA-IT-Si verzeichnen in diesem Jahr einen besonders großen Zulauf – fast 300 Teilnehmer haben die Veranstaltungen in der ersten Jahreshälfte besucht. Mit der MF APP AG und der proRZ Rechnenzentrumsbau GmbH konnten außerdem zwei neue Partner für die Initiative gewonnen werden.

Wir danken Ihnen für Ihr Interesse an unseren Events und freuen uns auf ein Wiedersehen nach der Sommerpause. Am **13.09.2012** meldet sich die KA-IT-Si mit der nächsten Veranstaltung zurück.

Informationen zum Vortrag und die Möglichkeit zur Anmeldung gibt es demnächst auf http://www.ka-it-si.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2012	
12.07.	4. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
21.-26.07.	Blackhat USA 2012 (Las Vegas/US)
26.-29.07.	DEFCON 20 (Las Vegas/US)
August 2012	
06.-08.08.	DFRWS 2012 (DFRWS, Washington/US)
08.-10.08.	21th USENIX Security Symposium (Usenix, Bellevue/US)
19.-23.08.	Crypto 2012 (IACR, Santa Barbara/US)
20.-24.08.	SecSE 2012 (SINTEF, Prag/CZ)
27.08.	Sommerakademie 2012 (ULD Schleswig-Holstein, Kiel)
September 2012	
17.-21.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
18.09.	Anwendertag IT-Forensik 2012 (Fraunhofer SIT, Darmstadt)
24.-27.09.	CPSSE-Schulung (Secorvo College, Karlsruhe)
25.-26.09.	D·A·CH Security (GI/OCG/BITKOM/SI/TeleTrusT, Konstanz)

Fundsache

Am 12.06.2012 hat das US-amerikanische NIST eine Überarbeitung der Special Publication SP 800-121 „Bluetooth-Security“ veröffentlicht, die nun auch die Schutzmechanismen von Bluetooth v4.0 umfasst.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Juli 2012



Als gestern noch Zukunft war

Erinnern Sie sich noch? Bush ist neuer US-Präsident, Scharping tritt als Bundesverteidigungsminister zurück. Der Kanzler heißt Schröder, der Formel-1-Weltmeister wieder Schumacher und der gerade erst eingeführte Euro „Teuro“: wir schreiben das Jahr 2002. Noch immer gibt es kein betriebsbereites UMTS-Mobilfunknetz, obwohl die Lizenzen schon seit zwei Jahren versteigert sind. Gerade erst wurde der AES nach dreijährigem Auswahlverfahren zum Nachfolger des DES gekürt. Online-Banking-Transaktionen werden mit einfachen TAN-Listen autorisiert, Apple hat den ersten iPod vorgestellt. Niemand weiß, was ein ‚Smartphone' sein soll, Compaq wird von HP übernommen und Mannesmann Mobilfunk heißt nun Vodafone D2. Und im Juli erscheint die erste Ausgabe der „Secorvo Security News“.

Zehn Jahre, 480 Seiten und knapp 1.000 Nachrichten liegt dieses Ereignis nun zurück. Die Themen und Herausforderungen, die uns in den vergangenen zehn Jahren beschäftigt haben, werden uns zweifellos auch im kommenden SSN-Jahrzehnt begleiten.

Allerdings wird es nicht leichter für IT-Sicherheit und Datenschutz. Daten werden in wachsendem Umfang Cloud-Diensten anvertraut, die IT wird sich mehr und mehr von einer Infrastruktur- zu einer Service-Dienstleistung entwickeln. Die Endgeräte werden kleiner, leistungsfähiger und unabhängiger – und zukünftig, ob wir das wollen oder nicht, auch direkt mit anderen Endgeräten (POS-Terminals, Ticket-Kontrollgeräten, medizinischen Geräten, Zugangssystemen, SmartMetern etc.) kommunizieren. Immer mehr digitale Spuren werden unser Verhalten detailliert protokollieren; zugleich werden zentrale Konfiguration und Kontrolle der Endgeräte schwieriger – eine Entwicklung, der das geltende Datenschutzrecht und heutige IT-Sicherheitskonzepte nur begrenzt gewachsen sind.

Wir werden diese Entwicklung weiterhin kritisch begleiten. Wenn Sie uns anlässlich des zehnten Geburtstags der SSN dazu ermutigen möchten, freuen wir uns über einen Kommentar von Ihnen.



Inhalt

Als gestern noch Zukunft war

Security News (2002-2012)

Neuer SHA-Standard

Security Tools: „Top 75”

SigG-Novelle

iTAN

WAF-Auswahlhilfe

Der König ist tot ...

Mifare-Cloning

SSL-Authentifikation für alle

iPhone Security

c = m

Secorvo News

Freie Plätze sichern

Security Awareness Symposium

Veranstaltungshinweise

secorvo
security consulting

Security News (2002-2012)

Neuer SHA-Standard

Am 28.08.2002 gab das US-amerikanische NIST einen neuen Secure Hash Standard (SHS) bekannt, der den SHS (FIPS PUB 180) aus dem Jahr 1993 ab 01.02.2003 ersetzt. FIPS PUB 180-2 umfasst neben SHA-1 drei weitere Algorithmen, die jeweils einen 256 (SHA-256), 384 (SHA-384) und 512 (SHA-512) bit langen Ausgabewert erzeugen. Die neuen Hashfunktionen ermöglichen ein höheres Sicherheitsniveau für digitale Signaturen: Ab einer Schlüssellänge von 1.500 bit (RSA) bzw. 168 bit (DSS) ist bislang der Hashwert das kryptografisch schwächste Glied.

SSN 09/2002 – Selbst zehn Jahre später wird der Standard noch nicht durchgängig unterstützt.

Security Tools: „Top 75"

Als Ergebnis einer Umfrage in der Newsgroup des Nmap Netzwerk-Scanners wurde eine Liste der 75 beliebtesten Sicherheits-Tools publiziert. Darin werden die Tools mit Bezugsquelle vorgestellt und bewertet. Diese Security Tools ermöglichen Administratoren, die Sicherheit ihrer Systeme und Netzwerke zu überprüfen – erleichtern allerdings auch die Durchführung von Angriffen.

SSN 03/2003 – Diese auf heute 125 Tools erweiterte Liste bietet immer noch einen guten Überblick.

SigG-Novelle

Am 19.11.2004 hat der Bundestag in zweiter und dritter Lesung das deutsche Signaturgesetz (SigG) novelliert. Zentrale Änderung: Für die Beantragung eines qualifizierten Signaturschlüssel-Zertifikats genügt nunmehr ein PIN-TAN-basierter Prozess – der eigenhändig unterschriebene Antrag mit Vorlage des Personalausweises ist bei bestehenden Kunden nicht mehr erforderlich. Damit kommt die Novelle den deutschen Banken entgegen, die eine Vereinfachung der Prozesse gefordert hatten, um ihre Bankkarten zu Signaturkarten aufwerten zu können. Die Bundesregierung erhofft sich mit diesem Schritt eine erhebliche Ausweitung der nach wie vor nur marginalen Verbreitung qualifizierter Signaturen; freilich fehlen trotz dieser Verfahrensvereinfachung noch immer die seit vielen Jahren versprochenen Anwendungen für „Otto Normalsignierer", die für ihn einen erkennbaren Zusatznutzen darstellen und einen Technikwechsel rechtfertigen.

SSN 11/2004 – Auch 2012 sind SigG-Signaturen per Bankkarte und Anwendungen dafür Mangelware.

iTAN

Auf Phishing-Angriffe reagieren jetzt auch die deutschen Banken mit zusätzlichen Sicherheitsmerkmalen. Die Postbank meldete am 07.08.2005, dass sie ihr PIN-TAN-Verfahren um ein iTAN genanntes Merkmal ergänzt: Zukünftig sind die TAN auf der Liste indexiert. Bei jeder Transaktion schickt der Bankserver den Index, und nur die passende TAN ist gültig. Dieser einfache Challenge-Response-Mechanismus entwertet abge-"phishte" TAN. Die iTAN schützt nicht vor allen Angriffen, erhöht aber die Sicherheit des Online-Bankings deutlich.

SSN 08/2005 – Der Anfang vom Ende des PIN-TAN-Verfahrens. Die Jagd hat begonnen.

WAF-Auswahlhilfe

Das Web Application Security Consortium (WASC) hat die Version 1.0 der „Web Application Firewall Evaluation Criteria" vorgelegt. Dabei handelt es sich um eines der ersten Dokumente, in welchem Entscheidern und Firewall-Architekten ein ausführlicher Katalog wichtiger Anforderungen an eine Web Application Firewall (WAF) zur Verfügung gestellt wird. Diese Anforderungsliste erleichtert den Vergleich, die Bewertung und die Auswahl geeigneter WAF-Lösungsansätze und verfügbarer Produkte

SSN 01/2006 – Noch immer sind WAFs kein Standard-Schutzmechanismus von Web-Applikationen.

Der König ist tot ...

... es lebe der König: Am 01.07.2007 wurde der ISMS-Standard ISO/IEC 17799:2005 vom Technical Committee JTC 1/SC 27 in ISO/IEC 27002:2005 „Information technology – Security techniques – Code of practice for information security management" umbenannt. Inhaltlich blieb er unverändert. Mit der Umbenennung hat die ISO einen wichtigen Beitrag zur Bereinigung der babylonischen Namensverwirrung im Bereich der sicherheitsrelevanten Standards geleistet – nach ISO/IEC 27001:2005 und ISO/IEC 27006:2007 existiert jetzt der dritte Standard im Nummernkreis 270xx. Die Nummerierung verdeutlicht die „Verwandtschaft" zu ISO 9001 (Qualitäts-) und ISO 14001 (Umweltmanagement).

SSN 08/2007 – Mittlerweile ist die ISO-Reihe 270xx sechsteilig und nicht mehr weg zu denken.

Mifare-Cloning

Auf dem Jahreskongress des Chaos Computer Clubs stellten Karsten Nohl und Henryk Plötz am 28.12.2007 einen Angriff auf das Authentifikationsverfahren kontaktloser Mifare-Chipkarten vor. Dem vom Hersteller geheimgehaltenen, etwa 15 Jahre alten „CRYPTO1"-Algorithmus waren sie mit einer

Mikroskop-Analyse des Chip auf die Spur gekommen, um dann nach kryptographischen Schwächen (zu kleiner Zufallswert, lineares Schieberegister) darin zu suchen. Zu dieser Krypto-Schwachstelle gibt es nun den passenden „Mifare-Cloner“: Am 12.03. 2008 haben Forscher der Radboud Universiteit Nijmegen ein Video in YouTube veröffentlicht, auf dem sie zeigen, wie sie mit minimalem Aufwand Mifare-basierte Zugangskarten duplizieren. Von der Attacke betroffen sind Tausende von Anwendungen mit einer Milliarde ausgegebenen Karten, vom Betriebsausweis über die Kantinenkarte bis zum bargeldlosen Bezahlsystem im öffentlichen Nahverkehr, sofern sie Mifare-Chips des Typs MF1 IC S50 oder S70 verwenden. Fein raus ist, wer seine Anwendung bereits auf den neueren Mifare DESFire (MF3 IC D40) migriert hat – statt einer etwas ältlichen Stromchiffre verwendet er bei der Authentifikation wahlweise DES oder TripleDES.

SSN 03/2008 – Eingesetzt werden sie noch immer. Ende 2009 hat es auch Mitbewerber Legic erwischt.

SSL-Authentifikation für alle

SSL – seit zehn Jahren unter dem Namen Transport Layer Security (TLS) genormt – ist ein bekanntes, bewährtes und deshalb von seinem ursprünglichen Zweck, der Absicherung von Webzugriffen, auch auf andere Bereiche wie z. B. VPN oder WLAN übertragenes Sicherheitsprotokoll. Sollte man meinen. Auch sollte sich im Jahr 20 nach der Erstveröffentlichung des X.509 Standards herumgesprochen haben, dass Zertifikate naturgemäß öffentliche Daten sind und für sicherheitsrelevante Operationen das private Gegenstück des per Zertifikat bestätigten öffentlichen Schlüssels benötigt wird.

Umso größer die Verwunderung, als Microsoft am 10.03.2009 im Security Bulletin MS09-007 einräumte, dass die SSL-Komponente in Windows – vom Veteranen Windows 2000 bis zum neuesten 64-Bit-System – bei der Client-Authentifikation jahrelang patzte: Zwar wurde die Gültigkeit des vorgelegten Zertifikats geprüft; der im Standard vorgeschriebene Schritt, per Signatur der ausgetauschten Protokollnachrichten zu verifizieren, dass der Client auch den passenden privaten Schlüssel verwendet, wurde jedoch eingespart. Tatsächlich akzeptierte der Server also jeden Client mit irgend einem gültigen Zertifikat - ob nun dem eigenen oder einem fremden.

Durch das weite Einsatzspektrum von SSL/TLS sind wahrscheinlich nicht nur IIS-basierte Webanwendungen von diesem Bug betroffen, sondern jede zertifikatsbasierte VPN-, WLAN- und NAC-Anmeldung, sofern dabei der Microsoft-eigene RADIUS-Dienst IAS zum Einsatz kommt. Vielleicht haben sich die Microsoft-Entwickler bei der Implementierung auf das SSL-Diagramm in Wikipedia verlassen – das den wichtigen Verifikationsschritt ebenfalls fehlerhaft darstellt. Manchmal geht Studieren doch über Probieren.

SSN 03/2009 – Blindes Vertrauen in die Implementierung von Sicherheitsprotokollen ist gefährlich.

iPhone Security

In nicht wenigen Unternehmen hält derzeit Apples iPhone Einzug. Trotz seiner nach wie vor deutlichen Nachteile bei Business-Anwendungen gegenüber RIMs BlackBerry wiegen „Sex-Appeal“ und Nimbus des Geräts auch bei Führungskräften oft schwerer. Wie sicher aber sind Unternehmensdaten auf einem iPhone? Was ist von der Hardware-Verschlüsselung und anderen Schutzmechanismen zu halten? Lassen sich iPhones ohne Inkaufnahme zusätzlicher Risiken in die IT-Infrastruktur integrieren? Diesen Fragen ist Jörg Völker auf den Grund gegangen – und hat die Ergebnisse seiner Untersuchungen nun in der Fachzeitschrift „Datenschutz und Datensicherheit“ (DuD) veröffentlicht.

SSN 06/2010 – Die ungebrochene Popularität von Smartphones hält das Thema im Brennpunkt.

c = m

Kryptografie kann so einfach sein. Das dachen wohl auch die Programmierer der Entwicklerversion von Ruby bei der Implementierung des RSA-Verfahrens: Wenn $c = m^e \bmod n$ zu berechnen ist – dann geht das mit $e := 1$ am schnellsten. Damit folgt: $c = m \bmod n$, $m < n \Rightarrow c = m$. Falls Sie mit dieser Ruby-Version zwischen dem 01.09. und dem 04.11.2011 RSA-Schlüssel erzeugt haben, sollten Sie diese schnellstmöglich ersetzen.

SSN 11/2011 – Hoffentlich haben Rivest, Shamir und Adleman das nicht lesen müssen...

Secorvo News

Freie Plätze sichern

Die Schulung zum T.I.S.P.-Zertifikat mit den Autoren des T.I.S.P.-Buchs am **17.–21.09.2012** ist fast ausgebucht. Das nächste T.I.S.P.-Seminar (und letzte in 2012) findet vom **12.–16.11.2012** statt – frühzeitige Anmeldung wird empfohlen.

Security Awareness Symposium

Am **11.–12.09.2012** sind wir mit dem 8. Security Awareness Symposium wieder zu Gast in der Buhlschen Mühle in Ettlingen. Das Programm ist noch in Abstimmung – wer das Event auf keinen Fall verpassen möchte, kann sich aber bereits heute online anmelden. Wir freuen uns auf Ihr Kommen!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2012	
06.-08.08.	DFRWS 2012 (DFRWS, Washington/US)
08.-10.08.	21th USENIX Security Symposium (Usenix, Bellevue/US)
19.-23.08.	Crypto 2012 (IACR, Santa Barbara/US)
20.-24.08.	SecSE 2012 (SINTEF, Prag/CZ)
27.08.	Sommerakademie 2012 (ULD Schleswig-Holstein, Kiel)
September 2012	
11.-12.09.	8. Security Awareness Symposium (Secorvo, KA-Ettlingen)
17.-21.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
18.09.	Anwendertag IT-Forensik 2012 (Fraunhofer SIT, Darmstadt)
24.-27.09.	CPSSE-Schulung (Secorvo College, Karlsruhe)
25.-26.09.	D·A·CH Security (GI/OCG/BITKOM/SI/TeleTrusT, Konstanz)
Oktober 2012	
09.-11.10.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
12.10.	1. Freiburger Datenschutztag (vivaSoft/Datenschutz individuell, Freiburg)
23.-26.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2012



Sprachmartialisierung

Erst verwirren sich die Worte.
Dann verwirren sich die Begriffe.
Und schließlich verwirren sich die Sachen.

Konfuzius (551-479 v.Chr.)

Schon immer ist der Fachjargon der IT-Sicherheit mit sprachlichen Anleihen aus dem Militärischen gespickt. Ein Einbruchsversuch in ein IT-System ist ein „Angriff", extern erreichbare Rechner isolieren wir in „demilitarisierten Zonen" (DMZ) und mögliche Bedrohungen beschreiben wir als „Angriffsvektoren". Das mag historische Gründe haben – inzwischen haben wir uns daran gewöhnt. Hilfreich war das allerdings nie. So ist es schwierig, Laien für Schutzmaßnahmen zu gewinnen, wenn man von drohenden „Angriffen" schwadroniert – das klingt maßlos überzogen. Überzeugender ist der Hinweis auf mögliche „Eindringlinge", die „Daten entwenden" – digitale Einbruchsszenarien liegen eher im Bereich des Vorstellbaren.

Sprache ist aber, wie wir nicht erst seit Orwells „Neusprech" wissen, nicht nur Ausdruck unserer Weltsicht. Sie beeinflusst auch unsere Wahrnehmung, mittelfristig unser Denken und langfristig unser Verhalten. Wie wirksam ein konsequentes Sprachuniversum sogar offensichtliche Unmenschlichkeit rechtfertigen kann, ließ sich in Deutschland wiederholt (zuletzt bei der RAF) beobachten.

Inzwischen hat die militärische Diktion auch die Politik erreicht. Ob sich Politiker die martialischen Bezeichnungen wegen ihrer Medienwirksamkeit zu Eigen gemacht haben oder das mediale Dauerfeuer die Ursache ist: Seit 2011 haben wir ein „Nationales Cyber-Abwehrzentrum". Wenn ein Staat eine solche Institution benötigt, rechnet er offenbar mit drohenden Cyber-Schlachten – auf gut Deutsch: dem Cyberkrieg, einem „organisierten und unter Einsatz erheblicher Mittel mit Waffen und Gewalt ausgetragenen Konflikt, dessen Handlungen auf die Verletzung und Tötung des Gegners zielen". Bei allem Respekt vor den Möglichkeiten digitaler Spionage und Sabotage – ist es wirklich „Krieg", was wir realistischer Weise befürchten müssen? Und wann fühlt sich da jemand zum „Erstschlag" genötigt?



Inhalt

Sprachmartialisierung

Security News

Web-App-Krümel

Ende der Übergangsregelung

Wer die Vergangenheit kontrolliert...

Datenschutz in der Cloud

Awareness wirkt

Secorvo News

Vertieftes Know-How

Teamverstärkung

Trutzburg für jeden

Veranstaltungshinweise

secorvo
security consulting

Security News

Web-App-Krümel

Nur 3 % der Entwickler seien an Sicherheit von Software interessiert – zu diesem Schluss kommt SANS-Autor Frank Kim in seinem Blog-Eintrag vom 23.07.2012 nach Zählung der Security-Vorträge auf Entwicklerkonferenzen. Dem widersprechen die Ergebnisse der (inzwischen zwölften) WhiteHat-Studie zu sicherheitsrelevanten Schwachstellen in Webanwendungen vom 17.07.2012: Danach hat die Zahl schwerer Schwachstellen pro Anwendung in den vergangenen Jahren signifikant abgenommen. Allerdings werden im Schnitt noch immer zu viele Schwachstellen gefunden.

Zahlreiche neue Tools unterstützen die Entwicklung sicherer Software. Zur Integration von Sicherheit in die agile Software-Entwicklung hat SAFECode am 16.07.2012 das lesenswerte White-Paper „Practical Security Stories and Security Tasks for Agile Development Environments" veröffentlicht. Bezüglich der Überprüfung der Sicherheit von Software bietet die aktuelle Übersicht über 62 freie und kommerzielle Webanwendungsscanner aus dem Juli 2012 mit Benchmarks nach verschiedenen Kriterien eine Entscheidungshilfe. Für das virtuelle Patchen ist in vielen Apache-Webservern heute mod_security im Einsatz. Seit dem 26.07.2012 ist mod_security auch für die Webserver IIS und ngnix verfügbar.

Eingebettet in ein Gesamtkonzept eines erweiterten Software Development Life Cycle aus Entwicklerschulung und -sensibilisierung, Sicherheitsaudits, Monitoring und Blocking tragen solche Tools auch zu einer Reduktion von Sicherheits-Schwachstellen bei. Security-Vorträge auf Entwicklerkonferenzen könnten dann irgendwann obsolet werden.

Ende der Übergangsregelung

Am 31.08.2012 läuft die letzte Übergangsfrist der BDSG-Novelle von 2009 ab. Verschiedene Newsletter und Seiten aus dem Datenschutz- und E-Commerce-Spektrum fordern daher zum Durchforsten der zur Werbung genutzten Adressdatenbanken auf; viele Anbieter bitten ihre Mailing-Empfänger bereits um neue Einwilligungen.

Tatsächlich führt der Fristablauf nicht zu größeren Änderungen. Von § 47 Nr. 2 BDSG sind nur vor dem 01.09.2009 zum Zweck der Werbung (§ 28 Abs. 3-5 BDSG) erhobene Daten betroffen. Die Voraussetzungen für die Zulässigkeit der Versendung von E-Mail-Newslettern sind im Wesentlichen durch § 7 Abs. 2 und 3 UWG und die elektronische Einwilligung durch §§ 6 Abs. 2 und 13 Abs. 2 TMG geregelt.

Die Versendung von E-Mail-Werbung an Bestandskunden steht – vorbehaltlich eines Kundenwiderspruchs – auch zukünftig nicht unter einem Einwilligungsvorbehalt und darf auch weiterhin über einen „Opt-Out"-Mechanismus realisiert werden.

Die BDSG-Novelle von 2009 hat lediglich eine Angleichung an diese schon seit 2001 bzw. 2004 geltenden Vorschriften vorgenommen. Die vor 2009 bestehenden Erlaubnistatbestände sind zwar teils eingeschränkt, teils erweitert (und in der Verständlichkeit reduziert) worden; sie gelten jedoch im Wesentlichen fort. Eine neue Einwilligung ist nur erforderlich, wenn keiner der Erlaubnistatbestände ohne Betroffenenbeteiligung greift und keine dokumentierte Einwilligung vorliegt.

Wer bislang Datenschutzvorgaben eingehalten hat, muss nicht befürchten, dass er mit Ablauf der Übergangsfrist seine Kunden nicht mehr anschreiben darf.

Wer die Vergangenheit kontrolliert...

...kontrolliert die Zukunft, sagt die Ingsoc-Partei in George Orwells 1984. Für elektronische Geldgeschäfte gilt sinngemäß: Wer die Benutzerschnittstelle kontrolliert, kontrolliert den Benutzer. Beim Online-Banking manifestiert sich das Problem unter dem Schlagwort Man-in-the-Browser. Dass ca. 60% der Varianten des Zeus-Trojaners selbst von aktueller Antivirus-Software nicht erkannt werden, veranlasste die ENISA in einer Pressemeldung vom 05.07.2012 zur Warnung an die Banken, doch besser davon auszugehen, dass alle Kunden-PCs infiziert sind, so dass deren Browser-Anzeige und -Transaktionen von Angreifern beeinflusst werden können. Die ENISA empfiehlt daher, zur Prüfung durch den Benutzer Transaktionsdaten auf einem zweiten, vertrauenswürdigen Gerät anzuzeigen. Online-Banking mit TAN-Listen sollte man tunlichst nur noch auf frisch gebooteten, sauberen Systemen nutzen, wie z. B. Bankix.

Auch am Point-of-Sale muss man inzwischen mit solchen Angriffen rechnen – und dort helfen weder TAN-Generator noch Bankix: Am 12.07.2012 demonstrierten Forscher von SRLabs in einem ARD-Beitrag, wie sich die Firmware von weit verbreiteten POS-Terminals manipulieren lässt. Mehrere von SRLabs entdeckte Schwachstellen erlauben, über Netzwerk oder lokale Schnittstellen einen „Man-in-the-POS" einzuschleusen. Keine der Schwachstellen erlaubt es, das zertifizierte Sicherheitsmodul des Geräts zu manipulieren – aber das ist auch gar nicht nötig, da das Modul nur die Protokollschritte des Zahlungsverfahrens kontrolliert und nicht das Display und PIN-Pad. So können Angreifer direkt an der Quelle phishen – denn wer die Benutzerschnittstelle kontrolliert...

Datenschutz in der Cloud

Die Art. 29 Datenschutzgruppe hat am 01.07.2012 eine Stellungnahme zum Datenschutz bei Cloud Computing veröffentlicht. Neben einer Zusammenfassung der typischen Datenschutzrisiken und Empfehlungen zur Herstellung von Datenschutzkonformität hebt sie die Durchführung einer umfassenden Risikoanalyse durch den Cloud-Nutzer hervor. Bezüglich der meist komplexen Unterauftragnehmerstrukturen wird in Anlehnung an die Europäischen Standardvertragsklauseln empfohlen, eine Haftung des Cloud-Anbieters für Unterauftragnehmer, das Einholen des Einverständnisses des Auftraggebers zu Unterauftragnehmern und die obligatorische Weitergabe der Vertragspflichten an diese vertraglich zu verankern.

Darüber hinaus listet die Stellungnahme zu berücksichtigende Vertragsinhalte bei der Cloud-Beauftragung auf, die über die Liste in § 11 Abs. 2 BDSG zur Auftragsdatenverarbeitung hinausgehen, darunter bspw. eine Standortliste der Verarbeitungsorte. Ebenso findet sich eine Liste der Kategorien von zu verlangenden technisch-organisatorischen Maßnahmen. Es wird mehrfach hervorgehoben, dass ein starkes Verhandlungsungleichgewicht zwischen Nutzer und Anwender keine Rechtfertigung für den Verzicht auf Datenschutzanforderungen darstellt.

Interessant ist die Einschätzung der Safe Harbor Relevanz: Daneben wird in jedem Fall eine vertragliche Vereinbarung gefordert, die Datenschutzanforderungen konkretisiert. Außerdem sollen vom Dienstleister zusätzlich zur Selbstzertifizierung Nachweise über die Erfüllung der Datenschutzanforderungen erbracht werden. Damit enthält die Stellungnahme wichtige Hinweise und Mindestanforderungen an die Vertragsgestaltung.

Awareness wirkt

Im Juli berichtete The Register, dass bei der niederländischen Chemiefirma DSM die Aufmerksamkeit einiger Angestellten verhinderte, dass Schadsoftware in das Intranet des Unternehmens eingeschleust wurde. Die Mitarbeiter übergaben der IT-Abteilung auf dem Firmenparkplatz entdeckte USB-Sticks – auf denen sich, wie eine Analyse ergab, Malware befand, die zu einer Infektion geführt hätte.

Fokussierte Angriffe dieser Art sind inzwischen keine Seltenheit mehr. Nur Unternehmen, die es nicht dem Zufall überlassen, wie kompetent Mitarbeiter auf Gefährdungen und Eindringversuche reagieren, haben gegen solche Attacken eine realistische Chance.

Am **11.–12.09.2012** treffen sich Verantwortliche aus zahlreichen Unternehmen in der Buhlschen Mühle in Ettlingen auf dem von Secorvo organisierten "8. Security Awareness Symposium", um über erfolgreiche Sensibilisierungsmaßnahmen und ihre Erfahrungen aus eigenen Awareness-Kampagnen zu diskutieren.

Secorvo News

Vertieftes Know-How

Festigen Sie vorhandenes Wissen, schließen Sie Lücken, ergänzen Sie Ihre Erfahrungen und Kenntnisse um aktuelle Erkenntnisse der Informationssicherheit mit einer Schulung zum T.I.S.P. Lassen Sie sich von den Autoren des T.I.S.P.-Buchs vom **17.–21.09.** oder **12.–16.11.2012** auf die anschließende Zertifikatsprüfung vorbereiten.

Wie sich Sicherheit von Beginn an in den Softwareentwicklungsprozess integrieren lässt, erfahren Sie in der Zertifikatsschulung "Certified Professional for Secure Software Engineering (CPSSE)" am **24.–27.09.2012** in Karlsruhe.

Alles, was Sie für die Konzeption und den Betrieb einer Unternehmens-PKI wissen müssen, vermitteln wir Ihnen auf unserer PKI-Schulung am **23.–26.10.2012.**

Alle Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Teamverstärkung

Seit dem 01.08.2012 verstärkt Sven Köhler das Secorvo-Consulting-Team. Die Schwerpunkte des erfahrenen Sicherheitsspezialisten liegen im Risiko- und Notfallmanagement, bei Sicherheitsaudits sowie der Zertifizierung nach IT-Grundschutz und dem IDW Prüfungsstandard 980 für die Prüfung von Compliance Management Systemen.

Trutzburg für jeden

Mit steigendem Leistungsbedarf nehmen die Herausforderungen zu, die bei der Planung und Gestaltung eines sicheren Serverraums oder Rechenzentrums auch von kleinen und mittleren Unternehmen zu bewältigen sind.

Markus Schäfer (proRZ Rechenzentrumsbau GmbH) gibt mit seinem Vortrag auf dem kommenden KA-IT-Si Event am **13.09.2012** einen Überblick über die Anforderungen an eine moderne zentrale IT und stellt Best-Practice-Maßnahmen zu deren sicherer Realisierung vor. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2012	
11.-12.09.	8. Security Awareness Symposium (Secorvo, KA-Ettlingen)
13.09.	Trutzburg für jeden (KA-IT-Si, Kalrsuruhe)
17.-21.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
18.09.	Anwendertag IT-Forensik 2012 (Fraunhofer SIT, Darmstadt)
24.-27.09.	CPSSE-Schulung (Secorvo College, Karlsruhe)
25.-26.09.	D·A·CH Security (GI/OCG/BITKOM/SI/TeleTrusT, Konstanz)
Oktober 2012	
09.-11.10.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
12.10.	1. Freiburger Datenschutztag (vivaSoft/Datenschutz individuell, Freiburg)
15.-17.10.	IDACON 2012, (WEKA-Akademie, Würzburg)
16.-18.10.	it-sa 2012, (SecuMedia Verlag, Nürnberg)
22.-26.10.	OWASP AppSec USA 2012, (OWASP Foundation, Austin/US)
23.-24.10.	ISSE 2012, (TeleTrusT/eema, Brüssel)
23.-26.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2012



Das „Einweg-Paradigma“

Wer mit aufmerksamem Blick bewährte Schutzmaßnahmen in Bereichen außerhalb der Informationstechnik verfolgt, kann ein Phänomen beobachten, dass ich das „Einweg-Paradigma“ nennen will.

Ein Sanitäter oder Arzt, der sich und seine Patienten vor Infektionen schützen will, verwendet Einweg-Handschuhe, eine Einweg-Spritze, Einweg-Spatel und desinfizierte Einweg-OP-Kittel. Spurensicherer verhindern mit Einweg-Überschuhen und Einweg-Overalls die Kontamination eines Tatorts. Mit Einweg-Taschentüchern versuchen wir bei einem Schnupfen die Ansteckungsgefahr zu bannen. Den Fahrradhelm tauschen wir nach einer heftigen Kollision, und im Fahrzeug schützt der Einweg-Airbag die Insassen. Einweg-Alkoholtester bewahren die Testperson vor Infektion und den Tester vor Manipulation. Einweg-Gläser und –Trinkbecher aus Kunststoff oder Karton verhindern Schnittverletzungen, Einweg-Kontaktlinsen Unfälle. Kleine Kinder wickeln wir in Einweg-Windeln. Einweg-Verpackungen sorgen für hygienisch einwandfreie Lebensmittel, und Einweg-Umschläge schützen unsere Briefe während des Transports vor unbefugter Kenntnisnahme und Beschädigung.

Zwar belastet der Erfolg dieses Einweg-Paradigmas unsere Umwelt. Dennoch ist der Sicherheitsgewinn meist erheblich. In der modernen Informationstechnik hingegen – dort, wo Einweg-Lösungen nicht einmal die Umwelt belasten würden – beschränken wir uns geradezu antiquarisch auf's Reparieren: Die Bugs im Betriebssystem werden *gefixt*, der Browser beim Auftauchen von Zero-Day-Exploits *gepatcht*, die Web-Applikation mit Schwachstelle bekommt ein *Update*. Man stelle sich einmal vor, die Löcher in OP-Handschuhen würden in ähnlicher Weise über Jahre mit Flicken gedichtet.

Ach, wie schön wäre doch ein Einweg-Betriebssystem mit Einweg-Browser: morgens gestartet und abends gelöscht – keine Chance für Exploits, und der Patch-Marathon hätte endlich ein Ende.



Inhalt

Das „Einweg-Paradigma“

Security News

Nicht ganz zufällig

Kontrollierter Benutzer

Elektronische Rechnungen

VoIP- und UC-Bedrohungen

Mitarbeiterscreening

Speicherforensik

Secorvo News

Heute schon gefacebookt?

Wissen auffrischen

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Nicht ganz zufällig

Forscher der Uni Cambridge veröffentlichten am 10.09.2012 eine Analyse, der zufolge Kriminelle an einem manipulierten POS-Terminal (vgl. SSN 08/2012) von einer eingelegten EMV-Bankkarte Transaktionsdaten abzapfen könnten, die sich später am Geldautomaten einspielen und in Bares umwandeln lassen. Die technische Ursache des Problems ist, dass manche Geldautomaten einen mehr oder minder vorhersagbaren (und damit unbrauchbaren) „Zufallswert" als Schutz gegen Replay-Angriffe verwenden. Bei der Lektüre des Papiers weiß man nicht, worüber man mehr den Kopf schütteln soll: Darüber, dass die Entwickler als „Unpredictable Number" (UN) einen fortlaufenden Zähler verwendeten, dass bei Abnahmetests nur geprüft wird, ob vier nacheinander erzeugte UN sich unterscheiden, oder dass man als Reverse-Engineer echte Geldautomaten günstig bei eBay erstehen kann.

Vielleicht ist es keine so gute Idee, wichtige Teile des Schutzes des Bankkunden in die Hand der Hersteller von POS-Terminals und Geldautomaten zu legen.

Kontrollierter Benutzer

Ein prägnantes Beispiel, wozu die in SSN 08/2012 thematisierte Kontrolle der Benutzerschnittstelle durch einen Angreifer missbraucht werden kann, wurde am 04.09.2012 aufgedeckt. Dabei klinkt sich ein Man-in-the-Browser-Trojaner in eine Online-Banking-Sitzung ein und verweist auf „technische Probleme", derentwegen zunächst eine „Testüberweisung" durchgeführt, mit dem ChipTAN-Generator geprüft (sic!) und freigegeben werden müsse. Die Transaktion ist allerdings echt. Noch perfider ist der Trojaner, vor dem das BKA bereits am 15.07.2011 warnte (vgl. SSN 07/2011) – er täuscht eine irrtümliche Gutschrift auf dem Konto des Opfers vor, die nun „zurücküberwiesen" werden müsse. Schließlich gibt es da noch den im Juli 2012 aufgetauchten Telefonbanking-Trojaner, der zum „Datenvergleich" Angaben zum Kontoinhaber abfragt – zuletzt auch die Telefonbanking-PIN.

„Technische Probleme" sind ein bei Trojanern beliebter Vorwand für seltsame Anweisungen. Ihnen sollten daher mit größter Skepsis begegnet werden.

Elektronische Rechnungen

Am 02.07.2012 hat das Bundesministerium für Finanzen in einem Schreiben an die obersten Finanzbehörden der Länder die Auswirkungen des nach längerer Verhandlung mit dem Bundesrat am 01.11.2011 verabschiedeten Steuervereinfachungsgesetzes 2011 (vgl. SSN 06/2011) auf elektronische Rechnungen präzisiert. Danach ist eine qualifizierte elektronische Signatur nicht mehr Voraussetzung für die umsatzsteuerrechtliche Anerkennung. Statt dessen muss lediglich ein „innerbetriebliches Kontrollverfahren" die korrekte Übermittlung der Rechnung sicherstellen. Stimmen die Angaben zu Leistung, Leistendem, Entgelt und Zahlungsempfänger dürfe davon ausgegangen werden, dass die Übermittlung fehlerfrei erfolgt ist. Dafür genügt zukünftig ein manueller Abgleich der Rechnung bspw. mit den zugehörigen Auftrags- oder Vertragsunterlagen. Die Zustimmung des Empfängers zum elektronischen Rechnungsversand kann nun auch durch Annahme der AGB oder konkludentes Handeln erfolgen.

Damit sind qualifizierte elektronische Signaturen wieder um eine „Killerapplikation" ärmer.

VoIP- und UC-Bedrohungen

Gebührenbetrug bleibt eine der zentralen Bedrohungen gegen IP-basierte Telefonie (VoIP) und Unified Communications (UC). Dies geht aus dem im August veröffentlichten Bericht der SecureLogix Corporation vom 12.06.2012 hervor. Dort wurden für verschiedene Szenarien die jeweils relevanten Bedrohungen auf Grundlage der berichteten Vorfälle der vergangenen sechs bis 12 Monate identifiziert. Danach sind Einzelschäden von 100.000 US$ und mehr nicht ungewöhnlich. Sie entstehen entweder durch massive Anwahl von Premium- und Mehrwertdiensten oder durch eingedrungene Angreifer, die Telefoniekapazitäten „vermieten". Bei letzteren sind zudem weitere illegale Aktivitäten wie Voice SPAM oder Social Engineering möglich. Auch moderne Smartphones – eher Kleinformatcomputer mit Telefonie-App und nicht ausgereiften Sicherheitskonzepten – sind inzwischen Quellen für Gebührenbetrug, wie der Lookout Mobile Security Report 2012 vom 05.09.2012 bestätigt.

Unternehmen, die VoIP- oder UC-Anlagen einführen, dürfen derzeit nicht davon ausgehen, dass sie bereits gehärtete Systeme erhalten – im Auslieferungszustand sind diese meist auf maximale Funktionalität, nicht aber auf Sicherheit konfiguriert. Und das kann teuer werden, wie die angeführten Studien eindrucksvoll belegen.

Mitarbeiterscreening

Der Bundesfinanzhof hat mit Urteil vom 19.06.2012 die Zulässigkeit von Mitarbeiterscreenings zur Erlangung eines AEO-Zertifikats „Zollrechtliche Vereinfachungen/Sicherheit" bestätigt. Die Erteilung des Zertifikats, das Erleichterungen bei der Abwicklung grenzüberschreitenden Warenverkehrs ermöglicht, ist abhängig von einer Überprüfung des Personals

des Antragstellers gegen die Listen der VO Nr. 2580/2001 und VO Nr. 881/2002.

Dabei handelt es sich um Antiterrorlisten, die durch den Europäischen Rat nach den Vorgaben des Gemeinsamen Standpunkts 2001/931/GASP erstellt werden. Sie unterliegen zwar einer halbjährigen Überprüfung, der Rechtsschutz der Betroffenen ist jedoch schwach ausgeprägt. Finanzielle Zuwendungen an die gelisteten Personen sind verboten.

Der Bundesfinanzhof sieht den Abgleich durch den Arbeitgeber durch § 32 Abs. 1 Satz 1 BDSG erfasst. Verwendet würden ohnehin nur Stammdaten der Beschäftigten. Dem Arbeitgeber stünde das Einholen einer Einwilligung der Beschäftigten oder der Verzicht auf das Zertifikat frei. Daher handele es sich auch nicht um einen staatlichen Eingriff. Den Abgleich als Bedingung für die Zertifikatserteilung zu verlangen, sei verhältnismäßig.

Während die Entscheidung für die betroffenen Unternehmen ein gewisses Maß an Rechtssicherheit schafft, ist die Begründung äußerst fragwürdig. Das Verlangen des Abgleichs ist weder durch den Zollkodex (ZK) noch durch dessen Durchführungsverordnung gefordert. Die Verhältnismäßigkeit des Abgleichs mit den konkreten Terrorlisten wäre daher unter Abwägung von Transparenzpflichten und Rechtsschutzmöglichkeiten der Beschäftigten zu prüfen gewesen. Die Ausführungen zur Möglichkeit der Einwilligungseinholung sind aus Datenschutzsicht mangels Freiwilligkeit zudem rechtlich falsch. Letztlich liegt das Problem jedoch bei der Praxis der Verdächtigenlisten, die im Hinblick auf Datenschutz und Rechtsstaatlichkeit berechtigt in der Kritik stehen.

Speicherforensik

Am 18.09.2012 wurde Version 2.2 RC2 des Open-Source-Forensik-Tools Volatility freigegeben, das seit August die Betriebssysteme Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 sowie alle verfügbaren Service Packs und 64bit-Architekturen unterstützt. Insgesamt 67 Windows-Plug-Ins ermöglichen seitdem beispielsweise die Auswertung von Eventlogs im Hauptspeicher unter Windows XP und Server 2003 oder der Historie der CMD-Kommandozeile. Sogar Interaktionen in der GUI sind über die Erzeugung von Pseudo-Screenshots aus Fensterpositionsdaten rekonstruierbar.

Nun unterstützen 34 weitere Plug-Ins auch forensische Speicher-Analysen unter allen Linux-Derivaten (Debian, Ubuntu, OpenSuSE, Fedora, CentOS, Mandriva) ab Kernel 2.6.11 bis 3.5.

Volatility hat damit – wieder einmal – die Meßlatte für kommerzielle Lösungen in diesem Bereich deutlich höher gelegt und sollte heute bei keiner forensischen Incident Response mehr fehlen.

Secorvo News

Heute schon gefacebookt?

Ende 2011 waren nach einer Studie des Bitkom 74 % der deutschen Internet-Nutzer in einem „Sozialen Netzwerk“ registriert. Inzwischen dürften es einige mehr sein. Und in vielen Unternehmen drängen Marketing- und Personalabteilung auf eine Unternehmenspräsenz bei Facebook & Co. Meist ist ein erheblicher Teil der Mitarbeiter bereits „drin".

In den zu einem erheblichen Teil (Google+, facebook) von amerikanischen Anbietern betriebenen Social Networks lauern jedoch zahlreiche Fallen: Copyrightverletzungen, unkontrollierte Informationspreisgabe und Verstöße gegen Datenschutzbestimmungen gehören dazu.

Beim nächsten KA-IT-Si-Event "Heute schon gefacebookt?" am **08.11.2012** gibt der Jurist Michael Knopp einen Überblick über die wichtigsten Stolpersteine – und praktische Tipps, wie sie sich vermeiden lassen. Für ein besonderes Ambiente ist gesorgt: Erstmals ist die KA-IT-Si mit ihrer Veranstaltungsreihe in den stilvollen Räumlichkeiten der Buhlschen Mühle in Ettlingen zu Gast. Das Tagungszentrum liegt ca. 10-15 Minuten Fahrzeit vom Karlsruher Hauptbahnhof entfernt. Beginn der Veranstaltung ist um 18 Uhr. Um Anmeldung wird gebeten. Wir freuen uns auf spannende Diskussionen und interessantes Networking!

Wissen auffrischen

Unsere Seminare vermitteln nicht nur Grundlagen der IT-Sicherheit für Einsteiger in dem Gebiet (wie IT-Sicherheit heute, **20.–22.11.**), sondern stellen auch die "aktuellen Herausforderungen der Informationssicherheit" vor (**07.–08.11.**).

Experten mit mindestens drei Jahren Berufserfahrung in der Informations- bzw. IT-Sicherheit können ihre Kenntnisse mit dem T.I.S.P.-Zertifikat krönen (**12.–16.11.**). Das von Secorvo verfasste 500seitige T.I.S.P.-Buch Zentrale Bausteine der IT-Sicherheit (siehe die Leser-Rezensionen) ist im Preis eingeschlossen und wird allen Teilnehmern frühzeitig vor Seminarbeginn zugesandt.

Alle weiteren Seminarangebote, das druckfrische Jahresprogramm 2013 und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2012	
12.10.	1. Freiburger Datenschutztag (vivaSoft/Datenschutz individuell, Freiburg)
15.-17.10.	IDACON 2012, (WEKA-Akademie, Würzburg)
16.-18.10.	it-sa 2012 (SecuMedia Verlag, Nürnberg)
22.-26.10.	OWASP AppSec USA 2012 (OWASP Foundation, Austin/US)
23.-24.10.	ISSE 2012 (TeleTrusT/eema, Brüssel)
31.10.-03.11.	hashdays security & risk conference 2012 (DEFCON Switzerland, Luzern/CH)
November 2012	
07.11.	German OWASP Day 2012 (OWASP Germany, München)
08.11.	Heute schon gefacebookt? (KA-IT-Si, Ettlingen)
07.-08.11.	Aktuelle Herausforderungen der Informations-sicherheit (Secorvo College, Karlsruhe)
12.-17.11.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
22.-23.11.	36. DAFTA (GDD, Köln)

Fundsache

Als Pendant zu diversen Top Ten der Smartphone-Risiken veröffentlichte die enisa am 25.11.2011 einen Leitfaden, der die zehn wichtigsten Sicherheitsmaßnahmen detailliert, an die App-Entwickler denken sollten – leider noch ohne Plattform spezifische Hinweise zu iOS, Android & Co.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2012



Grenzen der Kooperation

Im Februar 2004 wurde Facebook als Studentennetzwerk gegründet. Vier Jahre danach war Facebook bereits international, auch auf deutsch, verfügbar, und die Gründung von Facebook Ireland Ltd. wurde angekündigt. Weitere vier Jahre später ist Facebook die unumstrittene Nummer Eins der sozialen Netzwerke mit geschätzt einer Milliarde Mitglieder. Eine rasante Entwicklung.

Seit 2010 rücken jedoch vermehrt Datenschutzprobleme in den Fokus. Die Hamburgische und die Schleswig-Holsteinische Datenschutzaufsicht sind gegen Facebook bzw. Fanpage-Betreiber vorgegangen. Eine österreichische Studentengruppe hat eine Reihe von Beschwerdeverfahren bei der irischen Datenschutzaufsichtsbehörde DPC angestoßen. Sogar die US-amerikanische Federal Trade Commission (FTC), zuständig für das Safe Harbor-Abkommen, ist eingeschritten und hat jährliche Audits vereinbart. Hinzu kommen diverse Datenschutzpannen.

Dabei überwiegt ein kooperativer Ansatz, um dem neuen Phänomen „Soziale Netzwerke" Rechnung zu tragen. Ein solcher gestalterischer Ansatz hat den Vorteil, unter Nutzung gesetzlicher Auslegungsspielräume passende Regeln zu entwickeln, die das Geschäftsmodell nicht zerstören, aber Gemeinwohlinteressen durchsetzen.

Kooperation darf aber nicht zur Anbiederung werden, bei der staatliche Autoritäten sich lächerlich machen und ihre Autorität verlieren. Das Gutachten der DPC zu Facebook vollbringt dies jedoch schon im Vorwort: Facebook habe zur vollsten Zufriedenheit kooperiert, dabei Empfehlungen und Best Practices akzeptiert. Ein genauerer Blick zeigt, dass facebook vielen Empfehlungen gar nicht oder nur ungenügend nachgekommen ist. Hinweise auf die vorliegenden Rechtsverstöße fehlen völlig, Sanktionsandrohungen finden sich nicht.

Um Grenzen zu setzen, muss auch Kooperation Grenzen haben.



Inhalt

Grenzen der Kooperation

Security News

Unselbständig

Ungebrochen

Unzufrieden

Unverändert

Ungeeignet

Unverzichtbar

Unumgänglich

Secorvo News

... zum Dritten

Heute schon gefacebookt?

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Unselbständig

Fast zwei Jahre nach Verabschiedung des unter Federführung des Bitkom entwickelten Datenschutzkodex für Geodatendienste am 01.12.2010 hat der Verein Selbstregulierung Informationswirtschaft e.V. Ende September die nach Abschnitt 6 des Kodex zu errichtende Website der zentralen Informations- und Widerspruchstelle vorgestellt. Sie bietet eine Suchmöglichkeit nach Geodaten anhand der Postanschrift und verweist auf die Widerspruchsverfahren der Anbieter (im Wesentlichen Google Streetview). Die gemeinsame telefonische Beratungsstelle (6.2) sucht man ebenso wie den Beschwerdeausschuss (8.2) und das Gremium zur Selbstkontrolle (7.2) vergeblich; dafür findet sich ein Einheits-Widerspruchformular.

Der Kodex selbst blieb bereits bezüglich der eingeräumten Betroffenenrechte hinter geltendem Datenschutzrecht zurück (Widerspruch erst nach Veröffentlichung). Und nennenswerte Bedeutung wird ihm offenbar seitens der Unterzeichner auch nicht eingeräumt – in den deutschsprachigen Datenschutzangaben zu Google Streetview wird er nicht einmal erwähnt.

Deutlicher als mit solcherlei Selbstregulierung kann man kaum nach einer Verschärfung des Datenschutzrechts rufen.

Ungebrochen

Am 02.10.2012 verkündete das NIST nach fünf Jahren den Gewinner des Wettbewerbs um den Hash-Standard SHA-3. Es ist der „Keccak"-Algorithmus, der sich vor allem durch zwei Eigenschaften gegenüber dem SHA-2 auszeichnet: Er beruht auf einem anderen Grundprinzip als die Familie der MD-Hashes bis einschließlich SHA-2, was zur Hoffnung berechtigt, dass sich mögliche künftige Angriffe auf SHA-2 nicht so einfach auf SHA-3 übertragen lassen. Und er lässt sich besonders effizient in Hardware realisieren – kaum verwunderlich, da die vier Keccak-Autoren, unter ihnen einer der Sieger des AES-Auswahlwettbewerbs, bei Halbleiterherstellern arbeiten, die beide Security-Chips im Portfolio haben.

Anders als beim AES ersetzt SHA-3 den Vorläufer nicht, sondern wird vom NIST als Ergänzung betrachtet, die für manche Einsatzfelder Vorteile bieten kann – und als Rückversicherung, falls SHA-2 eines Tages gebrochen werden sollte. Anwender des SHA-1 sollten nicht warten, bis SHA-3 in Produkten verfügbar ist: Der Sicherheitsgewinn durch den Wechsel zum SHA-2 (SSN 09/2002) ist deutlich größer als von SHA-2 zu SHA-3.

Unzufrieden

Auf Grundlage einer Rechtsprüfung der französischen Datenschutzaufsichtsbehörde (CNIL) hat die Art. 29 Gruppe (europäische Datenschutzaufsicht) Google am 16.10.2012 in einem offenen Schreiben zur Überarbeitung der Datenschutzerklärung und Nutzungsbedingungen vom 01.03.2012 aufgefordert. Im Anhang bescheinigen die Aufseher Google, dass die geltenden Richtlinien jegliche Begrenzung des Verarbeitungszwecks und des Gebrauchs personenbezogener Daten vermissen lassen.

Hauptkritikpunkte sind die mangelnde Transparenz Googles bezüglich der verarbeiteten Daten, die Verarbeitung und Zusammenführung von personenbezogenen Daten über Dienstgrenzen hinweg ohne Rechtsgrundlage oder Einwilligung, das Fehlen jeglicher Löschfristen und der Vorbehalt einer jederzeitigen Änderung der Richtlinien. Es folgen Empfehlungen zur besseren Gestaltung der Datenschutzrichtlinien, zur Einführung vereinfachter Opt-Out Mechanismen und zum Einholen von Einwilligungen in nicht offen ersichtliche Verarbeitungen. Die in Deutschland 2011 vereinbarten Regelungen zu Google Analytics (Ausschluss der dienstüberschreitenden Verwendung, Abschluss eines Auftragsdatenverarbeitungsvertrages und Anonymisierung der IP-Adressen) werden zur Nachahmung empfohlen – etwas voreilig vielleicht, tragen sie doch wenig zu mehr Transparenz der Verarbeitung bei. Sie stehen zudem unter dem Vorbehalt der Umsetzung der EU-Cookie-Richtlinie von 2009.

Unverändert

Das CA/Browser-Forum ist eine informelle Organisation von fünf Browser-Herstellern und ca. 30 kommerziellen CA-Betreibern, die u. a. das Prozedere festlegt, wie Root-Zertifikate in den Browsern vorinstalliert werden. Als eine Konsequenz aus den Trustcenter-Einbrüchen des vergangenen Jahres (SSN 09/2011) wurde diskutiert, das Forum zu reformieren und für interessierte Anwenderkreise zu öffnen, die darauf angewiesen sind, dass Vertrauensanker tatsächlich vertrauenswürdig sind. Wie am 05.10.2012 bekannt wurde, stimmten die Mitglieder jedoch für einen geschlossenen Club.

Die Browser-Hersteller haben die künftige Entwicklung ohnehin in der Hand: Im August 2012 trat der DANE/TLSA-RFC in Kraft, nach dem Serverbetreiber eigene SSL/TLS-Zertfikate im DNS publizieren und Clients sie per DNSSEC validieren können. Sobald die Browser- oder Plugin-Entwickler diese Alternative alltagstauglich umsetzen, dürften öffentliche Root-CAs an Stellenwert einbüßen.

Ungeeignet

Am 19.09.2012 beschloss die Bundesregierung einen Gesetzesentwurf zur Förderung der elektronischen Verwaltung, mit dem auf Bundesebene Hindernisse bei der Einführung elektronischer Verwaltungsverfahren beseitigt werden sollen. Neben der qualifizierten elektronischen Signatur sind nun auch De-Mail und elektronische Formulare unter Verwendung der eID-Funktion des Personalausweises als Ersatz für die Schriftform vorgesehen. Bundesbehörden werden verpflichtet, hierfür den Zugang zu eröffnen, und das De-Mail-Gesetz wird um die Möglichkeit ergänzt, über den Verzeichnisdienst die Zugangseröffnung gegenüber der Verwaltung zu erklären. Bundesbehörden sollen zudem zur elektronischen Aktenführung übergehen und Papierdokumente – wenn sie aus rechtlichen Gründen nicht weiter benötigt werden – entsorgen (sic!).

Es darf bezweifelt werden, dass dem E-Government auf diesem Weg messbare Impulse gegeben werden: fast jede Regelung des Gesetzes liefert den adressierten Behörden eine Ausnahme von der Umsetzungspflicht, die ergänzten Verfahren sind (wie die qualifizierte elektronische Signatur) wenig verbreitet, und ein Großteil der Regelungen hinkt bereits praktizierten Verfahren um Jahre hinterher. Da wirkt die Berechnung der Ersparnisse wie blanker Zweckoptimismus: In 82 Millionen Fällen pro Jahr soll die Bearbeitungszeit je Bürger um acht Minuten sinken – 10 Stunden in 75 Lebensjahren.

Unverzichtbar

Seit dem 02.10.2012 ist das automatisierte Sichtungs-Tool Forensic Scanner verfügbar. Es ist mit 44 Plugins für die Bereiche „System“ und „User“ vorkonfiguriert. Besonders bei Erstuntersuchungen von Windows-Domaincontrollern oder Terminalservern spielt dieses Werkzeug seine Stärken aus, da es sowohl einzelne als auch Gruppen von Benutzerkonten analysieren kann und die Ergebnisse in ASCII-Dateien ausgibt.

Die am 26.09.2012 stark erweiterten und überarbeiteten 243 Plugins des „großen Bruders“ RegRipper detaillieren die Bereiche „System“ (49) und „User“ (106) deutlich weiter, so dass die mit dem Forensic Scanner gelieferten Anhaltspunkte vertieft untersucht werden können. Doch Vorsicht – der korrekte Sicherheitskontext (psexec -s cmd.exe), in dem der Forensic Scanner zur Ausführung gebracht wird, entscheidet darüber, ob er auf die zu untersuchenden Daten zugreifen kann. (Das lässt sich einfach prüfen, indem man mit beiden Werkzeugen dasselbe Windows-Benutzerprofil analysiert und die Ergebnisse für identische Plugins vergleicht.)

Unumgänglich

Am 10.10.2012 ist auf THC die Version 2.0 des THC-IPv6-Toolkits veröffentlicht worden. Es enthält zahlreiche Tools, mit denen inhärente Schwachstellen von IPv6 demonstriert werden können, vor denen eine Personal Firewall für IPv4 nicht schützt. Für Administratoren ist es zugleich ein guter Werkzeugkasten, um die eigenen Netzwerke auf IPv6 zu untersuchen oder sie zu auditieren.

Das Toolkit belegt, dass die Hacker-Community ihre IPv6-Hausaufgaben gemacht hat: Zur Ausnutzung der inhärenten Schwachstellen von IPv6 stehen bereits alle Werkzeuge zur Verfügung. Zwar wird IPv6 nicht in einem „magischen Moment“ IPv4 ablösen. Dennoch: Selbst wenn die IPv6-Einführung im eigenen Netz noch nicht auf der Tagesordnung steht, wird es für Betreiber und Administratoren Zeit, sich mit IPv6 auseinanderzusetzen, um Angreifern im Verlauf einer Umstellung nicht blindlings ins Messer zu laufen – zumal in der Standard-Konfiguration von Windows IPv6 bereits aktiviert ist.

Secorvo News

… zum Dritten

Die dritte und letzte Gelegenheit für IT-Sicherheitsexperten, ihre Kenntnisse in diesem Jahr mit dem T.I.S.P.-Zertifikat zu krönen, bieten wir am **12.-16.11.** Allen Teilnehmern wird vor Seminarbeginn das von Secorvo verfasste 500seitige Begleitbuch zum T.I.S.P. (Zentrale Bausteine der IT-Sicherheit) zur Vorbereitung zugesandt.

Heute schon gefacebookt?

In vielen Unternehmen drängen Marketing- und Personalabteilung auf eine Unternehmenspräsenz bei Facebook & Co, und meist ist ein erheblicher Teil der Mitarbeiter bereits „drin". In den zum großen Teil von amerikanischen Anbietern betriebenen Social Networks lauern jedoch zahlreiche Fallen, wie Copyrightverletzungen, unkontrollierte Informationspreisgabe und Verstöße gegen Datenschutzbestimmungen.

Zu diesen Fragen gibt der Jurist Michael Knopp am **08.11.2012** beim letzten KA-IT-Si-Event dieses Jahres einen Überblick und praktische Tipps. Für ein besonderes Ambiente ist gesorgt: Erstmals ist die KA-IT-Si mit ihrer Veranstaltungsreihe in den stilvollen Räumlichkeiten der Buhlschen Mühle in Ettlingen zu Gast (Anfahrt; ca. 10-15 Minuten S-Bahn-Fahrt vom Karlsruher Hauptbahnhof). Beginn der Veranstaltung ist um 18 Uhr. Um Anmeldung wird gebeten. Wir freuen uns auf spannende Diskussionen und ein interessantes Networking!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2012	
31.10.-03.11.	hashdays security & risk conference 2012 (DEFCON Switzerland, Luzern/CH)
November 2012	
05.-06.11.	TISP Community Meeting (TeleTrusT, Köln)
07.11.	German OWASP Day 2012 (OWASP Germany, München)
08.11.	Heute schon gefacebookt? (KA-IT-Si, Ettlingen)
09.11.	Zur Rolle des CISO/IT-Sicherheitsbeauftragten (GI-FG SECMGT, Frankfurt)
12.-17.11.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
22.-23.11.	36. DAFTA (GDD, Köln)
27.-30.11.	DeepSec 2012 (DeepSec, Wien)
Dezember 2012	
03.-04.12.	IsSec/ZertiFa 2012 (Computas, Berlin)

Fundsache

Am 30.07.2012 hat der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) die Ergebnisse einer Befragung von 1.000 Internet-Nutzern ab 14 Jahren und 800 IT-Leitern, CIOs, Datenschutzbeauftragten und Geschäftsführern zu Datenschutz und Informationssicherheit veröffentlicht. Die 30seitige Studie gibt nicht nur Einblick in Organisation, Kosten und Technik der Informationssicherheit in deutschen Unternehmen, sondern zeigt auch den großen Anteil von Internet-Nutzern, die aufgrund von Sicherheitsbedenken die Inanspruchnahme von Online-Diensten verweigern.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Knobloch, Michael Knopp (Editorial), Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

November 2012



Überflüssig

„Nachweisbar, sicher, zuverlässig“. Klingt gut, was die Deutsche Telekom ihren De-Mail-Kunden verspricht. Allein – heißt das, dass T-Online-E-Mails weder sicher noch zuverlässig sind? 1&1 bewirbt De-Mail mit „sicherem digitalen Briefversand“ – muss man daran bei web.de, gmx und den E-Mail-Postfächern von Geschäftskunden zweifeln?

Der tatsächliche Vorteil von De-Mail gegenüber einer herkömmlichen E-Mail ist schnell benannt: Die Identität des Senders und vor allem der Empfang sind wie bei einem Einschreiben nachweisbar. Nutznießer sind daher in erster Linie die Absender: Mit der Aktivierung eines De-Mail-Accounts ermöglicht der Empfänger jedem De-Mailer eine nicht abstreitbare Zustellung. Anders als beim Einschreiben gilt die De-Mail jedoch als zugestellt, sobald sie im Postfach liegt – auch im Urlaub. Und damit starten auch etwaige Fristen.

Die wahren Profiteure sind jedoch die Provider: Ihnen bietet sich die einmalige Chance, den (D)E-Mail-Versand wie SMS transaktionsbezogen abzurechnen – und so am Rückgang des Briefverkehrs der Unternehmen zu Gunsten von E-Mails mitzuverdienen.

Das Geschäftsmodell hat jedoch einen Haken, wie jetzt auch die Telekom und 1&1 erkannt haben: Da eine De-Mail wie ein eingeschriebener Brief dem Sender in Rechnung gestellt wird, profitiert vor allem der Anbieter, der die Großversender (Versicherungen, Banken, Behörden) für den Dienst gewinnen kann. Telekom und 1&1 fordern daher eine Umsatzbeteiligung von der Deutschen Post, die die De-Mail derzeit bei ihren Geschäftskunden bewirbt.

Die Interessen der Endnutzer bleiben dabei auf der Strecke – darüber kann auch das „Schutzversprechen“ der De-Mail-Anbieter nicht hinwegtäuschen. Denn „sicher und zuverlässig“ sind (ggf. verschlüsselte) E-Mails auch ohne De-Mail. Und in den extrem seltenen Fällen, in denen eine Nachweisbarkeit erforderlich ist, genügt das gute alte Einschreiben vollauf. Hoffen wir, dass der Markt es richtet.



Inhalt

Überflüssig

Security News

Das Tracking und die Standards

Die Eltern und das Filesharing

Das BSI und die Macs

Die Biometrie und die Software

Das OWASP und die DuD

Das Online-Banking und die mTAN

Die Taube und die Nachricht

Secorvo News

500 T.I.S.P.-Zertifkate

Eröffnung des Kryptologikums

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Das Tracking und die Standards

Beim „Tracken“ von Internet-Benutzern stehen sich Datenschützer und Werbewirtschaft scheinbar unversöhnlich gegenüber. Umso erstaunlicher die jüngsten Fortschritte bei technischen Ansätzen zur Abwehr von Tracking: So hat am 06.11.2012 auch Google die sehr versteckte Implementierung von „Do Not Track“ (DNT) für Google Chrome 23 angekündigt. Deutlich offensiver geht Microsoft vor, die mit dem Internet Explorer 10 DNT als Standard aktivieren. Damit haben sie eine hitzige Diskussion ausgelöst, die in einem Apache-Patch gipfelt, der die DNT-Option von IE 10 ignoriert.

Ergänzend hat das W3C am 02.10.2012 die Working Drafts für die Standards Tracking Preference Expression und Tracking Compliance and Scope veröffentlicht. Angesichts technischer Entwicklung, Standards und öffentlichen Diskussionen wächst die Hoffnung, dass sich DNT zu einem Werkzeug entwickelt, mit dessen Hilfe Benutzer ihren Willen zukünftig unmissverständlich und durchsetzbar zum Ausdruck bringen können.

Die Eltern und das Filesharing

Die Entscheidungen zur Störerhaftung des Anschlussinhabers bei Urheberrechtsverstößen sind seit dem 15.11.2012 um ein höchstrichterliches Urteil reicher. Mit der Feststellung, dass Eltern ihre Kinder zwar über Verbote aufklären müssen, dann aber bei Urheberrechtsverletzungen nicht wegen einer Aufsichtspflichtverletzung haften, hat der BGH eine weitere Streitfrage geklärt.

In dem entschiedenen Fall hatte der 13jährige Sohn der Beklagten 147 Audiodateien über einen längeren Zeitraum via Tauschbörse zum Download angeboten; die Icons der verwendeten Tausch-Software waren sogar auf dem Desktop seines Rechners zu sehen. Die Vorinstanzen hatten aus § 832 Abs. 1 BGB Aufsichtspflichten abgeleitet, die über eine einfache monatliche Verlaufskontrolle auf dem Rechner sowie die Installation eines „Security-programms“, das die Installation weiterer Programme verhindern sollte, hinausgingen: Danach hätten die installierten Programme über die Systemsteuerung überprüft werden müssen. Der BGH hat diese Pflichten auf Aufklärung reduziert, sofern mit der Einsichtsfähigkeit des Kindes zu rechnen ist.

Damit gewichtet der BGH zugleich das Gefahrenpotential des Internetzugangs als Schädigungsinstrument niedriger. Daher könnte das Urteil auch bei zukünftigen Entscheidungen zu den Pflichten von Internetanschlussinhabern zu zurückhaltenderen Forderungen führen.

Das BSI und die Macs

Lange hat sich zum Thema Mac OS beim BSI nicht viel bewegt – die Vorabversion des IT-Grundschutz-Bausteins MacOSx datiert vom Januar 2012. Aktuelle Mechanismen wie die Vollverschlüsselung vor allem mobiler Geräte mit FileVault 2 sucht man vergeblich. Am 15.10.2012 hat das BSI nun Empfehlungen zur sicheren Nutzung von Macs unter Apple OS X Mountain Lion veröffentlicht. Leider bleiben die Hinweise überwiegend oberflächlich oder schaffen Verwirrung: So widerspricht das Dokument den Empfehlungen des BSI im Anti-Botnet Beratungszentrum zum Einsatz von Virenschutzprogrammen unter Mac OS.

Dabei sollte man sich als Mac OS User besser nicht in Sicherheit wiegen – das belegt schon eine kurze Suche in der CVE-Liste. So lange weder Apple noch die NSA oder CISecurity aktuelle Security Guidelines für OSx veröffentlicht haben, bieten die Empfehlungen des BSI immerhin einen ersten Einstieg in die Sicherheitskonfiguration eines Macs.

Die Biometrie und die Software

Zumindest in Business-Laptops sind Fingerabdrucksensoren zur Benutzerauthentifikation inzwischen weit verbreitet. Sie vereinfachen das Betriebssystem-Login – und hinterlassen das gute Gefühl, den Laptop „biometrisch“ gesichert zu haben.

Tatsächlich ist es mit dem Schutz nicht ganz so weit her, wie schon am 28.08.2012 bekannt wurde: Geräte, die mit Sensoren der Firma UPEK ausgestattet waren, speichern die Windows-Passwörter ihrer Benutzer AES-verschlüsselt in der Registry – durch einen Implementierungsfehler allerdings so, dass es Mitarbeitern von ElcomSoft gelang, die Passwörter auszulesen.

Das wäre wenig mehr als ein Bug unter vielen – wenn da nicht die (inzwischen von der Webseite des Anbieters gelöschte) Liste der Hersteller wäre, die den UPEK-Sensor einsetzen: Acer, Asus, Dell, Gateway, Lenovo, MSI, NEC, Samsung, Sony und Toshiba. Sucht man auf der Webseite der (erst im Juli 2012 für 356 Mio. USD erworbenen) Apple-Tochter AuthenTec, zu der UPEC seit 2010 gehört, nach näheren Informationen, stößt man auf den lapidaren Hinweis: „AuthenTec's Smart Sensor products are no longer available.“

Gelöst ist das Problem (anders lautenden Ankündigungen zum Trotz) offenbar bisher nicht. Daher können wir nur dringend dazu raten, die entspre-

chenden Treiber zu deinstallieren und den Sensor nicht für das Windows-Login zu nutzen – selbst wenn die Festplatte des Rechners verschlüsselt ist.

Das OWASP und die DuD

Die OWASP AppSecUSA 2012 lockte am 25. und 26.10.2012 ca. 800 Interessierte nach Austin, und am 07.11.2012 trafen sich über 200 Teilnehmer beim OWASP Day Germany 2012 in München zum Thema sichere Webanwendungen. Beide Veranstaltungen zeichneten sich durch eine durchgängig sehr hohe Qualität der Vorträge und (den Teilnehmerzahlen sei Dank) vielfältige Möglichkeiten zum Networking aus. Die Vorträge aus München stehen inzwischen zum Download bereit. Die steigenden Teilnehmerzahlen unterstreichen die wachsende Bedeutung der Anwendungssicherheit. Interessierte finden auf den Seiten des deutschen Chapters der OWASP sowie im Schwerpunktheft 11/2012 der DuD einen guten Einstieg in das Thema.

Das Online-Banking und die mTAN

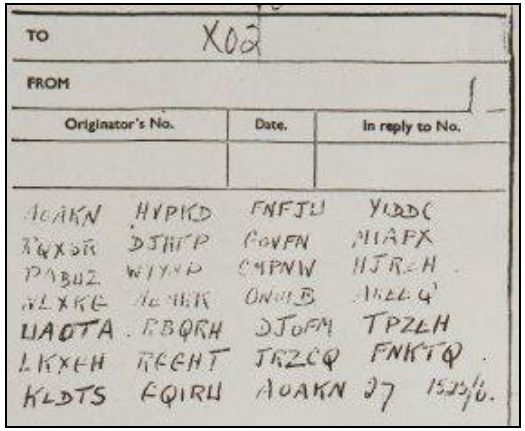
Am 13.11.2012 hat das Berliner Landeskriminalamt eine Warnung für Nutzer des mTAN- (oder SMS-TAN)-Verfahrens veröffentlicht. Diese Bedrohung ist nicht ganz neu – schon am 25.09.2010 hatte David Barroso in seinem Blog über Erweiterungen des Banking-Trojaners ZeuS zu einem „Man-in-the-Mobile"-Trojaner gewarnt (siehe auch Fundsache SSN 9/2010). Jetzt scheinen SMS-Trojaner deutsche Bankkunden im großen Stil ins Visier zu nehmen.

Der Angriff ist denkbar einfach – und hebelt den „getrennten Kanal" zur Übersendung der TAN vollständig aus. Der Trojaner fordert den Bankkunden am PC zum Download eines „Handy-Updates" auf – das anschließend dafür sorgt, dass jede SMS-TAN an den Angreifer weitergeleitet wird.

Gegen diesen Angriff ist nur ein einziges Kraut gewachsen: Die Geistesgegenwart des Nutzers. Denn strikte „Kanaltrennung" kann nur funktionieren, wenn niemals Software direkt oder indirekt über den (möglicherweise befallenen) PC auf das Smartphone übertragen wird.

Die Taube und die Nachricht

Die am 01.11.2012 von BBC News veröffentlichte verschlüsselte Nachricht, die in Südengland am Skelett einer Brieftaube gefunden wurde und wahrscheinlich von einem Sergeanten der Royal Air Force aus dem Ende des Zweiten Weltkriegs stammt, konnte bisher nicht entschlüsselt werden. Wer sich über Weihnachten daran versuchen möchte: Hier ist der Chiffretext.



Secorvo News

500 T.I.S.P.-Zertifkate

Jetzt ist es amtlich: Mitte November erhielt der 500ste T.I.S.P.-Absolvent sein Zertifikat. Das vom Bundesverband IT-Sicherheit (TeleTrusT) entwickelte Expertenzertifikat, das dreijährige Berufserfahrung in der IT-Sicherheit voraussetzt, hat sich damit als berufsqualifizierender Nachweis für Informationssicherheit durchgesetzt und genießt hohe Anerkennung.

Das von Secorvo verfasste, 500-seitige Begleitbuch zum T.I.S.P.-Seminar „Zentrale Bausteine der Informationssicherheit" (80 Euro) bietet eine Zusammenfassung des T.I.S.P.-Grundlagenwissens in 22 Kapiteln – eine unverzichtbare Lektüre für lange Winterabende. Wer sich zu einem T.I.S.P.-Seminar bei Secorvo anmeldet, erhält das Buch zur Vorbereitung übersandt. Nächster Termin: **15.–19.04.2013**.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Eröffnung des Kryptologikums

In das kommende Jahr startet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit einem Highlight: Am **31.01.2013** werden wir im Zentrum für Kunst und Medientechnologie (ZKM) das „Kryptologikum" des Karlsruher Institute of Technology (KIT) eröffnen. Ähnlich dem Mathematikum in Gießen, dem Dynamikum in Pirmasens und dem Technoseum in Mannheim bietet das Kryptologikum in einer zunächst dreitägigen Ausstellung (vom 01.-03.02. 2013) Kryptographie zum „Begreifen". Die Exponate veranschaulichen kryptographische Prinzipien, und es werden historische Verschlüsselungsmaschinen gezeigt, die Kriege entschieden haben.

Das Eröffnungsevent beginnt um 18 Uhr im Kubus des ZKM in Karlsruhe. Zur Einstimmung bieten wir um 16 und 17 Uhr eine Führung zur voll funktionsfähigen Zuse Z22 an, die im ZKM ausgestellt ist.

Wir freuen uns auf Ihre Teilnahme – und empfehlen Ihnen eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2012	
03.-04.12.	IsSec/ZertiFa 2012 (Computas, Berlin)
27.-30.12.	29th Chaos Communication Congress (29C3) (Chaos Computer Club, Hamburg)
Januar 2013	
15.-17.01.	OMNICARD 2013 (in TIME berlin, Berlin)
31.01.	Eröffnung des Kryptologikum (KIT, ZKM & KA-IT-Si, Karlsruhe)
Februar 2013	
06.-07.02.	23. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
19.-20.02.	20. DFN Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2013	
05.-09.03.	CeBIT (Deutsche Messe, Hannover)
11.-14.03.	CPSSE-Schulung (Secorvo College, Karlsruhe)
12.-15.03.	Black Hat Europe 2013 (Blackhat, Amsterdam/NL)
18.-21.03.	Security Engineering (Secorvo College, Karlsruhe)

Fundsache

Jedes Kryptoverfahren ist immer nur so sicher wie seine Schlüssel – dieses Prinzip wird leider beim Design von Sicherheitslösungen allzu häufig missachtet. Am 16.11.2012 hat das US-amerikanische NIST als Special Publication SP 800-133 konkrete Empfehlungen zur Schlüsselgenerierung veröffentlicht – ein ‚Must Read' für jeden Systemdesigner.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Michael Knopp.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Dezember 2012



Das Analoge im Digitalen

Es mutet manchmal eigenartig an, wie bereitwillig viele Menschen die Risiken der digitalen Welt ignorieren. Bruce Schneier zeichnet in seinem jüngsten Crypto-Gram diese „schöne neue Welt" sogar als eine Art „digitaler Leibeigenschaft" – mit Amazon, Apple, Facebook und Google in der Rolle der Feudalherren, denen ihre Vasallen alles anvertrauen. Aus der Fürstenperspektive gibt es natürlich wenig Grund, die Legitimität dieses einseitigen Vertrauensverhältnisses und der Möglichkeit absoluter Kontrolle in Zweifel zu ziehen. Merkwürdig stimmt allerdings, dass Milliarden Nutzer sich begeistert in diese Abhängigkeit begeben – und sogar zu glühenden Anhängern werden, die bereitwillig mithelfen, nicht nur das Mantra ihres Herrn zu verbreiten, sondern es eifernd gegen jeden Skeptiker oder Kritiker und gegen alle Anhänger anderer Fürsten zu verteidigen.

Einige bemühen zur Rechtfertigung immerhin Fatalismus: „Warum ich die iCloud benutze? Apple weiß doch ohnehin alles über mich…". Dabei kämen die meisten von ihnen im wirklichen Leben kaum auf ähnliche Ideen: „Warum sollte ich meinem Nachbarn nicht meine Kreditkarte und die EC-Karte mit PIN anvertrauen? Den Haustürschlüssel hat er doch auch schon…" Helfen könnten daher bewährte Strategien aus der analogen Welt auch in der digitalen:

- Vertraue Dritten nie blind – sondern immer nur so, dass du das Vertrauen auch jederzeit wieder entziehen kannst.
- Setze nie alles auf eine Karte.
- Vertraue nie unbegrenzt – behalte immer einen Rest Kontrolle.

Weder frühmittelalterliche Fürstenhuldigung noch Bequemlichkeit oder Kostenfokussierung sind eine angemessene Haltung für Risikobewertung und Schadensbegrenzung. Aber wie formulierte Marie Freifrau Ebner von Eschenbach (1830-1916) doch so treffend: „Die glücklichen Sklaven sind die erbittertsten Feinde der Freiheit."



Inhalt

Das Analoge im Digitalen

Security News

Rechtsverstoß Double-Opt-In

Smart Meter Profiles

Löschen nach Regeln

Cyberentschlossenheit

Neues vom Bundestrojaner

Keylogger

Neujahrsputz

Secorvo News

Eröffnung des Kryptologikums

Sichere Systeme

Veranstaltungshinweise

secorvo
security consulting

Security News

Rechtsverstoß Double-Opt-In

Am 27.09.2012 hat das OLG München mit einer Entscheidung für große Verunsicherung gesorgt, nach der die Bestätigungsanfrage beim Double Opt-In-Verfahren zur E-Mail-Werbung als unzumutbare Belästigung zu betrachten ist, wenn sie nicht nachweislich vom Empfänger veranlasst wurde.

Dies wird von der Beratungsszene und Anbietern kontrovers diskutiert. Klar ist: § 7 Abs. 2 Nr. 3 UWG verbietet E-Mail-Werbung ohne ausdrückliche und nachweisbare Einwilligung. Das Double-Opt-In soll daher sicherstellen, dass keine werbliche Ansprache via E-Mail erfolgt, wenn die Einwilligung nicht vom Inhaber der dabei angegebenen E-Mail-Adresse auf Anforderung bestätigt wird. Der BGH hat 2004 in anderer Konstellation bereits entschieden, dass ein Double Opt-In den notwendigen Nachweis der elektronischen Einwilligung führen kann.

Nun kann ein Teil eines Authentifizierungs- und Schutzmechanismus ohne werbliche Inhalte naturgemäß eigentlich keine unzumutbare Belästigung sein, solange sie durch einen Webseiteneintrag veranlasst wurde. Dieser freilich muss genauso wie die spätere Bestätigung protokolliert und aufbewahrt werden. Allerdings kann bei einer Anmeldung über ein Webformular selbst bei Protokollierung kein personenbezogener Veranlassungsnachweis gelingen – es sei denn, der Nutzer würde sich auf andere Weise authentifizieren. Dann wäre jedoch eine Bestätigung (und damit auch die E-Mail-Benachrichtigung) überflüssig. Für die Versender von E-Mail-Newslettern und -Werbung bleibt jedoch bis zur höchstrichterlichen Klärung das Risiko, für das Double Opt-In-Verfahren abgemahnt zu werden.

Smart Meter Profiles

Das Weihnachtsgeschenk des BSI vom 21.12.2012 sind Version 1.1.7 der Protection Profiles für Smart Meter Gateways und Version 1.0 der Protection Profiles der in Smart Meter Gateways enthaltenen Security Modules. Die Funktionalitäts- und Interoperabilitätsanforderungen wurden in der Technischen Richtlinie TR-03109 (Version 1.0, Release Candidate) spezifiziert. Alle drei Dokumente sollen zusammen mit dem Referentenentwurf der Rechtsverordnung nach § 21i EnWG Anfang 2013 von der EU notifiziert und damit für die Entwicklung von Komponenten der so genannten „intelligenten Energienetze“ rechtlich bindend werden.

Zwar handeln die Spezifikationen alle wichtigen Sicherheitsaspekte von der Authentifikation bis zur verschlüsselten Übermittlung systematisch ab. Themen des Datenschutzes werden jedoch – trotz Mitwirkung des BfDI – auf gerade einer der 90 Seiten behandelt, beschränkt auf Pseudonyme und Übertragungsschutz. Fragen nach Erforderlichkeit, Zweckbindung oder Datensparsamkeit bleiben ausgeklammert: die Protection Profiles sorgen also auch bei unzulässiger Erhebung für einen guten Schutz. Die Frage der Rechtmäßigkeit der mit Smart Meter Gateways geplanten und möglichen Verarbeitung von Verbraucherdaten bleibt damit dem politischen Diskurs vorbehalten.

Löschen nach Regeln

Die Festlegung von Regellöschfristen für verarbeitete personenbezogene Daten ist eine der größten praktischen Herausforderungen des Datenschutzrechts. Ausgelöst durch Veröffentlichungen der Toll Collect GmbH über ihr Datenschutz-Löschkonzept schrieb der DIN Anfang 2012 ein vom BMWI gefördertes Projekt im Programm „Innovation mit Normen und Standards“ aus, um die Möglichkeit einer standardisierten Vorgehensweise für die Entwicklung von Löschkonzepten zu untersuchen.

Am 10.12.2012 wurde nun die in intensiver Diskussion mit Datenschützern aus Industrie und Aufsichtsbehörden von Secorvo erarbeitete Leitlinie zur Entwicklung eines Löschkonzepts (Dr. Volker Hammer, Karin Schuler) vorgestellt. Die zuständige ISO/IEC-Arbeitsgruppe hat Interesse an einer Fortsetzung der Standardisierungsarbeiten signalisiert; sofern die Finanzierung der Arbeiten durch Förderunternehmen gesichert werden kann, könnte nun unter deutscher Federführung ein internationaler Lösch-Standard für personenbezogene Daten entstehen. Bei Interesse stellen wir gerne einen Kontakt her – E-Mail an redaktion-security-news@secorvo.de genügt.

Cyberentschlossenheit

Das Europäische Parlament hat am 22.11.2012 eine Entschließung zur Cybersicherheit und Verteidigung angenommen. Darin werden EU-Institutionen und Mitgliedstaaten aufgefordert, unter Einbindung privater Unternehmen Maßnahmen zu ergreifen. Die Zustandsfeststellungen dokumentieren vor allem ein EU-weit uneinheitliches Vorgehen gegen Cyberattacken – trotz gewachsener Bedrohung. Insbesondere sähen nur wenige Staaten bislang den Schutz ihrer IT-Infrastrukturen als Teil ihrer Sorgfaltspflichten, nur zehn Mitgliedstaaten besäßen eine nationale Strategie, und mangels Meldungen bestünde eine hohe Dunkelziffer an Angriffen.

Gefordert werden ein gemeinsames Weißbuch, eine gründliche Erfassung der Angriffe und Bewertung der Gefahren, eine koordinierte Reaktion auf EU-Ebene und die Erarbeitung von Notfallplänen in Kooperation mit der ENISA. Schließlich wird sogar

die Anerkennung eines schweren Cyber-Angriffs als Solidaritätsfall und Kriegsgrund postuliert.

Die Entschließung signalisiert zwar Entschlossenheit; die Maßnahmenvorschläge erscheinen jedoch als ein willkürliches Sammelsurium von Ausbildungsförderung bis Kriegserklärung. Der Weg zu einer geschlossenen Strategie ist noch weit.

Neues vom Bundestrojaner

Am 17.10.2012 hatte die SPD-Fraktion der Bundesregierung in einer kleinen Anfrage 55 spannende Fragen zum Bundestrojaner gestellt – unter anderem zur Weigerung der Fa. DigiTask, dem BfDI Einsicht in den Quellcode zu gewähren. Am 10.12.2012 wurden nun die Antworten der Bundesregierung vom 21.11.2012 veröffentlicht. Einige sind durch einen Hinweis auf die Vertraulichkeitsstufe (VS-NfD) ersetzt. Dennoch enthält das Dokument interessante Details – u. a. den Hinweis, dass Skype-Telefonate nicht abhörbar seien und mit einer vom BKA selbst entwickelten Überwachungssoftware erst Ende 2014 gerechnet werden könne.

Keylogger

Heutige Hardware-Keylogger sind günstig (ca. 60$), bescheren Aufmerksamkeit (wie im Fall vom 23.10.2012), arbeiten beinahe transparent und speichern mehrere GB Tastendrücke. Sofortmaßnahmen für den Finder sind Passwortwechsel, polizeiliche Spurensicherung, Sicherung der Gebäude-Zutrittsprotokolle und ggf. in Abstimmung mit Datenschutz und Betriebsrat eine Raumüberwachung oder die Hinterlegung der Adresse eines Honeypots auf dem Logger.

Ähnlich hässlich ist die am 25.10.2012 von Ryan Barnett auf der AppSecUSA präsentierte Idee: Dabei infiziert eine Web Application Firewall ausgewählte „Besucher“ mit dem Browser Exploitation Framework (kurz BeEF) per Angriff auf Web Browser-Schwachstellen, um dann z. B. einen Software-Keylogger zu platzieren.

Manchmal kommt ein Keylogger auch nicht allein: Scannen Sie daher nicht nur regelmäßig Ihr System, sondern prüfen Sie auch von Zeit zu Zeit Ihre Schnittstellen – oder sorgen Sie mit Klebstoff für eine feste Verbindung von Tastaturstecker und PC.

Neujahrsputz

Wer gleich zu Beginn des neuen Jahres die Angriffsfläche seines PCs reduzieren möchte, sollte Java in seinen Browsern deaktivieren. Denn während es kaum noch einen guten Grund gibt, mit aktiviertem Java im Browser zu surfen, öffnen unsichere Java-Versionen Angreifern Tür und Tor: Von lediglich drei im Jahr 2011 stieg die Zahl der 2012 veröffentlichten Security Vulnerabilities des JRE auf beeindruckende 58 – stattliche 23 davon mit der höchsten Gefährdungsstufe 10.

Hilfreiche Anleitungen um Java mit wenig Aufwand wirksam aus dem Browser zu verbannen finden Sie bei Andrew Tech Help, Brian Krebs oder OSXDaily.

Secorvo News

Eröffnung des Kryptologikums

In das Jahr 2013 startet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit einem besonderen Highlight: Am **31.01.2013** werden wir im Zentrum für Kunst und Medientechnologie (ZKM) das „Kryptologikum“ des Karlsruher Institute of Technology (KIT) eröffnen. Ähnlich dem Mathematikum in Gießen, dem Dynamikum in Pirmasens und dem Technoseum in Mannheim bietet das Kryptologikum in einer zunächst dreitägigen Ausstellung (vom 01.-03.02. 2013) Kryptographie zum „Begreifen“. Die Exponate veranschaulichen kryptographische Prinzipien und es werden historische Verschlüsselungsmaschinen gezeigt, die Kriege entschieden haben.

Das Eröffnungsevent beginnt um 18 Uhr im Kubus des ZKM in Karlsruhe. Wir freuen uns auf Ihre Teilnahme – und empfehlen Ihnen eine schnelle Anmeldung.

Sichere Systeme

Technisch verursachte Sicherheitsvorfälle können in der Regel auf eine von drei Ursachen zurückgeführt werden: Konfigurationsfehler, Programmierfehler oder ein fehlerhaftes Systemkonzept. Die letzte dieser Ursachen ist oft besonders heikel: Sie entsteht durch das Zusammenspiel komplexer Einzelkomponenten und lässt sich zumeist nur durch einen teuren Systemwechsel beseitigen.

Um dieses Problem an der Wurzel zu packen, haben wir gemeinsam mit dem Institut für Kryptographie und Sicherheit (IKS) am Karlsruhe Institute of Technology (KIT) ein Seminar für Systementwickler konzipiert, in dem wir in das Konzept des „Security by Design“ einführen: Security Engineering – Anleitung zur Entwicklung sicherer Systeme am 18.-21.03.2012.

Im April folgt die nächste Schulungen zum T.I.S.P. Zertifikat – von den Autoren des T.I.S.P.-Buchs. Nutzen Sie die Gelegenheit, Ihre Qualifikation abzurunden und zertifizieren zu lassen. Alle weiteren Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter
http://www.secorvo.de/college

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Januar 2013	
15.-17.01.	OMNICARD 2013 (in TIME berlin, Berlin)
31.01.	Eröffnung des Kryptologikums (KIT, ZKM & KA-IT-Si, Karlsruhe)
Februar 2013	
06.-07.02.	23. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
19.-20.02.	20. DFN-Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2013	
05.-09.03.	CeBIT (Deutsche Messe, Hannover)
11.-14.03.	CPSSE-Schulung (Secorvo College, Karlsruhe)
12.-15.03.	Black Hat Europe 2013 (Blackhat, Amsterdam/NL)
18.-21.03.	Security Engineering (Secorvo College, Karlsruhe)
April 2013	
09.-11.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
15.-19.04.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
16.-17.04.	Datenschutztage 2012 (Forum für Datenschutz, Wiesbaden)
23.-26.04.	PKI (Secorvo College, Karlsruhe)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Volker Hammer, Kai Jendrian, Michael Knopp, Sven Köhler.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2013



Der dritte Faktor

Jüngst erregten Eric Grosse, Googles Vice President für Security Engineering, und sein Kollege Mayank Upadhyay mit einer Veröffentlichung in der Januar/Februar-Ausgabe von IEEE Security & Privacy Aufsehen. In dem achtseitigen Aufsatz Authentication at Scale stellen sie ihre Konzepte einer skalierbaren und Benutzer freundlichen Zwei-Faktor-Authentifikation vor und bezeichnen Googles two-step verification feature (2sv), „adopted by millions", als eines der „largest two-factor authentication deployments in the world".

Deutschen Online-Bankern dürfte diese Einschätzung höchstens ein mitleidiges Lächeln entlocken – besteht das Verfahren doch im Wesentlichen darin, dass 2sv-Nutzern beim erstmaligen Login auf einem neuen oder fremden Device eine sechsstellige Zufallszahl via SMS zugesandt wird, die sie eintippen müssen: mTAN lässt grüßen.

Insgesamt belegt die Publikation den Erfahrungsrückstand des Internet-Giganten: Das Konzept von „2sv Cookies" als Credential und die Überzeugung, wiederholte Authentifikationen durch „Delegation" an ein Device-Credential vermeiden zu können, entstammen dem prätrojanischen Zeitalter.

Zwar gestehen sie zu, das 2sv durch cleveres Phishing und Malware bedroht sein könnte. Ihre Antwort darauf ist jedoch die Bindung des Cookie-Credentials an den SSL-Client – und nicht die Einsicht, dass Vertrauen in ein programmierbares Mehrzweck-Gerät wie ein Smartphone oder ein PC niemals eine gute Idee sein kann. Denn ein starkes Authentifikationsverfahren braucht einen dritten Faktor: das „uncheatable device" – ein Gerät zur Prüfung und Anzeige eines Credentials, das dem Zugriff eines Angreifers wirksam entzogen ist.

Deutsche Banken und Sparkassen haben das längst verstanden und bieten TAN-Generatoren wie chipTAN oder PhotoTAN, um Überweisungen zu authentisieren. Vielleicht werden diesmal aus den Gejagten die Jäger: Was liegt näher, als solche TAN-Generatoren auch für andere wichtige Authentifikationen zu verwenden?



Inhalt

Der dritte Faktor
Security News
Aus dem Giftschrank
Gegengift
Umgang mit Giftstoffen
Digitale Giftanalyse
Heimliches Gift
Secorvo News
Winderlektüre
Zertifikate
Ausgebucht
Veranstaltungshinweise
Fundsache

secorvo
security consulting

Security News

Aus dem Giftschrank

Pass-the-Hash (PtH) und verwandte Attacken sind eine Bedrohung von Windows-Systemen, die seit vielen Jahren bekannt und schwerwiegend, aber nicht prinzipiell auszuschließen sind: Ein Angreifer, der Systemrechte auf einem Windows-System erlangt hat – oder sich gar auf einer der unter Eingeweihten kursierenden Methoden eine permanente Hintertür einrichten konnte – kann mit Tools wie WCE oder mimikatz die Credentials der an diesem System momentan oder kürzlich angemeldeten Benutzer aus dem Hauptspeicher auslesen. Dies betrifft Kerberos-Tickets und NTLM-Hashes, mit denen sich der Angreifer auch ohne Passwort im Netzwerk anmelden kann, LM-Hashes (selbst unter Windows 7), die per Online-Service zu einem Passwort zurück gerechnet werden können, und oft sogar Klartext-Passwörter. Am 11.12.2012 veröffentlichte Microsoft nun ein Whitepaper mit Ratschlägen, wie man derartigen Attacken begegnen kann. Die darin propagierten Ansätze werden von einigen Fachleuten als unzureichend oder praxisuntauglich kritisiert. Einig ist man sich allerdings – auch mit früheren Artikeln – darin, was *nicht* hilft: beispielsweise Smarcard-Logon oder der Verzicht auf NTLM zugunsten von Kerberos.

Alle Empfehlungen laufen letztlich darauf hinaus, es gar nicht erst zu einer Infektion kommen zu lassen: Erstens sollte man unbedingt verhindern, dass Angreifer unter Windows Systemzugriff auf den Hauptspeicher erlangen können (durch eine Vielzahl von ineinander greifenden Maßnahmen von der Festplattenverschlüsselung über Software-Restriction, strikter Kontrolle lokaler Administrationsrechte bis zur Deaktivierung von Schnittstellen). Und zweitens sollte man sich nicht mit hohen Berechtigungen an Maschinen anmelden, bei denen nicht hinreichend sicher ist, dass „Erstens" erfolgreich war, um einem Angreifer die Credentials nicht auf dem Silbertablett zu servieren.

Gegengift

Die Isolierung des Browsers auf dem eigenen System ist ein probates Mittel zur Eindämmung unerwünschter Infektionsfolgen. Eine nahe liegende Möglichkeit ist das Browsen in virtuellen Maschinen – mit gängigen Virtualisierungslösungen ist das Ergebnis jedoch oft schwergewichtig und behäbig.

Eine leichfüßige Alternative sind Sandbox-Lösungen, mit denen die „Nebenwirkungen" eines infizierten Objekts im Browser oder Dokumentenviewer eingeschränkt werden können. Beispielhaft sei hier das am 16.12.2012 in Version 3.76 publizierte Tool Sandboxie empfohlen, bei dem alle Schreibzugriffe innerhalb einer geschlossenen Umgebung erfolgen. Wird eine Sandboxie-Session beendet, werden alle Downloads, Änderungen an Dateien usw. zuverlässig verworfen. Das Konzept stellt eine Form des im Editorial der SSN 9/2012 diskutierten Einweg-Paradigmas dar. Im Sinne des *Defense-in-Depth* ist eine solche Sandbox-Lösung ein einfaches, aber wirksames Gegengift gegen unerwünschte Nebenwirkungen.

Umgang mit Giftstoffen

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat am 08.01.2013 eine Broschüre mit Tipps und Informationen zum datenschutzbewussten Umgang mit Facebook herausgegeben. Darin werden anhand von Screenshots die wichtigsten Einstellungen erläutert, die man zum Selbstschutz vornehmen sollte: Verwendung von Pseudonymen (entgegen den unwirksamen Nutzungsbedingungen), Verhinderung von Tracking, Unterbindung der Profilsuche über Google und der Verwendung personenbezogener Daten für Werbeanzeigen. Es wird vor der Facebook-Chronik und der Freigabe eigener Adressbücher für die Freunde-finden-Funktion gewarnt und deutlich auf die Erforderlichkeit einer Einwilligung für die Veröffentlichung von Daten Dritter hingewiesen.

Die Tipps und Hinweise sind leicht verständlich und umfassend. Dabei wird deutlich, wie weit Facebook von „Datenschutz by default" entfernt ist. Der pragmatische Ansatz, Datenschutz durch Information der Nutzer zu fördern, solange das Durchsetzen der Datenschutzanforderungen bei einem internationalen Anbieter stockt, ist zu begrüßen.

Digitale Giftanalyse

Ist Gefahr im Verzug, muss man schnell handeln. Daher kommt es bei forensischer Incident Response darauf an, mögliche Beweisdaten zügig zu sichern. In der Windows-Systemdatei NTUSER.DAT werden Tätigkeiten des jeweiligen Benutzerkontexts nachvollziehbar gespeichert – die Datei lässt sich im laufenden Systembetrieb und bei angemeldetem Benutzer jedoch weder auslesen noch kopieren, da Windows den Zugriff auf offene Dateien sperrt.

Dieses Zugriffsproblem löst die am 03.11.2012 erschienene Version 0.72 von ntfscopy komfortabel, indem des den Zugriff an der Windows-internen Zugriffskontrolle vorbei ermöglicht. Dabei kann der Slack-Space mitkopiert werden, um bereits gelöschte Einträge zu durchsuchen. Auch die zugehörigen NTFS-Metadaten und NTFS-Dateiattribute, die in der Regel nur sehr schwierig manipulierbar sind, sowie direkte Zugriffe auf einzelne Alternate Data

Streams einer Datei, in denen sich z. B. Malware verstecken kann, können abgespeichert werden.

Daraus extrahiert der Computer Account Forensic Artifact Extractor (cafae) aussagefähige Daten und Zeitstempel u. a. für Benutzerkontenaktivitäten (UserAssist-History, RecentDocs, OpenSavePidlMRU und MountPoints2), z. B. für USB-Geräte. Sehr hilfreich ist, dass die Zeitangaben sowohl im SleuthKit-Bodyformat als auch im log2timeline-Format erzeugbar und so für eine übergreifende Zeitlinienanalyse nutzbar sind.

Die Kehrseite der Medaille: Sicherheitsmanager und Revisoren werden sich zukünftig fragen müssen, wie integer das geprüfte Zugriffsberechtigungskonzept in Windows-NTFS-Dateisystemen ist, wenn solche Zugriffsmöglichkeiten (ohne Auditeintrag im Security-Eventlog) bestehen.

Heimliches Gift

Die Fraktionen von CDU/CSU und FDP überraschten am 10.01.2013 mit einer Neufassung des seit Ende 2010 vorliegenden Gesetzentwurfs zum Beschäftigtendatenschutz. Gegenüber dem bereits kontrovers diskutierten ersten Entwurf enthält die Neufassung einige gewichtige Änderungen: Als § 32m BDSG soll ein Absatz zur Beschäftigtendatenübermittlung im Konzern eingefügt werden, begleitet von Änderungen mit Relevanz für die Auftragsdatenverarbeitung im Ganzen. Der ohnehin schon unübersichtliche § 28 BDSG wird um Sondertatbestände für Beschäftigtendaten erweitert. Die Überwachungsbefugnisse der Arbeitgeber sind über den ersten Entwurf hinaus erweitert worden, etwa im Bereich der Call-Center oder der Videoüberwachung. Weitere Regelungen wurden durch unbestimmte Rechtsbegriffe oder Streichungen verwässert.

Die neu aufgenommenen Regelungen zur Beschäftigtendatenübermittlung im Konzern und zur internationalen Auftragsdatenverarbeitung reagieren auf einen tatsächlichen Bedarf. Sie kodifizieren aber lediglich bislang praktizierte Lösungsansätze. Neue interessensgerechte und vereinfachte Lösungen bringen sie nicht, etwa zur Auftragsdatenverarbeitung in unsicheren Drittstaaten.

Die plötzliche Eile ist angesichts der wenigen echten Innovationen und der vielen Mängel des Gesetzes nicht ratsam: Der Datenschutz braucht durchdachte Lösungen statt gesetzgeberischer Detailkorrektur von Rechtsprechung und -praxis. Das hat nun wohl auch die Bundesregierung eingesehen: Der Entwurf sollte zunächst schon am 16.01.2013 im Innenausschuss verhandelt werden, wurde jedoch kurzfristig – evtl. wegen der sich schnell verbreitenden Proteste aus Datenschutzkreisen – wieder von der Tagesordnung genommen. Am 30.01.2013 sollte er wieder in den Innenausschuss – und wurde am 29.01.2013 erneut von der Tagesordnung gestrichen.

Secorvo News

Winterlektüre

Frühabendliche Dunkelheit und Minustemperaturen laden ein zur gemütlichen Lektüre im Lesesessel oder vor dem Kamin. Sollten Ihnen dabei die Bücher ausgehen, so helfen wir gerne: Neben unserem 520seitigen T.I.S.P.-Buch „Zentrale Bausteine der Informationssicherheit“ können wir Ihnen – abhängig von Ihren fachlichen Präferenzen – Michael Knopps Aufsatz über Google und den Datenschutz (DANA 12/2012), Dr. Safuat Hamdys Beitrag über den OWASP Application Security Verification Standard (DuD 11/2012) und Hans-Joachim Knoblochs Vorstellung des zukünftigen SHA-3-Hash-Standards *Keccak* (KES 1/2013) ans Herz legen.

Zertifikate

Sollte sich unter Ihren guten Vorsätzen für das neue Jahr auch die Zertifizierung Ihrer Kenntnisse und Erfahrungen in der Informationssicherheit finden, können wir auch hier helfen: das nächste T.I.S.P.-Seminar findet statt vom **15.–19.04.2013** mit anschließender Prüfung am 20.04.2013. Die nächste CPSSE-Zertifizierung in sicherer Softwareentwicklung bieten wir bereits vom **11.–14.03.2013** an. Erstmalig zählt in diesem Jahr auch ein Seminar zu „Security by Design“ zu unserem Seminarangebot: Security Engineering vom **18.–21.03.2013**. Wir freuen uns darauf, Sie zu einer dieser Veranstaltungen bei uns begrüßen zu dürfen!

Alle Programme und die Möglichkeit zur Online-Anmeldung finden Sie unter
http://www.secorvo.de/college

Ausgebucht

Gerne hätten wir an dieser Stelle noch einmal für das KA-IT-Si-Event am 31.01.2013 im Karlsruher Zentrum für Kunst und Medientechnologie (ZKM) geworben, an dem die dreitätige Ausstellung des Kompetenzzentrums für Angewandte Sicherheits-Technologie (KASTEL) am KIT, „Kryptologikum – Kryptographie begreifen“ eröffnet wird. Mit über 200 Teilnehmern ist die Veranstaltung jedoch seit einer Woche komplett ausgebucht – und wir müssen auf die Ausstellung selbst vertrösten, die vom **01.–03.02.2012** im ZKM kostenlos besucht werden kann. Dafür bitten wir Sie, schon einmal den nächsten Termin vorzumerken: Das zweite diesjährige Event der KA-IT-Si findet statt am **14.03.2013** – Details folgen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2013	
01.-03.02.	Kryptologikum (KIT/KASTEL, ZKM Karlsruhe)
06.-07.02.	23. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
15.-17.02.	ShmooCon 2013 (The Shmoo Group, Washington/US)
19.-20.02.	20. DFN-Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2013	
05.-09.03.	CeBIT (Deutsche Messe, Hannover)
11.-14.03.	CPSSE-Schulung (Secorvo College, Karlsruhe)
12.-15.03.	Black Hat Europe 2013 (Blackhat, Amsterdam/NL)
18.-21.03.	Security Engineering (Secorvo College, Karlsruhe)
April 2013	
09.-11.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
15.-19.04.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
17.-18.04.	a-i3/BSI Symposium 2013 (a-i3/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)

Fundsache

In diesem Jahr macht Deloitte den Anfang: Die 2013 TMT Global Security Study gibt einen Einblick in die Einschätzungen, Schwerpunkte und Investitionen der 120 größten Unternehmen der Telekommunikations-, Medien- und Technologiebranche. Eine der zentralen Herausforderungen: "*Lack of sufficient awareness with employees*" (70 %).

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Februar 2013



Zertifikatsträume

Der Traum von der Zertifizierung von IT-Sicherheit begann vor 43 Jahren: Die am 11.02.1970 publizierten „Security Controls for Computer Systems“, allgemein bekannt als „Ware Report„, waren eine Pioniertat. Fasching ist vorbei, daher soll nicht auf zertifizierte Wetterstationen eingegangen werden: der aktuelle ernste Fall der am 11.01.2013 von der Überwachungsbehörde auf den Boden verordneten Boeing 787 zeigt die Tücken und Grenzen von Zertifizierungsverfahren und wirft die berechtigte Frage auf, warum die FAA die Zertifizierung des Dreamliner auslagerte – ausgerechnet an eine Sparte von Boeing.

Die in „How Certification Systems Fail„ von Murdoch, Bond und Anderson analysierten Beispiele zeigen: das ist kein Einzelfall. So fiel nach der Kompromittierung eines als „Common Criteria evaluated“ beworbenen PIN Entry Device auf, dass der wesentliche Schritt einer Überprüfung durch eine unabhängige Stelle („Common Criteria certified“) fehlte. Und bei einem nach FIPS 140 zertifizierten Gerät wurden nicht alle Software-Komponenten in die Untersuchung einbezogen. Woraus man wesentliche Anforderungen an eine Zertifizierung ableiten kann: Der Prüfgegenstand muss exakt und sinnvoll festgelegt und die Prüfkriterien müssen genau beschrieben sein. Für die Sicherheit im realen Einsatz müssen auch Einsatzumgebung und Betriebsprozesse betrachtet werden. Untersuchungen müssen detailliert dokumentiert und durch eine *unabhängige* Prüfinstanz verifiziert werden. Die Prüfberichte sollten veröffentlicht werden, um Transparenz zu schaffen und die Aussagekraft eines Zertifikats beurteilbar zu machen.

So betrachtet ist das BSI mit Common Criteria (CC) und ISO 27001 auf Basis von IT-Grundschutz auf einem guten Weg. Sofern die externe Prüfbegleitung noch mal überdacht wird klappt es vielleicht auch mit der Anerkennung des Grundschutz-Zertifikats als ISO 27001 *native*.



Inhalt

Zertifikatsträume

Security News

Passworthäufigkeiten

Nebenschauplätze

ZAP 2.0.0

Nicht-Nadel im Nicht-Heuhaufen

TLS = Turn to Latest Standards

Secorvo News

Schau mir in die Augen, Kleines

Security by Design

Zertifiziert

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Passworthäufigkeiten

Die Wahrscheinlichkeitsrechnung gehört nicht zu den Dingen, die dem Menschen in die Wiege gelegt sind, wie ein aktuelles Beispiel illustriert. In einer Prognose für das Jahr 2013 rief Deloitte am 14.01.2013 das Ende des Passwortzeitalters aus: 90 % aller User-Passwörter würden Hacking-Angriffen nicht standhalten. Die Autoren berufen sich auf eine „recent study" – die sich bei einem Blick in die angegebene Quelle als nicht mehr ganz taufrischer Blog-Eintrag von Mark Burnett vom 20.06.2011 entpuppt. Danach hätten 98,1 % der Nutzer aus seiner Sammlung von ca. 6 Mio. User/Password-Paaren eines der 10.000 häufigsten Passworte gewählt. Lädt man Burnetts Liste dieser 10.000 Passwörter mit Häufigkeit herunter, ergibt sich ein anderes Bild: 1,875 Mio. der Accounts verwenden eines der Top-10.000-Passwörter – ein knappes Drittel (gut 31 %). Auch andere Angaben Burnetts lassen sich mit den Zahlen nicht belegen: nicht 71 %, sondern 613.000 User (ca. 10,2 %) wählten eines der Top-500-Passwörter, und nicht 40 %, sondern lediglich 275.000 User (ca. 4,6 %) nutzten ein Top-100-Passwort.

Was lernen wir daraus? Erstens: Traue keiner Quelle, die du nicht selbst geprüft hast. Zweitens: Traue keiner Wahrscheinlichkeitsaussage, die du nicht selbst nachgerechnet hast. Drittens: Wechsle deine Passwörter. Denn moderne Cracker arbeiten mit Wörterbüchern aus „geleakten" Listen echter Passwörter, die sie durch Einfügung von Ziffern, Sonderzeichen und Zeichenersetzungen variieren. 10.000 Passwörter testet ein Cracker wie ophcrack in Millisekunden – da ist eine Trefferwahrscheinlichkeit von 31 % trotz allem ziemlich beängstigend.

Nebenschauplätze

Das Verwaltungsgericht Schleswig-Holstein hat in einem Beschluss vom 14.02.2013 die sofortige Anwendbarbeit eines Bescheides des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein gegen Facebook verneint. Das ULD hatte Facebook aufgefordert mit sofortiger Wirkung pseudonyme Nutzerkonten zuzulassen und gesperrte Konten wieder freizugeben.

Wesentlicher Streitpunkt der vorläufigen Entscheidung war die Zuständigkeit des ULD und die Anwendbarkeit des deutschen Datenschutz- und Telemediengesetzes. Maßgeblich ist hierfür, ob die deutsche Niederlassung von Facebook die personenbezogenen Daten, die bei der Account-Nutzung erzeugt werden, verarbeitet oder ob dies durch die irische Facebook Ltd. geschieht (§ 1 Abs. 5 BDSG, Art. 4 Abs. 1 DSRL). Ist keine von beiden Stellen verantwortlich, gilt das deutsche Recht gegenüber Facebook Inc. in den USA. Das Verwaltungsgericht hat – ohne weitere Begründung – angenommen, dass die irische Niederlassung verantwortlich ist, somit sei irisches Datenschutzrecht anwendbar. Bezüglich der deutschen Niederlassung wird festgestellt, dass diese offenkundig nur Akquise- und Marketingaufgaben wahrnimmt.

Die Urteilsbegründung beschränkt sich auf einen Verweis auf die Angabe von Facebook, warum die irische Niederlassung nach den Kriterien der Art. 29 Gruppe tatsächlich relevant für die Datenverarbeitung sei. Hätte dieses Vorgehen Bestand, wäre es außereuropäischen Unternehmen möglich, durch schlichte Erklärung der „Relevanz" einer Niederlassung sich den Staat mit der schwächsten oder säumigsten Harmonisierung des Datenschutzes auszuwählen. Das ULD hat bereits die Fortsetzung des Rechtsstreits angekündigt.

ZAP 2.0.0

Zur Untersuchung von Webanwendungen sind Webproxys ein unerlässliches Werkzeug. Am 30.01.2013 wurde Release 2.0.0 des im Rahmen eines OWASP-Projekts entwickelten Zed Attack Proxy (ZAP) veröffentlicht. In der neuen Version wurden beispielsweise der Spider durch einen AJAX-Spider ergänzt und eine Erkennung von Sessionzuständen eingeführt. Weitere Neuerungen betreffen die API zum ZED, die die Entwicklung von Add-Ons ermöglicht. Diese können aus dem laufenden ZAP heraus online bezogen werden. Zusammen mit der Funktionalität von aktiven Scans rückt der ZAP somit immer mehr in die Nähe von kommerziellen Webanwendungs-Scannern. Noch fehlt eine kontinuierliche Entwicklung und Veröffentlichung von Schwachstellenmustern unter Berücksichtigung gängiger Frameworks; kommerzielle Anbieter werden hier auf absehbare Zeit im Vorteil bleiben. Für einen schnellen Scan ist der ZAP jedoch allemal gut.

Nicht-Nadel im Nicht-Heuhaufen

H. D. Moore, Chief Security Officer von Rapid 7 und einer der Hauptentwickler des Metasploit Frameworks, hat im Januar einen Bericht zu den Schwachstellen im UPnP-Protokoll veröffentlicht. Schockierend ist daran nicht so sehr, dass UPnP unsicher ist oder unsicher eingesetzt wird, sondern die hohe Zahl der exponierten Systeme. Laut Studie haben 81 Mio. Systeme im Internet auf UPnP-Anfragen reagiert; 23 Mio. davon sind mutmaßlich anfällig für einen Angriff, bei dem beliebiger Code auf dem betroffenen System ausgeführt werden kann. Die Studie zeigt auch, dass eine Durchsuchung des Internet nach einer einzelnen Schwachstelle machbar ist – die Nadel im Heuhafen ist nicht mehr schwer zu finden. Gewöhnliche

Suchmaschinen wie Google oder Bing helfen dabei, massenhaft weitere Nadeln – verwundbare Systeme – aufzuspüren. So ließ sich in wenigen Minuten ein ungesicherter Drucker einer größeren Organisation identifizieren, der von jedermann über das Internet „ferngewartet" werden konnte.

Und es geht noch besser: SHODAN und Punkspider sind spezialisierte Suchmaschinen für online verfügbare Systeme und Dienste, die bestimmte Merkmale – wie z. B. Standard-Zugangsdaten oder Schwachstellen – aufweisen. Ein solches Angebot mag empören. Allerdings: wer sich nackt auf die Straße wagt, darf sich nicht über die daraus resultierende Aufmerksamkeit beschweren. Die Härtung von im Internet exponierten Geräten ist unerlässlich, will man Integrität und Verfügbarkeit der eigenen Netze und Systeme nicht gefährden.

TLS = Turn to Latest Standards

SSL, das seit Ende des letzten Jahrtausends eigentlich TLS heißt, ist seit 1995 ein praktisch unverzichtbarer Baustein der Netzwerksicherheit – ein großer Erfolg für die Schöpfer des Protokolls. Im Laufe der Jahre wurden jedoch zahlreiche Angriffe auf TLS entwickelt, die ein am 31.01.2013 veröffentlichtes Papier zusammenfasst. Wie aktuell das Thema ist, zeigt sich daran, dass nur wenige Tage später, am 04.02.2013 eine neue TLS-Attacke („Lucky 13„) bekannt wurde. Wie die 2011 publizierte BEAST-Attacke zielt Lucky 13 auf den CBC-Verschlüsselungsmodus häufig genutzter Cipher-Suites. Auch das BSI hatte Pech, dass Lucky 13 für die Empfehlungen zum sicheren Einsatz von TLS zu spät kam, die am 09.01.2013 als zweiter Teil der TR-02102 erschien. Obwohl TR-02102-2 über Kryptoverfahren hinaus geht und bspw. Angriffe gegen die TLS-Renegotiation berücksichtigt, fehlen wichtige Schutzmaßnahmen wie das Deaktivieren der TLS-Kompression gegen die 2012 veröffentlichte CRIME-Attacke. Eine gute Ergänzung ist daher die SSL/TLS-Best-Practice-Empfehlung des BSI an Unternehmen vom 16.01.2013.

Fast alle bekannten Attacken lassen sich bei Verwendung des seit August 2008 aktuellen TLS 1.2 (und dessen Updates) beherrschen. Nur wird diese Version noch viel zu selten genutzt. Immerhin ist ein Fallback auf das seit 1996 überholte SSL 2.0 seit März 2011 nicht mehr standardkonform. Höchste Zeit, dass Hersteller und Anwender auf den aktuellen Standard umsteigen.

Secorvo News

Schau mir in die Augen, Kleines

Schwächen und Grenzen einer Passwort-Authentifizierung werden spätestens bei der Eingabe eines 12stelligen, alpha-numerischen Passworts mit Sonderzeichen auf einem Tablet-Computer offenkundig. Alternativen sind überfällig - und umstritten. Kannte man biometrische Verfahren zur Authentifizierung früher nur aus Hollywoodfilmen wie „Mission Impossible", so werden neben Fingerabdruckscannern und automatischer Gesichtserkennung auch Retina-Scans bald zum Alltag gehören. Doch welche datenschutzrechtlichen Rahmenbedingungen gelten und welche Risiken birgt eine solche Methode? Diesen Fragen geht Friederike Schellhas-Mende (KIT, Zentrum für Angewandte Rechtswissenschaft) in ihrem Vortrag „Datenschutzkonformes Retina-Scanning" beim nächsten KA-IT-Si Event am **14.03.2013** nach. Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Gastgeber an diesem Abend ist das Fraunhofer IOSB in Karlsruhe, seit Anfang des Jahres Unterstützer der KA-IT-Si. Beginn ist um 18.00 Uhr. Wir freuen uns auf Ihre Anmeldung!

Security by Design

Wird Sicherheit von Anfang an bei der Konzeption eines Systems mitbedacht, lässt sie sich auch wirtschaftlich in hoher Qualität implementieren. Vor diesem Hintergrund hat Secorvo in Zusammenarbeit mit KIT und TeleTrusT das Qualifizierungszertifikat T.E.S.S. entwickelt. Mit der Schulung Security Engineering – Sichere Systeme durch Security by Design erwerben Sie die Zulassungsvoraussetzung für die T.E.S.S.-Prüfung. Nächster Termin: 23.-26.09.2013.

Am 15.-19.04.2013 bieten wir die erste diesjährige T.I.S.P.-Schulung an. Nutzen Sie die Möglichkeit, Ihre Qualifikation mit einem Feinschliff zu versehen und zertifizieren zu lassen. Weitere Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Zertifiziert

Am 03.02.2013 wurde das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz an die KomIT URS erteilt. Knapp zwei Jahre dauerte das von der CONNECT Karlsruhe vorbereitete Projekt von der Idee bis zum von Secorvo durchgeführten Audit. Der Aufwand hat sich nach Überzeugung von Frank Wondrak, Vorsitzender der Geschäftsführung KDRS/RZRS, gelohnt: Das Projekt habe konsequente Sicherheitsprozesse und ein durchgängiges, hohes Sicherheitsniveau erzwungen – wichtige Voraussetzung für den ordnungsgemäßen Betrieb und die Vertrauenswürdigkeit für die Kunden der kommunalen Datenverarbeitung.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2013	
05.-09.03.	CeBIT (Deutsche Messe, Hannover)
12.-14.03.	IMF 2013 (Fraunhofer IAO, Nürnberg)
14.03.	Schau' mir in die Augen, Kleines (KA-IT-Si, Karlsruhe)
12.-15.03.	Black Hat Europe 2013 (Blackhat, Amsterdam/NL)
April 2013	
09.-11.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
15.-19.04.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
17.-18.04.	a-i3/BSI Symposium 2013 (a-i3/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
24.-25.04.	BvD Verbandstag 2013 (BvD e.V., Berlin)
Mai 2013	
14.-16.05	13. Deutscher IT-Sicherheitskongress (BSI, Bonn)
14.05.	Forensik kompakt (Secorvo College, Karlsruhe)
15.-16.05.	14. Datenschutzkongress (EUROFORUM, Berlin)
26.-30.05.	Eurocrypt 2013 (IACR, Athen/GR)

Fundsache

Die vom BSI 2012 initiierte „Allianz für Cybersicherheit„ hat inzwischen zahlreiche Dokumente bereitgestellt, viele davon in einem offenen Download-Bereich. Die Dokumente reichen von Broschüren zur Management-Sensibilisierung (16.10.2012) über aktuelle Einschätzungen zur Sicherheitslage bis zu konkreten Konfigurationsempfehlungen (bspw. zu SSL/TLS, 16.01.2013).

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora (Editorial), Dr. Safuat Hamdy, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

März 2013



Cyber-Hype

Die IT-Sicherheit – pardon: Cyber-Sicherheit – ist *en vogue*. Kein Tag ohne spektakuläre Nachricht, keine Woche ohne Sicherheitsupdate. Sei es aus Überzeugung oder aus dem unverdrängbaren Bedürfnis, dem medialen Dauerbeschuss sichtbare Maßnahmen entgegenzusetzen, hat sich auch die Politik des Themas angenommen.

Wie bei vielen Hypes gehört es ab einem gewissen Punkt der unermüdlichen Wiederholung (siehe Catos „Ceterum censeo Carthaginem esse delendam!“) zum guten Ton, bei diesem Thema etwas vorweisen zu können. Mit dem Nationalen Plan zum Schutz der Informationsinfrastrukturen vom Juni 2005 richtete das BMI unter anderem ein Nationales IT-Lagezentrum im BSI ein – eine begrüßenswerte Einrichtung, sorgte sie doch dafür, dass die mit IT-Sicherheitsfragen befassten Behörden ihre Erkenntnisse austauschten und Aktivitäten koordinierten. Eine größere Schlagkraft bei reduziertem Aufwand wäre zu erwarten gewesen – aber der Hype nahm gerade erst Anlauf. Mit der Cyber-Sicherheitsstrategie des BMI vom Februar 2011 wurde die Zuständigkeit des BSI auf kritische Infrastrukturen ausgedehnt. Nun legt das BMI nach: Der Referentenentwurf zu einem „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ vom 05.03.2013 sieht neben einer Pflicht von Betreibern kritischer Infrastrukturen zur Auditierung und Meldung von Vorfällen die Schaffung von 100 Cyber-Sicherheits-Planstellen beim BSI vor. Da will der Bundesnachrichtendienst nicht zurückstehen: am 24.03.2013 wurde bekannt, dass der Aufbau einer Abteilung zur „Abwehr von Cyberangriffen“ mit bis zu 130 IT-Sicherheitsspezialisten geplant ist.

Bei allem Respekt vor der Wichtigkeit des Themas und dem Engagement der Beteiligten: Ab einem gewissen Punkt erzeugt die behördliche Beschäftigung mit Cyber-Sicherheit mehr Kosten als Nutzen. Denn jeder der knappen Spezialisten fehlt in den Unternehmen, und die Planstellen wollen erst verdient sein. Wirtschaftsminister Günter Rexrodt brachte es Mitte der 90er Jahre auf den Punkt: „Die Wirtschaft findet in der Wirtschaft statt.“ Und da gehört sie auch hin.



Inhalt

Cyber-Hype

Security News

TLS Workarounds

Aus bester Quelle

Hacker leben gefährlich

Harmlose Bestandsdaten

Datenschutzzertifikat

AppSec News

Secorvo News

Internet bleibt zertifiziert

Frühjahrsbildung

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

TLS Workarounds

Eine häufig empfohlene Übergangslösung zum Schutz gegen die in den SSN 02/2013 erwähnten BEAST- und Lucky 13-Angriffe gegen SSL/TLS ist, ältere Cipher Suites auf Basis der RC4-Chiffre zu nutzen – stets mit etwas schlechtem Gewissen, da RC4 in der Vergangenheit bereits Schwächen, bspw. in WEP, gezeigt hatte.

Wie berechtigt solche Skepsis war, erwies sich am 13.03.2013, als das „Lucky 13"-Forscherteam, verstärkt um Dan Bernstein, seine neuesten Erkenntnisse zu RC4 in TLS publizierte und nunmehr von dessen Gebrauch abrät. Damit gehen langsam die Übergangslösungen aus – der Umstieg auf TLS 1.2 mit AES-GCM-basierten Cipher Suites ist damit noch dringlicher als in den letzten SSN dargestellt.

Aus bester Quelle

Dass Code-Signaturen nicht die Abwesenheit von Schadcode sicher stellen, sondern – bestenfalls – die Herkunft der betreffenden Software, sollte mittlerweile Allgemeinwissen sein.

Und nicht immer müssen Malware-Autoren fremde Code-Signing-Schlüssel kompromittieren, um auch noch diese Spuren zu verwischen: Am 04.02.2013 wurde gemeldet, dass Malware-Autoren eine brasilianische Briefkastenfirma nutzten, um ein offizielles Code-Signing-Zertifikat zu kaufen, und am 21.02.2013 wurde bekannt, dass dazu auch die Daten einer nicht mehr existierenden französischen Autohandelsfirma reichen. Freiwillige haben im Netz inzwischen Informationen über mehr als Hundert zum Signieren von Malware genutzter Code-Signing-Zertifikate zusammengetragen. Und am 06.03.2013 berichtete Brian Krebs über den schwunghaften Handel mit Android-Entwickler-Accounts, unter deren Registrierung Malware-Apps im Google Play Store eingestellt werden können.

Es scheint leider so, als ob Mechanismen zur Sicherstellung der Herkunft von Software nur gegen Malware-Autoren helfen, die zu klamm sind, um sich bei Bedarf ein offizielles Zertifikat oder eine Registrierung zu kaufen – und nicht wissen, wie man mit fremden Kreditkartendaten bezahlt.

Hacker leben gefährlich

Am 15.03.2013 wurde das vom NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallin (Estland) bei einer internationalen Expertengruppe in Auftrag gegebene Tallin Manual on the International Law Applicable To Cyber Warfare in London der Öffentlichkeit vorgestellt. Das 270 Seiten starke Dokument ist das Ergebnis einer dreijährigen Untersuchung der Anwendbarkeit internationalen Rechts im Falle eines „Cyberkriegs".

Die 20 Autoren stellen 95 Regeln (*black letter rules*) auf, an denen sich die NATO-Staaten im Falle eines Cyberkriegs halten sollen. So sind grundsätzlich – wie auch in einem konventionellen Krieg – die Auswirkungen auf die Zivilbevölkerung zu begrenzen. Das gilt allerdings nicht für „Hacktivisten", die im Rahmen der Auseinandersetzung zu Angriffszielen werden können: "*Individuals who directly participate in hostilities lose their protection from attack*" (Rule 35). Dabei werden unter ‚Mitwirkung' auch vorbereitende Tätigkeiten verstanden, wie „*identifying vulnerabilities in a targeted system or designing malware in order to take advantage of particular vulnerabilities*" (S. 120).

Das sind keine besonders ermutigenden Aussichten für Schwachstellenfinder. Und man muss kein Hellseher sein, um zu erraten, gegen wen sich wohl ein „Cyber-Präventivschlag" richten dürfte.

Harmlose Bestandsdaten

Der Gesetzentwurf der Bundesregierung zur Änderung des Telekommunikationsgesetzes (TKG) und zur Neuregelung der Bestandsdatenauskunft vom 09.01.2013 hat am 21.03.2013 den Bundestag passiert. Eine Neufassung war notwendig geworden, da das Bundesverfassungsgericht mit Beschluss vom 24.01.2012 die entsprechende Regelung im TKG aufgrund einer Verfassungsbeschwerde von Patrick Breyer (auch bekannt durch sein Engagement im Arbeitskreis Vorratsdatenspeicherung) für verfassungswidrig erklärt hatte.

Tatsächlich bewegt sich die Neuregelung auf dünnem Eis, auch wenn im Bundesrat wenig Widerstand zu erwarten ist. Denn die Bestandsdatenauskunft unterliegt weit geringeren Hürden als eine Verkehrsdatenauskunft, welche ein Ermittlungsverfahren wegen einer schweren Straftat (§ 100a StPO) voraussetzt: bei Bestandsdaten genügt eine Ordnungswidrigkeit.

Mit der Neufassung werden jedoch einige bislang allgemein als Verkehrsdaten verstandene Daten – wie bspw. die dynamische IP-Adresse – zum Bestandsdatum umdefiniert und damit der hohen Zugangshürde entzogen.

Passiert das Gesetz den Bundesrat, will Patrick Breyer erneut vor das Bundesverfassungsgericht ziehen. Bleibt zu hoffen, dass die Verfassungsrichter sich vom TKG-Neusprech nicht blenden lassen.

Datenschutzzertifikat

Nach längerer Pause wird dem De-Mail-Projekt der Bundesregierung neue Aufmerksamkeit zuteil. So hat der Bundesbeauftragte für den Datenschutz am 04.03.2013 die De-Mail-Datenschutz-Zertifizierung von 1&1 bekannt gegeben, drei Tage nach Herausgabe einer Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten mittels De-Mail. Und seit dem 05.03.2013 liegt ein neuer Referentenentwurf zu einem E-Government-Gesetz vor, das De-Mail als Kommunikationsmittel der Verwaltung in einer prominenten Rolle sieht.

Da die gesetzliche Regelung eines Datenschutzaudits nach § 9a BDSG seit nunmehr 12 Jahren vergeblich auf Umsetzung wartet, wurde die Datenschutzzertifizierung der De-Mail-Diensteanbieter in § 18 Abs. 3 Nr. 4 De-Mail-Gesetz direkt dem Bundesbeauftragten für den Datenschutz zugewiesen. Der Kriterienkatalog der Zertifizierung geht erstaunlich weit in die Prüfung der datenschutzunabhängigen Anforderungen des De-Mail-Gesetzes. Von besonderem Interesse sind die Festlegung einer Löschfrist von sieben Tagen für die Speicherung der IP-Adressen der Nutzer zu Sicherheitszwecken, die Ausführungen zur datenschutzgerechten Helpdesk-Gestaltung und die Forderung nach Negativfeststellungen in der Datenschutzerklärung der Diensteanbieter.

Die Handreichung zum Gebrauch von De-Mail enthält wertvolle Hinweise zur Durchführung einer Schutzbedarfsanalyse für personenbezogene Daten, während die Frage, wann zusätzlich zur De-Mail-Verwendung eine Ende-zu-Ende-Verschlüsselung erforderlich ist, mangels De-Mail-Nutzer wohl vorerst eher akademischer Natur bleibt.

Das E-Government-Gesetz will zudem ermöglichen, die De-Mail neben der qualifizierten elektronischen Signatur zur Ersetzung der Schriftform einzusetzen. Ob dies der De-Mail zum erhofften Durchbruch verhelfen kann, darf bezweifelt werden. Schließlich ist De-Mail ein Übermittlungs- und Zustellungsverfahren – zur Ersetzung der Schriftform wurde De-Mail nicht konzipiert.

AppSec News

Das deutsche OWASP Chapter richtet in diesem Jahr in Hamburg vom 20.-23.08.2013 die Sicherheitskonferenz AppSec Research 2013 aus. Die ersten zwei Tage sind Trainingseinheiten zur Sicherheit von (Web-)Anwendungen gewidmet, die beiden folgenden Konferenztage in einen akademischen und einen industriellen Track strukturiert.

Für beide Tracks sind Einreichungen (Industry bis 14.04. und Research bis 15.05.2013) willkommen. Ein zusätzliches Bon-Bon ist die Vergabe freier Tickets für die Konferenz im Rahmen einer monatlichen Ticket-Challenge – in der eine versteckte Schwachstelle zu finden und ein Exploit einzureichen ist.

Secorvo News

Internet bleibt zertifiziert

In den SSN 04/2010 berichteten wir über die erfolgreiche Erstzertifizierung des DE-CIX nach ISO 27001 auf der Basis von IT-Grundschutz.

Drei Jahre später zahlte sich das kontinuierliche und konsequente Management der Informationssicherheit beim DE-CIX aus: Die Re-Zertifizierung wurde erfolgreich bestanden und das Zertifikat mit der Nummer BSI-IGZ-0139-2103 ausgestellt – damit wird Internet-Traffic mit Peaks von 2,5 TBit/s weiterhin zertifiziert sicher übertragen.

Alle Beteiligten konnten bestätigen, dass sich die Qualität des ISMS in den vergangenen drei Jahren noch einmal deutlich verbessert hat, während die Aufwände spürbar reduziert werden konnten. Der Security Officer des DE-CIX dazu: „Viele reden von integraler Sicherheit. Die Zertifizierung hat beim DE-CIX dafür gesorgt, dass wir sie konsequent leben."

Frühjahrsbildung

Noch sind einige wenige Plätze unserer drei April-Seminare zu haben: IT-Sicherheit heute vom 09.-11.04.2013, der T.I.S.P. vom 15.-19.04.2013 und PKI vom 23.-26.04.2013.

Zertifikate, die erworbene Fachkenntnisse und Berufserfahrung in der IT-Sicherheit nachweisen, gewinnen immer mehr an Bedeutung. Daher bieten wir inzwischen drei Zertifizierungen an, von deren Qualität wir überzeugt sind:

Der T.I.S.P. steht für mehrjährige Berufserfahrung und fundiertes Grundlagen- und Expertenwissen in den wichtigsten Themengebieten der Informationssicherheit. Der CPSSE belegt vertiefte Kenntnisse in der Entwicklung von Softwarelösungen mit definierten Sicherheitseigenschaften – durch eine geeignete Gestaltung des gesamten Softwareentwicklungsprozesses. Der T.E.S.S. weist Kenntnisse in „Security by Design" nach – der Integration von Sicherheit in den gesamten Produktentwicklungsprozess, von der Idee über die Konzeption bis zur Realisierung in Hard- oder Software.

Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2013	
09.-11.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
15.-19.04.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
16.-17.04.	Datenschutztage 2013 (FFD, Wiesbaden)
17.-18.04.	a-i3/BSI Symposium 2013 (a-i3/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
24.-25.04.	BvD Verbandstag 2013 (BvD e.V., Berlin)
Mai 2013	
14.-16.05	13. Deutscher IT-Sicherheitskongress (BSI, Bonn)
15.05.	Cloud – aber sicher! (KA-IT-Si, Karlsruhe)
15.-16.05.	14. Datenschutzkongress (EUROFORUM, Berlin)
26.-30.05.	Eurocrypt 2013 (IACR, Athen/GR)
Juni 2013	
03.-07.06.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
05.-07.06.	Entwicklertag 2013 (VKSI & ObjektForum, Karlsruhe)
10.-11.06.	Cybersecurity 2013 (Handelsblatt & EUROFORUM, Berlin)

Fundsache

Die NSA, deren Akronym lange mit „No Such Agency“ übersetzt wurde, hat die interne Zeitschrift „Cryptolog“ („*a new vehicle for the interchange of ideas on technical subjects in Operations*“) deklassifiziert und am 24.03.2013 die Ausgaben 1/1974 bis 4/1997 als pdf veröffentlicht. Auch wenn einige Stellen geschwärzt wurden: der Schülerzeitungscharme vor allem der frühen Ausgaben ließ sich nicht wegretuschieren.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2013



XP Forever

Der Support von Windows XP wird von Microsoft am 08.04.2014 eingestellt: Ab diesem Zeitpunkt werden keine neuen Sicherheitspatches mehr veröffentlicht. Bedeutet dies, dass damit ein Umstieg auf eine neuere Windows-Version unvermeidlich ist? Insbesondere im industriellen Umfeld findet man zahlreiche Anwendungen, die nicht einmal für neuere Windows-Systeme freigegeben sind – da kann ein Betriebssystemwechsel aufwändig und riskant sein.

Die Antwort ist ein entschiedenes „kommt darauf an". Unter bestimmten Voraussetzungen und durch geeignete Maßnahmen kann Windows XP mit ruhigem Gewissen weiter betrieben werden. Eine der wesentlichen Vorraussetzungen ist, dass seitens der Anwendungen kein Änderungsbedarf vorliegt. Schließlich kann nicht ausgeschlossen werden, dass bei einem Anwendungsupdate unbekannte Fehler oder Betriebssystemfeatures Probleme verursachen.

Die geeigneten Schutzmaßnahmen leiten sich aus den möglichen Angriffsflächen ab, die man abhängig von Risiko und Einsatzzweck betrachten sollte. Um Angriffe am System selbst zu erschweren, die etwaige lokale Schwachstellen ausnutzen, sollte der Zugang zum System geschützt werden. Schwieriger ist der Schutz vor netzbasierten Angriffen: Hier kann die Ausnutzung von möglichen Schwachstellen nur durch eine netzseitige Einschränkung der Kommunikation erschwert oder unterbunden werden. Konkret könnte dies durch die Bildung von isolierten Netzsegmenten realisiert werden oder durch die Vorschaltung von „Industrial Firewalls" zur Abschottung des Systems.

Restrisiken verbleiben, wenn Anwendungen erfordern, dass Dienste auf dem XP-System erreichbar sein müssen – bei Client-Betriebssystemen ist das aber nicht die Regel. Vor einem Wechsel lohnt jedenfalls eine kritische Analyse – denn nicht für jeden Einsatzzweck ist „neu" = „besser".



Inhalt

XP Forever

Security News

Orkan im Schnapsglas

Software ohne Sicherheitszertifikat

„Nicht kritisch" ...

Neue Auskunftsregeln

Verzweifelt ...

REMnux IV.

Secorvo News

Sommerbildung

Cloud, aber sicher!

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Orkan im Schnapsglas

Am 12.04.2013 hat die Deutsche Post per Presse-interview nach einjähriger Vorbereitungszeit ihren Ausstieg aus der De-Mail-Akkreditierung verkündet. Grund für den Ausstieg ist § 4 Abs. 2 Nr. 1, 3 De-Mail-Gesetz. Dieser legt fest, dass von dem Nutzer bei Eröffnung eines De-Mail-Kontos Name, Geburtsort, Geburtsdatum und Anschrift zu erheben sind, nachgewiesen u. a durch den amtlichen Ausweis. Die Post plante, hierfür ihr Postident-Verfahren einzusetzen, in dessen Rahmen – wohl mit Rücksicht auf die Aufzeichnungspflicht in § 8 Geldwäschegesetz – zusätzlich die Personalausweisnummer erhoben wird. Der Bundesdatenschutzbeauftragte versagte hierfür die Akkreditierung, da die Erhebung der Personalausweisnummer nach dem Gesetz für De-Mail – wie im übrigen, bisher unbeanstandet, auch nach Signaturgesetz und -verordnung sowie nach § 111 Abs. 1 TKG beim SIM-Karten Versand – nicht erforderlich und damit unzulässig ist.

Zeitgleich hat sie Beschwerde bei der EU-Kommission gegen das am 19.04.2013 vom Deutschen Bundestag verabschiedete (und noch nicht vom Bundesrat bestätigte) E-Government-Gesetz eingelegt, das die De-Mail als weiteren die Schriftform ersetzenden Kommunikationsweg zur öffentlichen Verwaltung vorsieht. Die Beschwerde sieht einen Verstoß gegen die Notifizierungspflicht und richtet sich gegen den indirekten Ausschluss des E-Postbriefs als Schriftformersatz gegenüber Behörden, der nur durch qualifizierte elektronische Signatur, De-Mail mit sicherer Anmeldung oder per Formular und eID des Personalausweises möglich ist.

Angesichts der geringen Verbreitung aller betroffenen Verfahren dürfte der reale Nachteil sich in Grenzen halten, zumal das E-Government-Gesetz eine Hintertür für sonstige sichere Verfahren lässt. Bemerkenswert ist allerdings die Kompromisslosigkeit, mit der die Deutsche Post erhebliche Investitionen an einer vergleichsweise leicht zu berücksichtigenden Datenschutz-Beanstandung scheitern lässt – da liegt der Verdacht nahe, dass es sich hier um einen Vorwand zum Gesichtsverlust freien Rückzug aus einem drohenden Kostengrab handelt.

Software ohne Sicherheitszertifikat

... ist die Überschrift eines am 16.04.2013 veröffentlichten Prüfungsergebnisses des Bundesrechnungshofes zum neuen Personalausweis und der zugehörigen AusweisApp. Darin wird besonders kritisiert, dass die verbindliche Zertifizierung der Software – mit 4,2 Mio. Euro Entwicklungskosten nicht gerade ein Schnäppchen – durch das BSI nicht bis Ende 2012 erfolgt ist. Seit zwei Jahren findet sich der „Bürgerclient“ auf der Liste laufender Zertifizierungen des BSI. Der Bundesrechnungshof verweist auf mögliche Haftungsrisiken für den Bürger aufgrund der fehlenden Bewertung der Gesamtsicherheit des nPA-Systems. Denkwürdig wird es im Abschnitt 1.3, in dem eine Stellungnahme des BMI paraphrasiert wird: „Es ergebe keinen Sinn, wenn der Hersteller, in diesem Fall das Bundesamt, sein selbst erstelltes Produkt anschließend zertifiziere. Da das Bundesamt die Software verteile, bekräftige es damit die ausreichende Sicherheit des Produkts.“

Offensichtlich hat das BMI die peinliche Panne beim Start der AusweisApp am 09.11.2010 (SSN 11/2010) erfolgreich verdrängt – keine 24 Stunden dauerte es bis zur Kompromittierung. Fehler passieren – aber man sollte doch wenigstens etwas daraus lernen.

„Nicht kritisch“ ...

... ist die Einstufung der Sicherheitslücke, die am 12.03.2013 im Microsoft Security Bulletin MS13-027 adressiert wurde. Damit kann es einem Angreifer durch Einstecken eines präparierten USB-Sticks gelingen, einen Rechner vollständig zu kompromittieren und administrative Rechte zu erlangen – auch wenn an dem Rechner kein Benutzer angemeldet ist. Daher empfehlen wir abweichend von der Einstufung von Microsoft dringend die Installation der entsprechenden Patches – auch an nicht vernetzten IT-Systemen. Betroffen von der Sicherheitslücke sind fast alle Microsoft-Betriebssysteme.

Neue Auskunftsregeln

Am 21.03.2013 hat der Bundestag das Gesetz zur Änderung des Telekommunikationsgesetztes (TKG) und zur Neuregelung der Bestandsdatenauskunft verabschiedet. Die Neuregelung war erforderlich geworden, nachdem das Bundesverfassungsgericht wesentliche Teile der Bestandsdatenauskunft nach § 113 TKG nur mit Auflagen und bis zum 30.06.2013 fortgelten ließ. Das Gesetz folgt den Vorgaben des Urteils, indem es die Auskunft vom Vorliegen weiterer Rechtsgrundlagen abhängig macht, die die anfragenden Behörden mitzuteilen haben.

Eine deutliche Festlegung der in Betracht kommenden Rechtsgrundlagen oder eine Eingrenzung der Voraussetzungen findet jedoch kaum statt. Der neu eingeführte § 100j StPO setzt lediglich die Erforderlichkeit zur Sachverhaltsklärung oder zur Bestimmung des Aufenthaltsortes eines Beschuldigten voraus. Bezüglich der Abfrage von Daten wie PINs oder Login-Informationen wird lediglich vorausgesetzt, dass eine Rechtsgrundlage zu deren Nutzung vorhanden sein muss, da ihre Abfrage sonst nicht erforderlich wäre.

Aussagen zu eben diesen Rechtsgrundlagen fehlen. Den Maßgaben des Bundesverfassungsgerichts mag durch die teilweise Abschrift der Urteilsbegründung Rechnung getragen worden sein. Eine Stärkung der Grundrechte der Betroffenen stellt diese Gesetzesreparatur sicher nicht dar.

Verzweifelt ...

... ist der Ton des „State of Software Security Report“ mit dem bezeichnenden Untertitel „*The Intractable Problem of Insecure Software*“, den das amerikanische Unternehmen Veracode am 08.04.2013 im fünften Jahr in Folge veröffentlicht hat. In der Einleitung werden klare Worte über den inakzeptablen Zustand der Sicherheit vieler Software-Produkte ausgesprochen. Die aktuellen Probleme werden auf 44 Seiten ausführlich dargestellt und bewertet.

Mancherorts ist die Nachricht bereits angekommen: In Zusammenarbeit mit der KA-IT-Si widmet der diesjährige Entwicklertag 2013 am 05.06.2013 diesem Thema einen eigenen Track.

REMnux IV.

Mit der Ubuntu-basierten Distribution REMnux V4 steht seit dem 09.04.2013 nach fast 15 Monaten eine gründlich aktualisierte und erweiterte Toolsammlung für die Malwareanalyse zur Verfügung.

Die kompakte Zusammenstellung und Konzentration auf das Wesentliche wurde beibehalten. Nun gibt es REMnux neben der bekannten Live CD auch als direkt einsatzfähige, virtuelle Appliance. Darin wurden die bisherigen Malwareanalysebereiche für Hauptspeicher, Netzwerk, Web und insbesondere PDF aktualisiert. Da die Analysetätigkeiten hauptsächlich auf der Terminalkommandozeile durchgeführt werden, wurde die Bash-Alias-Vorbelegung deutlich verbessert, so dass man nun sehr komfortabel und schnell mit dem Werkzeugkasten arbeiten kann. Für die Analyse von unbekannten Binärdateien wurden die Unterstützung für XOR (NoMoreXOR, brutexor, XORBruteForcer) und PE (pev, dism-this, ExeScan, udis86) deutlich ausgeweitet.

Eine besonders sinnvolle Ergänzung ist das am 19.03.2013 erschiene Werkzeug ProcDot von CERT.at, mit dem auf der Basis von Sysinternals ProcMon- und PCAP-Logdateien automatisiert eine graphische Zeitlinie erstellt werden kann. Das überarbeitete Cheat-Sheet ermöglicht am Reverse Engineering von Malware Interessierten einen Schnelleinstieg.

Secorvo News

Sommerbildung

So sicher, wie der Sommer kommt, steigen auch die Anforderungen im Bereich Informationssicherheit. Die Antwort darauf heißt kontinuierliche Weiterbildung. Zum Beispiel beim Schlagwort „Security by Design“: In unserem Seminar "Security Engineering" zeigen wir Ihnen Ende September, wie Sicherheit von Beginn an in Entwicklungsprozesse einbezogen werden kann, anstatt das Thema erst zum Schluss ‚aus der Schublade zu kramen'. Die Qualität steigt, ohne die Entwicklungskosten nach oben zu treiben. Schließlich können Sie Ihre Kenntnisse durch die Zertifikatsprüfung T.E.S.S. zertifizieren lassen.

Ihre Berufserfahrung und Ihr Know-How im Bereich Informationssicherheit können Sie in diesem Sommer gleich zu zwei Gelegenheiten bei Secorvo mit dem T.I.S.P.-Zertifikat krönen: Im Juni und im September bieten wir eine T.I.S.P.-Schulung mit nachfolgender unabhängiger T.I.S.P.-Prüfung an.

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Cloud, aber sicher!

Die Vorbehalte gegenüber der Nutzung von Clouddiensten sind insbesondere in Deutschland hoch. Dabei werden vor allem Sicherheitsbedenken als große Hürde genannt. Das vom Bundesministerium für Wirtschaft und Technologie geförderte Projekt ‚MimoSecco' (Middleware for Mobile and Secure Cloud Computing) will hier Abhilfe schaffen: Die Karlsruher Unternehmen CAS und WIBU-SYSTEMS entwickeln in Zusammenarbeit mit dem KIT (EISS, AIFB) eine Lösung, bei dem Nutzer von mobilem Cloud Computing die Kontrolle über ihre Daten behalten.

Das im Projekt entworfene und bisher umgesetzte Lösungskonzept stellt Daniel Eichhorn (WIBU-SYSTEMS AG) in seinem Vortrag beim nächsten KA-IT-Si-Event "Cloud, aber sicher!" am **15.05.2013** anlässlich der Cloudzone in der Messe Karlsruhe vor.

Das Event findet ausnahmsweise an einem *Mittwoch* statt und beginnt bereits um *17 Uhr*. Als KA-IT-Si-Teilnehmer haben Sie außerdem die Möglichkeit, die Messe vorab kostenfrei zu besuchen. Ein zusätzliches Schmankerl ist die Ausstellung mehrerer Exponate des Kryptologikum – spannend für alle, die an der Eröffnungsveranstaltung im Januar nicht teilnehmen konnten. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2013	
14.-16.05	13. Deutscher IT-Sicherheitskongress (BSI, Bonn)
15.05.	Cloud, aber sicher! (KA-IT-Si, Karlsruhe)
15.-16.05.	14. Datenschutzkongress (EUROFORUM, Berlin)
26.-30.05.	Eurocrypt 2013 (IACR, Athen/GR)
Juni 2013	
03.-07.06.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
05.-07.06.	Entwicklertag 2013 (VKSI & ObjektForum, Karlsruhe)
10.-11.06.	Cybersecurity 2013 (Handelsblatt & EUROFORUM, Berlin)
13.06.	Swiss Cyber Storm 4 (Swiss Cyber Storm Association, Luzern/CH)
17.-18.06.	DuD 2013 (COMPUTAS Gisela Geuhs GmbH, Berlin)
Juli 2013	
04.07.	5. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
08.-10.07.	IFIP Sec 2013 (IFIP, Auckland/NZ)

Fundsache

Knackige Fakten über den täglichen Gebrauch von Mobilgeräten präsentieren die am 04.04.2013 erschienenen „European Mobile Insights“, die anlässlich des Norton Cybercrime Reports 2012 ermittelt wurden. Dass zwei Drittel aller Nutzer von Smartphones oder Tablets ihr Gerät mit PIN oder Passwort schützen, klingt etwas optimistisch – dass einem Drittel schon einmal ein Gerät abhanden kam, eher beunruhigend.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Mai 2013



Im Überwachungsstaat

Am 15.05.2013 veröffentlichte eine interdisziplinäre Arbeitsgruppe der Deutschen Akademie der Technikwissenschaften (acatech) ein 36seitiges Positionspapier zur „Privatheit im Internet“. Neben der Neudefinition etablierter Begriffe („De-Kontextualisierung“ statt Zweckänderung und „Persistenz“ statt unzulässiger Speicherung) gibt das Papier Handlungsempfehlungen: Vermittlung einer „Kultur der Privatheit“ durch Bildung und Ausbildung, Eckpunkte für einen globalen Rechtsrahmen (wie informierter Einwilligung und der Möglichkeit zur Löschung und Befristung) und – schließlich sind die Autoren überwiegend Hochschullehrer – Geld für Forschung.

Wer die Wirklichkeit kennt, kann ob dieser bemühten Beschwörung eines „Kulturwandels“ durch Bildung, Gesetzgebung und Forschung nur den Kopf schütteln. Der Schutz personenbezogener Daten im Internet leidet weder unter einem Mangel an Regulierung oder Aufklärung noch unter zu wenig Verschlüsselung – sondern schlicht an einem dramatischen Umsetzungs- und Kontrolldefizit. Verstöße gegen geltendes Datenschutzrecht wie Webtracking, intransparente Datenschutzerklärungen oder unwirksame Einwilligungen sind so zahlreich wie augenfällig – und trotz wirksamer Instrumente zur Ahndung in der Regel ohne Konsequenzen für die Verantwortlichen. Daher leben wir bereits in einem Überwachungsstaat, der zumindest „ex post“ umfassende Persönlichkeitsanalysen erlaubt: Bewegungsprofile (Mobilfunk), Interessen (Webseitenbesuche, Recherchen), Käufe, Zahlungsverhalten und persönliche Kontakte (Social Networks). Davor schützen weder „Selbstdatenschutz“ noch Risikobewusstsein. Vielleicht hofften wir, dass die Datenmenge eine Analyse verhindert – dank „Big Data“ ist auch dieser Trost heute Makulatur.

Immerhin wirkt die Überwachung noch nicht „ex ante“. Doch es wird bereits mit Szenarien für Verhaltensprognosen experimentiert. Wenn wir es auch da zu einem Umsetzungsdefizit kommen lassen, ist die Fiktion von „Minority Report“ bald harte Realität.



Inhalt

Im Überwachungsstaat

Security News

Untergeschobene Straftat

Wer trackt mich da?

Cloud Computing Extreme

Update-Dschungel

Datenschutz bei Apple

Code-Erkenner

Secorvo News

5. Tag der IT-Sicherheit

Security by Design

Veranstaltungshinweise

Fundsachen

Security News

Untergeschobene Straftat

Nachdem das Bundeskriminalamt bereits im März vor einer neuen Variante der BKA-Ransomware gewarnt hat, die mit kinderpornographischem Material arbeitet, ist nun eine Variante im Umlauf, die kinderpornographische Fotos auf befallene Rechner lädt. Die Schadsoftware, die eine Rechnersperrung im Auftrag des BKA vortäuscht und zur (angeblichen) Wiederfreischaltung eine Geldüberweisung fordert, nutzt mit dieser jüngsten Variante die Bedrohung mit strafrechtlicher Verfolgung als zusätzliches Druckmittel.

Nach § 184b Abs. 4 Strafgesetzbuch (StGB) ist bereits der Besitz kinderpornographischer Darstellungen strafbar. Der Rechtsprechung genügt hierbei bereits ein bedingter Vorsatz, d. h. es reicht aus, dass Anhaltspunkte für den Besitz oder dessen Inkaufnahme vorliegen. Nach dieser Rechtslage bleibt den Betroffenen nur, ihre Datenträger sorgfältig auf von der Ransomware eingeschmuggeltes Material zu untersuchen und dieses unwiederbringlich zu löschen. Wer auf Nummer sicher gehen will, sollte den gesamten Datenträger vollständig überschreibend formatieren.

Auch die Übergabe der Datenträger an die Ermittlungsbehörden ist eine Option – verbleiben die Bilder jedoch nach Entfernung der Rechnersperrung auf dem Gerät, tritt unmittelbar die Strafbarkeit ein. Mit einer Weitergabe des Datenträgers an private Helfer kann zudem bereits der Straftatbestand des „einem anderen Verschaffens" erfüllt sein.

Im Unterschied zu bisherigen Ransomware-Varianten, die die Verfolgung verbreiteten Fehlverhaltens wie etwa Urheberrechtsverletzungen vortäuschten, setzt diese Variante das Opfer zusätzlich der Gefahr einer Strafverfolgung aus – zukünftig ein weiteres Problem der sicheren Tatsachenfeststellung bei forensischen Analysen und bei der Ahndung solcher Straftaten.

Wer trackt mich da?

Bekanntermaßen listen Datenschutzerklärungen auf Webseiten nur selten alle Datenweitergaben auf. Eine beeindruckende Visualisierung aller aktuellen Tracking-Verbindungen liefert das Firefox Browser-Plugin „Collusion" (Version 0.27 vom 28.03. 2013): Die Webtracker aller besuchten Seiten werden in einer dynamischen Grafik zusammengeführt. So werden die heimlichen „Datenkraken" des Netzes transparent: je größer der Netzknoten, desto mehr Verbindungen – und Daten über das Surfverhalten.

In den Händen einer Datenschutz-Aufsichtsbehörde ließe sich das Plugin unschwer zu einem Goldesel erweitern: Findet das Tool in der Datenschutzerklärung nicht alle verbundenen Domänen, könnte es automatisch einen Mahnbescheid drucken...

Cloud Computing Extreme

Schon seit einigen Jahren forscht IBM an Verfahren zur homomorphen Verschlüsselung. Derartige Verfahren würden es u. a. erlauben, Daten in der Cloud nicht bloß in verschlüsselter Form zu speichern, sondern auch verschlüsselt zu verarbeiten. Nur der Eigentümer der Daten könnte danach das (korrekte) Ergebnis einer Berechnung entschlüsseln.

Am 05.04.2013 gab eine Gruppe von IBM-Forschern die Software-Bibliothek HElib zur homomorphen Verschlüsselung als Open-Source Projekt frei. Ein praktischer Einsatz wird allerdings schnell an Grenzen stoßen: Momentan ist eine Berechnung auf verschlüsselten Daten ca. 100 Millionen Mal langsamer als die gleiche Berechnung auf dem Klartext. Dies ist jedoch ein ernst zu nehmender Fortschritt: Vor einem Jahr hätte die Berechnung noch einen um das Zehnfache höheren Aufwand erfordert.

Wer die Arbeitsweise solcher Kryptoverfahren besser verstehen will, muss nicht den Quellcode von HElib analysieren, sondern kann sich vergleichbare Algorithmen von der neuesten Version des Lernwerkzeugs CrypTool visualisieren lassen.

Update-Dschungel

Die Kennzahlen, die der IT-Sicherheitsdienstleister Secunia in seinem am 14.05.2013 veröffentlichten „Secunia Vulnerability Report 2013" präsentiert, sollten für IT-Verantwortliche Anlass sein, ihr derzeitiges Patch-Management kritisch zu prüfen: Der Report belegt, wie wichtig es ist, Sicherheitsschwachstellen bei *jeder* genutzten Software zu beobachten, sie zu bewerten und erforderlichenfalls darauf zu reagieren.

Zwar sind die Patch-Mechanismen der Hersteller in den vergangenen Jahren besser geworden. Dennoch bleibt die Herausforderung, viele Quellen im Blick zu behalten, wie der im April veröffentlichte „Secunia PSI Country Report – Q1 2013" an Zahlen für Deutschland belegt: Auf einem durchschnittlichen PC sind 75 verschiedene Programme installiert; davon stammt ca. 1/3 von Microsoft. Zwar wird Microsoft-Software in der Regel automatisch aktualisiert – allerdings betreffen 68% aller Schwachstellen Programme anderer Anbieter.

Daher muss ein PC schlimmstenfalls über bis zu 50 verschiedene Update-Mechanismen oder Quellen

aktuell gehalten werden – was zumindest im geschäftlichen Umfeld kaum manuell zu leisten ist.

Datenschutz bei Apple

Das Landgericht Berlin-Mitte hat die Apple Inc. Anlässlich einer Klage des Verbraucherzentrale Bundesverband e.V. (vzbv) am 30.4.2013 zur Unterlassung des Gebrauchs von weiten Teilen ihrer „Apple Datenschutzrichtlinie“ verurteilt.

Apple räumt sich in den beanstandeten Klauseln umfassende Verwendungsrechte an personenbezogenen Daten aus der Nutzung der Website, Bestellvorgängen oder der Verwendung von Apple Produkten ein. Das Landgericht sah in der Datenschutzrichtlinie durch die Einbeziehung in die Bestellvorgänge auf der Internet-Seite Allgemeine Geschäftsbedingungen und prüfte somit Datenschutzrecht nicht direkt, sondern unter dem Gesichtspunkt der unangemessenen Benachteiligung durch die Unvereinbarkeit der Bestimmungen mit wesentlichen Grundgedanken des Datenschutzgesetzes.

Beanstandet wurden vor allem die unterbliebene Differenzierung nach den Erhebungsvorgängen und den diesbezüglichen Rechtsgrundlagen sowie die Unbestimmtheit bei der Angabe, welche Daten zu welchen Zwecken verwendet werden – sofern überhaupt ein Zweck benannt wurde. Außerdem werde der Eindruck erweckt, dass der Nutzer unabwendbar in die Verwendung der Daten einwillige, teilweise sogar zu Lasten Dritter.

Bemerkenswert und im vorliegenden Kontext folgerichtig ist die Einordnung der Datenschutzrichtlinie, die ansonsten lediglich an § 13 Abs. 1 TMG gemessen würde, als AGB. Mit Apple hat sich ein weiteres Großunternehmen unter Berufung auf irisches Datenschutzrecht strengeren Vorgaben entziehen wollen, was auf diese Weise unterbunden wurde.

Die vorgenommenen Beanstandungen treffen in ähnlicher Weise eine Reihe weiterer App-Store und Shop-Anbieter, die sich bezüglich ihrer Datenverwendung wenig festlegen und eingrenzen. Sollte das Urteil rechtskräftig werden, dürften sich eine Reihe von Anbietern mit Unterlassungsansprüchen konfrontiert sehen.

Code-Erkenner

In Zeiten, in denen selbst Cyberwar-Trojaner Open-Source-Software enthalten, ist es für den Reverse Engineer, Qualitätsprüfer oder Forensiker hilfreich, schon vorab zu wissen, welche bereits bekannten Software-Bausteine ein zu untersuchender Binärcode beinhaltet.

Dies will die neue Code-Suchmaschine „Rendezvous“ erleichtern, die von Forschern in Cambridge am 14.05.2013 vorgestellt wurde. Eine Online-Demoversion kann bereits beliebige Linux Binaries (im x86/ELF Format) gegen eine große Liste bekannter Open-Source-Software abgleichen.

Secorvo News

5. Tag der IT-Sicherheit

Gemeinsam mit dem CyberForum e.V. und der IHK Karlsruhe und KASTEL veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **04.07.2013** den „5. Tag der IT-Sicherheit“. Beginn ist um 14.00 Uhr im Haus der Wirtschaft (Saal Baden) der IHK Karlsruhe.

Die diesjährige Keynote widmet sich der Sicherheit mobiler Geräte. Prof. Dr. Rainer Gerling, Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft, nimmt eine vergleichende Sicherheitsanalyse gängiger Handy-Betriebssysteme vor. Es folgen weitere praxisnahe Fachvorträge zu den Themen Cybersicherheit und Grundschutz (BSI), Umgang mit Sozialen Netwerken (Deutsche Bahn) und IT-Security Management Strategie (SAP). Gelegenheit zum fachlichen und persönlichen Erfahrungs- und Gedankenaustausch bieten die Networking-Pausen.

Nähere Informationen zum Programm und die Möglichkeit zur Online-Anmeldung finden Sie unter www.tag-der-it-sicherheit.de

Wir freuen uns auf Ihre Anmeldung!

Security by Design

Die wirksame und vorausschauende Implementierung von Sicherheit in komplexen Lösungen ist auch dann noch eine Herausforderung, wenn die Entwicklung sich konsequent an dem Prinzip „Security by Design“ orientiert – und erst recht, wenn Sicherheit erst im Laufe des Entwicklungsprozesses als zusätzliches „Feature“ angeflanscht wird.

Einen systematischen und vertieften Einstieg in „Security by Design“ bietet das von Secorvo entwickelte Seminar „Security Engineering – Sichere Systeme durch Security by Design“ vom 23.-26.09. 2013. Inzwischen kann die dort erworbene Qualifikation auch mit einem T.E.S.S.-Zertifikat nachgewiesen werden.

Die Möglichkeit zum Erwerb des T.I.S.P.-Zertifikats bietet Secorvo im Herbst 2013 gleich an zwei Terminen. Alle weiteren Seminartermine sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2013	
03.-07.06.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
05.-07.06.	Entwicklertag 2013 (VKSI & ObjektForum, Karlsruhe)
10.-11.06.	Cybersecurity 2013 (Handelsblatt & EUROFORUM, Berlin)
13.06.	Swiss Cyber Storm 4 (Swiss Cyber Storm Association, Luzern/CH)
17.-18.06.	DuD 2013 (COMPUTAS Gisela Geuhs GmbH, Berlin)
Juli 2013	
04.07.	5. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
08.-10.07.	IFIP Sec 2013 (IFIP, Auckland/NZ)
27.07.-01.08.	Blackhat USA 2013 (Blackhat, Las Vegas/US)

Fundsachen

Wie wirksam Antivirenschutz ist und wie gefährlich das Leben ohne, das zeigt der aktuelle „Microsoft Security Intelligence Report“ (SIR), Volume 14. Seit Juni 2006 werden in dem halbjährlichen Bericht Daten von Microsoft-Produkten und -Diensten analysiert – eine der umfassendsten Datenbasen der Windows-Welt.

Ein Bild sagt mehr als tausend Worte: Nach diesem Motto präsentiert das US-amerikanische Unternehmen ThreatMetrix wesentliche Gefährdungen und Schutzmaßnahmen für die mobile Arbeit in unsicheren Umgebungen in einer anschaulichen Infografik mit dem sprechenden Titel „Don't Lose Your Caffeine Buzz to Cybercrime“.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Sven Köhler

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2013



Überraschung?

Die Aufregung irritiert – als hätte das Editorial der SSN 5/2013 noch einer Bestätigung bedurft. Denn auch vor der Offenlegung von Prism waren die weit gehenden Berechtigungen der amerikanischen Sicherheitsbehörden bekannt; auch die Aufgaben der NSA sind lange kein Geheimnis mehr. Selbst die Mitwirkung der großen „Datensammler" kann man längst öffentlich nachlesen: So dokumentiert Google in seinem Transparenzbericht staatliche Auskunftsersuchen – auch die von US-Behörden.

Mehr noch: Die staatlichen Zugriffe sind vielleicht nicht nett, aber legitim. Denn selbstverständlich ist es eine der wichtigsten Aufgaben einer gesellschaftlichen Ordnung, deren Mitglieder vor inneren und äußeren Bedrohungen zu schützen – dem wird auch kaum jemand widersprechen. Sogar Zweifel an der Verhältnismäßigkeit der Zugriffe verlieren an Gewicht, wenn man auf die Zahlen sieht: 19.000 betroffene Facebook-Profile in sechs Monaten – das sind 0,0018 % der weltweit 1.060.627.980 Nutzerprofile (Stand Juni 2013).

Und wer einwendet, dass die amerikanischen doch weit von unseren deutschen Verhältnissen abweichen, der beweist Realitätsferne. Denn auch hierzulande haben Strafverfolgungsbehörden im Rahmen der Beweiserhebung Zugriff auf Daten – dank §§ 70, 95 StPO ganz ohne richterlichen Beschluss. Googles Transparenzbericht belegt, dass deutsche Behörden ein Fünftel der amerikanischen Anfragezahl beisteuern – fast im Verhältnis der Einwohnerzahlen.

Wer freimütig seine persönlichen Daten oder die seines Unternehmens auf ausländische Server kopiert, darf sich zumindest nicht wundern, wenn sie damit dem unkontrollierten Zugriff staatlicher Stellen preisgegeben sind. Dabei ist diese Preisgabe meist nicht zwingend: Manchmal spart sie Geld (wenigstens temporär oder theoretisch), und manchmal liefert sie einen (wenigstens gefühlten) Bequemlichkeitsgewinn. Und fast immer gibt es Alternativen – andere Anbieter oder auch technische Lösungen, die unerwünschte Zugriffe z. B. durch Verschlüsselung wirksam verhindern.



Inhalt

Überraschung?

Security News

Der Vergangenheit verpflichtet

GSTOOL 4.8

Auto-Ripper

10 Jahre Top 10

Der Zukunft zugewandt

LobbyPlag

Nachlese IPv6-Kongress

Secorvo News

IPv6-Whitepaper

5. Tag der IT-Sicherheit

T.I.S.P.-Zertifizierung

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Der Vergangenheit verpflichtet

Schon seit einiger Zeit hat Microsoft Mechanismen wie DEP und ASLR in Windows integriert, die dafür sorgen sollen, dass Schadcode, der über eine nicht gepatchte oder unbekannte Schwachstelle in eine Anwendung eingeschleust wurde, nicht ausgeführt wird. Leider werden diese Mechanismen eher selten genutzt, weil sie nicht nur Schadcode, sondern auch manche krude implementierte, aber legitime (Alt-) Software am Ablauf hindern.

Das *Enhanced Mitigation Experience Toolkit* (EMET) von Microsoft, dessen Version 4.0 am 17.06.2013 erschien, hilft aus dieser Zwickmühle, indem es erlaubt, diese Mechanismen nur für diejenigen Anwendungen zu aktivieren, die sie problemlos vertragen. Zusätzlich schlägt die neue Version Alarm, wenn populäre Webseiten wie Google unvermutet TLS-Zertifikate „unüblicher" Trustcenter, bspw. aus den Niederlanden oder der Türkei nutzen.

GSTOOL 4.8

Ein kleiner Schritt für das GSTOOL, aber ein gewaltiger Sprung in der Funktionalität für die Erstellung von IT-Sicherheitskonzepten nach IT-Grundschutz: Das am 07.06.2013 veröffentlichte Servicepack 3 zur Aktualisierung auf die Version 4.8 enthält neben Fehlerkorrekturen und der nun offiziell unterstützten Anbindung aktuellerer SQL-Server-Versionen die Möglichkeit, selbst definierte Bausteine inklusive ihrer Gefährdungen und Maßnahmen in eine andere GSTOOL-Datenbank zu importieren. Bausteine, die für einen IT-Verbund entwickelt wurden, können so weiter verwendet werden.

Das funktioniert an sich recht gut, allerdings wird man auf Konflikte beim Import nicht direkt hingewiesen, beispielsweise wenn eine benutzerdefinierte Maßnahmen-Nummer vor dem Import bereits vergeben war. In unseren Tests wurde dem Titel eine Tilde (~) vorangestellt, so dass man die Kollision zumindest entdecken kann.

Der Umstieg auf Version 4.8 und die Export-/Importfunktionen sollten gründlich getestet werden, zumal eine Rückportierung in Version 4.7 nicht einfach möglich ist. In Anbetracht des Duke Nukem-haften Entwicklungszyklus für Version 5.0 gehen wir davon aus, dass die mit dem aktuellen Servicepack um sehr nützliche Funktionen erweiterte Version 4.8 noch einige Zeit Bestand haben wird.

Auto-Ripper

Mit dem am 14.05.2013 veröffentlichten Wrapper-Skript auto_rip von Corey Harrell für den RegRipper 2.8 ist es nun sehr komfortabel möglich, die seit dem 29.04.2013 verfügbaren 285 RegRipper-Plugins entweder vollständig oder spezifisch nach Kategorien auszuführen. Die dabei verwendete Methodik leitet Kategorien aus einem Untersuchungsschritt (z. B. „Examine User Profiles") und zugehörigen forensischen Artefakten (z. B. extrahiert aus 18 zugeordneten Plugins) ab. Damit können z. B. zielgerichtet für ein Windows-Benutzerkonto alle Aktivitäten der Kategorie „*User Account File/Folder Access Activity*" untersucht werden.

Das Skript liefert unter Windows und Linux zuverlässige Ergebnisse (auch mit eigenen Plugins) und kann insbesondere für solche forensischen Analysen empfohlen werden, bei denen der Untersuchungsgegenstand konkret benannt und sehr eng eingegrenzt ist, da es die Erhebung nicht relevanter Informationen vermeidet.

10 Jahre Top 10

Happy Birthday OWASP Top 10! Am 12.06.2013 wurde pünktlich zum 10. Geburtstag Version 2013 der weithin anerkannten Übersicht über wesentliche Risiken für (Web-)Anwendungen veröffentlicht. Die Übersicht ist auch nach zehn Jahren noch ein wichtiges und aktuelles Awareness-Dokument, das eindrücklich relevante Gefährdungen dokumentiert. So sind auch diesmal die Änderungen zur Vorversion leider nicht gravierend, und es lohnt, die Hitliste an betroffene Führungskräfte und Entwickler weiterzugeben.

Wer aus erster Hand mehr über die Top 10 erfahren möchte, hat im August die Möglichkeit dazu: Auf der OWASP AppSec EU in Hamburg wird – neben vielen anderen spannenden Vorträgen – auch einer der Top 10-Autoren sprechen.

Der Zukunft zugewandt

Falls es noch eines weiteren Beweises bedarf, dass die Malware-„Industrie" stets mit der Zeit geht, dann belegen dies zwei Meldungen aus dem Juni: Am 03.06.2013 thematisierte das Blog der New York Times, dass der berüchtigte Online-Banking-Trojaner Zeus vermehrt über infektiöse URLs verbreitet wird, die auf populären Fan-Seiten in Facebook & Co. hinterlassen werden – E-Mails stoßen offenbar heutzutage entweder auf zu viel Misstrauen oder sind schlicht unpopulär geworden.

Und am 06.06.2013 wies ein Malware-Analytiker bei Kaspersky auf den bisher (mutmaßlich) ausgefeiltesten Trjoaner unter Android hin. Zwar muss der Anwender noch eine Spam-SMS – bald schon einen Facebook-Beitrag? – anklicken, damit sich die Malware installiert. Danach nutzt sie jedoch eine Lücke im Betriebssystem, um sich zu verbergen und vor

Entfernung zu schützen. Die Zeit, in der SMS bedenkenlos als „sicherer Kanal“ für TANs genutzt werden konnte, scheint sich rapide ihrem Ende zu nähern.

LobbyPlag

Transparenz in die Diskussion der europäischen Datenschutz-Grundverordnung bringt das am 06.06.2013 veröffentlichte Online-Projekt LobbyPlag 2.0 der Initiative europe-v-facebook.org: Über 3.100 systematisierte Änderungsvorschläge und eine Hitliste der zehn Datenschutz freundlichsten und unfreundlichsten Vorschläge mit einer Zuordnung zu den verantwortlichen Mitgliedern des EU-Parlaments finden sich darin.

Ernüchternd: In beiden „Top-10“-Listen steht ein deutscher Parlamentarier auf Platz eins, in der Negativ-Liste finden sich insgesamt zwei Deutsche. Nun ja, die nächste Europawahl kommt bestimmt.

Nachlese IPv6-Kongress

Am 06. und 07.06.2013 – genau ein Jahr nach dem IPv6 World Flag Day – fand bereits der fünfte IPv6-Kongress statt. Unter den zahlreichen Beiträgen rund um IPv6 gab es auch mehrere Vorträge zum Thema IPv6-Sicherheit. Herausragend war der gemeinsame Vortrag von Marc Heuse und Fernando Gont zum Thema Security Assessment von IPv6-Netzen. Dabei wurden ausgewählte Beispiele anhand der von den jeweiligen Autoren entwickelten Toolkits THC-IPv6 bzw. IPv6 Toolkit teilweise live vorgestellt. Es wurde nicht nur deutlich, dass die IPv6-Sicherheitseigenschaften gängiger Betriebssysteme und Firewalls namhafter Hersteller noch Verbesserungsbedarf aufweisen, sondern auch, wie nützlich der Einsatz der Toolkits ist, um sich dem Thema IPv6 (in Testnetzen!) ‚spielerisch' zu nähern.

Auch bei den Beiträgen zur Planung, Migration und betrieblichen Praxis war das Thema Sicherheit unterschwellig präsent. Neben der Gelegenheit, die eigenen Netze im Rahmen der Umstellung gründlich „aufzuräumen“, wurde mehrfach darauf hingewiesen, dass Unternehmen, die sich nicht ernsthaft mit IPv6 auseinandersetzen, eine bedeutende Entwicklung des Internets zu verschlafen drohen. Aufgrund des wachsenden Angebots durch Provider (auch an Endkunden) dürften die ersten Anfragen nach einer Erreichbarkeit über IPv6 nur noch eine Frage der Zeit sein.

Wer auch zukünftig (sicher) über das Internet erreichbar sein möchte, sollte sich bald mit IPv6 und den (sicherheits-) technischen Implikationen für die eigene Infrastruktur auseinandersetzen.

Secorvo News

IPv6-Whitepaper

Am 10.06.2013 ist das Secorvo White Paper „IPv6 - Die grundlegenden Funktionen, Bedrohungen und Maßnahmen“ (pdf, 65 Seiten) von Dr. Safuat Hamdy erschienen. Nach einer Einführung in die grundlegenden Eigenschaften von IPv6 werden protokollspezifische Bedrohungen, weitere Sicherheitsaspekte und mögliche Gegenmaßnahmen erläutert.

5. Tag der IT-Sicherheit

Bereits zum fünften Mal findet am **04.07.2013** der "Tag der IT-Sicherheit" statt, den die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) jährlich gemeinsam mit dem CyberForum e.V., der IHK Karlsruhe und KASTEL veranstaltet. Beginn ist um 14.00 Uhr im Haus der Wirtschaft (Saal Baden) der IHK Karlsruhe.

Im Rahmen der diesjährigen Keynote „Smartphone-Sicherheit“ nimmt Prof. Dr. Rainer Gerling, Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft, eine vergleichende Sicherheitsanalyse gängiger Handy-Betriebssysteme vor. Es folgen weitere praxisnahe Fachvorträge zu den Themen Cybersicherheit und Grundschutz (BSI), Umgang mit Sozialen Netwerken (Deutsche Bahn) und IT-Security Management Strategie (SAP).

Gelegenheit zum fachlichen und persönlichen Erfahrungsaustausch bietet die Networking-Pause mit kleiner Ausstellung. Detaillierte Informationen zum Programm und die Möglichkeit zur Online-Anmeldung finden Sie unter
www.tag-der-it-sicherheit.de

Wir freuen uns auf Ihre Anmeldung!

T.I.S.P.-Zertifizierung

Das T.I.S.P.-Zertifikat für Information Security Professionals entwickelt sich derzeit zu einer Standard-Qualifikation von IT-Sicherheitsexperten: erste Unternehmen erwarten von ihren Sicherheitsbeauftragten eine T.I.S.P.-Zertifizierung; allein im ersten Halbjahr 2013 wurden 60 Zertifikate erteilt.

In diesem Jahr bietet Secorvo noch zweimal die Möglichkeit zur Zertifizierung: vom **16.–20.09.2013** und vom **21.–25.10.2013**. Angemeldete Teilnehmer erhalten vorab das von Secorvo verfasste Begleitbuch zum T.I.S.P. – über 500 Seiten konzentriertes und aktuelles Wissen zur Informationssicherheit.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2013	
04.07.	5. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
08.-10.07.	IFIP Sec 2013 (IFIP, Auckland/NZ)
27.07.-01.08.	Blackhat USA 2013 (Blackhat, Las Vegas/US)
August 2013	
01.-04.08.	DEF CON 21 (DEFCON, Las Vegas/US)
04.-07.08.	13th Annual DFRWS Conference 2013 (DFRWS, Monterey/US)
14.-16.08.	22nd USENIX Security Symposium (USENIX, Washington/US)
18.-22.08.	Crypto 2013 (IACR, Santa Barbara/US)
20.-23.08.	OWASP AppSec Europe Research 2013 (OWASP Foundation, Hamburg)
26.08.	Sommerakademie 2013 (ULD Hamburg, Kiel)
September 2013	
16.-20.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
23.-26.09.	Security Engineering (Secorvo College, Karlsruhe)

Fundsache

Am 19.06.2013 publizierte das BSI eine vergleichende 163seitige Studie zur Sicherheit von fünf verbreiteten Content Management Systemen (CMS). Die Ergebnisse sind ernüchternd – und sollten bei betroffenen Unternehmen zu Maßnahmen führen.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2013



Vertrauen verspielt

Das Konstrukt ist sehr elegant. Lässt ein Unternehmen personenbezogene Daten seiner Kunden oder Mitarbeiter durch einen Dritten verarbeiten – Lettershop, CRM-Anbieter, Rechenzentrum oder IT-Dienstleister – wird dies als „Auftragsdatenverarbeitung“ geregelt: Die Verantwortung für den Schutz und die ausschließlich zweckbezogene Verarbeitung bleibt beim Unternehmen, der Auftragnehmer erhält konkrete vertragliche Weisungen, wie die Verarbeitung zu erfolgen hat, der Auftraggeber überzeugt sich davon, dass diese auch umgesetzt werden - und der Gesetzgeber behandelt die Verarbeitung so, als ob sie im Unternehmen verbleiben würde.

Kommt das nichteuropäische Ausland ins Spiel wird es kompliziert. Denn dort entspricht das Schutzniveau nicht überall dem der EU. Um das Konzept zu retten, wurden Ende des letzten Jahrtausends mit den USA die „Safe Harbor Principles“ vereinbart. Am 26.07.2000 von der EU-Kommission in Kraft gesetzt postulieren sie bei US-Unternehmen, die dieser Selbstverpflichtung beitreten, ein ausreichendes Datenschutzniveau.

Doch die eleganteste Konstruktion hilft nichts, wenn sie mit der Wirklichkeit wenig zu tun hat. Schon im April 2010 meldeten die Datenschutz-Aufsichtsbehörden Zweifel an und verpflichteten deutsche Unternehmen, die die Verarbeitung personenbezogener Daten an amerikanische Unternehmen auslagern, Nachweise für die Einhaltung der Grundsätze einzufordern.

Da die nach deutschem Recht unzulässige Datenweitergabe an Nachrichtendienste nun amtlich ist, haben die Aufsichtsbehörden der EU-Kommission eine Aufkündigung des Abkommens empfohlen (siehe ‚Unsicherer Hafen'). So schmerzlich das insbesondere für internationale Unternehmen sein dürfte: Es ist sehr zu hoffen, dass die EU diesmal Rückgrat zeigt – und die Persönlichkeitsrechte nicht auf demselben Altar opfert, auf dem sie bereits Flugpassagierdaten und Bankdaten (SWIFT) dem Großen Bruder dargebracht hat.



Inhalt

Vertrauen verspielt

Security News

Recht auf Verschlüsselung

Datenschutz abmahnfähig

Unsicherer Hafen

NTFS-Analysen

Secorvo News

Anti-Prism-Party

Expertenwissen

Rückblick 5. Tag der IT-Sicherheit

Wie ich lernte, Malware zu lieben

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Recht auf Verschlüsselung

Der BGH hat in einem Beschluss vom 26.02.2013 festgestellt, dass Behörden nicht verlangen können, dass Unternehmen interne Informationen mittels unverschlüsselter E-Mail an sie weitergeben. Die Behörde muss wenigstens alternative Kommunikationswege zulassen. Dabei komme es nicht darauf an, ob die Mitteilung tatsächlich Betriebs- oder Geschäftsgeheimnisse umfasst. Der BGH geht damit über ein Urteil des Brandenburgischen Oberlandesgerichts vom 11.09.2012 hinaus, das noch auf das Vorliegen von Geschäftsgeheimnissen abgestellt hatte.

Auch wenn das Urteil zunächst nur auf Behörden Anwendung findet, die eine ausschließlich elektronische Übermittlung von Informationen fordern, wertet es den Schutz elektronischer Kommunikation deutlich auf und trägt der Tatsache Rechnung, dass unverschlüsselte E-Mails keinen technischen oder organisatorischen Schutz vor unberechtigter Kenntnisnahme genießen.

Datenschutz abmahnfähig

Das OLG Hamburg hat in einem Urteil vom 27.06.2013 der datenschutzrechtlichen Informationspflicht aus § 13 Abs. 1 S. 1 TMG den Status einer das Marktverhalten regelnden Norm zugesprochen. Es widerspricht damit dem von Datenschützern kritisierten Urteil des KG Berlin vom 29.04.2011.

Bei § 13 Abs. 1 TMG handelt es sich um die Pflicht von Telemediendiensteanbietern, vor allem also Betreibern von Websites oder Apps, zu Beginn der Nutzung über Art, Umfang und Zwecke einer Verwendung personenbezogener Daten oder deren Verarbeitung außerhalb der Europäischen Union zu informieren, in der Regel in einer von jeder Seite aus erreichbaren Datenschutzerklärung.

Konsequenz des Urteils ist die Möglichkeit für Mitbewerber, Interessensverbände, Verbraucherschutzverbände sowie die Industrie- und Handelskammern, Unterlassungstäter nach § 8 Abs. 1 UWG wegen einer unlauteren Wettbewerbshandlung nach § 4 Nr. 11 UWG abzumahnen, wie es für Verletzungen der Impressumspflicht schon lange möglich ist.

Die Entscheidung stützt sich hauptsächlich auf die durch das KG Berlin vernachlässigten Erwägungsgründe der europäischen Datenschutzrichtlinie, die auch das Ziel der Wettbewerbergleichstellung als Begründung angeben.

Obgleich eine weitere Abmahnwelle aus überwiegend datenschutzfernen Interessen sicher nicht wünschenswert ist, dürfte das sich abzeichnende Risiko effektiver als das Bußgeld nach § 16 Abs. 2 Nr. 1 TMG zur Durchsetzung der Informationspflicht verhelfen und Bewegung in die hiermit verbundenen Fragen wie die Aufklärung über die Datenverarbeitung beim Einsatz von Webtracking-Tools oder die Datennutzung durch die Betreiber sozialer Netzwerke bringen.

Unsicherer Hafen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte als Konsequenz der umfassenden Kommunikationsüberwachung der NSA am 24.07.2013 von der EU-Kommission die Aussetzung des Safe-Harbor-Abkommens – der Selbstverpflichtung zahlreicher amerikanischer Unternehmen auf das europäische Datenschutzniveau. In der Liste des US-Handelsministeriums finden sich so klangvolle Namen wie Microsoft, Apple, Facebook, Google, Yahoo und AOL – hinreichend bekannt aus einschlägigen Veröffentlichungen zur Prism-Affäre. Ebenso soll die Anerkennung eines angemessenen Datenschutzniveaus auf Grundlage der EU-Standardvertragsklauseln mit Blick auf die USA eingestellt werden.

Die Konferenz sieht die Ausnahmeregelung des Safe Harbor-Abkommens für Maßnahmen zur nationalen Sicherheit oder auf Grundlage entsprechender Gesetze durch die verdachtsunabhängige, flächendeckende Überwachung als überschritten an. Die Vorgaben der Standardvertragsklauseln, die die Zusicherung enthalten, dass die jeweiligen nationalen Gesetze des Staates des Datenempfängers keine Regelungen enthalten, die den Datenschutz gravierend beeinträchtigen (Klausel 5 b), könnten ebenfalls unter den gegenwärtigen Bedingungen in den USA nicht eingehalten werden. Art. 4 des Kommissionsbeschlusses zu den Standardvertragsklauseln erlaubt den Aufsichtsbehörden unter diesen Umständen die Aussetzung.

Sollten sowohl das Safe-Harbor-Abkommen als auch die Standardvertragsklauseln als Möglichkeit zur Sicherung eines angemessenen Datenschutzniveaus wegfallen, würde ein großer Teil der derzeitigen Datenübermittlungen in die USA, bspw. im Rahmen der Cloud-Nutzung oder durch deutsch-amerikanische Unternehmensverbünde rechtswidrig. Betroffen sind von dieser Maßnahme allerdings nicht nur amerikanische Anbieter, sondern auch deutschen Unternehmen, die auf der Grundlage von Safe Harbor personenbezogene Daten übermitteln: sie handeln ordnungswidrig.

NTFS-Analysen

Mit der am 08.07.2013 veröffentlichten graphischen Oberfläche gnea von TZWorks lassen sich forensische Analysen von NTFS-Dateistrukturen sehr effizient durchzuführen. gnea baut auf den Werkzeugen ntfswalker und wisp auf und kann auch Skripte mit spezifischen Einstellungen und Filterparametern für eine vollautomatische Erhebung erzeugen.

Als statische Datenquellen können sowohl DD- und VMware-Images sowie extrahierte $MFT-Dateien genutzt werden. Sogar im laufenden Betrieb kann auf NTFS-Laufwerke zugegriffen werden – wichtig vor allem für die *in vivo*-Analyse von Servern.

Besonders empfiehlt sich gnea für die Hashwertprüfung von Dateiobjekten in NTFS-Dateisystemen, da ntfswalker die MD5- und SHA1-Hashwerte direkt und ohne Nutzung einer Windows-API errechnet – ein unschätzbarer Vorteil, wenn Schadsoftware im Spiel ist und nichts so ist wie es scheint.

Secorvo News

Anti-Prism-Party

Nach dem ungeplanten *Coming out* der US-Geheimdienste starren viele Nutzer wie das Kaninchen auf die Schlange. Dabei gibt es – wie Sie wissen – zahlreiche Schutzmaßnahmen, die ausländischen Nachrichtendiensten das Datensammeln wenigstens erschweren.

Um dieses Wissen allen zugänglich zu machen, die sich angesichts der aktuellen Nachrichten um den Schutz ihrer Daten sorgen, veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem Cyberforum und dem IT-Sicherheits-Kompetenzzentrum KASTEL am **05.09.2013** im Karlsruher Zentrum für Medientechnologie (ZKM) eine öffentliche Anti-Prism-Party. Zahlreiche Sicherheitsexperten werden erläutern, wie sich E-Mails und Festplatten verschlüsseln, Surfspuren vermeiden sowie Online-Banking und Filesharing sichern lassen. Schicken Sie Verwandte, Freunde und Bekannte! Beginn ist um 18 Uhr, der Eintritt ist frei. Für gute Stimmung sorgen die Curbside Prophets, bekannt von ihren Auftritten 2012 und 2013 auf Das Fest.

Informationen rund um die Anti-Prism-Party gibt es in den kommenden Wochen in einem wöchentlichen Newsletter und auf Twitter.

Expertenwissen

Die Quelle der meisten Sicherheitsschwachstellen findet sich im Entwicklungsprozess. Mit dem Prinzip „Security by Design“ soll das Übel an der Wurzel gepackt werden, um bereits bei der Konzeption und Implementierung von IT-Lösungen Sicherheitsziele wie Verfügbarkeit, Vertraulichkeit, Integrität und Datenschutz in Architektur und Umsetzung zu integrieren.

Wie „Security by Design“ bei der Systementwicklung wirksam umgesetzt werden kann, lernen Sie auf der Zertifikatsschulung "Security Engineering – Sichere Systeme durch Security by Design" vom 23.-26.09.2013, die Sie mit dem Zertifikat T.E.S.S. (TeleTrusT Engineer for Systems Security) abschließen können.

Vom 21.-25.10.2013 können Sie Ihr Expertenwissen und Ihre Berufserfahrung in Informationssicherheit mit der T.I.S.P.-Schulung und einem T.I.S.P.-Zertifikat krönen. Zur Vorbereitung erhalten Sie nach Ihrer Anmeldung das T.I.S.P.-Begleitbuch „Zentrale Bausteine der Informationssicherheit“.

Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Rückblick 5. Tag der IT-Sicherheit

Wer den wieder sehr gut besuchten 5. Tag der IT-Sicherheit bei der IHK Karlsruhe am **04.07.2013** verpasst hat, findet die Presseberichte und alle Vortragsunterlagen (zu den Themen Smartphone-Sicherheit, Cybersicherheit und Grundschutz, Umgang mit Sozialen Netwerken und IT-Security Management Strategie) ab sofort auf http://www.tag-der-it-sicherheit.de.

Wie ich lernte, Malware zu lieben

Seit Jahren nimmt die Verbreitung von Malware zu und täglich kommen neu Arten von Viren, Würmern und Trojanern hinzu. Bedingt durch das immer bessere Sicherheitsbewusstsein der Benutzer und bessere Erkennungsraten von Antivirensoftware ändert Malware ständig die Infektionswege.

Einen Einblick in die Arbeitsweise von moderner Malware gibt Dr. Matthias Schmidt (1&1 Internet AG) mit seinem Vortrag beim KA-IT-Si Event „Dr. Seltsam, oder wie ich lernte, Malware zu lieben“ am **19.09.2013** ab 18 Uhr im Panoramasaal der IHK Karlsruhe. Anhand praktischer Beispiele werden neue Infektionswege aufgezeigt und mobile Malware beleuchtet, die sprunghaft an Zuwachs gewinnt.

Im Anschluss an den Vortrag haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking".
Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2013	
01.-04.08.	DEF CON 21 (DEFCON, Las Vegas/US)
04.-07.08.	13th Annual DFRWS Conference 2013 (DFRWS, Monterey/US)
14.-16.08.	22nd USENIX Security Symposium (USENIX, Washington/US)
18.-22.08.	Crypto 2013 (IACR, Santa Barbara/US)
20.-23.08.	OWASP AppSec Europe Research 2013 (OWASP Foundation, Hamburg)
26.08.	Sommerakademie 2013 (ULD Hamburg, Kiel)
September 2013	
02.-06.09.	SecSE2013 (SINTEF, Regensburg)
05.09.	Anti-Prism-Party, (KA-IT-Si, ZKM Karlsruhe)
16.-20.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
17.-18.09.	D A CH Security (GI/OCG/BITKOM/TeleTrusT, Nürnberg)
19.09.	Dr. Seltsam, oder wie ich lernte, Malware zu lieben (KA-IT-Si, IHK Karlsruhe)
23.-26.09.	Security Engineering (Secorvo College, Karlsruhe)

Fundsache

Am 13.03.2013 veröffentlichte der BITKOM den Leitfaden „Sicheres Cloud Computing". Das eine oder andere klang schon im März befremdlich: „... wer Cloud Computing nutze, verliere die Kontrolle über seine Daten. Diese Befürchtungen sind unberechtigt." Angesichts der jüngsten Erkenntnisse ist eine Überarbeitung nun dringend anzuraten...



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Michael Knopp, Jochen Schlichting.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2013



Macht und Missbrauch

Die Geschichte lehrt dauernd,
aber sie findet keine Schüler.

Ingeborg Bachmann (1926-1973)

Wird Menschen Macht verliehen, so ist dies – sofern man jedem Menschen eine unverletzliche Würde zugesteht – immer zugleich mit der Übertragung großer Verantwortung verbunden. In der Praxis neigen Menschen mit Macht allerdings dazu, deren Wirkungsbereich auszudehnen – und missbrauchen sie nicht selten, wenn auch häufig mit vermeintlich besten Absichten.

Schon früh haben die Staatstheoretiker der Aufklärung erkannt, dass Machtmissbrauch institutionell verhindert werden muss. „Checks and Balances", wie Baron de Montesquieu (1689-1755) sie 1748 in seinem fundamentalen Werk „De L'esprit des Loix" (Vom Geist der Gesetze) forderte, wurden daher zur konstitutionellen Basis moderner Verfassungsstaaten: Gewaltenteilung, Verfassungsgerichte, Untersuchungsausschüsse oder mehrere am Gesetzgebungsprozess beteiligte Kammern (Bundesrat/Bundestag) sind Ausfluss dieses Prinzips.

Aber Machtmissbrauch findet auch im (vermeintlich) Kleinen statt, wenn Kontrollen versagen: Die Erniedrigungen in US-Gefängnissen im Irak entsprangen derselben Geisteshaltung wie die Überwachung der UN und von Ehepartnern durch NSA-Mitarbeiter mit Hilfe von Prism: dem Verlust des Respekts vor der Würde des Anderen und dem Irrglauben, dass verliehene Macht über geltende Regeln erhebt.

Fehlen Kontrollen vollständig und kann man nicht auf die Hilfe Dritter hoffen, bleibt Betroffenen häufig nur der Selbstschutz. Das gilt auch für ein Internet, das zunehmend zu einer – in neuem Sinn „gesetzlosen" – Überwachungsinfrastruktur degeneriert. Wer es bisher eher vertrauensselig nutze, sollte spätestens jetzt beginnen, sich aktiv um den Schutz seiner Daten und Metadaten zu kümmern.

Wie das geht, zeigen wir in diesen SSN – und am 05.09.2013 auf der größten Verschlüsselungsparty Süddeutschlands im Karlsruher ZKM.



Inhalt

Macht und Missbrauch

Security News

Kommunikationsdatenschutz

Kommunikationskanalschutz

Verbindungsdatenschutz

Metadatenschutz

Clouddatenschutz

Zugangsdatenschutz

Secorvo News

Karlsruhe schützt sich selbst

Wie ich lernte, Malware zu lieben

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Kommunikationsdatenschutz

Wer seine Kommunikationsinhalte im Internet vor Dritten schützen will, sollte nach dem TNO-Prinzip ("*Trust No One*!") agieren. In der Praxis bedeutet das den Einsatz von Werkzeugen, die eine Ende-zu-Ende-Verschlüsselung unter Verwendung von als sicher geltenden kryptografischen Verfahren bieten. In der Praxis ist das jedoch oft nicht ganz einfach – vor allem Laien sind daher leicht überfordert.

Dennoch gibt es zahlreiche Lösungen. So stehen seit vielen Jahren mit GnuPG und S/MIME standardisierte, sogar kostenlose Schutzmechanismen für die Verschlüsselung von E-Mails zur Verfügung, die in vielen E-Mail-Clients standardmäßig integriert oder durch Plugins leicht ergänzt werden können. Eine Schritt-für-Schritt-Anleitung bietet zum Beispiel das Unabhängige Landeszentrum für Datenschutz (ULD) in Schleswig-Holstein.

Sogar für Webmail-Lösungen gibt es Javascript basierte Werkzeuge zur Verschlüsselung mit GnuPG wie GPG Javascript Plugins, Mailvelope oder WebPG. Allerdings ist der Einsatz von Javascript Encryption nicht unumstritten – zumindest sollten dafür verbreitete und durch viele Experten getestete Bibliotheken wie bspw. die Stanford Javascript Crypto Library eingesetzt werden.

Aber auch für die inzwischen weit verbreiteten *Instant Messaging*-Dienste wie WhatsApp, Google Chat, iMessage oder Facebook Messaging (sowie weitere Jabber/XMPP basierte Dienste) gibt es Schutzmöglichkeiten. Zum einen lassen sich durch das Off-the-Record-Protokoll (OTR) XMPP-basierte Chats durch Plugins oder den Einsatz von Clients mit direkter OTR-Unterstützung absichern.

Eine sichere Alternative zu asynchronen Messaging Diensten auf iPhone oder Android-Handies bietet die Software Threema. Die App sorgt für eine Ende-zu-Ende-Verschlüsselung unter Verwendung der offenen Krypto-Bibliothek NaCl – ein gutes Beispiel, denn hier wurden kryptografische Verfahren nicht selbst implementiert (was in der Praxis meist dazu führt, dass der Hersteller über zahlreiche Fallstricke stolpert).

Kommunikationskanalschutz

Zur Absicherung von Kommunikationskanälen im Internet hat sich SSL/TLS durchgesetzt. Web-Angebote sollten heute anbieterseitig bestmöglich mit SSL/TLS geschützt werden; umgekehrt sollte jeder Nutzer darauf achten, diese Protokolle (mit starken kryptografischen Verfahren) zu nutzen.

Für die Web-Browser Firefox und Chrome gibt es beispielsweise das nützliche Plugin HTTPS Everywhere, das automatisch für einen bestmöglichen Schutz durch SSL/TLS sorgt. Aber auch beim Zugriff des E-Mail-Clients auf das Postfach sollte die Nutzung von SSL/TLS selbstverständlich sein – dazu müssen im Client die entsprechenden Protokolle (IMAP4/TLS oder POP3/TLS, SMTP/TLS) und Ports (993 oder 995, 465) ausgewählt werden.

Bei der Nutzung von SSL/TLS sollte man zudem auf die Verwendung von „Perfect Forward Secrecy“ (PFS) achten. Dabei handeln Client und Server für jede Verbindung einen neuen symmetrischen Schlüssel aus, der von beiden Seiten nach Verbindungsende gelöscht wird und den ein Angreifer aufgrund des Verfahrens zur Aushandlung auch nicht später gewinnen kann. PFS erfordert die Verwendung einer Ciphersuite, die „Ephemeral Diffie-Hellman“ (TLS-DHE oder TLS-ECDHA) verwendet – spezifiziert bereits im Januar 1999 in TLS 1.0 (RFC 2246).

Als Achillesferse von SSL/TLS hat sich in den vergangenen Jahren der Umgang mit Zertifikaten erwiesen – nur wenn Nutzer sich auf deren Authentizität verlassen können ist der Aufbau vertrauenswürdiger verschlüsselter Kommunikationskanäle mit SSL/TLS möglich.

Verbindungsdatenschutz

Der Schutz von bei der Nutzung von Webdiensten anfallenden Verbindungsdaten erfordert die Verwendung von Anonymisierungsdiensten wie Tor, I2P, JAP oder spezieller VPN-Lösungen. Dabei wird durch kryptografische Verfahren und hintereinander geschaltete Server verschleiert, welche Endsysteme eine Kommunikationsverbindung nutzen. Zum gleichzeitigen Schutz der Kommunikationsinhalten sollten Anonymisierungsdienste grundsätzlich zusammen mit Ende-zu-Ende-Verschlüsselungslösungen eingesetzt werden.

Zu beachten ist allerdings, dass Sender und Empfänger nur auf Netzwerkebene anonymisiert werden – gibt der Browser (über die Metadaten) oder der Benutzer selbst in der Anwendung seine Identität preis, ist der Dienst nutzlos.

Metadatenschutz

Beim Surfen im Internet fallen – neben den Verbindungsdaten - viele weitere Metadaten, wie z. B. die besuchte Webseite, der verwendete Browser oder die Verweildauer an, auch bei der Nutzung von Anonymisierungsdiensten. Die Auswertung dieser Metadaten wird auch als *Tracking* bezeichnet. Wer sich ein Bild davon verschaffen möchte, welche Daten er mit einem einfachen Webseitenaufruf an wen übermittelt, sollte sich mal bei Panopticlick der *Electronic Frontier Foundation* (EFF) umsehen oder das Firefox-Plugin Collusion installieren.

Das Verwischen von Spuren beim Surfen ist heute eine echte Sisyphos-Arbeit. Eine gute Hilfestellung liefern dabei die Anregungen des „*Surveillance Self-Defense-Project*“ der EFF. Ein gewisses Maß an Kontrolle über die versendeten Metadaten behält man durch eine kontrollierte Verwaltung der Cookies, eine selektive Steuerung von Javascript und die eingeschränkte Übermittlung weiterer Daten mit Hilfe geeigneter Plugins wie z. B. NoScript, CookieManager oder RefControl.

Clouddatenschutz

Der beste Schutz von Daten in der Cloud ist – die eigene Cloud. Diesem Credo folgt das Projekt mit dem sprechenden Namen ownCloud: Es ermöglicht die Installation einer eigenen Cloud zur Speicherung von Daten oder zur Synchronisation von Kalenderdaten.

Alternativ sollte man bei der Verwendung fremder Cloud-Dienste seine Daten grundsätzlich verschlüsseln. Die Verschlüsselung muss dazu auf dem Client stattfinden, und auch nur der Client sollte sich im Besitz der notwendigen Schlüssel befinden („*Trust No One*“). Ein Werkzeug, das einen solchen Ansatz realisiert, ist BoxCryptor, das plattformübergreifend für verbreitete Cloud-Anbieter zur Verfügung steht.

Statt dessen kann man auch verschlüsselte Datencontainer in der Cloud ablegen. Dieses Verfahren erlaubt zwar kein so komfortables Arbeiten, bietet aber ein hohes Schutzniveau. Das freie Programm TrueCrypt ermöglicht die Anlage und Nutzung solcher Datencontainer – nicht nur in der Cloud, sondern auch auf der eigenen Festplatte, dem USB-Stick oder als sicherer Backup-Container.

Zugangsdatenschutz

Zu guter Letzt bleibt noch die Absicherung der Zugangsdaten – vulgo: Passworte – zu genutzten Web-Diensten. Angesichts der heute verfügbaren Werkzeuge und Rechenkapazität zum Knacken von Passwörtern sind vor allem zwei Dinge wichtig: Passwörter müssen eine hohe Qualität besitzen und sollten auf keinen Fall mehrfach verwendet werden. Die daraus erwachsenden Anforderungen an Passwörter und den Umgang damit können Menschen kaum noch leisten.

Abhilfe bieten „Passwort-Tresore“, die diese mit kryptografischen Mitteln absichern. Ein Beispiel hierfür ist die *Open Source*-Lösung KeePass, die auch plattformübergreifend verfügbar ist. Für Passwörter von Webdiensten empfiehlt sich die Nutzung von PwdHash zur Ableitung von Passwörtern in Abhängigkeit von der besuchten URL aus einem Master-Passwort – dieser Ansatz schützt zugleich vor Phishing.

Secorvo News

Karlsruhe schützt sich selbst

Ganz gleich ob elektronische Nachrichten, Internet-Recherchen oder Einträge in Sozialen Netzwerken: stehen die Server im Ausland, bedienen sich, wie wir nun wissen, nationale Geheimdienste nach Bedarf an den Datensammlungen.

Diesen Zugriffen muss man nicht tatenlos zusehen, denn viele der Daten müssten gar nicht erst anfallen. Schließlich gibt es Schutzmechanismen zuhauf – und viele davon sogar kostenlos. Häufig scheitert der Selbstschutz aber an unzureichenden Kenntnissen der Nutzer oder der (vermeintlichen) Komplexität der Hilfsprogramme.

Um diesem Mangel abzuhelfen lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL), dem CyberForum und dem ZKM | Zentrum für Kunst und Medientechnologie (ZKM) zur ersten Karlsruher "Anti-Prism-Party" am **05.09.2013** ab 18 Uhr ins ZKM ein (Eintritt frei).

Dort werden Karlsruher IT-Sicherheitsexperten vorführen, wie leicht man sich schützen kann – von der Verschlüsselung von E-Mails bis zum anonymen Surfen im Web ist für jeden etwas dabei. Für die musikalische Untermalung der größten Verschlüsselungsparty Süddeutschlands sorgen ab 20.00 Uhr die vom Karlsruher FEST bekannten Curbside Prophets.

Wie ich lernte, Malware zu lieben

Die Verbreitung von Malware nimmt stetig zu und täglich kommen neue Arten von Viren, Würmern und Trojanern hinzu. Auch die Infektionswege ändern sich ständig – auch aufgrund des immer besseren Sicherheitsbewusstseins der Benutzer und der besseren Erkennungsraten und größeren Verbreitung von Antivirensoftware.

Dr. Matthias Schmidt (1&1 Internet AG) gibt mit seinem Vortrag „Dr. Seltsam, oder wie ich lernte, Malware zu lieben“ beim nächsten KA-IT-Si-Event am **19.09.2013** ab 18 Uhr im Panoramasaal der IHK Karlsruhe einen Einblick in die Arbeitsweise von moderner Malware. Anhand praktischer Beispiele werden neue Infektionswege aufgezeigt und mobile Malware beleuchtet, die sprunghaft an Zuwachs gewinnt.

Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2013	
02.-06.09.	SecSE 2013 (SINTEF, Regensburg)
05.09.	Anti-Prism-Party, (KA-IT-Si, ZKM Karlsruhe)
16.-20.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
17.-18.09.	D A CH Security (GI/OCG/BITKOM/TeleTrusT, Nürnberg)
19.09.	Dr. Seltsam, oder wie ich lernte, Malware zu lieben (KA-IT-Si, IHK Karlsruhe)
23.-26.09.	Security Engineering (Secorvo College, Karlsruhe)
Oktober 2013	
01.10.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
08.-10.10.	it-sa 2013 (NürnbergMesse GmbH, Nürnberg)
14.-16.10.	13. IDACON (WEKA-Akademie, Würzburg)
14.-17.10.	CPSSE-Schulung (Secorvo College, Karlsruhe)
21.-25.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
22.-23.10.	ISSE 2013 (TeleTrusT e.V./eema, Brüssel)
25.-27.10.	FIfF Jahrestagung 2013 (FifF e.V., Siegen)

Fundsache

In einem seiner jüngsten Essays, publiziert am 23.08.2013 in Forbes, beschäftigt sich Bruce Schneier mit unserer Risikoaversion. Sein Fazit: Maßnahmen zum Schutz vor von Menschen ausgehenden Risiken verfehlen meist das Ziel – weil Menschen sich anpassen. Gelegentlich verursacht die Schutzmaßnahme selbst sogar höhere Schäden.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2013



Lasst euch nicht verwursten!

Freiheit ist ein kompliziertes Ding. Als „Abwesenheit von Zwang“ ist sie schlicht utopisch – der Begrenztheit von Ressourcen und der Endlichkeit des Lebens können sich Menschen nun einmal nicht entziehen. Auch gesellschaftlich stößt sie an Grenzen, und das nicht erst in der Freiheit des Anderen – Beschränkungen sind sogar essentielle Voraussetzung für reale Freiheit: Die Festlegung und Durchsetzung von Regeln definiert erst die Räume, in denen Freiheit stattfinden kann. Diese Freiräume wiederum sind vor ihrer Abschaffung zu schützen. Daher setzt das Grundgesetz – aus bitterer Erfahrung – in Art. 20 auch Regierung und Gesetzgebung klare Grenzen.

Umfang und Eingriffstiefe der Freiheitsbeschränkungen sind politisch umstritten: Wie viel soziale Umverteilung, Gängelung und Kontrolle müssen dem Souverän zugemutet werden, um seine Freiheit wirksam zu schützen? Unstreitig aber ist, dass Freiheit zentrale Voraussetzung ist für die persönliche Entfaltung (Art. 2 GG) – und allein diesem Zweck müssen Maßnahmen zur Erhaltung der inneren und äußeren Sicherheit in einer freiheitlichen Gesellschaftsordnung dienen. Sicherheit darf nie zum Selbstzweck werden, sondern ist ein (zweifellos wichtiger) Beitrag zur Freiheitsermöglichung.

Die schleichende Mutation des Internet zu einer Überwachungsinfrastruktur – durch Tracking, Profiling und den Zugriff von Sicherheitsbehörden – ist dabei, den offenbar noch immer unterschätzten Beitrag des Internet zur Entwicklung der Menschheit zu ersticken. Wer mit Brockhaus, Bibliothek und Bundesbahn aufgewachsen ist, der weiß, dass Wissen nie leichter zugänglich, Transparenz von Wirtschaft, Wissenschaft und Politik nie größer und die ortsübergreifende Zusammenarbeit von Menschen nie leichter war als heute. Wer diese Freiheit will, sollte sich dafür einsetzen. Mindestens durch Selbstdatenschutz. Einer der unsterblichen Cartoons F. K. Waechters (1937-2005) bringt es auf den Punkt: „Wenn ihr Schiss habt vor der Freiheit geht zurück in euren Stinkstall und lasst Euch verwursten!“



Inhalt

Lasst euch nicht verwursten!

Security News

Zwiebel gegen Riesen

4get RC4

Protest gegen PRISM

Schutz vor Safträubern

Unerwünschte Werbung

Highlights der AppSecEU

Secorvo News

Rückblick

Verstärkung

Ausblick

Wer hat, der hat.

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Zwiebel gegen Riesen

Staatliche Sicherheitsdienste wie die NSA scheinen mit juristischen Hebeln, viel Geld und Mittelsmännern jedermanns Privatsphäre über deren Spuren im Internet überwachbar machen zu wollen. Der NSA kommt dabei zugute, dass viele Internetriesen wie Google oder Facebook in den USA firmieren. Auch freie Projekte, wie der Anonymisierungsdienst TOR stehen im Fokus. Am 08.09.2013 zeigte die brasilianische Fernsehshow „Fantastico" NSA-Enthüllungsfolien, die suggerieren, dass TOR-Nutzer nicht völlig anonym sind. Nutzer älterer TOR-Versionen sind dabei wegen vermuteter Krypto-Schwächen besonders gefährdet. Auch könnte die NSA eigene TOR-Knoten betreiben. Jüngere wissenschaftliche Arbeiten zur Anonymität zeigen, dass die Nutzer-Anonymität auch durch die Auswertung von TOR-Datenströmen bedroht sein kann.

Wer Wert auf seine Privatsphäre legt, sollte sich daher nicht allein auf Anonymisierungsdienste verlassen, sondern sich bemühen, möglichst wenig Spuren zu hinterlassen (z. B. durch den Verzicht auf die Nutzung vor allem ausländischer Sozialer Netzwerke und die Sperrung von Tracking-Diensten im Browser) und seine Datenverbindungen wirksam verschlüsseln.

4get RC4

Den Veröffentlichungen vom 05.09.2013 zufolge kann die NSA einen großen Teil des (SSL-)verschlüsselten Datenverkehrs lesen. Details zu den betroffenen Verfahren, Protokollen oder Schlüssellängen wurden nicht publiziert, daher kann selbst der Experte Bruce Schneier, der über Hintergrund-Informationen verfügt, die Risiken nur spekulativ abwägen.

Eine plausible Spekulation ist, dass die NSA die RC4-Chiffre entschlüsseln kann, die zumindest beim Einsatz in WEP nachweislich gebrochen ist. Anwender, die diese Befürchtung teilen, können in Firefox, Chrome oder Internet Explorer die RC4-basierten SSL/TLS Cipher-Suites deaktivieren. Gegen BEAST und ähnliche Attacken, derentwegen RC4 von vielen SSL/TLS-Servern angeboten wird, gibt es andere Abhilfe, speziell auf Browser-Seite. Auch der am 24.09.2013 veröffentlichte Entwurf der neuen NIST Guidelines zu TLS (siehe Fundsache) sieht, anders als die am 13.03.2013 zurückgezogene Vorgängerversion, keine Nutzung des RC4 mehr vor.

Protest gegen PRISM

Am 05.09.2013 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Beschluss zu den Berichten über die Telekommunikationsüberwachung durch ausländische Nachrichtendienste gefasst. Der Beschluss fordert die deutschen und europäischen Regierungs- und Legislativorgane auf, im nationalen und internationalen Recht einen umfassenden Schutz der Privatsphäre zu verankern. Verfassungswidrige Kooperationen deutscher Dienste seien aufzuklären und ggf. abzustellen. Es sei weiter zu prüfen, ob eine Begrenzung des Routings von europäischen TK-Verbindungen auf Netze innerhalb der EU möglich sei. Die anonymen Nutungsmöglichkeiten von Telekommunikationsangeboten seien auszubauen.

Angesichts der Überwachung seien Fluggastdatenabkommen und Überwachungsprogramm auf den Prüfstand zu stellen und völkerrechtliche Abkommen zum Datenschutz zu schließen oder Handel von einem ausreichenden Datenschutz abhängig zu machen. Im Gegensatz noch zu einer Presseerklärung vom Juli (SSN 7/2013) wird jedoch keine Aussetzung des Safe Harbor Abkommens oder der Anwendung Europäischer Standardvertragsklauseln gefordert. Insgesamt vermittelt die Entschließung eher den Eindruck von Hilflosigkeit.

Schutz vor Safträubern

Mobile Geräte sind – vor allem unterwegs – äußerst praktische Helfer. Wäre da nicht das Problem der Stromversorgung: Wer transportiert schon gerne Ersatz-Akku und Ladekabel in der Jackentasche. Praktisch, dass auf Konferenzen, Bahnhöfen usw. immer häufiger öffentliche Ladestationen zu finden sind. Doch Vorsicht: Schon auf der DEF CON 2011 warnte der IT-Sicherheitsexperte Brian Markus vor „Juice Jacking", dem Diebstahl von Daten während des Aufladens mobiler Geräte. Möglich wird dies, weil die Geräte meist ein USB-Kabel zum ‚Stromtanken' verwenden. Dabei werden fast immer auch Daten übertragen, denn die höhere Stromstärke ermöglicht ein schnelleres Laden. Übrigens funktioniert Juice Jacking auch ‚rückwärts' – ein manipuliertes Smartphone kann während des USB-Ladevorgangs auch auf die Daten des Strom spendenden Rechners zugreifen.

Schutz bietet das USBCondom des IT-Sicherheitsexperten Stephen A. Ridley, das dieser am 12.09.2013 per Twitter ankündigte. Der Adapter schleift nur Strom führende Anschlüsse durch, sodass keine Daten abgegriffen werden können. Wer viel unterwegs ist, sollte die Anschaffung des Adapters für 10 US$ erwägen.

Unerwünschte Werbung

Nach Verzicht des Bundesrats auf die Anrufung des Vermittlungsausschusses vom 20.09.2013 kann das

Gesetz gegen unseriöse Geschäftspraktiken in Kraft treten. Das Gesetz bringt Verschärfungen im Bereich der unerlaubten Werbung und Einschränkungen für die Abmahnungspraxis im Bereich des Urheberrechts.

Durch das Gesetz werden zunächst die Regelungen für unerwünschte Werbung durch eine Ergänzung der Definition der unzumutbaren Belästigung um die fehlende Kenntlichmachung von Werbung nach § 6 Abs. 1 TMG verschärft. Entscheidender ist jedoch die Verschärfung des möglichen Bußgeldes von 50.000 auf 300.000 Euro. Zur Begrenzung des Missbrauchs von Abmahnungen im Urheberrecht werden aus dem bislang weitgehend wirkungslosen § 97a UrhG die unbestimmten Rechtsbegriffe weitgehend gestrichen. Für private Nutzer werden die Abmahnkosten durch Festsetzung eines fiktiven Streitwertes (wie bereits beim ersten Gesetzentwurf geplant) auf etwa 100 Euro begrenzt. Außerdem wird der so genannte ‚fliegende Gerichtsstand' für Privatpersonen abgeschafft. Private Urheberrechtsverletzer müssen nun an ihrem Wohnsitz verklagt werden. Ausuferungen bei der Abmahnung von Urheberrechtsverletzungen wird hierdurch ein ernst gemeinter Riegel vorgeschoben.

Highlights der AppSecEU

Auf der mit über 400 Teilnehmern sehr gut besuchten OWASP AppSec Research 2013 EU in Hamburg (20.08.-23.08.2013) hielten Angela Sasse und Thomas Roessler wegweisende Keynotes. Angela Sasse setzte sich intensiv mit dem Spannungsfeld zwischen Security und Usability auseinander und gab zahlreiche Denkanstöße. Thomas Roessler zeigte die Herausforderungen auf, die mit der Einbindung von immer mehr Endgeräten ins WWW und dem Übergang von traditionellen Webanwendungen hin zu Rich-Client-Applications im Browser einhergehen: „Good-bye Web Security, welcome Web Application Security". Die Vorträge sind als Präsentationen und als Videos verfügbar.

Secorvo News

Rückblick

Wer die größte Verschlüsselungsparty Deutschlands am 05.09.2013 im ZKM Karlsruhe mit mehr als 600 Besuchern verpasst hat, darf sich auf die „zweite Staffel" freuen: Wegen der großen Nachfrage gibt es Anfang 2014 eine inhaltlich erweiterte Neuauflage – „Anti-Prism-Party 2.0". Bis dahin entschädigen vielleicht die Handouts und Anleitungen zu den vorgestellten Schutzmechanismen sowie die Zusammenstellung hilfreicher Links.

Verstärkung

Seit August 2013 verstärkt der Datenschutz-Experte Christoph Schäfer das Secorvo-Team. Er ist Wirtschaftsrechtler und GDD-zertifizierter Datenschützer mit über fünf Jahren intensiver praktischer Erfahrung als externer und interner Datenschutzbeauftragter.

Ausblick

Der ständigen Weiterentwicklung des Themas IT-Sicherheit trägt das Seminar IT-Sicherheit heute mit der Behandlung aktueller Fragestellungen Rechnung, das Secorvo College vom **12.-14.11.2013** anbietet. Hier erfahren Sie das Wesentliche über die aktuellen Entwicklungen und Bedrohungen, und lernen Best Practice-Vorgehensweisen kennen, mit denen Sie Ihr Unternehmen effizient schützen können.

Auf die wichtigste Ursache von Sicherheitslücken, nämlich fehlerhafte Software, zielt die Zertifikatsschulung CPSSE (**14.-17.10.2013**). Das Seminar vermittelt die Grundlagen der sicheren Software-Entwicklung; mit der Zertifikatsprüfung belegen Sie Ihre Qualifikation als *Certified Professional for Secure Software Engineering*.

Für alle Spezialisten, die sich mit Verschlüsselungsinfrastrukturen – auch als *Public Key Infrastructure* (PKI) bezeichnet – beschäftigen, ist unser Seminar PKI am **19.-22.11.2013** ein besonderer ‚Leckerbissen'. Von Konzeption über Aufbau und Betrieb vermittelt das Seminar für jede Fragestellung sowohl die wesentlichen theoretischen und praktischen Grundlagen als auch einen reichen Erfahrungsschatz aus 15 Jahren PKI-Projektarbeit.

Alle Termine und Seminarangebote – auch bereits für 2014 - sowie die Möglichkeit zur Online-Anmeldung finden Sie unter
http://www.secorvo.de/college

Wer hat, der hat.

Eher außerhalb des Wahrnehmungsbereichs der IT-Security bleibt in vielen Unternehmen das „Software Asset Management". Dabei lauern auch hier zahlreiche Gefährdungen. „SAM für Kenner" ist daher das Thema des nächsten KA-IT-Si Events am **07.11.2013** um 18 Uhr im Raum TelemaxX des CyberForum e.V. in Karlsruhe. Marcel Lepkojis (CONNECT Karlsruhe GmbH) wird in seinem Vortrag Sicherheitsaspekte des Software Asset Managements vorstellen und Schutzmaßnahmen empfehlen. Anschließend haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim Buffet-Networking.

Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2013	
08.-10.10.	it-sa 2013 (NürnbergMesse GmbH, Nürnberg)
14.-16.10.	13. IDACON (WEKA-Akademie, Würzburg)
14.-17.10.	CPSSE-Schulung (Secorvo College, Karlsruhe)
22.-23.10.	ISSE 2013 (TeleTrusT e.V./eema, Brüssel)
November 2013	
07.11.	Wer hat, der hat. (KA-IT-Si, Karlsruhe)
12.-14.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
13.-15.11.	37. DAFTA (GDD, Köln)
14.-15.11.	Smart Energy 2013 (Fachhochschule Dortmund)
14.11.	Future IT-Kongress 2013 (AppSphere AG, Ettlingen)
18.-21.11.	OWASP AppSec USA 2013 (OWASP Foundation, New York)
19.-22.11.	PKI (Secorvo College, Karlsruhe)
21.-22.11.	DeepSec ISDC 2013 (DeepSec GmbH, Wien)

Fundsache

Das NIST hat am 24.09.2013 den 64seitigen Draft einer Neufassung der Special Publication 800-52 zur Auswahl und Konfiguration von SSL/TLS-Implementierungen veröffentlicht. Auch wenn mancher angesichts der Verflechtungen von NIST und NSA die Guidelines mit Vorsicht genießen wird, spiegeln sie doch den State-of-the-Art (soweit öffentlich bekannt) wider. Obendrein gibt der Anhang einen Überblick über die Ansätze zur Überwindung der anderen Misere von SSL/TLS: dubiosen Trustcentern und fragwürdigen Serverzertifikaten (vgl. u. a. SSN 09/2011).

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Sven Köhler, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Oktober 2013



Die Waffen der Freunde

Die Enthüllungen Edward Snowdens über die nachrichtendienstliche Tätigkeit unserer Verbündeten lassen uns mit dem unguten Gefühl des Ausgeliefertseins zurück. Dabei gerät in der Diskussion um die Legitimität solchen Handelns leicht ein wichtiger Aspekt aus dem Blick, der eine nähere Betrachtung verdient.

Es steht außer Frage, dass ein Nachrichtendienst mit ausreichenden personellen, finanziellen und gesetzlichen Möglichkeiten fast jede Information gewinnen kann. IT-Sicherheitsmaßnahmen können das erschweren, aber nicht verhindern, denn es gibt wirksame klassische nachrichtendienstliche Mittel (Observation, Infiltration), die ohne Informationstechnik zum Ziel führen.

Bedeutsamer als die Frage des ‚Ob' ist hingegen die Frage des ‚Wie'. Denn die Wahl des nachrichtendienstlichen Mittels kann in einer Informationsgesellschaft weit reichende Konsequenzen haben. Entschlüsselt ein Nachrichtendienst eine kryptierte Nachricht mit Hilfe geballter Rechenleistung, ist das folgenlos für Dritte. Etwas gänzlich anderes ist es allerdings, wenn ein Nachrichtendienst von Herstellern Hintertüren in Soft- oder Hardware einbauen lässt, Einfluss auf die Standardisierung von Kryptosystemen nimmt (wie beispielsweise die Wahl Elliptischer Kurven) oder Zufallszahlengeneratoren manipuliert. In diese Kategorie gehören auch „TKÜ-Schnittstellen", die deutsche TK-Provider für das unbeobachtete Mitschneiden von Kommunikationsinhalten durch Bedarfsträger bereithalten müssen. Alle Maßnahmen dieser Art haben einen gefährlichen Seiteneffekt: Sie schaffen verborgene Angriffspunkte. Damit untergraben sie die Sicherheit der IT-Infrastruktur einer ganzen Gesellschaft.

Angesichts der wachsenden Bedeutung von IT-Infrastrukturen für moderne Gesellschaften gehören nachrichtendienstliche Mittel, die solche unverantwortlichen Kollateralschäden verursachen, völkerrechtlich geächtet. Neben dem Atomwaffensperrvertrag, der Biowaffen- und der Chemiewaffenkonvention benötigen wir daher eine UN-Cyberwaffenkonvention, die den Einbau von Backdoors in Standards, Algorithmen, Programme und Hardware unterbindet.



Inhalt

Die Waffen der Freunde

Security News

EU-Datenschutzreform

ISO 2700{1,2} runderneuert

EU-Krypto-Empfehlungen

Web of the Living Dead

Nichtflüchtiger Speicher

Fingerabdrücke auf Reisen

Heimlich, still und leise ...

Secorvo News

Auf dem Laufenden

Wer hat, der hat.

Die Zukunft ist mobil

Veranstaltungshinweise

secorvo
security consulting

Security News

EU-Datenschutzreform

Mit einer beeindruckenden Zustimmung von fast 93 % hat der Innenausschuss des EU-Parlaments am 21.10.2013 den konsolidierten Entwurf der EU-Datenschutzgrundverordnung angenommen. Nun geht der Verordnungsentwurf in die Verhandlung mit EU-Rat und EU-Kommission.

Neben der Neuregelung der Bestellungspflicht eines Datenschutzbeauftragten, die für alle Firmen gelten soll, die Daten von mehr als 5.000 Betroffenen verarbeiten, ist vor allem die geplante Bußgeldhöhe beachtlich: Bis zu 100 Mio. Euro respektive 5 % des Jahresumsatzes sollen künftig als Bußgeld verhängt werden können.

Als Folge der NSA-Enthüllungen ist auch die so genannte Anti-FISA-Klausel (*Foreign Intelligence Surveillance Act*) wieder enthalten, die auf Druck der USA entfernt worden war. Sie regelt, dass europäische Unternehmen private Daten von EU-Bürgern nur dann an Drittstaaten (außerhalb der EU) weitergeben dürfen, wenn es hierfür eine eindeutige gesetzliche Grundlage in Europa gibt. Zudem soll Profiling ausdrücklich unter den Einwilligungsvorbehalt des Betroffenen gestellt werden. Schließlich ist die Einführung einer neuen EU-Datenschutzaufsicht vorgesehen.

Nicht alles aus dem Entwurf wird nach den Verhandlungen mit den Mitgliedstaaten und der EU-Kommission übrig bleiben. Der ehrgeizige Plan ist jedoch, die Verhandlungen bis Mai 2014 zum Abschluss zu bringen. Damit könnte die EU-Datenschutzreform noch vor der Europawahl Gesetzeskraft erlangen.

ISO 2700{1,2} runderneuert

Am 04.10.2013 hat die ISO nach acht Jahren eine runderneuerte Version des ISMS-Standards ISO 27001 veröffentlicht. Durch die Überarbeitung wurde der ISO/IEC 27001:2013 an andere Managementstandards angeglichen. Zudem wurden viele Anpassungswünsche aus den vergangenen Jahren berücksichtigt, so dass nun an vielen Stellen des Standards klarere Begrifflichkeiten verwendet werden als in der Vorgängerversion. Augenfällig ist der Verzicht auf den *Plan-Do-Check-Act*-Zyklus: Dabei ist das Prinzip nicht verschwunden, wird jedoch nicht mehr explizit erwähnt – die Grundidee liegt dem Standard weiterhin zu Grunde.

Gleichzeitig mit dem ISO 27001 wurde ein deutlich veränderter ISO/IEC 27002:2013 veröffentlicht. Die neue Version des ISO 27002 empfiehlt einen Satz von 114 *Controls*, aufgeteilt auf 35 *Control Objectives*. An vielen Stellen wurde offensichtlich aufgeräumt, allerdings ist die neue Ordnung nicht immer intuitiv. So fragt man sich z. B., warum der Abschnitt ‚*Mobile devices and teleworking*' unter ‚*Organization of information security*' angesiedelt wurde. Eine Hilfestellung bei der Einarbeitung in die Neuauflage der beiden Standards bietet der „Transition Guide" des britischen BSI.

EU-Krypto-Empfehlungen

Am 29.10.2013 hat die Enisa eine Empfehlung zu Kryptoalgorithmen, Schlüssellängen und Krypto-Protokollen veröffentlicht. An dem 96seitigen Report wirkten namhafte europäische Kryptologen wie Vincent Rijmen (Autor des AES), Arjen Lenstra und Christoph Paar mit. Zwar hätte die 27seitige Literaturübersicht z. B. zu Gunsten eines Hinweises auf *Perfect Forward Secrecy* bei TLS etwas kürzer ausfallen dürfen. Aber in Verbindung mit der Übersicht von Damien Giry zu den gängigen Schlüssellängen-Empfehlungen und den in den SSN 9/2013 vorgestellten NIST-Empfehlungen zu TLS vom 24.09.2013 bietet das Dokument eine gute Übersicht über die derzeit als sicher geltenden Kryptoverfahren und die zu empfehlende Parametrisierung.

Web of the Living Dead

Am 14.10.2013 publizierte der Forscher Georg Lukas seine Hintergrund-Analyse der Default-Präferenz schwacher SSL/TLS-Cipher-Suites in neuen Android-Versionen. Die Tatsache an sich ist noch kein Beinbruch. Bei näherem Hinsehen zeigt sich aber exemplarisch, wie es durch (vorgeschobene?) Anforderungen nach (Rückwärts-)Kompatibilität und die nicht hinterfragte Übernahme veralteter Vorgaben dazu kommen kann, dass die Sicherheitskonfiguration aktueller Systeme einen seit zehn Jahren überholten Stand der Technik widerspiegelt.

Drei Lehren lassen sich daraus ziehen: Erstens dürfen Anwendungsentwickler in Sicherheitsbelangen nicht blind davon ausgehen, dass das genutzte System oder Framework „es schon richtig macht". Zweitens: Es gibt für Nachrichtendienste – gerade bei Open-Source-Software – subtilere Methoden als Hintertüren einzubauen: Sorge dafür, dass es neben dem richtigen noch einen „unverzichtbaren" alternativen Weg gibt, Sicherheit zu konfigurieren – und mache es Entwicklern und Anwendern möglichst einfach, letzteren zu wählen.

Und drittens: Manchmal muss man alte Zöpfe zügig abschneiden, um in Sachen Sicherheit voran zu kommen – auch wenn es weh tut. Zur Übung sei empfohlen, einmal im Browser (wie in SSN 9/2013 beschrieben) RC4 zu deaktivieren und dann die Webseiten von BSI, BNetzA und BND zu besuchen.

Nichtflüchtiger Speicher

Am 08.10.2013 wurde Release 2.3 des Open-Source-Tools für Speicher-Forensik Volatility für den letzten Feinschliff freigegeben. So umfasst Volatility nun Profile für die Hauptspeicheranalyse bis Windows 7 und Server 2012. Neue Window-Plugins erkennen und extrahieren Einträge des *Master File Table* von NTFS-Dateisystemen und des *Master Boot Records*; damit können auf der Festplatte gelöschte Indexeinträge rekonstruiert und der Nachweis erbracht werden, dass Daten im Dateisystem existierten, die mit klassischen ‚Post-Mortem'-Forensikwerkzeugen nicht mehr auffindbar sind. Mit dem Carving-Plugin filescan kann man aus dem Hauptspeicher einen großen Teil zuvor geladener Dateien zurückgewinnen – auch wenn die Quelle (SD-Karte, USB-Stick) nicht mehr verfügbar ist. Und mit etwas Aufwand lässt sich ein Plugin zur Extraktion von Bitlocker-Schlüsseln erstellen.

Ebenfalls neu ist die Unterstützung der Versionen 10.5 bis 10.8.3 von Mac OSX; eine iOS-Untertützung fehlt allerdings noch. Dafür kann die VMware-Hauptspeicheranalyse nun auch auf States (.vmss) und Snapshots (.vmsn) erfolgen.

Erneut hat Volatility die Meßlatte für kommerzielle Forensik-Werkzeuge deutlich höher gelegt. Der Einstieg in die Nutzung des freien Tools wird unterstützt von Cheat-Sheets, die auch einem Forensik-Laien erste Analysen erlauben.

Fingerabdrücke auf Reisen

Bereits vor der Einführung waren der elektronische Reisepass (ePass) und die zugrunde liegende EU-Verordnung umstritten. Im Kern der Kritik stand die Zwangserhebung von Fingerabdrücken als biometrisches Sicherheitsmerkmal, das vor Betrug schützen soll. Ein Bochumer bestritt die Zulässigkeit dieses Vorgehens und klagte gegen die Stadt und die Erfassung seiner Fingerabdrücke. Das Verwaltungsgericht Gelsenkirchen hatte Zweifel an der Rechtmäßigkeit der EU-Verordnung und legte den Fall dem Europäischen Gerichtshof (EuGH) zur Vorabentscheidung vor.

Am 17.10.2013 fällte der EuGH das Urteil. Nach Ansicht der Richter ist die Speicherung von Fingerabdrücken zwar ein Eingriff in die Privatsphäre, im Kampf gegen Betrug sei dieser aber gerechtfertigt. Damit wurde auch die Rechtmäßigkeit der EU-Verordnung bestätigt.

Heimlich, still und leise …

… ist auf der Webseite des BSI die 13. Ergänzungslieferung der IT-Grundschutzkataloge als Online-Version erschienen. Damit stehen einige lang ersehnte Bausteine wie Windows 7-Client, Windows Server 2008 und Webanwendungen bereit. Eine weitere wesentliche Neuerung ist die durchgängige Einführung von Prüffragen, die auch als Basis für Zertifizierungsaudits dienen können. Eine Zusammenfassung der Neuerungen gibt einen guten Überblick über alle Änderungen.

Secorvo News

Auf dem Laufenden

Es gibt verschiedene Möglichkeiten, sich hinsichtlich der aktuellen Entwicklungen der Informationssicherheit auf dem Laufenden zu halten. Als Leser der Secorvo Security News kennen Sie schon eine sehr effiziente Möglichkeit. Eine weitere ist der Besuch des Seminars „IT-Sicherheit heute", welches Secorvo College vom **12.–14.11.2013** in Karlsruhe anbietet. Aktuelle Bedrohungen, konkrete Risiken und Best Practice-Lösungswege stehen in diesem Kompaktseminar im Vordergrund. Noch wenige Plätze sind frei.

Unseren geballten Erfahrungsschatz aus 15 Jahren erfolgreichen PKI-Projekten, von Konzeption über Aufbau bis zum Betrieb, haben wir im Seminar PKI (**19.–22.11.2013**) gebündelt – ein Leckerbissen für alle, die sich mit Public Key-Infrastrukturen beschäftigen. Auch hier sind nur noch wenige Plätze verfügbar. Unser Seminarangebot, alle Termine des Jahres 2014 und eine Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Wer hat, der hat.

„Software Asset Management für Kenner" ist das Thema des nächsten KA-IT-Si-Events am **07.11.2013** um 18 Uhr im Raum TelemaxX des CyberForum e.V. in Karlsruhe. Marcel Lepkojis (CONNECT Karlsruhe GmbH) wird in seinem Vortrag Sicherheitsaspekte des *Software Asset Managements* vorstellen und Schutzmaßnahmen empfehlen. Anschließend gibt es – wie gewohnt –Gelegenheit zum „Buffet-Net(t)working". Wir freuen uns auf Ihre Anmeldung!

Die Zukunft ist mobil

Im Zentrum des diesjährigen Future IT-Kongresses am **14.11.2013** im Tagungszentrum der Buhlschen Mühle in Ettlingen, der sich mit allen Facetten des mobilen IT-gestützten Arbeitens befasst, stehen Datenschutz- und Sicherheitsaspekte des Mobile-, Cloud- und Social-Computing. Die begleitende Fachausstellung lädt zum Gespräch und Erfahrungsaustausch mit den Anbietern und Kongressteilnehmern (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2013	
04.-08.11.	CCS 2013 (ACM SIGSAG, Berlin)
07.11.	Wer hat, der hat. (KA-IT-Si, Karlsruhe)
08.11.	Sicherheitsmanagement für mobile Geräte (GI/SECMGT, Frankfurt)
12.-14.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
13.-15.11.	37. DAFTA (GDD, Köln)
14.11.	Future IT-Kongress 2013 (AppSphere AG, Ettlingen)
18.-21.11.	OWASP AppSec USA 2013 (OWASP Foundation, New York)
19.-22.11.	PKI (Secorvo College, Karlsruhe)
21.-22.11.	DeepSec ISDC 2013 (DeepSec GmbH, Wien)
Dezember 2013	
02.-03.12.	IsSec/ZertiFA 2013 (COMPUTAS Gisela Geuhs GmbH, Berlin)
10.-11.12.	2. DFN Workshop Datenschutz (DFN-CERT Services GmbH, Hamburg)
27.-30.12.	30th Chaos Communication Congress (30C3) (Chaos Computer Club, Hamburg)
Januar 2014	
21.-23.01.	Omnicard 2014 (in TIME berlin, Berlin)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Christoph Schäfer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

November 2013



Potjomkin kehrt zurück

Man schrieb das Jahr 1787. Grigori Alexandrowitsch Potjomkin, Oberbefehlshaber der russischen Armee, Großadmiral der Schwarzmeerflotte, Generalgouverneur von Südrussland und Günstling (möglicherweise sogar heimlicher Ehemann) der Kaiserin Katharina der Großen hatte zahlreiche Siedlungen in Neurussland gegründet, aufgebaut und besiedeln lassen. Anlässlich einer Inspektionsreise in die neuen Provinzen soll er, um seiner Herrscherin zu imponieren, entlang des Wegs bemalte hölzerne Kulissen aufgestellt haben, die beeindruckende Bauwerke – Kirchen, Verwaltungsgebäude, Wehranlagen – vortäuschen sollten.

Unweigerlich blitzt die Erinnerung an diese Geschichte auf, liest man von den neuen Schutzmaßnahmen, die die Helfershelfer der NSA gerade ankündigen – wie die Verschlüsselung von E-Mails bei Microsoft, Google und Yahoo oder *Perfect Forward Secrecy* bei Twitter. Denn keine dieser Maßnahmen verhindert den Datenzugriff eines Nachrichtendienstes direkt über den Anbieter. Zu befürchten ist, dass mit dem wachsenden Laieninteresse an der IT-Sicherheit das allgemeine Tarnen und Täuschen zunimmt. Schon heute erleben wir, dass eine ‚Verschlüsselung' sich bei genauem Hinsehen als Zeichenersetzung oder gar als Kompressionsalgorithmus entpuppt, dass Passworte im Programmcode versteckt oder Remote-Zugänge durch Geheimhaltung der URL geschützt werden. In naher Zukunft könnten sich solcherart kompetenzfreie Implementierungen von Schutzmechanismen seuchenartig verbreiten.

Traurig daran: Auch gut implementierte, wirksame Schutzmaßnahmen werden unter Attrappenverdacht geraten. Wie Potjomkin: Seine Fassaden waren echt, wie nicht nur der inkognito mitreisende österreichische Kaiser Joseph II. später bestätigte. Das Täuschungsgerücht hatte ein Neider am Hofe Katharinas, der Diplomat Georg von Helbig, in die Welt gesetzt. Und es hält sich bis heute hartnäckiger als die Wahrheit.



Inhalt

Potjomkin kehrt zurück

Security News

TLS-Backdoor

Schranken der Einwilligung

ULD vs. Facebook II

ForGe

Entlastung für Provider

Secorvo News

T.I.S.P. Community Meeting

Weiterbildung 2014

Anti-Prism-Party 2. Staffel

Teamverstärkung

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

TLS-Backdoor

In den vergangenen Wochen wurde mehrfach über die Möglichkeiten der NSA spekuliert, mitgeschnittene, TLS-geschützte Protokolle zu entschlüsseln. Dabei gerieten sowohl der RC4 (siehe SSN 9/2013) als auch die zumeist fehlende *Perfect Forward Secrecy* unter Verdacht. Inzwischen häufen sich die Hinweise, dass die NSA eine dritte Möglichkeit besitzt, die Dan Shumov und Nils Ferguson bereits im August 2007 auf der *Rump Session* der internationalen Kryptografenkonferenz Crypto'07 der IACR beschrieben hatten: Der vom NIST in erster Fassung im Mai 2007 publizierte Standard *Recommendation for Random Number Generation Usind Deterministic Random Bit Generators* (SP 800-90A) enthält einen auf Elliptischen Kurven basierenden Zufallszahlengenerator, der nach einem Blog-Eintrag von Bruce Schneier vom 15.11.2007 offenbar auf Drängen der NSA aufgenommen wurde: der Dual_EC_DRBG.

Im Appendix A des Standards werden drei Generatoren, bestehend aus einer elliptischen Kurve und jeweils zwei festen Kurvenpunkten *P* und *Q* spezifiziert. Der Trick: Ist die mathematische Relation (der diskrete Logarithmus *e*) zwischen diesen beiden Punkten bekannt, so lassen sich aus einem einzigen Output des Generators alle weiteren Zufallszahlen voraussagen. Nachträglich lässt sich *e* nicht berechnen – sollte aber die NSA die Punkte aus einem vorab gewählten *e* konstruiert haben, wäre *e* eine perfekte Backdoor. Das könnte erklären, warum der NIST-Standard empfiehlt, lediglich 16 Bits des Outputs nicht als Teil des Zufallswerts zu verwenden – üblich ist, maximal die Hälfte der Bits zu verwenden. Mit Kenntnis von *e* und einem Zufallswert kann man die fehlenden 16 Bit nämlich leicht durch *Brute Force* (65.536 Varianten) gewinnen. Zwar erlaubt der Standard, *P* und *Q* selbst gemäß ANSI X9.62 zu erzeugen. Für eine Zertifizierung nach FIPS 140-2 sind dann aber eigene Testvektoren erforderlich, die das Zertifikat verzögern – ein Aufwand, der zumindest bei den bisher zertifizierten Produkten gescheut wurde. So ist Dual_EC_DRBG auch in OpenSSL unverändert enthalten (wenn auch nicht als Default).

Ein TLS-Client schickt beim initialen *Handshake* eine Zufallszahl – und erzeugt wenig später das *Pre Master Secret*, aus dem der symmetrische Verschlüsselungs-Schlüssel (*Master Secret*) abgeleitet wird, mit demselben Zufallszahlengenerator. Nutzt der TLS-Client den Dual_EC_DRBG, könnte die NSA mit geringem Aufwand aus der ersten Zufallszahl den Schlüssel ableiten. Fatal: Diese Backdoor hebelt auch *Perfect Forward Secrecy* aus. Einziger wirksamer Schutz: Dual_EC_DRBG nicht verwenden.

Schranken der Einwilligung

Bereits am 17.07.2013 hat das Bundesverfassungsgericht in einem nun veröffentlichten Kammerentschluss zu der verbreiteten Versicherungspraxis, umfassende Schweigepflichtentbindungen gegenüber Ärzten, Kranken- und Rentenkassen von den Versicherten zu fordern, Stellung genommen.

Es obliege den Gerichten bei klarer Disparität der Vertragspartner und fehlendem besonderen gesetzlichen Schutz für die Bewahrung der informationellen Selbstbestimmung zu sorgen. Die Schweigepflichtentbindungen seien auf die tatsächlich erforderlichen Informationen zu begrenzen. Soweit dies im Voraus nicht möglich sei, sei ein entsprechendes schrittweises Verfahren zu verwenden. Dem Versicherten könne ein eigenständiges Modifizieren vorformulierter Erklärungen nicht zugemutet werden.

Die Entscheidung ist auf Einwilligungen zwischen ungleich starken Partnern im Allgemeinen übertragbar. Sie bestätigt einmal mehr das Erfordernis, Einwilligungen eng und bestimmt auf das Erforderliche zu begrenzen, will man nicht eine spätere Feststellung deren Nichtigkeit riskieren.

ULD vs. Facebook II

Am 09.10.2013 hob das Schleswig-Holsteinische Verwaltungsgericht mehrere Anordnungen des ULD auf, die von Betreibern von Facebook-Fanseiten deren Deaktivierung aufgrund mangelnden Datenschutzes verlangten (SSN 10/2012). Daraufhin teilte das ULD am 01.11.2013 mit, dass es Berufung gegen das Urteil eingelegt hat.

Gleich, ob einem bei Thilo Weicherts Kampf gegen Facebook eher die Parallele zu Don Quijotes Kampf gegen die Windmühlen oder die zu David gegen Goliat in den Sinn kommt – die Entscheidung des VG Schleswig ist in jedem Fall beachtlich. Denn nach – vermutlich unstreitiger – Auffassung des ULD verstößt Facebook gegen das Telemediengesetz: Durch die Statistik-API Facebook Insights werden Nutzer persönlich erfasst, was nach deutschem Recht einer ausdrücklichen Einwilligung bedarf. Facebook bietet hingegen nicht einmal eine Widerspruchsmöglichkeit.

Das Gericht vertritt die Auffassung, dass Betreiber von Fanseiten keinen Einfluss auf die Datenverarbeitung bei Facebook haben und deswegen für sie auch nicht (mit)verantwortlich sind. Das ist zwar einerseits nachvollziehbar, aber ein ‚Geschmäckle' bleibt: Muss man sich nur die ‚richtigen' Anbieter suchen, um aus der rechtlichen Verantwortung für

einen Internetauftritt zu kommen? Dank dem ULD wird diese Frage jetzt weitere Instanzen beschäftigen.

ForGe

Bereits im September 2013 wurde der *Forensic Test Image Generator* ForGe veröffentlicht. ForGe stellt einen komfortablen Baukasten unter GP-Lizenz bereit, mit dem für unterschiedliche Testfälle Images für NTFS-Dateisysteme automatisiert erzeugt werden können. Unterstützt werden derzeit die Implementierung von *Alternate Data Streams*, Änderungen von Datei-Endungen, Datei-Slack, Merging und Löschung von Dateien. Zusammen mit dem integrierten Zeitlinienmanagement auf Metadatenebene von NTFS kann man damit sehr gut wiederkehrende Prüfungen für Analysewerkzeuge spezifizieren. Zwar existiert mit Forensig^2 seit 2009 ein Forensik-Tool deutscher Herkunft mit ähnlicher Ausrichtung, das allerdings nie allgemein verfügbar war. ForGe beendet damit erstmals die Knappheit datenschutzrechtlich unbedenklicher Testdaten.

Entlastung für Provider

Das OLG Stuttgart hat am 22.10.2013 über die Kostentragung zu einer Abmahnung eines Betreibers einer Blog-Plattform entschieden. Ein Anspruch des Abmahnenden auf Kostenerstattung gegen den Betreiber wegen der urheberrechtswidrigen Fotoverwendung eines Seitennutzers wurde abgelehnt.

Nach Auffassung des Gerichts hafte der Hosting-Provider, der nach Erhalt der Abmahnung das fragliche Bild sofort entfernt habe, weder auf Schadensersatz, noch als Störer auf Unterlassung. Erst nach unterbliebener Handlung entstehe die Störereigenschaft. Aus demselben Grund könne von dem Host-Provider auch keine Unterlassungserklärung verlangt werden, da er nicht zur Untersuchung der Blogbeiträge verpflichtet sei.

Durch die Entscheidung wird die Rechtssicherheit für Provider von Internetdiensten gesteigert. Sie bedeutet aber auch, dass für ein sicheres Vermeiden von Ansprüchen ein schnelles Handeln ohne Klärung der Vorwurfsberechtigung erforderlich ist.

Secorvo News

T.I.S.P. Community Meeting

Zum siebten Mal fand am 04.-05.11.2013 in Berlin das T.I.S.P. Community Meeting statt. 100 T.I.S.P.-Absolventen waren angereist, um mit Kollegen aus allen Branchen aktuelle Fragestellungen der Informationssicherheit zu diskutieren und Erfahrungen auszutauschen. Schwerpunktthemen waren Security by Design, Risiko-Management und die Umstellung auf IPv6. Das nächste T.I.S.P. Community Meeting wird am 03.-04.11.2014 wieder in Berlin stattfinden. Wem zur Teilnahme (nur) noch das T.I.S.P.-Zertifikat fehlt, dem bietet Secorvo College am **24.-28.03.2014** die nächste Möglichkeit, es zu erwerben.

Weiterbildung 2014

Für die frühzeitige Planung Ihrer Weiterbildungsmaßnahmen 2014 empfehlen wir einen Blick in das Seminarangebot von Secorvo College. Soll es ein Update zu aktuellen Themen der Informationssicherheit sein? Oder umfassende Informationen zum Aufbau und dem Betrieb einer PKI? Oder aber eine Zertifizierung zur Dokumentation Ihrer Qualifikation, wie z. B. der T.I.S.P., der CPSSE oder der T.E.S.S.? Gerne sind wir für Sie da.

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Anti-Prism-Party 2. Staffel

Mehr als 600 Besucher nahmen an der größten Verschlüsselungsparty Süddeutschlands unter dem Motto „Karlsruhe schützt sich selbst“ am 05.09.2013 im ZKM | Karlsruhe teil. Nach diesem großen Erfolg startet das neue KA-IT-Si-Jahr am 12.02.2014 mit der Anti-Prism-Party 2. Staffel, wieder im ZKM. Ab 18 Uhr werden unsere Experten in kompakten 10-minütigen Kurzvorträgen live vorführen, wie aktuelle und überwiegend kostenlose Schutzmechanismen für Smartphone, Browser und E-Mail-Client installiert, konfiguriert und genutzt werden. Auch für Besucher der 1. Staffel werden spannende neue Themen darunter sein.

Im Anschluss öffnet das Kryptologikum im ZKM seine Pforten. Neben Führungen durch die Ausstellung gibt es auch diesmal die Möglichkeit, sich an verschiedenen Stationen Schutzmechanismen von Karlsruher Sicherheitsexperten vorführen und erklären zu lassen. Aktuelle Informationen zur Anti-Prism-Party gibt es in einem eigenen Newsletter und auf Twitter (damit auch die NSA informiert ist).

Teamverstärkung

Erneut hat das Secorvo-Team Zuwachs bekommen: Seit dem 01.11.2013 unterstützt uns Dr. Yun Ding. Sie ist Diplom-Informatikerin mit über 16 Jahren Berufserfahrung; ein gutes Drittel dieser Zeit war sie verantwortlich für die Entwicklung von Schutzmechanismen wie z. B. kryptografischen Modulen, IT-Lösungen im Gesundheitswesen und Security-Architekturen für Smartphones.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2013	
02.-03.12.	IsSec/ZertiFA 2013 (COMPUTAS Gisela Geuhs GmbH, Berlin)
10.-11.12.	2. DFN Workshop Datenschutz (DFN-CERT Services GmbH, Hamburg)
27.-30.12.	30th Chaos Communication Congress (30C3) (Chaos Computer Club, Hamburg)
Januar 2014	
17.-19.01.	ShmooCon 2014 (The Shmoo Group, Washington/US)
21.-23.01.	Omnicard 2014 (in TIME berlin, Berlin)
Februar 2014	
04.-06.02.	Cloudzone 2014 (Karlsruher Messe- und Kongress-GmbH, Karlsruhe)
05.-06.02.	24. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
12.02.	Anti-Prism-Party 2. Staffel (KA-IT-Si, Karlsruhe)
18.-19.02.	21. DFN Workshop "Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)

Fundsache

Das BSI hat am 26.11.2013 eine Studie zur Sicherheit industrieller Steuerungssysteme (kurz: ICS) veröffentlicht. Sie umfasst eine wertvolle Gegenüberstellung relevanter Industrie- und Sicherheits-Standards und konkrete Vorschläge für die Durchführung von Sicherheitsaudits.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Michael Knopp, Christoph Schäfer, Jochen Schlichting.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

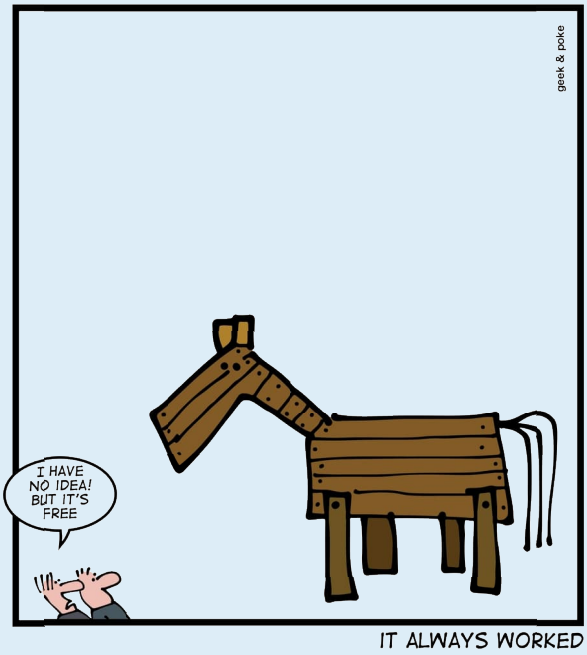
Secorvo Security News

Dezember 2013

Auf den Punkt

Robert Musils „Der Mann ohne Eigenschaften" ist ein Meilenstein der deutschsprachigen Literatur des 20. Jahrhunderts. Allerdings dürfte selbst der eine oder andere Literaturbegeisterte vor den über 1.000 Seiten des unvollendeten Werks zurückschrecken. Nun hat am 11.11.2013 der begnadete Zeichner Nicolas Mahler eine auf 150 Seiten verdichtete Fassung von Musils Hauptwerk publiziert: als Comic.

„Manche Menschen nutzen ihre Intelligenz zum Vereinfachen, manche zum Komplizieren", wusste schon Erich Kästner. Ersteres ist mir sympathischer – denn oft legt eine kompromisslose Verkürzung eine Kernaussage in aller Klarheit bloß. Daher habe ich für diese News das bereits verfasste Editorial durch einen Cartoon von „Geek & Poke" ersetzt, den wir mit freundlicher Genehmigung des ebenfalls begnadeten, aber (zu Unrecht) weniger bekannten Hamburger Zeichners Oliver Widder hier wiedergeben. Schöne Weihnachten.





Inhalt

Auf den Punkt

Security News

PCI DSS 3.0

Mangel an Beweisen

Bundesrat bremst EU-Verordnung

Sicherheit für ICS

Volatility goes CybOX

GroKo und die Sicherheit

GroKo und der Datenschutz

Secorvo News

Zertifikate helfen

Anti-Prism-Party 2. Staffel

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

PCI DSS 3.0

Das PCI *Security Standards Council* hat am 07.11.2013 die Version 3.0 des in der Finanzwelt verbreiteten Zertifizierungs-Standards zum Schutz von Konto- und Kreditkartendaten PCI DSS veröffentlicht. Der neue Standard tritt am 01.01.2014 in Kraft, während der Version 2.0 noch eine Übergangsfrist bis zum 31.12.2014 eingeräumt wird. Einige Anforderungsänderungen, die bei betroffenen Unternehmen ggf. hohe Aufwände erzeugen, bleiben bis zum 01.07.2015 erst einmal *Best Practices* und werden erst danach verbindlich. Unterstützende Arbeitshilfen werden Anfang 2014 bereitgestellt.

Eine Übersicht über die Änderungen von der Version 2.0 auf 3.0 findet sich in den Dokumenten des PCI SSC „Summary of Changes" und „Version 3.0 Change Highlights". Viele der Änderungen in den 112 Seiten des Standards betreffen Klarstellungen und Anpassungen von Anforderungen an den Stand der Technik. Bahnbrechende neue Anforderungen sind nicht enthalten – allerdings werden einige *Best Practices* wie Requirement 8.5.1 „... *use unique authentication credentials for each customer*" festgeschrieben. Für alle, die mit Version 2.0 des PCI DSS vertraut sind, bietet es sich an, die Änderungsdokumente durchzuarbeiten; Neueinsteiger sollten sich gleich mit der Version 3.0 auseinandersetzen.

Mangel an Beweisen

Vor dem Landesarbeitsgericht Hamm ist das Land Nordrhein-Westfalen mit der fristlosen Kündigung zweier IT-Mitarbeiter wegen urheberrechtswidrigen Filesharings auf dienstlichen Rechnern gescheitert. Kern der Begründung des Gerichts im Urteil vom 06.12.2013 sind Mängel in der Beweisführung. So wurden die Rechner, auf denen (nach einer Abmahnung an die Adresse einer Kreispolizeibehörde wegen des illegalen Downloads eines Musikstücks) verschiedene Musiktitel und Filme gefunden worden waren, nicht zügig sichergestellt. Schlimmer noch: Auf den von den beiden gekündigten Mitarbeitern überwiegend genutzten Rechnern gab es keine personalisierten Nutzer-Accounts.

Das Urteil unterstreicht einmal mehr die Notwendigkeit, ausschließlich mit personalisierten Nutzer-Accounts zu arbeiten und feste Prozesse für Störungen oder Richtlinienverstöße festzulegen, damit im Falle eines Vorfalls eine forensische Beweisführung möglich wird.

Bundesrat bremst EU-Verordnung

Der Bundesrat hat in einer Stellungnahme vom 29.11.2013 erhebliche Bedenken gegen den Entwurf einer europäischen Verordnung über Maßnahmen zum europäischen Binnenmarkt der elektronischen Kommunikation geltend gemacht. Die Bedenken richten sich zunächst grundsätzlich gegen den Erlass einer weiteren direkt geltenden Verordnung, die Teile des Telekommunikationsgesetzes ersetzen und hinter dem Schutz- und Regelungsniveau des deutschen Rechts zurückbleiben würde. Kritisiert wird auch die Vielzahl unbestimmter Rechtsbegriffe und fehlender Definitionen. Davon betroffen sind insbesondere die telekommunikationsspezifischen Regelungen zum Datenschutz.

Insgesamt hat der Bundesrat eine Reihe von begründeten Bedenken zusammengetragen, die hoffentlich bei der weiteren Entwicklung der europäischen Gesetzgebungsvorhaben berücksichtigt werden.

Sicherheit für ICS

In der Welt der industriellen Steuerungen (ICS) bewegt sich etwas, wie das BSI ICS-Security Kompendium (vgl. Fundsache SSN 11/2013) und der von der Enisa am 04.12.2013 veröffentlichte Good Practice Guide zur Etablierung von CERT-Strukturen im ICS-Umfeld zeigen. Der Paradigmenwechsel, dass industrielle Steuerungen keine eigene Welt mit eigenen Gesetzmäßigkeiten bilden, sondern als Teil der gesamten IT-Infrastruktur betrachtet werden müssen, kann – Stuxnet sei dank – offenbar als vollzogen betrachtet werden.

Auch bei den Herstellern werden inzwischen Schwachstellen bei früher als „Non-IT" betrachteten Komponenten via Patch geschlossen, wie das am 04.12.2013 veröffentlichte Beispiel von Siemens' Servoantrieben zeigt: Die offenen netzwerkseitigen Zugangswege wurden durch ein Firmware-Update beseitigt. Schwachstellen werden inzwischen durchaus ernst genommen – und zügig abgestellt.

Zu beachten ist allerdings, dass bei der Planung des Betriebs von Steuerungen zukünftig auch die Aufwände für die Beobachtung von Schwachstellen, die Beurteilung der Relevanz von Updates und die Aktualisierung von Komponenten eingeplant werden.

Volatility goes CybOX

Für das freie Forensic-Tool Volatility ist seit dem 05.09.2013 das Plugin CybOXer verfügbar, das die Spezifikation Cyber Observable eXpression (CybOX) (eine Hersteller unabhängige Beschreibungssprache für Hinweise auf Schadsoftware-Muster) von MITRE unterstützt. Damit kann während der Analyse automatisiert auf einzelne oder ganze Gruppen von Indicators of Compromise (IoC) geprüft werden.

Ca. 110 öffentliche IoCs kann man u. a. von IOC Bucket beziehen; allerdings gehen bei der Script-Konvertierung in das CybOX-XML-Format ca. 10 % der IoCs aufgrund der Verwendung von nicht standardisierten Elementen verloren. So ist eine händische Nachbearbeitung unvermeidlich; anschließend aber läuft die Massenanalyse komfortabel, stabil und flott.

GroKo und die Sicherheit

Der Koalitionsvertrag von Union und SPD vom 27.11.2013 sieht die Einführung eines IT-Sicherheitsgesetzes mit verbindlichen Mindestanforderungen an die IT-Sicherheit für kritische Infrastrukturen vor. Unter anderem soll eine Meldepflicht für erhebliche IT-Sicherheitsvorfälle eingeführt werden.

Zum Schutz vor Spionage soll ein rechtlich verbindliches Abkommen verhandelt werden, um Bürger, Regierung und Wirtschaft vor schrankenloser Ausspähung zu schützen – keine ganz überraschende Forderung in einem demokratischen Rechtsstaat. Die europäischen Telekommunikationsanbieter sollen verpflichtet werden, ihre Kommunikationsverbindungen mindestens innerhalb der EU zu verschlüsseln und keine Daten direkt an ausländische Nachrichtendienste weiterzuleiten. Immerhin.

GroKo und der Datenschutz

Der Begriff „Datenschutz" findet sich an 35 Stellen im Koalitionsvertrag – das Thema hat Konjunktur. Allerdings bleiben die Vereinbarungen der Großen Koalition vage: Die EU-Datenschutzgrundverordnung soll zügig verabschiedet werden; dabei soll das deutsche Datenschutzniveau im Zweifel höher bleiben – wie das bei einer vereinheitlichenden Rechtsetzung einer EU-Verordnung funktionieren kann, wird nicht erläutert.

Sollte die Verordnung nicht rechtzeitig kommen, ist geplant, das Beschäftigtendatenschutzgesetz wieder auszugraben. Zum Ausgleich – da nun Sabine Leutheusser-Schnarrenberger als Justizministerin nicht mehr im Weg steht – soll, allen NSA-Affären zum Trotz, die Vorratsdatenspeicherung nach den Vorgaben der EG-Richtlinie kommen. Die ungeliebte ‚Stiftung Datenschutz' soll in die Stiftung Warentest integriert werden – wie (und zu welchem Zweck) auch immer. Schließlich soll in der EU auf Nachverhandlungen der Swift- und Safe-Harbour-Abkommen gedrängt werden – eine Idee, auf die die EU unlängst selbst gekommen ist. Bleibt zu hoffen, dass dem Datenschutz in den kommenden vier Jahren eine ebenso große Aufmerksamkeit zuteil wird wie im Koalitionsvertrag.

Secorvo News

Zertifikate helfen

Im Jahr 2013 Jahr wurde das 600ste T.I.S.P.-Zertifikat ausgestellt. Damit ist der T.I.S.P. auf dem besten Weg, zum bedeutendsten berufsqualifizierenden Nachweis für IT-Sicherheitsexperten in Deutschland zu werden. Die einwöchige T.I.S.P.-Schulung vermittelt einen vertieften Einblick in alle Gebiete der Informationssicherheit und hilft, verbliebene Wissenslücken zu schließen. Die nächsten Möglichkeiten, bei Secorvo ein T.I.S.P.-Zertifikat zu erhalten, bietem sich am 24.-28.03.2014 und am 19.-23.05.2015. Auf dem Seminar erleben Sie die Autoren des T.I.S.P.-Lehrbuchs „Zentrale Bausteine der Informationssicherheit" live.

Für den Fall, dass Sie sich „nur" beim Thema Informationssicherheit auf den aktuellen Stand bringen wollen, ist das Seminar IT-Sicherheit heute am 08.-10.04.2014 das Richtige für Sie. Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college



Anti-Prism-Party 2. Staffel

Die Vorbereitungen zur 2. Staffel der erfolgreichen Anti-Prism-Party am **12.02.2014** im Karlsruher ZKM ist in vollem Gange. Für Schüler und Auszubildende führen wir zwischen 10 und 16 Uhr zweistündige Sonderveranstaltungen durch, die sich aus einer Führung durch das Kryptologikum, einem ‚Security Kino' und Live-Demonstrationen zu verschiedenen Themen zusammensetzen. Aktuelle Informationen zur Anti-Prism-Party gibt es in einem eigenen Newsletter und auf Twitter.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2013	
27.-30.12.	30th Chaos Communication Congress (30C3) (Chaos Computer Club, Hamburg)
Januar 2014	
17.-19.01.	ShmooCon 2014 (The Shmoo Group, Washington/US)
21.-23.01.	Omnicard 2014 (in TIME berlin, Berlin)
Februar 2014	
04.-06.02.	Cloudzone 2014 (Karlsruher Messe- und Kongress-GmbH, Karlsruhe)
05.-06.02.	24. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
12.02.	Anti-Prism-Party 2. Staffel (KA-IT-Si, Karlsruhe)
18.-19.02.	21. DFN Workshop "Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2014	
24.-29.03.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)

Fundsache

Matthew Green von der Johns Hopkins University (Baltimore/US) publizierte am 02.12.2013 in seinem Blog zu *Cryptography Engineering* eine lesenswerte Analyse der wahrscheinlichen Möglichkeiten der NSA, auf SSL/TLS-geschützte Kommunikation zuzugreifen. Als sicher darf gelten: dank der Stärke des kryptographischen Protokolls muss sie sich verschiedener Tricks bedienen.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Christoph Schäfer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2014



Skurrile Welt

Es ist schon eine eigenartige Entwicklung, an die wir uns in den vergangenen Jahrzehnten gewöhnt haben.

Inzwischen erfahren wir fast täglich in den Nachrichten von erfolgreichen Angriffen auf IT-Systeme. Der ebenso vorhersehbare (wie wirkungslose) politische Reflex: ein Sicherheitsgesetz, das Unternehmen verpflichten soll, Vorfälle zu melden. Dabei dürfte in den weitaus meisten Fällen mindestens ein sicherheitsrelevanter Fehler in einer genutzten Software mitursächlich gewesen sein. Die Adressaten der Vorwürfe und politischen Maßnahmen sowie die Leidtragenden der wirtschaftlichen Folgen sind jedoch in der Regel die Opfer: nicht der Hersteller der fehlerhaften Software steht am Pranger, sondern der Anwender – und sei es, weil er ein Update nicht eingespielt hat.

In anderen Branchen wäre so etwas unvorstellbar: Würde man den Fahrer eines Autos nach einem Achsbruch verurteilen, weil er nicht umgehend auf eine fehlerärmere Achse des Herstellers „upgedatet" hat? Ihm zum direkten Schaden auch noch den des Reputationsverlusts auferlegen, anstatt den Achshersteller beim Namen zu nennen – und ihn mit Schadensersatzforderungen zu konfrontieren?

Während Verbraucherrechte ständig ausgeweitet werden stiehlt sich die Software-Branche bei Sicherheitsmängeln ihrer Produkte seit Jahren aus der Verantwortung.

Die Wurzel des Übels liegt allerdings tiefer. Dem Berufsstand des Software- und Webanwendungsentwicklers liegt bis heute keine einheitliche Berufsqualifikation zu Grunde. In der Praxis dominieren nicht selten branchenfremde Quereinsteiger, und in den existierenden Berufsausbildungen spielen Sicherheitsaspekte bei der Software-Architektur und der Kodierung nicht einmal eine Nebenrolle. Wenn wir sichere Software wollen, brauchen wir entsprechend qualifizierte Entwickler – und Zertifikate. Damit könnte sich „Software made in Germany" sogar zu einem Qualitätssiegel entwickeln. Bis dahin ist es allerdings noch ein steiniger Weg.



Inhalt

Skurrile Welt

Security News

Europäisches Aufständchen

Drum prüfe...

000507607999

Belästigende Empfehlungen

Offensicher

Zickzack-Kurs

Secorvo News

IT-Sicherheit 2014

Karlsruhe schützt sich selbst

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Europäisches Aufständchen

Bereits im Oktober 2012 (SSN 10/2012) hatte die Art. 29 Gruppe der Europäischen Datenschutzaufsichtsbehörden Google aufgefordert, die einheitliche Datenschutzerklärung vom März 2012 an das europäische Datenschutzrecht anzupassen. Nun zeitigen die anschließend in Frankreich, Spanien, Großbritannien, den Niederlanden, Italien und Deutschland eingeleiteten Verfahren erste Ergebnisse: In Spanien wurden Google Inc. 900 TEuro Bußgeld auferlegt, in Frankreich 150 TEuro. Die französische CNIL (*Commission nationale de l'informatique et des libertés*) hat Google außerdem verpflichtet, auf www.google.fr eine Pressemitteilung zu ihrer Entscheidung für 48 Stunden zu veröffentlichen. Google plant Rechtsmittel einzulegen.

CNIL und die spanische AEPD (*Agencia Espaniola de Protecciòn de Datos*) begründen die Bußgeldbescheide mit der Unklarheit der vorliegenden Datenschutzerklärung: Zweck, Löschfristen und Umfang der Verarbeitung der Daten seien nicht erkennbar, viele Aussagen enthielten ein „möglicherweise" oder stünden im Konjunktiv. Darüber hinaus behalte sich Google ohne Rechtsgrundlage vor, Daten der verschiedenen Dienste zusammenzuführen.

Bei den übrigen Datenschutzaufsichtsbehörden stockt das Verwaltungsverfahren. Daher ist Frau Reding zuzustimmen, dass die Verfahren weder durch die Höhe der Sanktionen noch mit ihrem schleppenden Verlauf geeignet sind, Google zu beeindrucken. Der Fall zeigt: Zur Durchsetzung europäischer Datenschutzvorstellungen bedarf es sowohl einer stärkeren europäischen Zusammenarbeit als auch wirksamerer Druckmittel.

Drum prüfe...

Am 29.12.2013 wurde die Website des OpenSSL-Projekts Opfer eines Angriffs. Medien in aller Welt berichteten über den Angriff und nannten eine Schwachstelle im eingesetzten Hypervisor als Ursache. Im Kontext zahlreicher anderer Attacken nicht einmal eine Randnotiz der Geschichte – hätte sich nicht im Laufe der Untersuchungen herausgestellt, dass unsichere Passwörter beim Hosting-Provider das Einfallstor waren.

So wurde der Vorfall zu einem lehrbuchmäßigen Beispiel für den verbreiteten Mangel an systematischer Ursachenanalyse: Anstatt zunächst die wahrscheinlichsten Fehlerquellen auszuschließen und Belege für den Ablauf des Angriffs zu suchen, mutierten Spekulationen zu Erkenntnissen. Dabei würde kein seriöser Handwerker einen Toaster als defekt deklarieren, ohne zuvor zu prüfen, ob beim Funktionstest auch der Netzstecker steckte.

000507607999

Auf dem 30. Chaos Communication Congress 30C3 in Hamburg stellten am 27.12.2013 zwei Forscher ihre Analyse einer neuartigen Bankautomaten-Malware vor. Die Angriffsmethode: Man bohre ein Loch in die Gehäusefront des Geldautomaten, um den USB-Port des dahinter montierten Windows-XP-Systems zu erreichen, und übertrage die Malware per USB-Stick. Mit der PIN „000507607999" ließ sich die Benutzeroberfläche der Malware aktivieren; darüber konnte nach Eingabe einer temporären PIN, die ein Automatenräuber telefonisch erfragen musste, der Bargeldbestand des Automaten gezielt dezimiert werden.

Bankautomaten-Malware ist nicht neu; erste Exemplare wurden bereits 2009 analysiert. Sie wird jedoch, wie die Malware Ploutus aus Mexiko, systematisch weiterentwickelt, begünstigt durch fortschreitende Standardisierung: So lassen sich Bankautomaten inzwischen über die CEN XFS API von Microsoft steuern.

Dennoch fällt es schwer zu glauben, dass ein solcher Angriff überhaupt möglich war. So ist die USB-Schnittstelle schon länger als wunder Punkt von Bankautomaten bekannt. Und bereits seit Jahren ist es nicht nur in Banken übliche Praxis, kritische Systeme zu härten – und dabei nicht benötigte Schnittstellen zu deaktivieren. Ein solcher Klick im BIOS hätte den betroffenen Instituten erhebliche Summen erspart.

Belästigende Empfehlungen

Bereits am 12.09.2013 erklärte der Bundesgerichtshof die Praxis, Webseitenbesuchern ein Formular zum Versenden einer Empfehlungs-E-Mail zur Verfügung zu stellen, für wettbewerbswidrig. Maßgeblich für die Einordnung solcher E-Mails als Werbung sei nicht, dass die Versendung durch unbekannte Nutzer veranlasst werde, sondern dass der Versand das Ziel habe, auf die Webseiten aufmerksam zu machen. Die Versandfunktion hierzu würde vom Seitenbetreiber zur Verfügung gestellt, und dieser träte als Absender in Erscheinung. Damit greife § 7 Abs. 2 Nr. 3 UWG, der E-Mail-Werbung ohne Einwilligung des Empfängers als unzumutbare Belästigung einstuft.

Eine rechtskonforme Gestaltung einer solchen Empfehlungsfunktion erfordert also mindestens, dass sie eine Nachricht im E-Mail-Programm des Seitennutzers erzeugt und dieser als Absender erscheint. Doch selbst dies könnte – je nach Intensität der werbenden Inhalte (z. B. Zusatztext zum Link, Logos) – als belästigende und damit unzulässige E-

Mail-Werbung gewertet werden. Webseitenbetreibern ist daher zu raten, die Empfehlungsfunktion ersatzlos zu streichen, um Abmahnungen zu vermeiden.

Offensicher

Wie sicher ist *Open Source*-Software? Der naive Glaube, dass die Veröffentlichung des *Source Codes* mehr oder weniger automatisch die Sicherheit eines Programms garantiere (keine Hintertüren, keine sicherheitskritischen Bugs, keine sicherheitsrelevanten Design-Fehler), hat sich wiederholt als Irrglaube entpuppt. Denn die prinzipielle Möglichkeit zur Code-Prüfung sagt wenig über die tatsächliche Durchführung. Auch muss der zum Download angebotene Binärcode nicht mit dem publizierten Quell-Code übereinstimmen – ein beliebtes Einfallstor für Angreifer (und Nachrichtendienste).

Dagegen hilft nur eine unabhängige Prüfung durch eine kompetente und vertrauenswürdige Instanz. Eine solche Initiative hat jetzt Matthew Green mit seinem *Open Crypto Audit Project* (OCAP) ergriffen. Am 20.12.2013 konnte er in seinem Blog den Start der öffentlichen Analyse von TrueCrypt verkünden – nachdem sein Sponsoring-Aufruf gut 64.000 US$ erbracht hatte. Sollte das Beispiel Schule machen, hätte die eine oder andere *Open Source*-Software bald die besten Argumente auf ihrer Seite.

Zickzack-Kurs

Nachdem die große Koalition sich darauf geeinigt hatte, ein neues Gesetz zur Vorratsdatenspeicherung zu entwickeln, legte am 12.12.2013 der Generalanwalt Pedro Cruz Villalòn am Gerichtshof der Europäischen Union seine Schlussanträge in der Vorabentscheidungsvorlage zur Vorratsdatenspeicherung vor. Prompt verkündete der neue Bundesjustizminister, erst das Urteil des EU-Gerichtshofs abwarten zu wollen. Auch das Innenministerium hat inzwischen die möglichen Auswirkungen des Urteils erkannt und sich zum Abwarten bekannt.

Die Schlussanträge zur Richtlinie 2006/24/EG kommen zu einem ähnlichen Ergebnis wie bereits 2010 das Bundesverfassungsgericht: Für die Beurteilung der Verhältnismäßigkeitsabwägung sei relevant, wie der Zugang zu den Daten geregelt wird. Da solche Regelungen fast völlig fehlten, sei die Richtlinie im Ganzen unverhältnismäßig. Verhältnismäßig sei höchstens eine Speicherdauer von einem Jahr. Zudem müsse der europäische Gesetzgeber zur Wahrung der Verhältnismäßigkeit Regeln erlassen, die möglicherweise außerhalb seiner Kompetenz lägen. Angesichts dieser Umstände wird es bis zu einem neuen Anlauf zur Vorratsdatenspeicherung sicherlich etwas dauern. Die Bundesregierung möchte sich auf EU-Ebene immerhin für eine zeitliche Beschränkung der Speicherung auf drei Monate einsetzen.

Secorvo News

IT-Sicherheit 2014

Mit dem Seminar „IT-Sicherheit heute“ bieten wir seit Jahrzehnt Jahr für Jahr einen vertieften Einblick in aktuelle Themen und Entwicklungen der IT-Sicherheit. Auch 2014 wurde das Programm thematisch ergänzt und aktualisiert. Nächster Seminartermin: 08.-10.04.2014.

Immer mehr Unternehmen – darunter Bertelsmann, VW und die Bundesdruckerei – erwarten von Mitarbeitern im Bereich Informationssicherheit ein T.I.S.P.-Zertifikat als Qualifikationsnachweis. Die nächste Gelegenheit, Ihre Qualifikation als Security-Spezialist zertifizieren zu lassen, bieten wir Ihnen vom 24.-28.03.2014 – mit den Autoren des T.I.S.P.-Begleitbuchs als Referenten.

Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.



Foto: Sandra Jacques

Karlsruhe schützt sich selbst

Mit über 650 Teilnehmern wurde die von der Karlsruher IT-Sicherheitsinitiative organisierte Anti-Prism-Party im September 2013 zur größten Verschlüsselungsparty Deutschlands. Am **12.02.2014** folgt nun die zweite Staffel: Neben weiteren Tipps und Empfehlungen zum „Selbstdatenschutz“ zeigt das Kryptologikum des Karlsruher Instituts für Technologie (KIT) historische und zeitgenössische Verschlüsselungstechnik zum „Be-Greifen“. Ein „Security Kino“ und eine Live-Hacking-Demo im Foyer des ZKM veranschaulichen die Erforderlichkeit von Schutzmaßnahmen.

Die wahrscheinlich größte Verschlüsselungsparty Europas beginnt um 18 Uhr. Der Eintritt ist frei; eine Anmeldung ist nicht erforderlich.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2014	
05.-06.02.	24. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
12.02.	Anti-Prism-Party 2. Staffel (KA-IT-Si, Karlsruhe)
17.-21.02.	Audit Challenge 2014 (Frankfurt School of Finance & Management, Frankfurt)
18.-19.02.	21. DFN-Workshop "Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2014	
24.-29.03.	T.I.S.P.-Schulung und Prüfung (Secorvo College, Karlsruhe)
April 2014	
08.-10.04.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen, Schutzmechanismen (Secorvo College, Karlsruhe)
08.-09.04.	Datenschutztage 2014 (FFD Forum für Datenschutz, Wiesbaden)
09.-10.04.	Security Forum 2014 (Hagenberger Kreis, Hagenberg/A)

Fundsache

Am 15.01.2014 hat das NIST eine überarbeitete Fassung der *Special Publication* SP 800-53 (Rev. 4) veröffentlicht. Die inzwischen 460 Seiten umfassenden *Security and Privacy Controls for Federal Information Systems* sind die amerikanische Version des IT-Grundschutzes – allerdings für drei Schutzbedarfsklassen: *low*, *moderate* und *high*. In Appendix H findet sich eine Abbildung auf die Controls des ISO/IEC 27001.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Michael Knopp, Sven Köhler, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Februar 2014



Zwischenbilanz

Neun Monate nach den ersten Enthüllungen Edward Snowdens über die Überwachungstätigkeit der NSA zeichnet sich die zukünftige Entwicklung ab. In seiner Rede vom 17.01.2014 machte Präsident Obama deutlich, dass sich allein bei der Überwachung amerikanischer Bürger und ausgewählter Staatsoberhäupter etwas ändern wird. Und RSA-CEO Art Coviello erklärte in seiner Keynote am 25.02.2014 unzweideutig: Auch amerikanische Sicherheitsunternehmen arbeiteten mit der NSA zusammen – und werden es auch künftig tun, wenn es um die (Sicherheits-) Interessen der USA geht. Selbst die Kritik namhafter Kryptologen vom 24.01.2014 zielt in erster Linie auf die Überwachung amerikanischer Bürger und die Schwächung von Sicherheitstechnologie ab. Vor diesem Hintergrund und den dank Snowden bekannten Fakten können wir daher dreierlei festhalten:

1. **Trust the Math**: Wie Bruce Schneier bereits am 06.09.2013 schrieb, gibt es keine Hinweise darauf, dass die NSA in der Lage ist, kryptografische Verfahren zu brechen, die von Kryptologen als ausreichend sicher angesehen werden. Wer „ausgemusterte" Verfahren und kurze Schlüssellängen meidet, liegt daher mit kryptografischem Ende-zu-Ende-Schutz immer richtig.
2. **Misstraue der Implementierung**: Auch gute kryptografische Verfahren lassen sich so implementieren, dass ein Angreifer leichtes Spiel hat – dank einer schwachen Schlüsselerzeugung (Pseudo-Zufall), einer Hintertür (Backdoor) oder einem Programmierfehler. Deutschen Herstellern und überprüfter oder zertifizierter Software gebührt diesbezüglich ein Vertrauensbonus.
3. **Misstraue den Vertrauensankern**: Sicherheit gibt es nicht aus dem Nichts – so wie man sich nicht am eigenen Schopf aus dem Sumpf ziehen kann, benötigt auch Sicherheit einen Vertrauensanker wie z. B. den Aussteller eines SSL-Zertifikats. Statt blindem Vertrauen ist hier eine kritische Prüfung Pflicht.



Inhalt

Zwischenbilanz

Security News

Zeit zum Wechsel

Facebook rechtswidrig

Kleiner Bug – große Wirkung

Durchsuchungsverbot

Gefahr aus dem IoT

Erweiterter Process Explorer

DIN-Norm Datenlöschung

Secorvo News

System Security

Herkunft verpflichtet.

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Zeit zum Wechsel

Die Ankündigung von Facebook, den Instant-Messaging-Dienst WhatsApp für 19 Mrd. US$ zu übernehmen, hat am 19.02.2013 für viel Wirbel gesorgt. Dieser Deal hat bei zahlreichen Nutzern das Interesse an sicheren Alternativen zu WhatsApp geweckt; auch die Stiftung Warentest stufte WhatsApp in einem am 26.02.2014 veröffentlichten Vergleichstest als „sehr kritisch" ein. Die stolze Nutzerzahl von ca. 450 Mio. könnte daher schon bald erodieren.

Bereits auf der ersten Karlsruher Anti-Prism-Party am 05.09.2013 stellten wir die aus der Schweiz stammende Alternative Threema vor. Zu einer weiteren Alternative könnte sich der Open-Source Messenger Surespot entwickeln. Die Offenheit des Quellcodes ist ein Plus für Surespot – Threema kann hingegen bei der Implementierung des Schlüsselaustausches punkten. Neben den Instant-Messengern mit Zwischenspeicherung von Daten bleibt die Nutzung von OTR über Jabber-basierte Chat-Dienste eine sichere Alternative – hierbei müssen allerdings beide Gesprächspartner online sein.

Die Downloads zur Anti-Prism-Party umfassen eine Installations- und Konfigurationsanleitung sowie weitere Informationen zur sicheren Nutzung von Internet-Diensten.

Facebook rechtswidrig

Die Berufungsentscheidung des Kammergerichts Berlin vom 24.02.2014 bestätigte Facebook, dass an Nicht-Mitglieder versandte Einladungen zur Registrierung wettbewerbswidrig und die AGB sowie die Datenschutzbestimmungen u. a. hinsichtlich der Gewinnung der Adressen rechtswidrig sind. Auch die unbestimmte, vergütungsfreie und vollständige Rechteübertragung der Inhalte an Facebook verstößt gegen geltendes AGB-Recht. Dasselbe gilt für die einschränkungslosen Änderungs- und die einseitigen Beendigungsklauseln. Die Entscheidung zum *Friend Finder* folgt der Rechtsprechung zu Empfehlungs-E-Mails (SSN 1/2014) und stellt fest, dass die Beteiligung des Nutzers bei der Versendung von Registrierungseinladungen an Dritte für die Einstufung als belästigende Werbung unmaßgeblich und die diesbezügliche Nutzereinwilligung in die Datenverwendung unwirksam ist.

Besonders brisant – und im Widerspruch zum Schleswig-Holsteinischen Verwaltungsgericht (SSN 2/2013) – wird die Anwendbarkeit deutschen Rechts bejaht: Als 100%ige Gesellschafterin habe ungeachtet aller Verträge Facebook Inc., USA, die Entscheidungsmacht. Eine Auftragsdatenverarbeitung käme in dieser gesellschaftsrechtlichen Konstellation nie in Betracht. Dieser Satz dürfte die meisten Konzerngesellschaften mit zentralen Verarbeitungsprozessen und ausländischer Muttergesellschaft mit Entsetzen erfüllen.

Kleiner Bug – große Wirkung

Die Zeilen 631 und 632 der Datei sslKeyExchange.c sehen eher harmlos aus – wird dort doch nur das eingerückte Statement „goto fail" wiederholt. Allerdings hat diese Einrückung weitreichende Wirkung – wie Apple am 21.02.2014 in einem Security Update mitteilen musste. Die offenbar bei der Entwicklung von OS X 10.9 eingeführte Änderung öffnet Man in the Middle-Angriffen auf Apple-Betriebssysteme Tür und Tor. Nach 46 Jahren werden damit Dijkstras Befürchtungen zur bitteren Realität – ein unverzügliches Update von OS X 10.9, iOS 7.0 und iOS 6.1 wird daher dringend empfohlen.

Durchsuchungsverbot

Mit einem nun ausführlich veröffentlichten Urteil vom 20.06.2013 hat das Bundesarbeitsgericht die Anforderungen an das Vorgehen bei Verdachtsmomenten gegen Beschäftigte weiter konkretisiert und den besonderen Rechtfertigungsbedarf für heimliche Überwachungsmaßnahmen verdeutlicht.

In dem entschiedenen Fall war ein Spind aufgrund eines Diebstahlsverdachts unter Einbeziehung des Betriebsrats, aber ohne Beteiligung des Betroffenen durchsucht worden. Dies führte im anschließenden Kündigungsschutzprozess wegen der Unverhältnismäßigkeit der Maßnahme zu einem Beweisverwertungsverbot.

Diese Entscheidung unterstreicht einmal mehr, dass das Vorgehen bei derartigen Untersuchungen klar geregelt und der Betroffenenbeteiligung und -information ein hoher Stellenwert eingeräumt werden sollte, um am Ende belastbare Feststellungen zu erhalten.

Gefahr aus dem IoT

Zunehmend werden Alltagsgegenstände mit eingebetteten Computern ausgestattet und über das Internet vernetzt, wie Babyphones, Videoüberwachungsanlagen oder Heimnetzwerksteuerungen. Das „Internet der Dinge" (*Internet of Things* – IoT), Mark Weisers Vision einer vernetzten Welt aus dem Jahr 1991, wird langsam Realität. Leider sind auch die damit verbundenen Gefahren inzwischen real. Symantec berichtete am 21.01.2014 über einen Linux-Wurm, der auf das IoT zielt. Der Wurm existiert für typische Chiparchitekturen des IoT.

Darauf ist das IoT jedoch nicht vorbereitet. Dort stehen wir bei der Sicherheit da, wo wir vor zwanzig Jahren bei PCs standen: Sicherheitsschwachstellen wurden nicht veröffentlicht, und falls Hersteller Patches bereitstellten, wussten die Benutzer nicht, wie diese zu installieren waren. Schlimmer noch: Soft- oder Firmware der Geräte sind im IoT oft älter als diese. Ist der Quellcode nicht vollständig verfügbar, kann nicht einmal ein Patch erzeugt werden.

Zudem sind die Geräte des IoT ständig mit dem Internet verbunden. Sie lassen sich mit der Suchmaschine Shodan sogar gezielt suchen. Dennoch werden auch solche Geräte mit einem Default-Passwort ausgeliefert. Da die Geräte meist keinen automatischen Update-Mechanismus besitzen, besteht die Gefahr, dass mit vermeintlichen Updates aus nicht autorisierter Quelle Firmware mit Hintertüren eingeschleust wird – wie bei dem am 18.02.2014 bekannt gewordenen Fall der intelligenten Haushaltsgeräte von Belkin Wemo.

Erweiterter Process Explorer

Am 29.01.2014 wurde der Process Explorer von Microsoft um eine hilfreiche Funktion ergänzt: Version 16 unterstützt nun VirusTotal-Abfragen für laufende Prozesse und die von diesen bei jedem Programmstart zahlereich hinzugeladenen Dynamic Link Librarieres. Ist die Funktion aktiviert, werden MD5-Summen gebildet und mit den Erkenntnissen von 50 verschiedenen Virenscannern bei VirusTotal abgeglichen. Ein blauer (‚gut') oder roter (‚böse') Zahlenwert weist dann auf „kritische Erkenntnisse" hin. Ein blaues Ergebnis ist allerdings eher eine „Tendenzaussage", schließlich gibt es Schadsoftware, die von diesem Werkzeug und vielen Antivirusprogrammen in einer Live-Umgebung nicht gefunden wird.

Bei der Aktivierung wird man um die Zustimmung zur Nutzungsvereinbarung von VirusTotal gebeten – in der man alle Verwertungsrechte für hochgeladene Daten an VirusTotal abtritt. Ach ja: Seit 2012 gehört VirusTotal zu Google.

DIN-Norm Datenlöschung

Im Dezember 2012 stellte Secorvo die DIN-Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten vor, die auf großes Interesse stieß. Ende 2013 startete daher ein von den Unternehmen Blancco, DATEV, Deutsche Bahn, Secorvo und Toll Collect gefördertes Projekt, in der die Leitlinie nun zu einer DIN-Norm weiterentwickelt wird. Am 12.02.2014 beschloss der DIN-Arbeitskreis für Identitätsmanagement und Datenschutz-Technologien (AK 05 im NIA 27) die Aufnahme eines Normungsprojekts.

Die Norm für Löschkonzepte soll bis zum Herbst 2015 verabschiedet werden. Die veröffentlichte Leitlinie gibt bereits heute wesentliche Hilfestellung für die Entwicklung eigener Löschkonzepte.

Secorvo News

System Security

Security Engineering – die Entwicklung inhärent sicherer Systeme – ist eine vergleichsweise junge Disziplin. In den vergangenen Jahren ist jedoch aus zahlreichen Erfahrungen und *Best Practices* ein sinnvolles Vorgehensmodell entstanden. Dabei wird die Sicherheit eines Systems aus unterschiedlichen Blickwinkeln betrachtet, um die vielfältigen Abhängigkeiten und externen Einflüsse bereits beim Systemdesign zu berücksichtigen.

In dem Seminar Security Engineering – Sichere Systeme durch Security by Design legen wir dar, wie Sicherheit in die Prozesse und Lebenszyklen der Systementwicklung integriert werden kann. Sie haben die Möglichkeit, Ihre erworbenen Kenntnisse anschließend mit dem T.E.S.S. zertifizieren zu lassen (**12.–15.05.2014**). Und falls Sie – schnell entschlossen – zuvor noch ein T.I.S.P.-Zertifikat erwerben wollen: vom **24. bis 28.03.2014** haben Sie die Gelegenheit dazu, es gibt noch einige wenige freie Plätze. Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Herkunft verpflichtet.

In modernen Informationssystemen (Stichwort *Data Warehouse* oder *Big Data*) erreicht die Verarbeitung von personenbezogenen Daten eine Komplexität, die die Umsetzung datenschutzrechtlicher Transparenzanforderungen erheblich erschwert. *Data Provenance* (Bestimmung der Datenherkunft) kann dabei unterstützen, die Herkunft und die Bearbeitung von personenbezogenen Daten sowie den Zugriff auf diese nachvollziehbar zu gestalten. Beim nächsten KA-IT-Si Event am **03.04.2014** um 18 Uhr in den Räumen des Fraunhofer IOSB in Karlsruhe zeigt Christoph Bier (Fraunhofer IOSB) in seinem Vortrag „Data Provenance. Auch Daten haben ihre Geschichte", wie die Datenschutzauskunft der Zukunft aussehen könnte.

Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2014	
24.-29.03.	T.I.S.P.-Schulung und -Prüfung (Secorvo College, Karlsruhe)
April 2014	
03.04.	Herkunft verpflichtet. (Karlsruher IT-Sicherheitsinitiative, Karlsruhe)
08.-10.04.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen, Schutzmechanismen (Secorvo College, Karlsruhe)
Mai 2014	
05.-09.05.	CPSSE (Certified Professional for Secure Software Engineering) – Schulung und Prüfung (Secorvo College, Karlsruhe)
07.-09.05.	1st DFRWS EU Conference (DFRWS, Amsterdam/NL)
11.-15.05.	Eurocrypt 2014 (IACR, Kopenhagen/DK)
12.-16.05.	Security Engineering – Schulung & T.E.S.S.-Prüfung (Secorvo College, Karlsruhe)
12.-14.05.	IMF 2014 (Fraunhofer IAO, Münster)
14.-16.05.	15. Datenschutzkongress (Euroforum, Berlin)

Fundsache

Das Portal Netzpolitik.orG verschenkt seit dem 19.02.2014 das im November 2013 erschienene Buch „Überwachtes Netz“ mit spannenden Beiträgen von Autoren wie Constanze Kurz, Frank Rieger, Markus Beckedahl, Peter Schaar, Bruce Schneier und Richard Stallman. Das Buch ist erhältlich als ePub, AZW3 oder PDF.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, Kai Jendrian, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2014



Im Netz der Spinne

Die Raumsonde Deep Space 1 wurde am 24.10.1998 zur Erforschung des Asteroiden (9969) Braille gestartet. Am 22.09.2001 nahm sie spektakuläre Bilder des Kometen 19P/Borrelly auf; am 18.12.2011 wurde sie schließlich deaktiviert.

Auch der israelische Gesichtserkennungsdienst face.com machte schon spektakulär auf sich aufmerksam. Im Juli 2011 gelang die Aufsehen erregende Erkennung von Emotionen, und im März 2012 die automatische Alterserkennung. Nach langer Freundschaft war die am 18.06.2012 von face.com bekannt gegebene Übernahme durch Facebook ein logischer Schritt. Euphorisch jubelte die Pressemitteilung: „By working with Facebook directly, and joining their team, we'll have more opportunities to build amazing products that will be employed by consumers – that's all we've ever wanted to do." Inzwischen erreicht die DeepFace getaufte Software mit Hilfe eines neuronalen Netzwerkes eine Treffergenauigkeit von 97,25 % bei der Identifikation von Personen auf einem Bild. Das menschliche Gehirn ist nur unwesentlich erfolgreicher – sofern es ebenso viele Personen kennt wie DeepFace...

Zwar wehrten sich die europäischen Datenschützer zuletzt erfolgreich gegen Facebooks Gesichtserkennung – frei nach Ovids Empfehlung in seiner Remedia amoris, die Liebe im Keim zu ersticken („Wehret den Anfängen"). Allerdings könnte es dafür bereits zu spät sein.

Denn anders als die Raumsonde Deep Space 1 macht DeepFace seine Analysen nicht im Orbit, sondern auf der Erde. Und es wäre sicherlich naiv zu hoffen, dass die Mission von DeepFace nach dreizehn Jahren durch Deaktivieren beendet wird. Denn DeepFace ist kein Forschungsprojekt, sondern eine Einnahmequelle, die perfekt in Mark Zuckerbergs selbst erklärter Mission passt, die Welt zu vernetzen.

Ein Schelm, wer dabei an eine Spinne denkt.



Inhalt

Im Netz der Spinne

Security News

Das NIST und das Vertrauen

Widerspruchsrecht bei Piwik

Full Disclosure ist tot – es lebe...

Datenschutzaufsicht zu BYOD

Nachweis des Nicht-Ereignisses

Geldfund

Secorvo News

Zertifikat mit Erkenntnisgewinn

Sicherheit ist programmierbar

Herkunft verpflichtet

Teamverstärkung

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Das NIST und das Vertrauen

NSA-Enthüllungen und der Verdacht einer Backdoor im NIST-Standard SP 800-90A für Zufallszahlengeneratoren (siehe SSN 11/2013) haben die Integrität des NIST-Entwicklungsprozesses für kryptographische Standards in Frage gestellt.

In einem öffentlichen Schreiben vom 17.02.2014 betont das NIST nun die Bedeutung der Unterstützung durch die weltweite Krypto-Gemeinde für die Akzeptanz von kryptographischen Algorithmen und bittet im Rahmen der bereits im November 2013 initiierten Überprüfung des Standardentwicklungsprozesses um Kommentare.

Die Prinzipien und Prozeduren sind als Draft NIST Interagency Report 7977 öffentlich verfügbar. Dazu zählen insbesondere die Transparenz, die Offenheit und der Ausgleich der Interessen unterschiedlicher Gruppen. Als Prozeduren kommen beispielsweise internationale kryptographische Wettbewerbe und die Veröffentlichung von Standardentwürfen zum Einsatz.

Allerdings betont das NIST, auch weiterhin eng mit der NSA (einer der Interessensgruppen) zusammen zu arbeiten, da Mitarbeiter der NSA über immense Erfahrung in der Kryptographie verfügen und das NIST per Gesetz verpflichtet ist, bei der Standardentwicklung die NSA zu befragen.

Bis zum 18.04.2014 können Kommentare eingereicht werden. Eine 90 Seiten umfassende Kommentarsammlung zum NIST SP 800-90A ist bereits verfügbar.

Widerspruchsrecht bei Piwik

Auch wenn die IP-Adressen von Seitenbesuchern mit dem Webanalyse-Tool Piwik nur anonymisiert erfasst werden, muss der Seitenbesucher eine Möglichkeit zum Widerspruch haben. Das entschied das LG Frankfurt am 18.02.2014 (Az. 3-10 O 86-12). Ein entsprechender Hinweis ist in die Datenschutzerklärung der Webseite aufzunehmen.

Damit liegt ein weiteres Urteil vor, welches die Möglichkeit einer wettbewerbsrechtlichen Abmahnung für Verstöße gegen das Telemediengesetz bejaht. Bereits das OLG Hamburg hatte mit seinem Urteil vom 27.06.2013 einen Verstoß gegen datenschutzrechtliche Informationspflichten ähnlich bewertet.

Folgt man dem Frankfurter Urteil, so muss jeder Webseiten-Betreiber „zu Beginn des Nutzungsvorgangs“ auf den Einsatz eines Webanalyse-Tools hinweisen, was bei enger Auslegung wohl bedeutet, dass sich vor dem Öffnen einer Webseite ein Pop-up-Fenster öffnen muss, welches den Besucher informiert. So etwas sieht kaum eine Webseite vor.

Dies ist eine ähnliche Forderung, wie sie die in Deutschland noch nicht umgesetzte „Cookie-Richtlinie“ (2009/136/EG) der EU enthält, die eine Einwilligung (Opt-in) für Cookies verlangt. Webseitenbetreiber sollten diese Entwicklungen im Auge behalten und in jedem Fall ihre Datenschutzerklärung aktuell und gut erreichbar halten.

Full Disclosure ist tot – es lebe...

Am 19.03.2014 hat John Cartwright, Gründer der im Jahr 2002 ins Leben gerufenen Mailing-Liste Full Disclosure, per E-Mail an die Mailing-Liste bekannt gegeben, dass er den Dienst einstellen wird. In der Liste wurden in den letzten zwölf Jahren viele wichtige Hinweise auf Sicherheitsschwachstellen anonym veröffentlicht. Die Security-Community wird diese wichtige Informationsquelle vermissen.

Das dachte sich auch Gordon Lyon – und kündigte am 25.03.2014 an, die Liste fortzuführen. Allerdings ist dafür eine Neuanmeldung erforderlich.

Datenschutzaufsicht zu BYOD

Bereits am 06.02.2014 hat der Hamburgische Landesdatenschutzbeauftragte seinen Jahresbericht für die Amtsjahre 2012/2013 vorgelegt und anhand der berichteten Vorkommnisse zu einer Vielzahl praktischer Datenschutzfragen Stellung genommen. Ein längerer Abschnitt ist dem Thema „Bring your own device“ (BYOD) gewidmet.

Die warnende Analyse des Berichts basiert auf der Prüfung der Container-Lösung DME-Extractor für iPhone und Android-Geräte in der hamburgischen Verwaltung. Grundsätzlich wird BYOD danach als sehr risikoreich eingeschätzt; der Bericht warnt vor einer Unterschätzung des Schutzbedarfs. Gefordert wird als Stand der Technik wenigstens ein Mobile Device Management, eine Container-Lösung, eine umfassende Nutzungsregelung für den Geräteeinsatz, vor allem bezüglich der Container-Löschung im Falle einer Wartung durch Dritte.

Vor einer Freigabe des Verfahrens wird ein umfassender Penetrationstest empfohlen. Die zum Bezug der verfahrensnotwendigen App (unter Android) erforderliche Registrierung des Nutzers bei Google wird wegen der verbundenen Datenübertragung von Beschäftigtendaten an Google als inakzeptabel angesehen. Allgemein seien die für die private Freizeitnutzung ausgelegten Geräte für die geschäftliche Verarbeitung von Daten mit möglicherweise hohem Schutzbedarf ungeeignet.

Vor dem Hintergrund der aufgezeigten Bedenken mutet das Résumé, der Einsatz sei sehr ‚risikoreich', inkonsequent an. Wünschenswert wäre eine klare Feststellung gewesen, dass der Einsatz bei Nichterfüllung der aufgestellten Anforderungen schlicht als rechtswidrig angesehen werden muss.

Die Stellungnahme kündigt eine abgestimmte Wertung der Datenschutzbeauftragten des Bundes und der Länder an. Diese wird sich hoffentlich in der Frage der Zulässigkeit eindeutiger festlegen, um Unternehmen eine rechtssichere Orientierung für den Datenschutz konformen Umgang mit BYOD-Bestrebungen zu geben.

Nachweis des Nicht-Ereignisses

Der BGH hat in einem Urteil vom 19.02.2014 seine Rechtsprechung zur Beweisführung bei streitigen Faxzugängen präzisiert. Die Vorinstanz hatte den Zugang – trotz vorgelegter Sendeberichte – ohne weitere Beweisaufnahme verneint, da der OK-Vermerk des Sendeprotokolls lediglich ein Indiz darstelle, aber keinen Anscheinsbeweis begründe.

Der BGH führt nun aus, dass bei vorliegendem Sendeprotokoll ein einfaches Bestreiten des Zugangs nicht ausreicht. Der Empfänger hat im Rahmen der so genannten sekundären Darlegungslast wenigstens darzustellen, welches Gerät er nutzt, ob dieses eine Verbindung verzeichnet hat, und – soweit vorhanden – sein Empfangsjournal vorzulegen. Anhand dieser Angaben hat das Gericht dann eine Beweiswürdigung vorzunehmen.

Einen Zuwachs an Rechtssicherheit bringt das Urteil jedoch weder für den Empfänger noch für den Sender. Sowohl Sendeprotokolle als auch Empfangsjournale sind regelmäßig nicht gegen Manipulationen geschützt, so dass sie nur schwache Anhaltspunkte darstellen. Das Versenden im Beisein eines Zeugen ist ein wirksamerer Beweis – umgekehrt lässt sich aber ein Nicht-Empfang schlechthin nicht bezeugen.

Da Empfangsprotokolle oft nur eine begrenzte Zeit zurückreichen und nicht wirksam gegen Manipulation geschützt werden können, und Faxgeräte zudem meist nicht nur einer Person zugänglich sind, dürfte ein wirksames Abstreiten des Empfangs in der Regel schwierig sein. Vor einer ungerechtfertigten Zurechnung schützt danach wohl nur ein vollständig digitaler Empfang mit ausführlichen und weit zurück reichenden Log-Protokollen – eine datenschutzrechtlich unschöne Lösung.

Geldfund

Die insolvente Bitcoin-Börse Mt. Gox hat am 20.03.2014 bekannt gegeben, ein Wallet mit 200.000 der vermissten 850.000 Bitcoins ‚gefunden' zu haben. Das entspricht – nach dem aktuellen Kurs – immerhin beachtlichen 90 Mio. US$. Offenbar kommen Bitcoins leicht unter die Räder: Zuletzt hatte am 27.11.2013 der britische Guardian über James Howells berichtet, der Bitcoins im Wert von 4,5 Mio. Pfund zusammen mit seiner Festplatte entsorgt hatte. Da war das Leben früher doch viel sicherer: 90 Mio. US$ in Scheinen verliert man nicht – in 50-Dollar-Bündeln wiegen diese 1,8 Tonnen.

Secorvo News

Zertifikat mit Erkenntnisgewinn

Auf rund 190 Jahre summiert sich die Berufserfahrung aus unterschiedlichen Tätigkeitsfeldern der Informationssicherheit der elf Secorvo-Referenten in der fünftägigen T.I.S.P.-Schulung. Die nächste Gelegenheit, von diesem Erfahrungsschatz als Teilnehmer eines Secorvo-T.I.S.P.-Seminars unmittelbar zu profitieren, bietet sich Ihnen **vom 19. bis 23.05.2014**.

Sicherheit ist programmierbar

Wenn grundsätzlich im Software-Entwicklungsprozess Sicherheit als wesentliches Entwurfskriterium von Anfang an berücksichtigt werden würde, dann gäbe es viele heutige Sicherheitsprobleme definitiv nicht. Doch was noch nicht ist, kann ja noch werden: Als Certified Professional for Secure Software Engineering (CPSSE) kennen Sie – oder Ihre Kollegen – die Techniken und Vorgehensweise von „Security by Design". Das nächste Seminar mit noch freien Plätzen findet statt **vom 05. bis 08.05. 2014**. (Online-Anmeldung).

Herkunft verpflichtet

"Data Provenance. Auch Daten haben ihre Geschichte." ist das Thema des nächsten KA-IT-Si-Events am **03.04.2014** um 18 Uhr im Max-Syrbe-Saal des Fraunhofer IOSB in Karlsruhe. Christoph Bier (Fraunhofer IOSB) wird in seinem Vortrag zeigen, wie die Datenschutzauskunft der Zukunft aussehen könnte. Anschließend gibt es – wie gewohnt – Gelegenheit zum „Buffet-Networking". Wir freuen uns auf Ihre Anmeldung.

Teamverstärkung

Wieder konnten wir eine Verstärkung für das Consulting-Team gewinnen: Am 01.03.2014 ist André Domnick zu uns gestoßen. Er bringt viel Erfahrung in den Bereichen sichere Softwareentwicklung und Web Application Security mit – und einen Bachelor in Information Security.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2014	
03.04.	Herkunft verpflichtet. (Karlsruher IT-Sicherheitsinitiative, Karlsruhe)
08.-09.04.	Datenschutztage 2014 (FFD Forum für Datenschutz, Wiesbaden)
09.-10.04.	Security Forum 2014 (Hagenberger Kreis, Hagenberg/AT)
Mai 2014	
05.-09.05.	CPSSE (Certified Professional for Secure Software Engineering) – Schulung und Prüfung (Secorvo College, Karlsruhe)
07.-09.05.	1st DFRWS EU Conference (DFRWS, Amsterdam/NL)
11.-15.05.	Eurocrypt 2014 (IACR, Kopenhagen/DK)
12.-14.05.	IMF 2014 (Fraunhofer IAO, Münster)
12.-16.05.	Security Engineering – Schulung & T.E.S.S.-Prüfung (Secorvo College, Karlsruhe)
14.-16.05.	15. Datenschutzkongress (Euroforum, Berlin)
19.-24.05.	T.I.S.P. - Schulung und Prüfung (Secorvo College, Karlsruhe)
21.-23.05.	Entwicklertag 2014 (VKSI, Karlsruhe)

Fundsache

Apple hat am 20.02.2014 eine aktualisierte Version der Dokumentation zur iOS Security veröffentlicht. Darin erläutert Apple viele Sicherheitsfeatures, über die bisher lediglich spekuliert werden konnte. Lesenswert.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Yun Ding, Dr. Safuat Hamdy, Kai Jendrian, Michael Knopp, Christoph Schäfer (Editorial), Jochen Schlichting.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2014



Was jetzt zählt

Nicht jeder IT-Sicherheitsverantwortliche wird dieses Editorial lesen können – denn der eine oder andere wird noch mit den Aufräumarbeiten nach „Heartbleed“ beschäftigt sein. Dennoch sollte in der unvermeidlichen operativen Hektik nicht übersehen werden, was genau dieser JAB (*Just Another Bug*) uns eigentlich lehren müsste.

IT-Sicherheit hat viel mit Vertrauen zu tun. Das ist aber mehr Not als Tugend – denn wünschen würden wir uns, dass wir uns von der Vertrauenswürdigkeit einer Soft-, Hard- oder Cloudwarelösung, der wir unsere Kommunikation oder unsere Daten anvertrauen, zuverlässig überzeugen könnten.

Leider funktioniert das meistens nicht. So steht der Aufwand für die Analyse oft in keinem realistischen Verhältnis zum Schutzbedarf der Daten – oder bedroht gar die Wirtschaftlichkeit des Geschäftsmodells des Nutzers. Zudem ist jede Analyse immer nur eine Momentaufnahme: Jede Änderung am System (Konfiguration, Firmware, Hardware, Software, ...) kann ein zunächst positives Urteil in sein Gegenteil verkehren. Was bleibt ist bestenfalls ein strenger Vertrag mit dem Anbieter, das Einspielen von Patches und die fromme Hoffnung, dass die eigene Infrastruktur verschont bleibt.

Allerdings gibt es Bereiche, in denen wir uns nicht mit solcherart halbblindem Vertrauen begnügen dürfen: den „Herzstücken“ unserer IT-Sicherheitsinfrastrukturen – zu denen angesichts der weiten Verbreitung und zentralen Bedeutung zweifellos OpenSSL gezählt werden muss. Es hilft auch nicht, wie nach dem Bekanntwerden von Prism gebetsmühlenartig nach „Security made in Germany“ zu rufen – denn unglücklicherweise war es gerade ein deutscher Programmierer, dem die Welt nun Heartbleed verdankt.

In den zentralen Organen unserer Infrastrukturen brauchen wir mit Methoden der sicheren Softwareentwicklung erzeugten und nachprüfbar verifizierten Code. Sich dabei lediglich auf die Offenheit des Sourcecodes zu verlassen, ist schlicht unverantwortlich.



Inhalt

Was jetzt zählt

Security News

Persilschein für Office 365

XP ist tot...

Ende der Verantwortungsabschiebung

Schutz durch Big Data

Open Source-Desaster

Secorvo News

PKI für Profis

Live Hacking

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Persilschein für Office 365

Mit seiner Cloud-Kollaborationslösung Office 365 will Microsoft seine Kunden von komplizierten Lizenzverträgen befreien. Die neuen nutzerbezogenen Lizenzmodelle können dabei zu hohen Einsparungen führen. Um das Angebot datenschutzrechtlich abzusichern, hat Microsoft ein Vertragskonstrukt entworfen, welches eine Vereinbarung zur Auftragsdatenverarbeitung mit Microsoft Irland (Standort des europäischen Rechenzentrums) vorsieht. Da die Lizenzverwaltung und der Support durch Microsoft USA erfolgen, ist außerdem der Abschluss von EU Model Clauses erforderlich. Die Vertragsvorlagen können über das Office 365 Trust Center bezogen werden.

Mit Schreiben vom 29.11.2011 hatte das Bayerische Landesamt für Datenschutzaufsicht bereits die grundsätzliche Eignung der Microsoft-Verträge bestätigt. Nach intensiven Diskussionen liegt nun mit Datum vom 02.04.2014 eine weitere Bestätigung der Artikel-29-Gruppe vor, die Microsoft seit dem 10.04.2014 als Persilschein nutzt. Dabei sollte man allerdings nicht vergessen, dass man für die Übermittlung im Rahmen von EU Model Clauses nach wie vor eine Rechtsgrundlage benötigt. Ob es zudem ratsam ist, einen erheblichen Teil der Unternehmensdaten in die Hand eines (US-) Dienstleisters zu legen, steht auf einem anderen Blatt.

XP ist tot...

Mit dem Sicherheitsupdate MS14-020 veröffentlichte Microsoft am 08.04.2014 die letzten Patches für Windows XP und Microsoft Office 2003. Beide Produkte erfreuen sich jedoch weiterhin großer Beliebtheit. Die britische Regierung, das Land Niedersachsen und weitere Großkunden schlossen daher Verträge über ein weiteres Jahr Support für ihre Systeme ab. Den meisten Nutzern der beiden Softwarepakete werden jedoch weitere Updates verwehrt bleiben.

Voraussichtlich wird die Zahl der Schwachstellen und Exploits ansteigen – auch weil Windows XP und Office 2003 sich mit den neueren Versionen große Teile des Quellcodes teilen. So lassen sich aus zukünftigen Sicherheitsupdates mit einfachen Reverse Engineering-Techniken wie binären Diff-Tools die behobenen Schwachstellen ausfindig machen – von dort ist der Weg zum funktionierenden XP-Exploit nicht mehr weit.

Immerhin: Eingebettete Alt-Systeme wie Bankautomaten sind von dem Problem meist nicht betroffen, da sie überwiegend Windows XP Embedded verwenden – und das wird bis 2016 mit Updates versorgt.

Ende der Verantwortungsabschiebung

In einem mit Spannung erwarteten Urteil hat der Europäische Gerichtshof am 08.04.2014 die Richtlinie zur Vorratsdatenspeicherung (RL 2006/24/EG) rückwirkend für ungültig erklärt. Die europarechtliche Pflicht zur Einführung einer Vorratsdatenspeicherung ist damit entfallen.

Der EuGH folgt in seinem Urteil weitgehend der Argumentation, die bereits das Bundesverfassungsgericht seinem Urteil zu Grunde gelegt hatte: Der schwerwiegende Eingriff in Art. 7 und 8 der Charta der Grundrechte der Europäischen Union sei nur verhältnismäßig, wenn die Verwendung der Daten anhand klarer Kriterien begrenzt, die Datensicherheit durch strikte Regeln gewährleistet und die Speicherdauer anhand objektiver Kriterien auf das absolut Notwendige beschränkt werde. Auch schreibe die Richtlinie keine Speicherung im Unionsgebiet vor, so dass nicht sichergestellt sei, dass die Umsetzung der Datensicherheitsanforderungen durch eine unabhängige Stelle der EU überwacht werden könne.

Zwar berührt auch nach Auffassung des EuGH die Vorratsdatenspeicherung nicht den Wesensgehalt der Chartagrundrechte. Doch kann sich jetzt keine Regierung eines Mitgliedsstaats mehr bei der Einführung einer Vorratsdatenspeicherung hinter einer europäischen Umsetzungspflicht verstecken.

Schutz durch Big Data

Am 25.03.2014 stellte Mark Hammell auf der Webseite der Facebook-Sicherheitsinitiative „protectthegraph“ vor, wie Facebook Security-Informationen automatisiert verarbeitet – mit hauseigenen Big Data-Techniken.

Die Komponente Feeds sammelt ständig sicherheitsnahe Informationen aus freien und abonnierten externen und eigenen Quellen und reichert diese mit Kontextdaten wie Ort und Zeit an. Dies können Daten von Malware-Diensten sein, Hinweise aus Infoportalen, Security-Blogs oder Informationen der eigenen Security-Teams.

Diese Daten werden jeweils als Thread-Datum im Hieve, dem Hadoop-Datawarehouse von Facebook archiviert. Das für Massendaten entwickelte Analysewerkzeug Scuba untersucht jedes neue Thread-Datum auf Trends oder Muster und startet Reaktionsprozesse – Blacklisting gefährlicher URLs, Benachrichtigung von Nutzern oder Alarmierung des Security-Teams.

In internen Tests habe dieses System die eingesetzten Antiviren-Produkte geschlagen. Dieses Ergebnis steht und fällt jedoch mit aktuellen externen Informationen, wie von Lösungsanbietern kritisiert wurde. Es deutet aber daraufhin, dass das Teilen von Information z. B. über erkannte Angriffsmuster oder eigene Vorfälle für alle Beteiligten – außer dem Angreifer natürlich – Vorteile bietet.

Innerhalb einiger Branchen gibt es dieses kooperative Vorgehen bereits. Was fehlt ist allerdings ein einheitliches Datenformat. Dessen Spezifikation wäre einmal eine sinnvolle Aufgabe für eine der zahlreichen Cybersecurity-Initiativen.

Open Source-Desaster

Gleich mehrere verbreitete Open Source-Lösungen standen in den vergangenen Wochen im Rampenlicht. Zunächst sorgte bekanntlich am 07.04.2014 das Security Announcement von OpenSSL, inzwischen als Heartbleed bekannt, für Furore (siehe Editorial). Die Schwachstelle ermöglicht das (spurlose) Auslesen von 64 kByte großen Speicherbereichen eines SSL-Servers. Der Programmierfehler wurde weder während des Reviews noch in den zwei darauffolgenden Jahren bemerkt, bis Neel Mehta von Google ihn entdeckte und dem OpenSSL-Team meldete.

Mit den Updates für iOS 7.1 vom 23.03.2014 und iOS 7.1.1 sowie die Safari Browser 6.1.3 und 7.0.3 vom 22.04.2014 behob Apple einen weiteren, als „Triple Handshake" bezeichneten Bug in der SSL/TLS-Implementierung sowie zahlreiche Schwachstellen in der Open-Source-HTML-Engine WebKit, die von Safari und vielen weiteren Browsern genutzt wird. Von den 27 Schwachstellen in WebKit wurden 26 durch Programmierfehler verursacht, die den Datenspeicher korrumpieren: Beim Besuch manipulierter Webseiten kann damit Code vom Angreifer auf dem Rechner des Opfers ausgeführt werden.

Das Google Chrome Security Team fand 18 der 26 Schwachstellen, da Chrome die Engine Blink verwendet, die im April 2013 aus dem Sourcecode von WebKit abgespaltet worden war. Dabei konnte Google 8.8 Millionen Codezeilen entfernen. Möglicherweise schlummern noch immer etliche Bugs in WebKit, die Google bereits in Chrome beseitigt hat – bis Apple sie eines Tages findet.

Schließlich erschien am 14.04.2014 der Bericht über den ersten Teil des Source-Code-Audits zu TrueCrypt. Er dokumentiert eine gründliche Prüfung des Bootloaders und des Kernel-Treibers. Zwar wurden keine gravierenden Schwachstellen aufgedeckt; dennoch gibt die Bewertung „*Overall, the source code for both the bootloader and the Windows kernel driver did not meet expected standards for secure code*" zu denken.

Zur Vermeidung von gravierenden Schwachstellen in so grundlegenden Bausteinen der Sicherheit sollte die Offenheit des Codes mit der gebotenen Professionalität beim Entwickeln und prüfen kombiniert werden (siehe SSN 01/2014). Hierzu bedarf es entsprechender Anreize und Ressourcen. Initiativen wie das Open Crypto Audit Project zeigen einen möglichen Weg dafür auf.

Secorvo News

PKI für Profis

Seit den späten 90er Jahren realisiert Secorvo PKI-Projekte. Der dabei entstandene, Produkt unabhängige Erfahrungsschatz in Sachen Konzeption, Aufbau, Betrieb und Weiterentwicklung wurde für das Seminar „PKI – Grundlagen, Vertiefung und Realisierung" in einem viertägigen Programm verdichtet. Die fünf Referenten des Seminars bringen zusammen über 90 Jahre Berufserfahrung in der IT-Sicherheit mit. Für den Einsteiger bietet die Schulung eine grundlegende, Produkt unabhängige Einführung, für den Profi eine vertiefende Auseinandersetzung mit den Möglichkeiten von Public Key Infrastrukturen. Nächster Seminartermin ist der 24. bis 27.06.2014.

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Live Hacking

Live-Hacking-Demos haben gelegentlich vor allem Show-Charakter – die vorgestellten Angriffe betreffen entweder längst ausgemusterte IT-Systeme oder führen für einen praktischen Angriff eher ungeeignete Spezialschwachstellen vor.

Nach dem großen Erfolg der Live-Vorführung eines äußerst wirkungsvollen WLAN-Angriffs auf der vergangenen Anti-Prism-Party am 12.02.2014 im Karlsruher ZKM werden Kai Jendrian und Jörg Völker von Secorvo den Angriff und einige einfache und elementare Maßnahmen zum Schutz der Privatsphäre auf der kommenden Veranstaltung der KA-IT-Si am **05.06.2014** erneut vorstellen (18 Uhr im Panoramasaal der IHK Karlsruhe).

Nach Vortrag und Diskussion haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" – diesmal über den Dächern von Karlsruhe. Weitere Informationen und die Möglichkeit zur Anmeldung auf www.ka-it-si.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2014	
05.-09.05.	CPSSE (Certified Professional for Secure Software Engineering) – Schulung und Prüfung (Secorvo College, Karlsruhe)
07.-09.05.	1st DFRWS EU Conference (DFRWS, Amsterdam/NL)
11.-15.05.	Eurocrypt 2014 (IACR, Kopenhagen/DK)
12.-14.05.	IMF 2014 (Fraunhofer IAO, Münster)
14.-16.05.	15. Datenschutzkongress (Euroforum, Berlin)
16.05.	Jahrestagung "Datenschutz im digitalen Zeitalter – global, europäisch, national" (Institut für Rundfunkrecht an der Universität zu Köln, Köln)
19.-20.05.	a-i3/BSI-Symposium 2014 (Arbeitsgruppe Identitätenschutz im Internet/BSI, Bochum)
21.-22.05.	BvD Datenschutztage (BvD e. V., Berlin)
21.-23.05.	Entwicklertag 2014 (VKSI, GI, Objekt-Forum, Karlsruhe)
Juni 2014	
23.-24.06.	DuD 2014 (Computas, Berlin)
23.-26.06.	OWASP AppSec EU 2014 (OWASP, Cambridge/UK)

Fundsache

Damn Vulnerable iOS App ist eine App, die alle gängigen Sicherheitslücken von iOS-Anwendungen enthält – sie ist „verdammt verwundbar". Diese App bietet Sicherheitsinteressierten eine Plattform, auf der sie iOS-Penetrationtests legal durchführen können.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, André Domnick, Kai Jendrian, Michael Knopp, Sven Köhler, Christoph Schäfer.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Mai 2014



Das Fressen und die Moral

Noch hat sich der von Edward Snowden aufgewirbelte Staub nicht gelegt, da feiern amerikanische Cloud-Anbieter schon wieder erste Siege im Kampf um europäische Kunden. Denn nicht nur Microsoft buhlt mit Office 365 um die Gunst der IT-Kostenreduzierer, auch Google hat den Markt entdeckt und mit Apps for Business eine Unternehmenslösung im Angebot. Die Vorteile einer „Alle-Büroanwendungen-ins-Netz"-Lösung sind offenkundig: Installation, Konfiguration und Wartung (Patches, Pflege) von Client- und Serversystemen entfallen, Lizenzkosten sind besser kalkulierbar und die Software ist ständig auf dem neuesten Stand. Diese Angebote sind eine Herausforderung für die traditionellen Geschäftsmodelle der Anbieter von Standardsoftware: sie sind billiger, aktueller und oft bedienungsfreundlicher als die gewohnten „Software-Boliden".

Microsoft versucht dieser Herausforderung durch die Flucht nach vorne zu begegnen und bemüht sich, die eigenen Kunden von Microsoft 365 zu überzeugen. Und stößt dabei auf Widerstand – denn die Übermittlung personenbezogener Daten in Drittstaaten, die dabei allein durch den Wartungszugriff aus den USA auf das Rechenzentrum in Irland unvermeidlich erfolgt, ist nicht ohne weiteres zulässig. Mit an das EU-Recht angepassten Verträgen und Vereinbarungen mit der Art.-29-Gruppe versucht Microsoft, eine saubere Rechtsgrundlage zu schaffen (siehe SSN 4/2014). Wer sich darauf einlässt, sollte wissen, dass von der rechtlich geforderten „Kontrolle" der Verarbeitung durch den Auftraggeber keine Rede sein kann – wer das nicht glaubt, der versuche einmal, eine Prozessbeschreibung für den Wartungszugriff von Microsoft zu erhalten.

Und noch eines: Wer mit dem Gedanken spielt, sein in Daten geronnenes Know-How auf fremde Server auszulagern, der sollte zumindest voher prüfen, wie schnell er den eigenen Betrieb wieder aufnehmen kann, sollte der Dienst eines Tages plötzlich nicht mehr zur Verfügung stehen.



Inhalt

Das Fressen und die Moral

Security News

Heartbleed und PKI Basics

Agentenfrühstück

Triple Handshakes

Revolution per Urteil

Aktuelle Studien

Kassierte Datenschutzaufsicht

Secorvo News

Seminare nach der Sommerpause

Selbstschutz zum Nachlesen

Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Heartbleed und PKI Basics

Am 09.05.2014 hat Netcraft aktuelle Zahlen zu Reaktionen auf die Heartbleed Schwachstelle veröffentlicht: 57 % der Betreiber betroffener Webseiten haben den Kopf in den Sand gesteckt und akzeptieren das Risiko. Ebenfalls bedenklich: Weitere 16 % ließen sich zwar ein neues Zertifikat ausstellen, nicht aber ein neues Schlüsselpaar. Daran wird deutlich, dass das Vertrauensmodell einer PKI noch nicht von jedem Betreiber verstanden wurde. Für einen korrekten Umgang mit Heartbleed empfehlen wir einen Blick in die Hinweise des DFN-CERT.

Agentenfrühstück

Jérome Nokin stellte am 17.04.2014 auf der Full-Disclosure-Mailingliste sein Angriffswerkzeug ePolicy 0wner vor. Es ermöglicht auf einfache Weise Schwachstellen behaftete Versionen von McAfees zentraler Management-Lösung für Virenschutz (bis v4.6.6) ‚zum Frühstück' zu kapern. Brisant ist, dass damit nicht nur der Management-Server, sondern auch alle darüber verwalteten Clients übernommen werden können. Ursachen dieser verketteten Schwachstelle sind die weltweit einheitliche Anmeldung am Management-Server (zur Aufnahme von zu verwaltenden Clients) und Schwachstellen in den Management-Protokollen, welche typische Angriffe via SQL-Injection (CVE-2013-0140) oder Directory Traversal (CVE-2013-0141) ermöglichen. Über die hoch privilegierten Virenschutz-Agenten können durch Ausnutzung dieser Schwachstellen die Client-Systeme über den Server angegriffen werden.

Dieses Problem hat nicht nur McAfee: auch bei Symantec Endpoint Protection (CVE-2013-1612) und AVG wurden ähnliche Schwachstellen gefunden. Ein Update oder – bei exponierten Systemen – eine Neuinstallation und Aktualisierung der betroffenen Systeme wird dringend empfohlen.

Agenten stellen generell eine Gefährdung dar, wie weitere aktuelle Beispiele z. B. bei Nagios-Agenten zeigen: Überwachte Server mit Schwachstellen im Nagios-Agent wurden gemäß den Recherchen von Link11 für das Mining von virtuellen Währungen genutzt. Die aktuellen Vorfälle machen einmal mehr dreierlei deutlich:

1. Auch Software, die Sicherheit schaffen soll, kann Schwachstellen enthalten: Haben Sie dies in Ihren Bedrohungsanalysen berücksichtigt?

2. Für Sicherheitssoftware braucht man Sicherheitskonzepte, die Angriffsmöglichkeiten der Agenten als Szenario umfassen.

3. Weniger kann mehr sein: Ein System, das keine Agenten hat, ist vielleicht nicht so schön administrierbar – dafür ist es schwieriger anzugreifen, wenn an anderer Stelle etwas schief geht.

Triple Handshakes

Die am 04.03.2014 publizierte TLS-Schwachstelle Triple Handshakes ging zwischen anderen „Bug-Aufregern" der vergangenen Monate unter. Dabei handelt es sich nicht um einen Implementierungs-, sondern um einen Designfehler im TLS-Protokoll, der mehrere gängige Webbrowser betraf und mittlerweise in allen großen Browsern beseitigt wurde (darunter Firefox, Chrome und Safari für iOS 7.1.1).

TLS definiert drei verschiedene Arten von „Begrüßungen": Ein *Standard Handshake* wird beim Aufbau einer TLS-Verbindung durchgeführt. Dabei authentifiziert sich oft nur der Server (z. B. die Webseite einer Bank). Nutzt der Client die gleiche SSL-Verbindung anschließend für den Zugriff auf eine geschützte Ressource, initiiert der Server einen *Renegotiation Handshake* für die nachträgliche Client-Authentifikation. Ein *Resumption Handshake* schließlich dient der Performanceoptimierung. Bei einem Triple-Handshakes-Angriff vermittelt ein Angreifer als Man-in-the-Middle die drei Handshakes und übernimmt schließlich als authentifizierter Client die Verbindung zum Server.

Die Sicherheit der einzelnen Handshake-Protokolle wurde formal nachgewiesen. Der Triple-Handshakes-Angriff nutzt jedoch eine subtile Interaktion zwischen den drei Protokollen. Das TLS-Protokoll wurde in den vergangenen 20 Jahren immer wieder um neue Funktionen erweitert und mit Bug-Fixes geflickt. Vielleicht ist es an der Zeit für einen komplett neuen Entwurf...

Revolution per Urteil

Mit seinem Urteil vom 13.05.2014 gegen Google Spain SL hat der EuGH Betroffenen das Recht zugesprochen, von Suchmaschinen die Streichung von Treffern aus der Ergebnisanzeige zu verlangen. Voraussetzung ist, dass die Treffer einer Suche nach dem Betroffenennamen sich auf personenbezogene Daten des Anspruchstellers beziehen, dieser überwiegende Interessen oder Grundrechtspositionen geltend machen kann und das europäische Datenschutzrecht anwendbar ist.

Damit bejaht der EuGH zugleich die Zuständigkeit der spanischen Datenschutzaufsicht und die Anwendbarkeit des spanischen Datenschutzrechts. Rechtsgrundlage der Suche sei das berechtigte Interesse gemäß Art. 7 f der DS-Richtlinie (RL 95/46/EG). Diese entfalle, sobald der Betroffene widerspreche und entgegenstehende, schutzwür-

dige Interessen geltend mache. Hierfür reiche es bereits, dass die Daten durch Zeitablauf nicht mehr für ihren Zweck erheblich sind. Die Beurteilung sei völlig unabhängig von der Datenquelle, der andere Interessen oder Ausnahmen (journalistische Zwecke z.B., Art. 9 DS-RL) zugrunde liegen können.

Der praktische Nutzen des schlüssigen Urteils ist allerdings begrenzt, da der Betroffene die Suchmaschinen nur einzeln und begrenzt auf den Anwendungsbereich der Datenschutzrichtlinie in Anspruch nehmen kann. Die klare Position zur nationalen Zuständigkeit dürfte allerdings Bewegung in die laufenden Streitigkeiten mit internationalen Internetriesen in Deutschland bringen.

Aktuelle Studien

In den Monaten April und Mai sind vier umfangreiche Reports zur aktuellen Sicherheitslage erschienen. Zunächst veröffentlichte am 15.04.2014 WhiteHat Security ihren „2014 Website Security Statistics Report“. Er dokumentiert die häufigsten Sicherheitsprobleme aus Anwendungssicht. Am 23.04.2014 folgte Verizon mit ihrem „2014 Data Breach Investigations Report“, der die Ergebnisse der Untersuchung von über 100.000 Sicherheitsvorfällen in Unternehmen zusammenfasst. Am 05.05.2014 publizierte das Ponemon Institute mit die „2014 Cost of Data Breach Study“, die sich den finanziellen Schäden von Sicherheitsvorfällen widmet. Am 12.05.2014 schließlich erschien der Bericht „Protecting personal data in online services: learning from the mistakes of others“ des britischen Information Commissioner's Office, in dem Schlussfolgerungen aus bekannt gewordenen Sicherheitsvorfällen gezogen werden („learning from the mistakes of others“).

Zusammen vermitteln die Ergebnisse der Studien einen aktuellen und schonungslosen Eindruck von der weltweiten IT-Sicherheitslage.

Kassierte Datenschutzaufsicht

Das Verwaltungsgericht Berlin hat am 13.01.2014 eine Löschanordnung des Berliner Datenschutzbeauftragten aufgehoben. Der betroffene Hersteller von Stadtkarten speichert bei sämtlichen Bearbeitungen Namen und Bearbeitungszeit der Beschäftigten einer beauftragten Agentur, um seine Urheberrechte nachweisen zu können. Da diese Daten in verschiedenen Urteilen zu Urheberansprüchen in der Beweisführung von Gerichten verlangt wurden, hat das VG Berlin die Erforderlichkeit und das berechtigte Interesse des Herstellers anerkannt.

Die Urteilsbegründung gibt allerdings zu denken. So geht das Gericht von § 28 Abs. 1 Nr. 2 BDSG als Erlaubnistatbestand aus, zitiert im Sachverhalt jedoch eine Einwilligungserklärung, die den Betroffenen abverlangt wurde – und Mängel aufweist. Die zulässige Speicherdauer wird nicht betrachtet; dafür stellt es die Praxis anderer Gerichte bei der Beweisführung im Urheberrechtsstreit pauschal über die Betroffeneninteressen. Offenbar haben auch Richter Nachholbedarf in Sachen Datenschutzrecht.

Secorvo News

Seminare nach der Sommerpause

Die T.I.S.P.-Schulung von Secorvo bereitet nicht nur auf die Zertifikatsprüfung vor, sondern bietet geballtes Erfahrungswissen aus über 200 Jahren Berufserfahrung in der Informationssicherheit. Wenn Sie davon profitieren möchten, merken Sie sich den 22.-26.09.2014 vor. Wollen Sie sich auf den aktuellen Stand beim Thema IT-Sicherheit bringen, empfehlen wir Ihnen die Teilnahme am Seminar IT-Sicherheit heute (30.09.-02.10.2014).

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Selbstschutz zum Nachlesen

Die auf den erfolgreichen Anti-Prism-Partys im September 2013 und Februar 2014 vorgestellten „Anleitungen zum Selbstschutz“ gibt es nun auch ausführlich: Sie erschienen in Ausgabe 5/2014 der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“. Die digitalen Fassungen der von Secorvo verfassten Beiträge sind über unsere Webseite abrufbar.

Tag der IT-Sicherheit

Am **09.07.2014** richtet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) gemeinsam mit der IHK Karlsruhe, dem CyberForum e.V. und KASTEL bereits den 6. Tag der IT-Sicherheit aus (ab 14 Uhr im Haus der Wirtschaft der IHK Karlsruhe).

Die diesjährige Veranstaltung beleuchtet IT-Sicherheit und Datenschutz aus der Compliance-Perspektive. Mit einer Keynote von Frau Dr. Birte Mössner, Leiterin Corporate Compliance und Datenschutz der EnBW, einem Beitrag von TechniData über das nicht immer einfache Verhältnis von IT-Managern und Sicherheitsverantwortlichen, einem Vortrag von Secorvo zu den datenschutzrechtlichen Fallstricken im Marketing und der Vorstellung der technischen Sicherheit bei 1&1 bieten vier Karlsruher Unternehmen kompetente Best Practice-Einblicke – flankiert von der Gelegenheit zum fachlichen „Networking“. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2014	
02.-03.06.	AREA41 Security Conference (DC4131 DEFCON Switzerland, Luzern/CH)
05.06.	Live Hacking (KA-IT-Si, Karlsruhe)
23.-24.06.	DuD 2014 (Computas, Berlin)
23.-26.06.	OWASP AppSec EU 2014 (OWASP Foundation, Cambridge/UK)
24.-27.06.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
Juli 2014	
09.07.	6. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
August 2014	
02.-07.08.	Blackhat USA 2014 (Blackhat, Las Vegas/US)
03.-06.08.	14th Annual DFRWS Conference 2014 (DFRWS, Denver/US)
07.-10.08.	DEF CON 21 (DEFCON, Las Vegas/US)
17.-21.08.	Crypto 2014 (IACR, Sanata Barbara/US)

Fundsache

Mitarbeiter von ESET, einem Anbieter von Virenschutzlösungen, haben mit einer am 18.03.2014 veröffentlichten, fast 70seitigen Studie eine umfassende Analyse der Schadsoftware-Kampagne „Windigo“ legt, in deren Verlauf über Jahre systematisch SSH-Credentials gestohlen und Webseitenbesucher auf infizierte Seiten umgeleitet wurden.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, Stefan Gora, Kai Jendrian, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Juni 2014



Die Vertrauensattacke

Während das US-amerikanische Repräsentantenhaus am 23.06.2014 mit überwältigender Mehrheit (293:123 Stimmen) der NSA untersagte, Hintertüren in US-amerikanische IT-Produkte einzubauen und die Internet-Aktivität amerikanischer Bürger ohne Gerichtsbeschluss zu überwachen, blieben wichtige Aspekte der Geheimdiensttätigkeit ungeregelt.

Vor dem Hintergrund der amerikanischen Überwachungsaktivitäten der vergangenen 20 Jahre wird ein bedenkliches Gesamtbild erkennbar. In den 90er Jahren versuchte die NSA vergeblich, sich den Zugriff auf verschlüsselte Daten zu sichern: Schwache Verschlüsselungsverfahren, wie der auf Drängen der NSA von 128 auf 56 bit Schlüssellänge verkürzte DES, waren durch öffentlich evaluierte, starke Verfahren wie den AES ersetzt worden. Und das „Law Enforcement Access Field" (LEAF), mit dem sie sich eine Entschlüsselungsmöglichkeit erhalten wollte, scheiterte 1994 an einer blamablen Protokollschwäche.

Danach verlegte sich die NSA auf eine verdeckte Universalstrategie – und attackierte jeden möglichen Angriffspunkt der entstehenden, auf SSL basierenden Vertrauensinfrastruktur:

- SSL-Serverbetreiber, deren geheimer SSL-Schlüssel die Entschlüsselung mitgeschnittener Kommunikation ermöglichte,
- Zertifizierungsinstanzen, die Schlüsselpaare erzeugten (und damit auch Zugang zu geheimen SSL-Schlüsseln besaßen),
- Zertifizierungsinstanzen, die der NSA falsche SSL-Zertifikate für Man-in-the-Middle-Angriffe ausstellten,
- möglicherweise auch (Open)SSL-Implementierungen, um Hintertüren in Soft- oder Firmware zu verankern und
- Standardisierungsgremien, um Zufallszahlengeneratoren mit Vorhersagemöglichkeit für die NSA zu etablieren (SSN 11/2013).

Das Ergebnis ist ein Scherbenhaufen: Vertrauensverlust in SSL, amerikanische Anbieter und die Standardisierung. Wer wird das kitten?



Inhalt

Die Vertrauensattacke

Security News

Sicherer im Netz mit Tails

Dämmer im Dunkel

Cyberabwehr in der Kritik

Ende der WLAN-Störerhaftung

E2E-Verschlüsselung in Chrome

Folgen des Suchmaschinenurteils

Secorvo News

Das Buch, der T.I.S.P. und das Zertifikat

6. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Sicherer im Netz mit Tails

Am 10.06.2014 wurde Version 1.0.1 des Live-Betriebssystems Tails veröffentlicht. Tails kann von einem USB-Stick gestartet werden und eröffnet den Internetzugang standardmäßig über das Tor-Netzwerk. Weitere Maßnahmen zum Schutz der Privatsphäre sind die Veränderung der MAC-Adresse sowie die GPG-Unterstützung des E-Mail-Clients. Um Angriffswege zu reduzieren ist zudem in der Grundeinstellung der Root-Account deaktiviert.

Im Test lief Tails auf verschiedenen Laptops einwandfrei, mit ordentlicher Bildschirmauflösung und WLAN-Unterstützung – ohne dass die Grundkonfiguration angepasst werden musste. Will man eine dauerhafte Datenpartition auf dem Stick anlegen, sollte man Tails von einem bereits laufenden Tails – beispielsweise von DVD gestartet – kopieren. Auf der verschlüsselten Partition können dann eigene Dateien abgelegt werden. Tails hinterlässt keine Spuren auf dem genutzten Rechner.

Tails macht einen durchdachten Eindruck und ist ein möglicher Weg, einen „ergrauten" XP-Rechner mit einem aktuellen Betriebssystem auszustatten – das gelingt sogar im „XP-Look", wenn man diese Option beim Starten auswählt.

Dämmer im Dunkel

TK-Unternehmen haben Transparenzberichte als Mittel entdeckt, um ihrer juristischen Machtlosigkeit gegenüber staatlichen Zugriffen zumindest ihren guten Willen zum Schutz der Kundendaten entgegenzusetzen. So bestätigt Vodafone in einem am 06.06.2014 veröffentlichen Bericht, in 29 Staaten Behörden Zugriff auf Telekommunikationsdaten gewähren zu müssen.

Dabei werden deutliche Unterschiede in Art und Umfang der Zugriffe erkennbar. In Deutschland müssen TK-Anbieter auf Grundlage von § 5 des Artikel 10-Gesetzes, § 110 Abs. 1 Nr. 5 TKG und § 27 TKÜV staatlichen Stellen Zugriff auf die bei ihnen gespeicherten Daten gewähren. Dazu speichern sie die relevanten Daten in einer so genannten *interception copy* („Überwachungskopie"), die dem Nachrichtendienst übergeben wird. Vorher werden die Daten nach vorgegebenen Suchbegriffen gefiltert – und nicht relevante Teile gelöscht.

Ein solch umständliches Vorgehen ist in zumindest sechs Staaten, die Vodafone nicht namentlich benennt, nicht erforderlich: Dort müssen TK-Anbieter Direktzugriffe gewähren. In Albanien, Ägypten, Indien, Malta, Katar, Rumänien, Südafrika, Türkei und Ungarn darf zudem nicht darüber berichtet werden, wie und in welchem Umfang Überwachungsmaßnahmen erfolgen. Auch ohne weitere Snowdens wissen wir nun immerhin, wer sich neben den USA noch an unseren TK-Daten bedient.

Cyberabwehr in der Kritik

Das holperige Kürzel ist Programm: Irgendwie ist niemand mit dem seit dem 01.04.2011 tätigen Nationalen Cyberabwehrzentrum (NCAZ) so recht glücklich. Die einen wundern sich, dass Deutschland mit zehn Mitarbeitern im „Cyberwar" bestehen will. Verfassungsrechtler schlagen Alarm, da die vorgeschriebene Trennung zwischen Nachrichtendiensten und Polizei durch das NCAZ ad absurdum geführt werde – immerhin arbeiten ihm das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz (BfV), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundeskriminalamt (BKA), die Bundespolizei (BPol), das Zollkriminalamt (ZKA), der Bundesnachrichtendienst (BND) sowie die Bundeswehr zu. Vernichtend äußert sich der Bundesrechnungshof in einem nicht öffentlichen Bericht, aus dem die Süddeutsche am 07.06.2014 zitierte: Danach sei das NCAZ „*nicht geeignet, die über die Behördenlandschaft verteilten Zuständigkeiten und Fähigkeiten bei der Abwehr von Angriffen aus dem Cyberraum zu bündeln.*" Der Nutzen der Einrichtung sei fraglich. Der Bundesrechnungshof rät, das „*Abwehrzentrum (...) mit eigenen Aufgaben und Kompetenzen für die Abwehr von Cyberangriffen*" auszustatten.

Allein das BMI sieht das NCAZ als Erfolgsgeschichte: Bis März 2013 habe es 900 nationale und internationale IT-Sicherheitsvorfälle bewertet. Sensationelle 1,2 Vorfälle pro Tag.

Ende der WLAN-Störerhaftung

Endlich hat der Bundesgerichtshof die Urteilsbegründung zu seinem am 08.01.2014 verkündeten Urteil zur Störerhaftung des Anschlussinhabers bei Urheberrechtsverletzungen veröffentlicht. Das Urteil schließt an die Entscheidung „Sommer unseres Lebens" an, in dem die Haftung bejaht worden war (SSN 06/2010). Im aktuellen Fall verwies der Beklagte auf die WLAN-Mitnutzung volljähriger Familienangehöriger, und der BGH verlangte lediglich eine überzeugende Darlegung, dass es weitere (familienangehörige) WLAN-Nutzer gäbe. Auch bei einer unzureichenden Sicherung könne eine Vermutung der Täterschaft des Anschlussinhabers nicht greifen. Schließlich ergebe sich selbst eine Überwachunspflicht von Minderjährigen (SSN 11/2012) erst bei Anzeichen für eine missbräuchliche Nutzung.

In einem ähnlichen Fall wies das AG Hamburg am 10.06.2014 die Haftung des Betreibers eines

Ferienhotels zurück, der seinen Mietern ein WLAN zur Nutzung anbot: Es erkannte ihn als Dienste-anbieter an, womit der Haftungsausschluss des § 8 TMG greift. Nach dieser Rechtsprechung sinkt das Risiko von Abmahnungskosten für Anschluss-inhaber, die Mieter oder Familienangehörige als Mitnutzer zulassen.

E2E-Verschlüsselung in Chrome

Am 03.06.2014 hat Google die Alpha-Version von „End-to-End“ angekündigt, eines Verschlüsselungs-tools für den Chrome-Browser. Überraschender-weise soll es nicht den S/MIME-Standard, sondern OpenPGP unterstützen und damit einen mit PGP und GnuPG kompatiblen, verschlüsselten E-Mail-Austausch ermöglichen.

Die Implementierung erfolgte in JavaScript. Es werden ausschließlich ECC-Schlüssel erzeugt; RSA-Keys können aber aus einem anderen Schlüsselring importiert werden.

Einige wichtige Fragen rund um die Implementie-rung beantwortet Google in einer FAQ. Nach der Testphase soll die End-to-End-Erweiterung im Google Web Store bereitgestellt werden. Jetzt wird es vor allem von der Bedienungsfreundlichkeit der Browser-Erweiterung abhängen, ob sich diese Lösung bei Privatnutzern durchsetzen kann.

Folgen des Suchmaschinenurteils

Als Reaktion auf das Suchmaschinenurteil des EuGH (SSN 05/2014) stellte Google ein Löschantragsfor-mular bereit, von dem bereits rege Gebrauch ge-macht wurde. Inzwischen hat Microsoft angekün-digt, mit seiner Suchmaschine Bing nachzuziehen.

Die Blockierung der Suchergebnisse erfolgt jedoch nur gegenüber europäischen Suchmaschinennut-zern; allen anderen werden die Ergebnisse weiter angezeigt. Da der EuGH in seinem Urteil Google Inc. als verantwortliche Stelle spanischem Datenschutz-recht unterworfen hat, reicht die regional begrenzte Sperrung jedoch nicht aus; sie muss für den gesamten Dienst des Betreibers erfolgen.

Zudem stellt die Authentifizierung der Antragsteller ein ungelöstes Problem dar. In der ersten Version des Formulars hatte Google rechtswidrig die Vorlage einer Personalausweiskopie verlangt; die aktuelle Version fordert eine Kopie eines „identifizierenden Dokuments“ – keine geeignete, Missbrauch aus-schließende Identifizierungsform. Für die Prüfung behält sich Google die Einschaltung der Aufsichts-behörden vor. Wie Anträge geprüft werden sollen, zu denen eine Begründung verlangt wird, ist derzeit noch offen.

Secorvo News

Das Buch, der T.I.S.P. und das Zertifikat

Mitte Juni haben wir die erweiterte, aktualisierte und überarbeitete Ausgabe unseres Grundlagen-buchs „Zentrale Bausteine der Informationssicher-heit“ fertiggestellt. Das auch für die Vorbereitung auf eine T.I.S.P.-Zertifizierung geeignete, 700 Seiten starke Begleitbuch ist bereits als E-Book (pdf) verfügbar; die gebundene Fassung ist noch im Druck, kann aber schon bestellt werden und wird voraussichtlich in der zweiten Julihälfte geliefert.

Die nächste Gelegenheit zur Vorbereitung auf das T.I.S.P.-Zertifikat bieten wir vom **22.–27.09.2014**., alternativ können Sie sich auf dem Seminar „IT-Sicherheit heute“ (**30.09.–02.10.2014**) auf den aktuellen Stand bringen lassen.



Alle Termine und Seminarangebote sowie die Mög-lichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

6. Tag der IT-Sicherheit

Bereits zum sechsten Mal findet am **09.07.2014** der „Tag der IT-Sicherheit“ statt, den die KA-IT-Si jährlich gemeinsam mit dem CyberForum e.V., der IHK Karlsruhe und KASTEL veranstaltet. Frau Dr. Birte Mössner, Leiterin Corporate Compliance und Daten-schutz der EnBW beleuchtet in ihrer Keynote die Relevanz des Datenschutzes im Compliance-Kon-text. Während TechniData auf das nicht immer einfache Verhältnis von IT-Managern und Sicher-heitsverantwortlichen und Secorvo auf die daten-schutzrechtlichen Fallstricke im Marketing eingeht, steht bei 1&1 die technische Sicherheit im Mittel-punkt. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2014	
09.07.	6. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
August 2014	
02.-07.08.	Blackhat USA 2014 (Blackhat, Las Vegas/US)
03.-06.08.	14th Annual DFRWS Conference 2014 (DFRWS, Denver/US)
07.-10.08.	DEF CON 21 (DEFCON, Las Vegas/US)
17.-21.08.	Crypto 2014 (IACR, Sanata Barbara/US)
20.-22.08.	23rd USENIX Security Symposium (Usenix, San Diego/US)
25.-25.08.	Sommerakademie (ULD Schleswig-Holstein, Kiel)
September 2014	
16.-19.09.	OWASP AppSec USA 2014 (OWASP Foundation, Denver/US)
16.-17.09.	D • A • CH Security (GI, OCG, BITKOM, SI, TeleTrusT, Graz/AT)
18.09.	Informationstag "Elektronische Signatur" 2014 (TeleTrust, Berlin)

Fundsache

Die Agentur der Europäischen Union für Grundrechte, der Europarat und die Kanzlei des Europäischen Gerichtshofs für Menschenrechte haben am 05.06.2014 ein gut strukturiertes, 220 Seiten starkes Handbuch zum Europäischen Datenschutzrecht in fünf Sprachen herausgegeben.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Juli 2014



Verdeckte Profilbildung

Mit Erfolg haben sich Datenschützer gegen die Speicherung der IP-Adresse (als ein oft auf eine natürliche Person beziehbares Datum) und von Cookies gewehrt, die eine Verknüpfung von zeitlich auseinanderliegenden Nutzungsvorgängen ermöglichen. Der EU waren letztere sogar die wenig technikneutrale „Cookie-Richtlinie“ (RL 2009/136/EG) wert.

Tatsächlich aber handelt es sich dabei um ein Randthema. Denn das Kernproblem ist nicht Identifikation, sondern Profilbildung: Gelingt es einem Webseitenanbieter, Nachrichtendienst oder – schlimmer noch – Werbungs-Vermittler (wie Google oder Facebook), Seitenzugriffe zu einem eindeutigen Profil zu verdichten, so entwickelt sich daraus ein äußerst aussagekräftiger „Schattenriss“ eines, wenn auch zunächst anonymen, Benutzers.

Dieses Internet-Verhaltensprofil wird dabei mehr und mehr zum Abbild unserer Identität. Für den Anbieter kommt es dabei nur auf die Wiedererkennung an – und die gelingt ihm auch ohne Cookies und IP-Adressen, z. B. durch *Canvas Fingerprinting*. Dabei werden mittels versteckter HTML5-Kommandos Unterschiede im Zeichensatz-Rendering identifiziert, die von Grafikkarte, Treiber-Versionen und installierten Zeichensätzen abhängen. Kombiniert mit anderen Browser-Spezifika wie aktiven PlugIns oder Konfigurationseinstellungen ist heute so eine nahezu eindeutige Rechner-Wiedererkennung möglich – unbemerkt vom Nutzer und nur durch ständigen Rechnerwechsel zu verhindern.

Daher springt das jüngst gefeierte „Recht auf Vergessen“ gegenüber Suchmaschinen (SSN 5/2014) zu kurz. Denn was ist das Wissen aus Veröffentlichtem gegenüber einem vollständigen Profil unserer Internet-Nutzung? Wenn technische Mechanismen eine solche Profilbildung gegen den Willen der Betroffenen nicht verhindern, mutiert das Internet – ganz ohne NSA und BND – unweigerlich von einer Informations- zu einer verdeckten Überwachungsinfrastruktur.



Inhalt

Verdeckte Profilbildung

Security News

Google-Projekt Zero

Telefonwerbung

Mit Licht ins WLAN

Europas großer Wurf

Einfallstor Virenschutz

Passwords are dead – again...

Secorvo News

Know-How-Update

3. Staffel der Anti-Prism-Party

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Google-Projekt Zero

In der Vergangenheit haben Google-Mitarbeiter zahlreiche Sicherheitslücken in Software gefunden, die im Zusammenhang mit Google-Produkten zum Einsatz kommen. Dazu gehören die OpenSSL Heart-Bleed-Schwachstelle und Schwachstellen in der Open-Source HTML-Engine WebKit (siehe SSN 04/2014). Motiviert durch diese Erfolge kündigte Google am 15.07.2014 an, unter dem Projekt-namen Zero ein Team mit Sicherheitsexperten auf-zubauen, das sich in Vollzeit um Internetsicherheit kümmern soll. Ihr Ziel: Zero-Day-Schwachstellen finden, bevor sie von Kriminellen oder staatlichen Behörden genutzt werden, um Rechner zu infizie-ren, sensible Daten zu stehlen oder Kommunikation zu überwachen. Die Bug-Suche ist dabei nicht auf Google-Produkte beschränkt, da deren Sicherheit oft von der Sicherheit fremder Software abhängt.

Google will die gefundenen Lücken ausschließlich an die betroffenen Hersteller melden und mit ihnen gemeinsam an einem Fix arbeiten. Anschließend werden alle Lücken in einer Datenbank veröffent-licht; dazu existiert bereits eine eigene Blogseite. Eine löbliche Initiative, die der Sicherheit von Soft-ware erneut Auftrieb geben könnte.

Telefonwerbung

Telefonwerbung unterliegt spätestens seit der Ein-führung des § 7 Abs. 2 Nr. 2 UWG im Jahr 2004 erheblichen Beschränkungen. Neben dem wettbe-werbsrechtlichen Einwilligungserfordernis ist auch die Verwendung der Telefonnummer zu Werbe-zwecken ein Fallstrick. Das Verwaltungsgericht Berlin hat in einem Urteil vom 07.05.2014 die anzulegenden Maßstäbe klargestellt.

Das Gericht wies die Klage gegen eine Anordnung des Berliner Beauftragten für Datenschutz und Informationsfreiheit ab, nach der die Klägerin die Praxis ihres Call-Centers beenden sollte, im Rahmen von telefonischen Kundenzufriedenheitsbefragun-gen eine Einwilligung in Werbeanrufe zu erbitten. Das Verwaltungsgericht bestätigt, dass dabei eine Verwendung der Telefonnummer für zwei unter-schiedliche Zwecke vorliegt. Während die Frage nach der Kundenzufriedenheit nach § 28 Abs. 1 Nr. 1 BDSG zulässig sei, habe die Frage nach einem Opt-In für Werbeanrufe bereits Werbecharakter. Hierfür sei § 28 Abs. 3 BDSG eine abschließende Spezialregelung. Erforderlich sei eine Einwilligung des Betroffenen vor dem Anruf.

Das sehr klare, wenn auch noch nicht rechtskräftige Urteil stärkt die Bedeutung der sorgsamen Diffe-renzierung von Einzelzwecken in einem Verfahren und stellt klar, dass Datenschutzrecht nicht durch eine Vermengung mit einem im Vordergrund stehenden Zweck umgangen werden darf.

Mit Licht ins WLAN

Das „Internet der Dinge“ hält noch viele Über-raschungen mit Sicherheitsimplikationen bereit. Eine davon hat Alex Chapman am 04.07.2014 in seinem Blog-Post „Hacking into Internet Connected Light Bulbs“ aufgedeckt: Bei der Analyse des Zu-sammenspiels von über das Internet verbundenen Lampen stellte er fest, dass das Wi-Fi-Passwort des Netzwerks, in dem sich die Lampen befinden, bei der Kommunikation zwar mit AES verschlüsselt wird, der verwendete Schlüssel aber in der Firmware der Lampen fest verdrahtet ist. Damit öffnen die Leuchten die Tür zum heimischen WLAN. Wer über Wi-Fi verbundene Geräte nutzt, sollte stutzig werden, wenn es an einer Eingabemöglichkeit für das WLAN-Passwort mangelt…

Europas großer Wurf

Vor gut zwei Jahren, am 04.06.2012, hatte die Europäische Kommission einen Verordnungsent-wurf zu Diensten der elektronischen Identifizierung und Vertrauensdiensten für elektronische Transak-tionen im Binnenmarkt vorgestellt. Nun wurde die Verordnung am 16.07.2014 vom Europäischen Rat angenommen. Sie tritt nach Veröffentlichung im Amtsblatt in Kraft und gilt ab dem 01.07.2016; zu diesem Zeitpunkt hebt sie die Signaturrichtlinie auf.

Die Verordnung regelt als unmittelbar geltendes Recht den Rechtsrahmen für elektronische Signa-turen, Siegel, Zeitstempel, Dokumente, Zustel-lungs- und Zertifizierungsdienste für die Webseiten-authentifizierung. Außerdem legt sie die Voraussetzungen für die Anerkennung von elektro-nischen Identifizierungssystemen fest und enthält Vorschriften für die Anbieter der genannten Dienste. Ohne Berücksichtigung geltender nationaler Regelungen legt die Verordnung Beweisregeln fest.

Dabei verweist fast jeder Artikel der Verordnung auf von der Kommission noch zu erlassende Rechtsakte zu technischen Spezifikationen, Verfahren, Maßnah-men, Meldeinhalten und intereuropäischen Abstim-mungen, ohne dass es hierfür klare Vorgaben gäbe. Für Deutschland wird nun die Anpassung einer Reihe von Gesetzen anstehen: Signaturgesetz, De-Mail-Gesetz, Personalausweisgesetz, Verwaltungs-verfahrensgesetze und viele weitere Regelungen sind von der Verordnung betroffen. Zu den Vertrau-ensdiensten gehören auch die in Deutschland bislang aus systematischen Gründen ausgeschlos-senen Fremdsignaturen, bei denen die Signaturer-

stellungseinheit Dritten überlassen wird. Umgekehrt entfällt die deutsche Sonderform der qualifizierten Signatur mit Anbieterakkreditierung.

Damit stehen dem elektronischen Rechtsverkehr nicht nur in Deutschland erhebliche Veränderungen bevor – ohne erkennbare Vertrauenssteigerung. Wie dabei die unvermeidliche Rechtsunsicherheit und die in einigen Bereichen erheblichen Umstellungskosten zu einer größeren Akzeptanz elektronischer Signatur- oder Identifikationstechniken führen sollen, bleibt das große Geheimnis des Verordnungsgebers. Offenbar wähnt sich dieses Paralleluniversum frei von der Geltung profaner Marktmechanismen.

Einfallstor Virenschutz

Virenschutz-Software soll vor Viren schützen – und schafft dabei neue Angriffsflächen, denn sie besitzt höchste Berechtigungen, die sie für Angreifer besonders interessant macht. Außerdem öffnet sie jede Schadsoftware – besitzt sie Schwachstellen, lassen diese sich daher besonders leicht ausnutzen.

Und tatsächlich ist es mit der Sicherheit von Anti-Viren-Software bei weitem nicht so gut bestellt, wie man erwarten könnte: Am 23.07.2014 veröffentlichte Joxean Koret die Ergebnisse seiner Analyse von 17 AV-Lösungen, die er eine Woche zuvor auf der SyScan360 in Singapur vorgestellt hatte. Seine Erkenntnisse machen sprachlos: die meisten Produkte laden Updates via HTTP, in 14 fand er klassische Schwachstellen wie *Heap Overflows*, *Remote Command Injection* und Fehler in Entpacker-Routinen – Ansätze wie ASVS sind den Herstellern offenbar unbekannt. Angesichts dieser Schwachstellen gehört der zentrale Virenscanner im Netz auf ein isoliertes System.

Passwords are dead – again...

Online-Passwortdienste füllen Passwortfelder aus, arbeiten plattformübergreifend, verwalten Passwörter von Millionen Nutzern – und stellen daher attraktive Angriffsziele dar. Im August werden Forscher der Universität Berkeley auf dem 23. Usenix Security Symposium eine Untersuchung zur Sicherheit von Online-Passwortmanagern vorstellen, die Schwachstellen in der Implementierung aller fünf untersuchten Produkte aufdeckte. So war das automatische Einloggen auf Webseiten via Bookmarklets angreifbar, drei Lösungen hatten XSS- oder CSRF-Schwachstellen, zwei prüften die Autorisierung beim *credential sharing* nicht, zwei waren über die Benutzeroberfläche angreifbar. Seit August 2013 sind die Hersteller informiert; LastPass und RoboForm haben die beanstandeten Schwachstellen nach eigenen Angaben inzwischen beseitigt.

Grundsätzlich sind Passwörter aber auch im Kopf nicht sicher und verursachen Kosten durch Passwort-Rücksetzungen und -Wechsel. Die Alternative sind lokal speichernde Passwortmanager – bei denen man sich allerdings selbst um die Verfügbarkeit kümmern muss.

Secorvo News

Know-How-Update

Der ständigen Weiterentwicklung des Themas IT-Sicherheit versuchen wir mit unserem Seminar „IT-Sicherheit heute“ Rechnung zu tragen: Das Programm unterziehen wir einer ständigen Aktualisierung und Überarbeitung. Besonders zu empfehlen als Auffrischung Ihres Basiswissens – die nächste Möglichkeit zur Teilnahme bieten wir vom **30.09.–02.10.2014** (anrechenbar mit 21 CPEs).

Wie sich sichere Softwareentwicklung in die Entwicklungsprozesse integrieren lässt, vermittelt unser Zertifikatslehrgang Certified Professional for Secure Software Engineering (CPSSE) vom **20.–24.10.2014**. Für Ihre T.I.S.P.-Zertifizierung bieten wir in diesem Jahr noch zwei Termine: vom **22.–26.09.2014** und vom **10.–14.11.2014** jeweils mit anschließender Prüfung – und der aktualisierten und überarbeiteten Neuauflage des T.I.S.P.-Buchs. Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

3. Staffel der Anti-Prism-Party

Zwei Auflagen der größten Cryptoparty Europas mit 650 bzw. 900 Teilnehmern gab es bereits. Doch aller guten Dinge sind drei – daher veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) anlässlich der Uraufführung des Edward-Snowden-Stücks „Ich bereue nichts“ am Badischen Staatstheater am **Samstag, 11.10.2014** eine dritte Staffel der Anti-Prism-Party. Dort erfahren Sie alles, was Sie schon immer über Verschlüsselung wissen wollten, aber bisher nicht zu fragen wagten.

Auf Bühnen und an Stationen in den Foyers des Staatstheaters zeigen Karlsruher IT-Sicherheits- und Datenschutzexperten in Live-Vorführungen, wie man Tracking verhindert, seine Passwörter wählt und geschützt aufbewahrt, E-Mails vor fremdem Zugriff schützt, Chats verschlüsselt und wie File-Sharing in der Cloud sicher wird. Derweil können sich Ihre Kinder zum Verschlüsselungsexperten ausbilden lassen. Krönender Abschluss ist ein **Anti-Prism-Plenum** im Kleinen Haus.

Aktuelle Informationen zum Programm der Anti-Prism-Party gibt es in einem eigenen Newsletter und auf Twitter.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2014	
02.-07.08.	Blackhat USA 2014 (Blackhat, Las Vegas/US)
03.-06.08.	14th Annual DFRWS Conference 2014 (DFRWS, Denver/US)
07.-10.08.	DEF CON 22 (DEFCON, Las Vegas/US)
17.-21.08.	Crypto 2014 (IACR, Santa Barbara/US)
20.- 22.08.	23rd USENIX Security Symposium (Usenix, San Diego/US)
25.- 25.08.	Sommerakademie (ULD Schleswig-Holstein, Kiel)
September 2014	
16.-17.09.	D • A • CH Security (GI, OCG, BITKOM, SI, TeleTrusT, Graz/AT)
16.-19.09.	OWASP AppSec USA 2014 (OWASP Foundation, Denver/Colorado)
22.-27.09.	T.I.S.P.-Schulung und Prüfung (Secorvo, Karlsruhe)
30.09.	Anwendertag IT-Forensik (Fraunhofer, Darmstadt)
30.09.-02.10.	IT-Sicherheit heute (Secorvo, Karlsruhe)

Fundsache

Am 30.06.2014 veröffentlichte die KPMG eine Studie zu den Auswirkungen des von der Bundesregierung geplanten IT-Sicherheitsgesetzes. Danach werden im Bereich der kritischen Infrastrukturen knapp 18.500 (Groß-)Unternehmen von den Meldepflichten erfasst, deren Bürokratiekosten sich auf 1,1 Mrd. € summieren werden – ein teures Vergnügen.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, Kai Jendrian, Michael Knopp, Sven Köhler

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2014



Semantische Authentizität

Eines der elementaren Schutzziele der Informationssicherheit ist die Authentizität. Sie bezeichnet die Echtheit und Vertrauenswürdigkeit einer Information. In der Fachliteratur wird Authentizität praktisch ausschließlich im Zusammenhang mit der technisch überprüfbaren Urheberschaft einer elektronischen Nachricht oder eines Datensatzes verwendet: Mit Schutzmechanismen wie digitalen Signaturen oder anderen, unter realistischen Annahmen praktisch unfälschbaren Authentikatoren stellt man sicher, dass ein Datum eindeutig einem technischen System oder menschlichen Urheber zugeordnet werden kann. Ein vernünftiger Ansatz in der Welt der IT-Sicherheit.

In der Welt der Informationssicherheit hingegen springt ein solches Verständnis zu kurz. Denn Echtheit und Vertrauenswürdigkeit einer *Information* sind mehr als die eines *Datums* – erstere erfordert nämlich nicht nur *syntaktische*, sondern auch *semantische* Authentizität. Zwar ist der Unterschied bei vielen technischen Vorgängen vernachlässigbar: Wer eine Transaktion elektronisch signiert, möchte damit die Echtheit seiner Willenserklärung bestätigen.

Wie steht es aber mit veröffentlichten Informationen? Am 26.02.2014 demonstrierte Bryan Seely, wie sich Angaben in Google Maps fälschen lassen – mit womöglich dramatischen Folgen z. B. für ein betroffenes Unternehmen (falsche Telefonnummer oder E-Mail-Adresse, Hinweis „Seit 01.01.2014 insolvent“ o. ä.). Hier würde ein Berechtigungskonzept mit strikter Identitätsprüfung helfen. Bei Wikipedia ist das schon schwieriger: Tendenziöse Beiträge, verdeckte Werbung oder vorsätzliche Falschaussagen lassen sich weder durch Peer Review noch durch Identitätsprüfungen ausschließen. Und wie kann man die Verbreitung von Fälschungen wie das Youtube-Video eines Adler-Angriffs auf ein Kleinkind wirksam verhindern?

Lösen wir dieses Authentizitätsproblem nicht, werden wir uns womöglich bald in einer Welt wiederfinden, in der sich Wahrheit und Lüge nicht mehr auseinanderhalten lassen.



Inhalt

Semantische Authentizität

Security News

Rechtsrisiko Spam-Filter

Die Yetis kommen

Klare Fristen

USB – eine ignorierte Gefahr

Kein privates Auskunftsrecht

Datenschutzfolgenabschätzung

Secorvo News

Zertifikate sind Trumpf

Gretchenfrage

„Das Buch“ auf der it-sa

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Rechtsrisiko Spam-Filter

Das LG Bonn hat mit einem Ende Juni veröffentlichten Urteil vom 10.01.2014 bestätigt, dass auch eine im Spam-Ordner gelandete E-Mail zugegangen ist – und einen Rechtsanwalt, dem so eine E-Mail mit einem Vergleichsangebot einer gegnerischen Partei entgangen war, zu 90.000 € Schadensersatz verurteilt. Erste Reaktionen auf das Urteil stellten das Konzept der Spam-Filter in Frage. Allerdings räumte der Beklagte in dem abgeurteilten Fall den Empfang der E-Mail ein; der rechtssichere Nachweis eines bestrittenen Zugangs einer E-Mail dürfte hingegen selbst mittels der Serverprotokolle des Absenders schwierig sein. Ein Anscheinsbeweis verbietet sich im Umkehrschluss zu § 5 Abs. 8 De-Mail-G und § 371a Abs. 2 ZPO.

Zweifellos besteht eine Rechtspflicht zur Prüfung von zugegangenen E-Mails; darin enthaltene Willenserklärungen sind wirksam (§ 130 Abs. 1 BGB), ob vom Empfänger wahrgenommen oder nicht. Wird eine E-Mail hingegen wie beim Greylisting vom Server temporär abgewiesen, erreicht sie die Sphäre des Empfängers nicht und gilt daher nicht als zugegangen. Abweisungen aufgrund einer Blacklist könnten allerdings als Nachrichtenunterdrückung gewertet werden – Spam-Filterung bleibt daher ein vermintes Gelände.

Die Yetis kommen

Am 31.07.2014 veröffentlichten die Kaspersky Labs Hintergründe über Crouching Yeti – eine Angriffswelle, der bisher 3.000 Unternehmen zum Opfer gefallen sind, darunter viele Maschinenbauer. Das Vorgehensmuster: Die IT des Ziel-Unternehmens wird über einen von drei Wegen infiziert: über maliziöse XDP-Dokumente, die mit individualisierten E-Mails, so genanntem Spear-phishing versandt werden, über präparierte SCADA-Softwarepakete, die statt der Originale auf Anbieterseiten platziert werden, oder über eine watering hole-Attacke, bei der gezielt branchentypische Webseiten gehackt werden – ein Besuch dieser Seiten infiziert dann das Zielunternehmen. Die Steuerung der Angriffe und der Abgriff von Daten erfolgen über gehackte Webserver.

Lehrreich sind die Details: So werden ausschließlich bekannte Exploits z. B. aus dem Metasploit-Umfeld genutzt; dagegen schützt ein aktueller Virenschutz. Den Austausch von Update-Paketen auf Hersteller-Webseiten kann eine Prüfung der Pakete nach dem Download aufdecken. Und im Netz des Opferunternehmens sucht die Malware gezielt nach SCADA-Systemen; deren Abschottung würde verhindern, dass sie gefunden und infiziert werden. Da die Yeti-Angriffe andauern, ist eine schnelle Maßnahmenumsetzung angeraten.

Klare Fristen

Am 03.07.2014 hat der BGH in seinem zweiten Revisionsurteil zur Speicherung von Verkehrsdaten durch die Deutsche Telekom bestätigt, dass eine Speicherfrist von sieben Tagen zum Zweck der Erkennung, Eingrenzung oder Beseitigung von Störungen (§ 100 Abs. 1 TKG) ausreicht. Damit wird die im Urteil des OLG Frankfurt vom 28.08.2013 festgelegte Frist bestätigt, die fehlende Wochenenddienste und die Bearbeitungsdauer bestimmter Meldungen berücksichtigt.

Die Festlegung von Löschfristen für Log-Daten ist ein ständiges Thema der Datenschutzpraxis. Zwar begründet der BGH die Frist einerseits mit den spezifischen Verhältnissen der Telekom; das Urteil selbst geht aber von deren Vergleichbarkeit aus. Die Sieben-Tage-Frist sollte daher für jegliche Form der Protokollierung zur Abwehr von Störungen und Angriffen als Obergrenze gewählt werden.

USB – eine ignorierte Gefahr

Am 07.08.2014 sorgten Carsten Nohl und Jacob Lell auf der BlackHat in Las Vegas mit ihrem Vortrag BadUSB für Aufsehen: Sie stellten vor, wie sich verbreitete USB-Controller umprogrammieren und in Angriffswerkzeuge verwandeln lassen. Zwar ist mindestens seit 2005 bekannt, dass USB-Geräte für Angriffe missbraucht werden können. Neu ist allerdings, dass ein Angreifer ohne spezielle Hardware handelsübliche USB-Sticks umprogrammieren kann. Zwar ist das Feature seit 1999 in der USB-Spezifikation als Device Firmware Upgrade vorgesehen – ein Einfallstor, über das schon die nPA-App stolperte (SSN 11/2010). Dass dieselbe Gefahr bei USB-Sticks lauert, wurde offenbar erst jetzt wahrgenommen.

Bis alle USB-Hersteller erklärt haben, ob ihre Geräte von BadUSB betroffen sind, sollten Sie daher bei der Nutzung fremder oder der Weitergabe eigener USB-Hardware zurückhaltend sein. Virenschutz oder Device Control helfen gegen diesen Angriff nicht, da das betroffene Device sich dem kontrollierenden Rechner gegenüber beliebig „maskieren“ kann.

Kein privates Auskunftsrecht

Der Bundesgerichtshof erteilte am 01.07.2014 dem Anspruch von Privatpersonen auf Auskunft über die Nutzeridentität bei einer Verletzung von Persönlichkeitsrechten eine klare Absage. In dem entschiedenen Fall wollte ein Arzt gegen Nutzer eines Bewertungsportals vorgehen und verlangte von dem Portalbetreiber Auskunft über deren Identität.

Das Zivilrecht kennt für solche Fälle einen Auskunftsanspruch aus § 242 BGB nach Treu und Glauben. In der Anfang August veröffentlichten Urteilsbegründung stellt der BGH jedoch klar, dass nach § 14 Abs. 1 Telemediengesetz Bestandsdaten von Nutzern nur für Zwecke des Anbieter-Nutzer-Verhältnisses verwendet werden dürfen. Eine anderweitige Erlaubnis muss auf das Telemediengesetz Bezug nehmen (§ 12 Abs. 2 TMG); das ist bei § 242 BGB nicht der Fall. Mangels datenschutzrechtlicher Erlaubnis darf der Portalbetreiber daher keine Auskunft geben.

So hat der BGH mit seinem Urteil zum Schutz von Pseudonymen im Internet beigetragen. Allerdings ist nach § 14 Abs. 2 TMG Ermittlungsbehörden Auskunft zu erteilen, so dass die Nutzeridentität per Strafanzeige aufgedeckt werden kann. Daher könnte nun das Strafrecht zum Vehikel zivilrechtlicher Auseinandersetzungen werden.

Datenschutzfolgenabschätzung

Fast neun Jahre hat die Entwicklung und Verabschiedung einer RFID-Strategie durch die EU-Kommission gedauert: vom Arbeitspapier zum Einsatz von RFID der Artikel-29-Gruppe (Arbeitsgruppe der europäischen Datenschutz-Aufsichtsbehörden) vom 28.09.2005 über die erste Konsultation der EU-Kommission und die öffentliche Konsultation vom 03.07.2006, deren Ergebnisse am 16.10.2006 publiziert wurden, bis zum Vorschlag einer RFID-Strategie vom 15.03.2007, deren Empfehlungen am 12.05.2009 angenommen wurden. Das Rahmenwerk für die dabei eingeführte Datenschutzfolgenabschätzung (PIA) wurde am 12.01.2011 vorgestellt und kurz darauf von der Artikel-29-Gruppe bestätigt.

Seit Juli 2014 gelten nun EU-weit technische Normen zur Nutzung von RFID (EN 16570:2014) und zur Datenschutzfolgenabschätzung (EN 16571:2014), konkretisiert in mehreren Technischen Richtlinien (CEN/TR 16670:2014, 16672:2014-16674:2014).

Damit werden eine einheitliche Informations- und Kennzeichnungspflicht durch ein neues RFID-Zeichen eingeführt und ein verlässlicher Rechtsrahmen geschaffen. Ein Schritt in die richtige Richtung: Mit der Einführung der Datenschutzfolgenabschätzung, die auch in der geplanten EU-Datenschutz-Grundverordnung vorgesehen ist, sollen die Standards für klare Vorgaben und mehr Transparenz sorgen.

Secorvo News

Zertifikate sind Trumpf

Wenn Sie zu den Kurzentschlossenen zählen, können Sie sich noch einen der letzten freien Plätze des Seminars „IT-Sicherheit heute“ (**30.09.-02.10.2014**, 21 CPEs) sichern. Oder im Oktober und November 2014 Ihre Erfahrungen und Kenntnisse auffrischen und mit einem Zertifikat krönen:

Wie integriert man sichere Softwareentwicklung in die Entwicklungsprozesse? Das ist Thema des Zertifikatslehrgangs „ISSECO Certified Professional for Secure Software Engineering (CPSSE)“ vom **20. bis 24.10.2014**. Wie es gelingt, die Sicherheit eines Gesamtsystems zu konzipieren, und wie sich dies in der Praxis umsetzen lässt, erfahren Sie im Zertifikatsseminar „Security Engineering – Sichere Systeme durch Security by Design (T.E.S.S.)“ vom **17. bis 22.11.2014**. Und vom **10. bis 14.11.2014** können Sie Ihr Know-How und Ihre mehrjährige Erfahrung im Bereich Informationssicherheit mit der Zertifizierung zum „TeleTrusT Information Security Professional (T.I.S.P.)“ abrunden.

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/college.

Gretchenfrage

Selber machen oder machen lassen? Cloud-Dienst oder eigenes Rechenzentrum? Wir haben zwei Anbieter gebeten, ihre Argumente mit uns auf der kommenden Veranstaltung der KA-IT-Si am **18.09.2014** (18 Uhr im Schalander, Karlsruhe) zu diskutieren: Herrn Kühne von Rittal, einem Unternehmen mit jahrzehntelanger Erfahrung im Bau von Rechenzentren und RZ-Modulen, und Herrn Kess von befine Solutions, dem jungen Anbieter der sicheren Kommunikationslösung Cryptshare. Wir freuen uns auf eine spannende Diskussion mit Ihnen!

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Lassen Sie den Abend im gemütlichen Biergarten des Schalander der Hoepfner-Burg ausklingen. Anmeldung unter www.ka-it-si.de.

„Das Buch“ auf der it-sa

Das Erscheinen der zweiten, gründlich überarbeiteten und erweiterten Auflage des T.I.S.P.-Buchs nehmen wir zum Anlass, Sie herzlich auf unseren „T.I.S.P.-Buch-Stand“ auf der it-sa am 07.-09.10.2014 einzuladen. Sie finden uns in Halle 12 (Stand 12.0-646). Gerne lassen wir Ihnen einen Registrierungscode zukommen, mit dem Sie Ihr kostenfreies E-Ticket (Tageskarte) ausdrucken können. Schicken Sie uns bei Interesse bitte eine kurze E-Mail an security-news@secorvo.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2014	
16.-17.09.	D • A • CH Security (GI, OCG, BITKOM, SI, TeleTrusT, Graz/AT)
16.-19.09.	OWASP AppSec USA 2014 (OWASP Foundation, Denver/Colorado)
18.09.	Informationstag "Elektronische Signatur" 2014 (TeleTrust, Berlin)
18.09.	Gretchenfrage (KA-IT-Si, Karlsruhe)
30.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
30.09.-02.10.	IT-Sicherheit heute (Secorvo, Karlsruhe)
Oktober 2014	
07.-09.10.	it-sa 2014 (NürnbergMesse GmbH, Nürnberg)
11.10.	Anti-Prism-Party 3. Staffel (KA-IT-Si, Karlsruhe)

Fundsache

Für verregnete letzte Urlaubstage ein paar Literaturtipps aus der SSN-Redaktion:

- Dave Eggers: Der Circle
- Marc Elsberg: Blackout – Morgen ist es zu spät, Zero – Sie wissen, was du tust
- Mark E. Russinovich: Zero Day, Trojan Horse, Rogue Code
- Neal Stephenson: Snow Crash, Cryptonomicon
- Daniel Suarez: Daemon: Die Welt ist nur ein Spiel, Darknet



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Michael Knopp, Sven Köhler, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2014



Nichts gelernt?

Diskussionen zur Inneren Sicherheit sind vermintes Gelände. Dort treffen – meist kraftvoll – Terroristenjäger auf Liberale und Datenschützer auf Nichts-zu-verbergen-Haber. Allem verbalen Hauen und Stechen zum Trotz ist aber in einem Punkt zumindest die heimliche Einigkeit groß: Auch wer „nichts zu verbergen" hat, mag sich nicht wie ein Staatsfeind behandeln lassen. Die eigenen E-Mails, SMS und Fotosammlungen möchte man als unbescholtener Bürger dann doch nur mit Personen des Vertrauens teilen – und nicht anlasslos mit unbekannten Staatsdienern.

So ist unstreitig, dass Kommunikationsdaten verschlüsselt gehören. Eigentlich keine große Sache – hätte man die Protokolle TCP/IP und DNS im Jahr 1981 gleich als das konzipiert, was sie heute sind: eine systemkritische Infrastruktur moderner Gesellschaften. Dann wären Verschlüsselungsmechanismen ein integraler Bestandteil des Internet und müssten nicht nachträglich aufgesetzt werden.

„Hätte, hätte, Fahradkette", würde Peer Steinbrück wahrscheinlich kommentieren. Denn einen wenigstens elementaren Schutz bei der Nutzung von Internet-Diensten hat nur, wer sich kümmert – zum Beispiel durch die Aktivierung von TLS beim Zugriff auf E-Mail-Konten oder die Verwendung von Chat-Programmen mit starker Verschlüsselung. Das ist, selbst für einen IT-Laien, so schwierig nicht. Angesichts des drastischen Vertrauenseinbruchs nach den Veröffentlichungen von Edward Snowden wäre eine spürbare Verhaltensänderung zu erwarten gewesen. Tatsächlich aber scheint die Wirkung schon wieder zu verblassen: das Vertrauen ins Internet wächst wieder, ohne dass sich substantiell viel geändert hat.

Mit unserer dritten „Anti-Prism-Party" wollen wir am 11.10.2014 erneut ein Zeichen gegen das „Weiter so" setzen, und hoffen, viele Tausend Besucher für eine sicherheitsbewusstere Nutzung des Internet zu gewinnen. Wer nicht kommen kann, dem sei unsere „Download"-Seite ans Herz gelegt.



Inhalt

Nichts gelernt?

Security News

Ende der Kulanz

Meine grüne Welle

Deutsche Post startet SIMSme

OWASP Guides – reloaded

Löschkriterien

CrypTool 2.0

Secorvo News

Sichere Systeme sind möglich

Anti-Prism-Party, zum Dritten

„Das Buch" auf der it-sa

Veranstaltungshinweise

secorvo
security consulting

Security News

Ende der Kulanz

Durch Online-Banking-Angriffe verursachte Schäden wurden bisher meist von den betroffenen Banken übernommen oder in außergerichtlichen Vergleichen geregelt. Auf die Zunahme von Phishing- und Trojanerangriffen haben die Institute in den vergangenen Jahren mit der Einführung neuer Schutzmechanismen wie SMS-TANs und TAN-Generatoren reagiert – und verweigern inzwischen gelegentlich die Schadensübernahme. Nun hat das LG Darmstadt in einem aktuellen Fall die Schadensersatz-Verweigerung mit Urteil vom 28.08.2014 bestätigt.

Da das von der beklagten Bank zur Verfügung gestellte Verfahren „Sm@rt-TAN-plus" eine Autorisierung der Überweisung mit Kennwort und EC-Karte fordere und die Überweisungsdaten auf dem TAN-Generator angezeigt würden, sei die Prüfung der Daten vor der Bestätigung der Transaktion (durch Eingabe der TAN) die Aufgabe des Kunden. Dieser müsse sich den durch die Verwendung der TAN entstandenen Rechtsschein zurechnen lassen, da die durch den Angreifer manipulierte Überweisung anhand der angezeigten Kontonummer und des Betrags für ihn erkennbar gewesen sei.

Es ist zu erwarten, dass Banken und Gerichte zukünftig die Verantwortung des Kunden bei Verwendung eines sicheren Online-Banking-Verfahrens höher ansetzen werden. Bei Schäden, die erst durch den leichtfertigen Umgang mit den Schutzmechanismen ermöglicht wurden, werden Verbraucher sich in Zukunft nicht mehr auf Kulanz und richterliches Wohlwollen verlassen können.

Meine grüne Welle

Auf der WOOT'14 (*8th USENIX-Workshop on Offensive Technologies*) stellten Forscher der Universität Michigan im August vor, wie verwundbar typische US-Verkehrsleitsysteme sind. Die untersuchten Ampeln kommunizieren über unverschlüsselte W-LAN-Kanäle, Voreinstellungen für Nutzername und Passwort wurden beibehalten, Kommandos des NTCIP-1202-Protokolls zur Verkehrssteuerung ließen sich per UDP an Ampelsteuerungen senden. Damit werden persönliche grüne Wellen und Verkehrsstaus auf Knopfdruck Wirklichkeit.

Eine ähnliche Verwundbarkeit der auch in Europa eingesetzten Verkehrsleittechnik von Sensys Networks zeigte Cesar Cerrudo, ebenfalls im August, auf der diesjährigen DEFCON. Das System erlaubt Code-Downloads ohne Integritätsprüfung und arbeitet ohne Verschlüsselung oder Authentisierung. Inzwischen liegen Software-Updates gegen die veröffentlichten Schwachstellen vor.

Da ausfallende Ampelsteuerungen ein Verkehrschaos auslösen können, werden Verkehrsleitsysteme in Deutschland zu Recht als kritische Infrastruktur angesehen. Dennoch ist auch hierzulande nach wie vor veraltete Technik im Einsatz. Auch hier ist Sicherheit ein Prozess, kein Zustand: Deshalb gehören regelmäßige Audits der Systeme, das Einspielen von Updates und Gespräche mit den Herstellern zu den regelmäßigen Aufgaben eines Sicherheitsmanagements.

Deutsche Post startet SIMSme

Am 13.08.2014 veröffentlichte die Deutsche Post AG ihren kostenfreien Messenger SIMSme. Nach anfänglichen technischen Schwierigkeiten läuft der Dienst inzwischen problemlos: Nutzer können Bilder, Nachrichten, Videos und andere Inhalte verschicken. Den Versand von Nachrichten, die sich wie bei Snapchat nach einer vorgegebenen Zeit selbstständig löschen, erlaubt ein 89-Cent-Upgrade.

Wie bei der oft empfohlenen schweizerischen WhatsApp-Alternative Threema werden die Daten Ende-zu-Ende-verschlüsselt, und das ausschließlich auf deutschen Servern. Der private Schlüssel kann bei einem persönlichen Treffen per QR-Code verifiziert werden. Eine anonyme Nutzung ist nicht möglich – zur Aktivierung benötigt man eine Telefonnummer. Ein Datenschutz-Patzer ist, dass der Sender mitgeteilt bekommt, wenn der Empfänger die Nachricht gelesen hat. Hier sollte die Post nachbessern und eine Deaktivierung dieser Funktion ermöglichen. Positiv sind hingegen die Nutzungsbedingungen hervorzuheben, die kompakt und übersichtlich gehalten sind. Im Gegensatz zu vielen insbesondere amerikanischen Anbietern verzichtet die Post darauf, sich Rechte an den Inhalten der Nutzer zu sichern.

Ein wenig Nacharbeit bei der handwerklichen Implementierungsqualität des aktuellen App-Releases sei der Deutschen Post allerdings angeraten: Vertrauen kann auch an Kleinigkeiten scheitern – zumindest bei Nerds.

OWASP Guides – reloaded

In diesem Sommer wurden zwei wichtige Arbeiten des OWASP zum Test von Anwendungen grundlegend überarbeitet. Am 11.08.2014 veröffentlichte OWASP Version 2.0 des Application Security Verification Standards (ASVS). Der ASVS dient zur Überprüfung der Umsetzung elementarer Sicherheitsmaßnahmen in Anwendungen und ist ein wichtiger Baustein sicherer Software. In die Überarbeitung sind zahlreiche Anmerkungen aus der Praxis einge-

flossen; die Lektüre lohnt sowohl für Anwendungsentwickler als auch für Tester. An Letztere wendet sich Version 4.0 des OWASP Testing Guide, der am 17.09.2014 publiziert wurde. Er enthält Praxistipps für die Durchführung von Sicherheitsüberprüfungen von Anwendungen.

Löschkriterien

Seit der Europäische Gerichtshof (EuGH) Mitte Mai die Suchmaschinenbetreiber als verantwortliche Stellen bestätigt (SSN 05/2014) und Betroffenen das Recht zugesprochen hatte, unter bestimmten Umständen die Löschung von Suchergebnissen zu verlangen, sind allein bei Google binnen vier Monaten 120.000 Anträge eingegangen. Da die Suchmaschinenbetreiber nicht allen Löschbegehren nachgekommen sind, sind zahlreiche Beschwerden bei den europäischen Datenschutzaufsichtsbehörden eingegangen.

Die Art. 29 Gruppe, das gemeinsame Gremium der europäischen Datenschutzaufsichtsbehörden, hat sich am 18.09.2014 nun auf erste Maßnahmen geeinigt. So wollen die Aufsichtsbehörden eine Übersicht über die von ihnen getroffenen Entscheidungen gewinnen und ähnliche, sowie besondere Fallkonstellationen identifizieren. Ziel ist die Entwicklung gemeinsamer Entscheidungskriterien. Auch wenn das kein einfacher Prozess werden dürfte, ist das allemal besser, als die Entscheidung den Suchmaschinenanbietern zu überlassen.

CrypTool 2.0

Das mehrfach preisgekrönte Krypto-Lernprogramm CrypTool erschien am 20.08.2014 in einer von rund 60 Open-Source-Entwicklern in siebenjähriger Entwicklungszeit rundumerneuerter Version 2.0. Die in Deutsch und Englisch verfügbare neue Version wird der Initiator und Gesamtprojektkoordinator, Herr Professor Esslinger, am 11.10.2014 auf der Karlsruher Anti-Prism-Party vorstellen (s. u.).

Secorvo News

Sichere Systeme sind möglich

Die Formulierung und Ausgestaltung angemessener Sicherheitsanforderungen an komplexe Systeme ist nicht trivial – aber möglich. Die Zertifikatsschulung Sichere Systeme dank System Security Engineering (T.E.S.S.) zeigt, wie Sicherheit erfolgreich in die Prozesse und Lebenszyklen der Systementwicklung integriert werden kann. Sie lernen aktuelle Standards, Vorgehensmodelle und Best Practices kennen und anwenden (17.-20.11.2014). Im Anschluss an die Schulung können Sie an der T.E.S.S. Prüfung teilnehmen, um Ihre erworbenen Kenntnisse mit dem T.E.S.S. Zertifikat bestätigen zu lassen. Speziell für die Entwicklung sicherer Software bieten wir die Zertifikatsschulung ISSECO Certified Professional for Secure Software Engineering (CPSSE) (20.-23.10.2014) an. Auf beiden Seminaren gibt es noch wenige freie Plätze.

Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Anti-Prism-Party, zum Dritten

Die „dritte Staffel“ der Anti-Prism-Party am **11.10.2014** findet anlässlich des Edward-Snowden-Stücks „Ich bereue nichts“ im Foyer des Badischen Staatstheaters Karlsruhe statt (ab 14 Uhr). Neben aktuellen Tipps und Empfehlungen rund um das Thema Selbstschutz im Internet wird das Kryptologikum des Karlsruher Instituts für Technologie (KIT) historische und zeitgenössische Verschlüsselungstechnik zum „Be-Greifen“ vorstellen. Ihre Kinder können Sie derweil in der Spion-Schule, die von der Pädagogischen Hochschule Karlsruhe betreut wird, zum Verschlüsselungsexperten ausbilden lassen oder zur Präsentation der KIT-Kinderuni schicken, die um 15 und 16:30 Uhr stattfindet. Krönender Abschluss ist ein Anti-Prism-Plenum um **19:30 Uhr** im Kleinen Haus des Staatstheaters Karlsruhe (Eintritt frei). Mehr zum Programm im APP-Newsletter.



„Das Buch“ auf der it-sa

Anlässlich des Erscheinens der zweiten, aktualisierten und erweiterten Ausgabe des T.I.S.P.-Buchs laden wir Sie am **07.–09.10.2014** herzlich zum Besuch unseres „T.I.S.P.-Buch-Stands“ auf der it-sa in Nürnberg ein. Sie finden uns in Halle 12 (Stand 12.0-646). Gerne lassen wir Ihnen einen Registrierungscode zukommen, mit dem Sie Ihr kostenfreies E-Ticket (Tageskarte) ausdrucken können. Schicken Sie uns bei Interesse bitte eine kurze E-Mail an security-news@secorvo.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2014	
07.-09.10.	it-sa 2014 (NürnbergMesse, Nürnberg)
07.-09.10.	14. IDACON 2014 (WEKA-Akademie, Würzburg)
11.10.	Anti-Prism-Party, 3. Staffel (KA-IT-Si, Karlsruhe)
14.-17.10.	Blackhat Europe 2014 (Blackhat, Amsterdam/NL)
14.-15.10.	ISSE 2014 (TeleTrusT/eema, Brüssel/BE)
20.-24.10.	CPSSE – Schulung und Prüfung (Secorvo, Karlsruhe)
November 2014	
03.-04.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
03.-07.11.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Arizona/US)
10.-15.11.	T.I.S.P. – Schulung und Prüfung (Secorvo, Karlsruhe)
13.11.	Future IT-Kongress 2014 (AppSphere AG, Ettlingen)
17.-21.11.	Security Engineering – Schulung und T.E.S.S.-Prüfung (Secorvo, Karlsruhe)
20.-21.11.	38. Datenschutzfachtagung (DAFTA) (GDD, Köln)
Dezember 2014	
01.-02.12.	IsSec/ZertiFA 2014 (Computas, Berlin)
09.-10.12.	3. DFN-Konferenz Datenschutz (DFN-CERT Services, Hamburg)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Sven Köhler, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2014



Der Anforderungs-Zyklus

Es gibt Erkenntnisse, die sich wie Naturgesetze in unserem Weltverständnis eingenistet haben, obwohl sie sich den in den Naturwissenschaften bewährten Beweisverfahren und Modellbildungen entziehen. Dazu zählen das Pareto-Prinzip („80:20-Regel") – und der Hype-Zyklus von Jackie Fenn (Gartner) aus dem Jahr 1995, der den charakteristischen Verlauf der Aufmerksamkeit für ein Thema beschreibt.

Auch in der IT-Sicherheit lässt er sich beobachten. Tatsächlich beschreibt der Zyklus sogar die Entwicklung der Systemanforderungen. Ein Blick auf die fast 40jährige Geschichte der modernen Kryptografie macht das deutlich: Nachdem das RSA-Verfahren von 1978 erste Bekanntheit erlangt hatte, verbreiteten sich Implementierungen wie die Open Source-Software PGP, die viel Wert auf ein vom Anwender kontrolliertes Vertrauensmodell legte (welchen Schlüssel halte ich für authentisch?). Mit der Verabschiedung des ersten deutschen Signaturgesetztes im Jahr 1997, das höchste Sicherheitsvorgaben für Zertifizierungsdiensteanbieter enthielt und von einem zunächst 350 Seiten starken Maßnahmenkatalog des BSI begleitet wurde, erreichte der Anforderungs-Zyklus seinen Höhepunkt.

Es folgte der Absturz. Trotz EU-weit vereinheitlichtem Signaturgesetz konnte keine Anwendung eine nennenswerte Zahl von Anwendern gewinnen; PGP- bzw. S/MIME-Verschlüsselung blieben eine Nerd-Beschäftigung. Sicherheitsexperten, Gesetzgeber und Entwickler hatten übersehen, dass der Aufwand für hohe Sicherheitsanforderungen den Nutzen einer Verschlüsselungslösung reduziert.

Nun haben Edward Snowdens Veröffentlichungen den Ruf nach Verschlüsselung wieder aufleben lassen. Gesucht werden jedoch transparente Lösungen, bei denen die Verschlüsselung automatisch erfolgt – z. B. in einem lokalen „Verschlüsselungs-Proxy", der dem Benutzer Verwaltung und Prüfung öffentlicher Schlüssel abnimmt. Aus Sicherheitssicht vielleicht nicht perfekt. Aber anwendbar.



Inhalt

Der Anforderungs-Zyklus

Security News

Des Pudels SSL-Kern

ULD gegen Facebook

Google-Token

Beweis-Last

Orientierung für Cloud-Nutzer

Secorvo News

Lesestoff

Forschen gegen das Ausforschen

T.I.S.P. und T.E.S.S.

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Des Pudels SSL-Kern

Am 14.10.2014 veröffentlichte das Google Security Team eine neu entdeckte Schwachstelle der SSL/TLS-Protokollfamilie und taufte sie auf den Namen POODLE. Sie ermöglicht einem Man in the Middle-Angreifer zunächst ein Downgrade der Verbindung auf die veraltete Version SSLv3 und anschließend einen Angriff auf dessen Block-Cipher-Modus CBC. Da nur stark veraltete Browser die aktuelle TLS-Version nicht unterstützen und inzwischen alle SSLv3-Cipher-Suites angreifbar sind, sollte SSLv3 in allen Clients und Servern deaktiviert werden.

Ein Blick auf die lange Reihe von Schwachstellen der komplexen SSL/TLS-Suite legt nahe, bei Sicherheitssoftware auch deren Komplexität als grundsätzliches Sicherheitsproblem im Auge zu behalten. Das einfache Design der Crypto-Bibliothek NaCl weist einen Ausweg.

ULD gegen Facebook

Nach Auffassung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) sind Fanpage-Betreiber für die Auswertung des Nutzungsverhaltens der Seitenbesucher durch Facebook verantwortlich. Daher hatte es gegenüber der Wirtschaftsakademie Schleswig-Holstein die Deaktivierung der Fanpage angeordnet, die das Verwaltungsgericht daraufhin in erster Instanz aufhob (siehe SSN 11/2013). Nun ist das ULD am 04.09.2014 in der Berufung beim Schleswig-Holsteinischen Oberverwaltungsgericht (OVG) gescheitert.

Bezüglich der Verantwortung der Fanpage-Betreiber kommt das OVG zu demselben Ergebnis wie die Vorinstanz: Fanpage-Betreiber seien zwar eigene Dienste-Anbieter; anders als bei einem Website-Betreiber, der Trackingcode in seine Seite einbettet, bestehe aber keinerlei Kontakt zu der Datenerhebung durch Facebook. Die Grundsätze der Störerhaftung kämen daher nicht zur Anwendung.

Zwar lässt das Urteil die Frage offen, ob das deutsche Datenschutzrecht anwendbar ist und die Datenverarbeitung durch Facebook dagegen verstößt. Entgegen den Verlautbarungen des ULD ist es jedoch überzeugend begründet. Für die Revision wird das ULD sich eine bessere Begründung für die Verantwortlichkeit der Seitenbetreiber einfallen lassen müssen. So einleuchtend und richtig die Forderung auch ist, dass ein Diensteanbieter nicht völlig von der Verantwortung für illegale Datenverarbeitungen seiner Dienstleister entbunden werden darf – sie muss sich auch mit rechtlichen Zurechnungsnormen begründen lassen.

Google-Token

Für die Anmeldung bei Google-Diensten wird schon länger die Zwei-Faktor-Authentisierung „2sv“ angeboten (siehe Editorial SSN 01/2013). Dabei wird ein Einmalpasswort als zweiter Faktor per SMS verschickt. Geklaute Login-Daten können so nicht dauerhaft genutzt werden; Angriffsmöglichkeiten durch Phishing bestehen aber nach wie vor. Und nicht jeder will Google seine Handy-Nummer anvertrauen – auch wenn diese Zurückhaltung in Zeiten von WhatsApp etwas hilflos anmuten mag.

Eine vielversprechende Alternative stellt der von Google am 21.10.2014 vorgestellte USB-Token „Security Key“ dar, der bereits ab sechs Euro erhältlich ist. Er unterstützt das PKI-basierte, von der Fast IDentity Online (FIDO-) Allianz spezifizierte Universal Second Factor Protocol (U2F). Neben Google gehören der Allianz Größen wie MasterCard, Microsoft, Nok Nok, NXP, Visa und Paypal an.

Leider ist das Verfahren eher für PC und Laptop gedacht als für das Anstecken an ein Smartphone. Auch ist zu hoffen, dass die Zahl der Allianz-Mitglieder steigt, damit man gute Authentisierung nicht irgendwann mit einem dicken Token-Schlüsselbund bezahlen muss.

Beweis-Last

Die Frage der Beweislastverteilung bei tatsächlichen oder vorgeblichen Hacking-Angriffen und Phishing-Attacken gewinnt zunehmend an Bedeutung. Das LG Coburg hat am 29.04.2014 den Streit über die Verbindlichkeit eines Ebay-Angebots zugunsten des Käufers entschieden, der einen Porsche Carrera sehr günstig erworben hatte. Der Ebay-Anbieter argumentierte, das Angebot sei nach einer Phishing-Attacke ohne seine Mitwirkung erstellt worden; der Porsche hätte gar nicht zum Verkauf gestanden.

Das LG Coburg sah den Beklagten für die unbefugte Account-Nutzung in der Beweispflicht. Einen Nachweis für die Phishing-Attacke konnte dieser jedoch nicht erbringen und die behauptete Anzeige bei der Polizei nicht belegen.

Das Urteil folgt dem Trend (siehe SSN 09/2014), das Risiko von Angriffen faktisch den System-Nutzern aufzubürden. Allerdings sind Phishing-Attacken und Hacking-Angriffe für Privatnutzer meist nur schwer nachweisbar; daher wäre wenigstens regelmäßig zu hinterfragen, ob das verwendete Authentifizierungssystem überhaupt geeignet ist, ein Handeln des Account-Inhabers hinreichend sicher zu belegen.

Orientierung für Cloud-Nutzer

Am 09.10.2014 veröffentlichten die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Düsseldorfer Kreis die Version 2.0 ihrer „Orientierungshilfe Cloud Computing". Die Broschüre geht darauf ein, dass nicht alles, was technisch möglich, auch rechtlich zulässig ist. Es erläutert ausführlich die rechtlichen Rahmenbedingungen der Cloud-Nutzung, vor allem bei Anbietern mit Sitz außerhalb der EU bzw. des Europäischen Wirtschaftsraums (EWR).

Vor dem Hintergrund der NSA-Affäre erklären die Datenschutz-Aufsichtsbehörden, dass sie sich vorbehalten, keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten zur Nutzung von Cloud-Diensten zu erteilen und zu prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind, solange der Zugriff ausländischer Nachrichtendienste nicht begrenzt wird.

Hunde, die bellen, beißen oft nicht: Die Verträge mit den relevanten Dienstleistern sind in der Regel nicht genehmigungspflichtig. Und die nebulöse Hoffnung auf eine „Begrenzung der Zugriffe ausländischer Geheimdienste" bleibt vage – und wäre, falls sie denn kommen sollte, wohl kaum überprüfbar. Davon abgesehen gibt das Dokument einen guten Überblick über die derzeitige Rechtslage.

Secorvo News

Lesestoff

Im Oktober erschien das Sonderheft 4/2014 iX Kompakt zum Thema „Security" – ein lesenswertes Kompendium mit 27 Beiträgen zu aktuellen Fragen der IT-Sicherheit. Zwei der Beiträge hat Secorvo beigesteuert: Einen Ansatz zur pragmatischen und effektiven Umsetzung von IT-Grundschutz in kleinen und mittleren Unternehmen von Kai Jendrian und Stefan Gora, und die Vorstellung eines strukturierten Vorgehens beim Testen der Sicherheit von Apps mit Hilfe von Threat Modeling von Dr. Yun Ding und Jörg Völker.

Bereits im August erschien ein Aufsatz von Kai Jendrian in Heft 8/2014 der DuD über den neu gefassten Standard ISO/IEC 27001:2013 – verfügbar zum Download auf unseren Webseiten.

Forschen gegen das Ausforschen

Abseits vom Katz-und-Maus-Spiel zwischen Angreifern und IT-Sicherheitsbeauftragten beschäftigt sich die IT-Sicherheits-Forschung mit Fragen von Übermorgen: Können wir Sicherheit beweisen? Wie können wir Vertrauen in der Cloud erzeugen? Welche Sicherheitsgarantien kann uns Technik liefern?

Auf der kommenden KA-IT-Si-Veranstaltung am **27.11.2014** werfen wir in zwei Vorträgen einen Blick in das Karlsruher Zukunftslabor der IT-Sicherheit und werden Lösungsansätze kennenlernen, die den Status des Laborversuchs bereits hinter sich haben. Gastgeber ist diesmal das Karlsruher „House of Living Labs" des Forschungszentrums Informatik. Für die ersten 25 schnell Entschlossenen bieten wir eine Führung durch dieses Zukunftslabor: vom intelligenten Stromzähler über Roboterkonzepte von morgen bis zum selbstfahrenden Auto mit Straßenverkehrszulassung (Führungsbeginn: 17 Uhr, Dauer: ca. 1 Stunde; Anmeldung unter www.ka-it-si.de).

Im Anschluss an die Veranstaltung haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking".

T.I.S.P. und T.E.S.S.

Vom 10. bis 14.11.2014 können Sie sich Ihre Kompetenz im Bereich Informationssicherheit mit dem Zertifikat „TeleTrusT Information Security Professional (T.I.S.P.)" bestätigen lassen (noch zwei freie Plätze). Nächster Termin des Zertifizierungsseminars im kommenden Jahr ist der 09. bis 13.03.2015. Als Teilnehmer des Seminars erhalten Sie die im August 2014 erschienene zweite, erweiterte Auflage des 700 Seiten starken Begleitbuchs „Zentrale Bausteine der Informationssicherheit" vorab zugesandt.

Die Komplexität von informationstechnischen Systemen wird zunehmend zum Sicherheitsrisiko. Dass und wie es dennoch möglich ist, komplexe Systeme sicher zu konzipieren und zu realisieren, ist Thema der viertägigen Zertifikatsschulung „T.E.S.S. – Sichere Systeme dank System Security Engineering" vom 17. bis 20.11.2014, die Sie durch die Teilnahme an der T.E.S.S.-Prüfung mit einem T.E.S.S.-Zertifikat abschließen können. Die Schulung zeigt, wie Sicherheit in die Prozesse und Lebenszyklen der Systementwicklung integriert werden kann. Sie lernen aktuelle Standards, Vorgehensmodelle und Best Practices kennen und anwenden (noch vier freie Plätze).

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/college.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2014	
03.-04.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
03.-07.11.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Arizona/US)
10.-15.11.	T.I.S.P. – Schulung und Prüfung (Secorvo, Karlsruhe)
17.-21.11.	Security Engineering – Schulung und T.E.S.S.-Prüfung (Secorvo, Karlsruhe)
20.-21.11.	38. Datenschutzfachtagung (DAFTA) (GDD, Köln)
Dezember 2014	
01.-02.12.	IsSec/ZertiFA 2014 (Computas, Berlin)
09.12.	German OWASP Day 2014 (OWASP Germany, Hamburg)
09.-10.12.	3. DFN-Konferenz Datenschutz (DFN-CERT Services, Hamburg)
Januar 2015	
16.-18.01.	ShmooCon 2015 (The Shmoo Group, Washington/US)
20.-22.01.	Omnicard 2015 (in TIME berlin, Berlin)

Fundsache

Wer Videoüberwachung einsetzen will, muss einen Vielzahl gesetzlicher Vorschriften beachten. Wie das nach Auffassung der Aufsichtsbehörden richtig geht, zeigt die aktuelle Broschüre des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

November 2014



Über den Wolken

Die Berichterstattung über den NSA-Untersuchungsausschuss wird immer mehr zur Realsatire. Schon über die parteipolitischen Zänkereien um die Befragung von Edward Snowden konnte man nur noch den Kopf schütteln. Als der Ausschuss schließlich um ein informelles Treffen in Russland bat, erteilte Snowden dem Vorhaben über seinen Anwalt eine Absage.

Einer der Höhepunkte der Ausschussarbeit war die Befragung der Datenschutzbeauftragten des BND im Oktober. Frau „Dr. F." konnte ihren offenbar reichlich angestauten Frust darüber loswerden, dass die BND-Führung ihre datenschutzrechtlichen Einschätzungen zwar zur Kenntnis nahm, ansonsten aber weitgehend ignorierte. Da wurde selbst die Peinlichkeit eines US-Spions in den Reihen des BND zur Randnotiz.

Möglicherweise ist aber auch nur Reinhard Meys „Über den Wolken" das Lieblingslied von Gerhard Schindler: Nach seiner Überzeugung ist die Freiheit des BND zumindest dort definitiv grenzenlos – und die Verfassung scheint plötzlich nichtig und klein. Denn die BND-Führung vertritt die Meinung, dass bei der Überwachung von Kommunikation über Satelliten per se kein deutsches Recht gelten kann – schließlich befinden sich diese im Weltraum. Die Abhörstation in Bad Aibling sei dabei ohne Bedeutung.

Wie hanebüchen diese Auffassung ist, weiß neben dem gesunden Menschenverstand auch die juristische Fachwelt. Ganz abgesehen davon, dass das Bundesverfassungsgericht dies bereits 1999 ausdrücklich feststellte.

Grundlage für die BND-Arbeit ist das G-10-Gesetz – und dieses ist dringend reformbedürftig. Wir benötigen gesetzliche Regelungen und eine effektive parlamentarische Kontrolle, die die Arbeit der deutschen Geheimdienste aus dem Weltraum zurück auf den Boden demokratischer Tatsachen holen. Und eine Amtsführung, die die verfassungsrechtlichen Grenzen ihrer Tätigkeit respektiert.



Inhalt

Über den Wolken

Security News

Grafikkarten als UKW-Sender

Placebo-Zertifikate

Kampf der Grundrechte

Stuxnet

Blinder Fleck

Secorvo News

Weiterbildung 2015

Zum Nachlesen

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Grafikkarten als UKW-Sender

Wie bekommt man einen isolierten PC dazu, Daten an ein Smartphone zu übermitteln – auch wenn dieser nicht vernetzt ist? Mit dieser Fragestellung haben sich Forscher der israelischen Ben-Gurion Universität beschäftigt und ihre Erkenntnisse am 29.10.2014 auf der Malcon 2014 präsentiert.

Grundidee ihres kuriosen Seitenkanalangriffes ist es, die Grafikkarte derart zu beeinflussen, dass über das Monitorkabel als Antenne ein Signal im UKW-Frequenzbereich ausgesendet wird. Dieses wird vom Smartphone empfangen und von einer zu diesem Zweck entwickelten App „AirHopper" dekodiert.

Auch wenn die Datenrate sehr niedrig ist und die Übermittlung nur über recht kurze Distanzen funktioniert, könnte ein Trojaner auf diesem Weg ausgespähte Kennworte und Daten auf ein Smartphone weiterleiten. In Umgebungen mit sehr hohen Anforderungen an die Vertraulichkeit sollte man daher auf eine angemessene Abschirmung des Raumes achten – und keine Smartphones hineinlassen. Letzteres verbietet sich ohnehin wegen der in PCs und Smartphones verbauten Bluetooth-Chips.

Placebo-Zertifikate

Die US-amerikanische Federal Trade Commission (FTC) hat am 17.11.2014 die Einigung in einem Verfahren gegen TRUSTe, Inc., bekanntgegeben. Dem Anbieter von Gütesiegeln für Online-Dienste wurde vorgeworfen, seit dem kommerziellen Auftreten (ab 2008) bei seinen Kunden nicht für eine entsprechende Änderung der Siegel gesorgt zu haben.

Außerdem habe TRUSTe zwischen 2006 bis 2013 in etwa 1.000 Fällen entgegen der Angaben zu den Siegeln die jährlich erforderliche Rezertifizierung nicht durchgeführt. TRUSTe wurde zur Zahlung von 200.000 USD und zu genauer Rechenschaftslegung über seine Aktivitäten in Bezug auf den *Children's Online Privacy Protection Act* (COPPA) und die Zertifizierung der Einhaltung der *Safe Harbor*-Anforderungen verpflichtet. In diesem Zusammenhang hat die FTC betont, dass sie nicht zögern will, zum Schutz der Verbraucher einzuschreiten, wenn Marktteilnehmer bei Selbstverpflichtungen ihren Versprechungen nicht nachkommen.

Die damit öffentlich gewordenen TRUSTe-Verfehlungen zeigen deutlich, dass im Bereich der Online-Dienste Gütesiegel derzeit mehr schaden als nutzen. Hinter dem Vertrauen, das Nutzer und Geschäftspartner dem Siegel entgegenbringen, steht häufig wenig oder nicht nachvollziehbare Substanz. Dieses (blinde) Vertrauen hält Nutzer oder Anwender jedoch von eigenen Vorsichtsmaßnahmen und Kontrollen ab. Anstelle eines Sicherheitszuwachses führen derartige „halbseidene" Siegel eher zum Gegenteil.

Kampf der Grundrechte

Nachdem die Lehrerbewertungsportale bereits 2009 „dran" waren, hat der Bundesgerichtshof (BGH) sich nun mit einem Internetportal zur Ärztebewertung beschäftigt. In seiner am 06.11.2014 veröffentlichten Urteilsbegründung bewertet der BGH die Meinungs- und Informationsfreiheit der Portalnutzer und deren Interesse an einem Austausch über ärztliche Leistungen höher als das Recht auf informationelle Selbstbestimmung und die Berufsfreiheit des klagenden Arztes.

Dabei hat der BGH die Beeinträchtigung der Ärzte durch die Auffindbarkeit der Bewertungen mit Suchmaschinen, die Gefahr anonymer Wertungen ohne wahren Sachverhaltsbezug, die aufgezwungene Vergleichssituation mit anderen Ärzten und die Wettbewerbskonsequenzen als durchaus substantiell angesehen. Im Gegensatz zu dem in diesem Punkt ähnlichen EuGH-Urteil zu Suchmaschinen orientiert sich der BGH aber eher an der Dogmatik der Meinungs- und Informationsfreiheit. Danach ist das entscheidende Kriterium, dass die Bewertungen sich auf die Sozialsphäre des Arztes (das Arbeitsleben) beschränken.

Der Konflikt zwischen informationeller Selbstbestimmung und Informationsfreiheit in einem wenig vergessenden und jedermann zugänglichen Internet beginnt sich gerade erst zu entfalten. Für den Informationsaustausch in sozialen Netzwerken steht er im Grunde noch bevor; Suchmaschinen und Bewertungsportale sind da erst der Anfang. In den Argumentationen stoßen unterschiedliche Grundwerte aufeinander (Kontrolle des Einzelnen über die eigenen Daten gegenüber gesellschaftlichem Informationsinteresse). Für die Bedeutung und Grenzen des Datenschutzes ist dies eine wesentliche und wegweisende, aber keineswegs einfache Auseinandersetzung.

Stuxnet

Am 11.11.2014 veröffentlichte das Kaspersky Lab neue Erkenntnisse zum Verlauf der Stuxnet-Angriffe auf Irans Atomprogramm 2009 bis 2010. Einfallstor waren demnach nicht USB-Sticks (SSN 10/2010), sondern Dienstleister. Alle besaßen Expertise in der Automatisierungstechnik (SCADA) im iranischen Energiesektor. Alle wurden mehrfach infiziert oder konnten ihre Systeme nie von Stuxnet

reinigen. Das erste Opfersystem wurde wenige Stunden nach der Kompilation von Stuxnet am 22.06.2009 infiziert. Der zunächst vermutete Infektionsweg USB-Gerät erscheint damit unwahrscheinlich. Das System gehörte der Foolad Technic Engineering Co. Über die Behpajooh Co. Elec & Comp. wurde auch Irans größter Stahlproduzent Mobarakeh Steel Company angesteckt. Von dort breitete sich eine Infektionslawine bis in ferne russische Niederlassungen aus. Infiziert wurden auch die Neda Industrial Group, Teilnehmer der US-Sanktionsliste und die Control-Gostar Jahed Company. Der fünfte Dienstleister, Partner im Iranischen Atomprogramm, wurde von drei Systemen aus gleichzeitig angegriffen, was E-Mail als Infektionsweg unwahrscheinlich macht. Letztlich fand der Schadcode über die dauerinfizierten iranischen Dienstleister seinen Weg zum Ziel.

Was bleibt ist die Erkenntnis, dass Vertrauensbildung mit Dienstleistern nicht zum laxen Umgang bei der (IT-) Sicherheit verleiten sollte. Die strikte Kontrolle von Fernzugriffen und eingebrachten Daten sowie vertragliche Regelungen zur Mindestsicherheit mit Dienstleistern bleiben auch dann sinnvolle Maßnahmen, wenn man sich mit seinem Dienstleister gut versteht.

Blinder Fleck

Am 18.11.2014 veröffentlichte Mark Schloesser Erkenntnisse der Rapid7 Labs über Schwachstellen in digitalen Videorecordern der Firma Hikvision – gleich mit Metasploit-Exploit. Die betroffenen Geräte sind weltweit für die digitale Videoüberwachung im Einsatz – ein Scan fand über 150.000 im Internet erreichbare Geräte. Neben einem Trivialpasswort für den Admin-Zugang zeigt der Bericht drei aktuelle Firmware-Schwachstellen, die durch Pufferüberlauf (das „Cross-Site-Scripting“ der 80er Jahre des vergangenen Jahrhunderts) einem Angreifer die volle Kontrolle über das Gerät ermöglichen. Ähnliche Schwachstellen zeigen die IP-Kameras desselben Herstellers.

Für Angreifer sind dies Einfallstore ins Intranet eines Unternehmens. Fremdgenutzt wird bereits die Rechenpower der Geräte, um Bitcoins zu minen. Und Einbrecher könnten aus der Ferne Beweisfotos ihrer Taten verschwinden lassen. Seit September ist der Hersteller informiert; Patches sind bisher nicht verfügbar.

Überwachungstechnik mit Fernzugriff wird gern genutzt, um Routinearbeit auszulagern. Sobald aber IP-Technik mit dem Intranet verbunden wird, muss sie sicher administriert werden (Standardfehler: Default-Passwort). Sie muss patchfähig sein und sollte daher von einem Hersteller stammen, von dem bekannt ist, dass er Patches liefert. Diese Aspekte müssen Gegenstand der Beschaffungsentscheidung sein. Ein sicherer Internet-Fernzugriff erfordert weitere Maßnahmen wie einen VPN-Zugang oder eine Firewall.

Secorvo News

Weiterbildung 2015

Auch im kommenden Jahr werfen wir mit dem dreitägigen Seminar IT-Sicherheit heute einen vertiefenden Blick auf aktuellen Angriffe, neue Bedrohungen und mögliche Schutzmechanismen. Der erste Termin ist der 03.-05.03.2015.

Mit dem anerkannten Expertenzertifikat TeleTrusT Information Security Professional (T.I.S.P.) können Sie Ihre Erfahrungen und Kenntnisse in der IT-Sicherheit dokumentieren und sichtbar machen. Die nächste Schulung (mit anschließender Zertifikatsprüfung) findet vom 09. bis 13.03.2015 statt.

Sie suchen ein Seminar, das Ihnen das Thema PKI praxisnah und produktunabhängig vermittelt? Seit über 15 Jahren führen wir PKI-Projekte durch – und haben aus unseren Erfahrungen und Einsichten das Seminar PKI – Grundlagen, Vertiefung, Realisierung entwickelt, das inzwischen mehr als 350 Teilnehmer besucht haben (Termin: 21.-24.04.2015).

Sollen Sie in Zukunft Ihren Datenschutzbeauftragten in seinen Aufgaben unterstützen und ihm zuarbeiten? Die Schulung Geprüfter Datenschutzkoordinator im Unternehmen bereitet Sie auf zwei intensiven Seminartagen darauf vor (28.-29.04.2015). Nach bestandener Prüfung erhalten Sie ein Zertifikat vom TÜV Rheinland.

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Zum Nachlesen

Im Dezemberheft der iX (12/2014, S. 64-71) erschien ein ausführlicher Beitrag der Secorvo-Experten André Domnick, Dr. Safuat Hamdy und Kai Jendrian zur systematischen Überprüfung der Sicherheit von Anwendungen.

Wer mehr von Secorvo lesen möchte, dem sei „das Buch“ empfohlen – „Zentrale Bausteine der Informationssicherheit“, erschienen Mitte 2014 in zweiter, aktualisierter und deutlich erweiterter Auflage, zugleich Begleitbuch des T.I.S.P.-Seminars. Je nach Präferenz als Hardcover oder E-Book (pdf) eine wunderbare, 720seitige Lektüre für den Lesesessel vor dem vorweihnachtlichen Kaminfeuer.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2014	
01.-02.12.	IsSec/ZertiFA 2014 (Computas, Berlin)
09.12.	German OWASP Day 2014 (OWASP Germany, Hamburg)
09.-10.12.	3. DFN-Konferenz Datenschutz (DFN-CERT Services, Hamburg)
Januar 2015	
16.-18.01.	ShmooCon 2015 (The Shmoo Group, Washington/US)
20.-22.01.	Omnicard 2015 (in TIME berlin, Berlin)
Februar 2015	
04.-05.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
24.-25.02.	22. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2015	
03.-05.03.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen & Schutzmechanismen (Secorvo, Karlsruhe)
09.-13.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Der am 21.10.2014 veröffentlichte Melani-Halbjahresbericht 2014/1 zur Informationssicherheitslage in der Schweiz und international stellt unterhaltsam und lesenswert aktuelle Informationen zu bekannt gewordenen Angriffen, Entwicklungen und Hintergründen vor.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Michael Knopp, Sven Köhler, Christoph Schäfer (Editorial)

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Dezember 2014



Im Überwachungsstaat

Es war ein Jubiläum, das niemand beging – 30 Jahre nach „1984“, dem Jahr von Orwells Überwachungsstaat. Wirkte der Schreck über Snowdens Veröffentlichungen so nach, dass uns das Feiern verging? Oder ist die Ursache beunruhigender: Sind wir Frösche im Kochtopf, dessen Wasser schleichend erwärmt wird? Fragen wir uns vielleicht: Können wir überhaupt (noch) etwas tun? Oder blenden wir die allgegenwärtige Überwachung aus und reden uns (immer noch) ein, dass wir nichts zu verbergen haben? Es ist ja noch nichts passiert (zumindest haben wir nichts gemerkt), und böse Tyrannen gibt es ohnehin nur in Geschichtsbüchern und Nachrichten aus fernen Ländern.

Wenn wir die Realität nicht zumindest teilweise ausblenden, wird es unangenehm. Wer mag WhatsApp, GMail oder Facebook noch nutzen, wenn er ständig daran denkt, dass jede Nachricht und jeder „Like“-Klick, jeder Chat und jede Internet-Suche mitgeschnitten, beobachtet und zu einem Bild von uns verdichtet wird, das nie mehr gelöscht und jederzeit ausgewertet werden kann? Aber das Smartphone ausschalten? Dann ist man nicht erreichbar! E-Mails verschlüsseln? Dann kann man sie nicht mehr mit jedem Client abrufen! Auf das Navi verzichten? Wer hat denn heute noch einen Autoatlas? („Papi, was ist ein Autoatlas?“)

Derweil schrumpft der Bereich, in dem unser Verhalten nur im Gedächtnis unserer Mitmenschen vergängliche Spuren hinterlässt. „Car-IT“ analysiert Fahrverhalten und Regelverstöße, „SmartHomes“ steuern Heizung und Beleuchtung, und abends erfreut „SmartTV“ mit individualisiertem Programmangebot. Vielleicht war es richtig, sich nicht an „1984“ zu erinnern. Denn was uns wirklich bevorsteht, hat Ray Bradbury („Fahrenheit 451“) 1953 zutreffender vorausgesehen: Wir leben in einem technologischen Wunderland, rundumversorgt und perfekt unterhalten, bei umfassender Kontrolle (zu unserer eigenen Bequemlichkeit) – und haben vor lauter Unterhaltungsglück vergessen, wie Freiheit und Erkenntnis schmecken.



Inhalt

Im Überwachungsstaat

Security News

Und wieder SSL...

Ein Klick für mehr Datenschutz

IM Encryption for the Masses

Türsteuerung gibt Zugang preis

Strafverfolgungspfründe

Ob Turing das gewollt hätte?

Internationaler Datenverkehr

Secorvo News

Zertifizierter Datenschutzkoordinator

Krönungsfest

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Und wieder SSL...

Am 08.12.2014 veröffentlichte der Security Engineer Adam Langley ein weiteres Poodle-Dilemma, von dem diesmal TLS betroffen ist. Das Protokoll füllt beim blockweisen Verschlüsseln den letzten Block per Padding auf. Der Empfänger muss die Gesamtlänge des Paddings prüfen – Load-Balancer von F5 und A10 Networks sowie einige Cisco-Geräte prüfen jedoch nicht und sind daher anfällig für Poodle. Wahrscheinlich ist die Wiederverwendung alter SSL-Funktionen die Ursache. F5 und A10 haben bereits Patches veröffentlicht.

Mit dem SSL Server Test von Ivan Ristić (Qualys) kann man die Verwundbarkeit des eigenen Servers testen. Grundsätzlich empfiehlt sich die Umstellung auf die aktuelle TLS-Version 1.2 mit AEAD-Blockverschlüsselung. Den Entwicklern der anfälligen Implementierungen empfehlen wir vor der Wiederverwendung von Security-Code sorgfältige Funktionstests.

Ein Klick für mehr Datenschutz

Social Plugins, die kleinen Spione der sozialen Netzwerke, die viele Betreiber von Internetseiten allzu freiwillig in ihren Quellcode einbinden, sind seit langem ein Dorn im Auge der Datenschützer. 2011 stellte Heise eine 2-Klick-Lösung für mehr Datenschutz vor (SSN 1/2012): Baute man den Code-Schnipsel in seine Seite ein, konnten die Social Plugins nicht ungefragt Daten übertragen. Stattdessen wurde der Benutzer über einen gesonderten Hinweis (erster Klick) gefragt, ob er z. B. eine „Like"-Meldung an das soziale Netzwerk übermitteln will. Erst nach seiner Bestätigung (zweiter Klick) wurde das Skript des Plugins aktiviert.

Zwei Klicks auf einer Internetseite sind eine Hürde, daher setzte sich die Heise-Lösung nicht flächendeckend durch. Mit Shariff hat Heise am 27.11.2014 nun einen Nachfolger in den Ring geschickt, bei dem nur noch ein Klick nötig ist. Die neuen Buttons sind einfache HTML-Links, die via CSS individuell gestalten werden können; sie müssen nicht mehr umständlich eingebettet werden.

IM Encryption for the Masses

Am 18.11.2014 hat Open Whisper Systems, der Spezialist für Verschlüsselungslösungen für Instant Messaging, seine Zusammenarbeit mit WhatsApp bekannt gegeben. In den letzten sechs Monaten hat man an einer Integration des TextSecure Protokolls gearbeitet. Die neueste Version von WhatsApp auf Android nutzt das Protokoll bereits transparent im Hintergrund. Auch wenn noch wichtige Funktionen wie die Verifikation der Schlüssel von Kommunikationspartnern, die Unterstützung von Gruppenchats und die Unterstützung anderer Plattformen fehlen, ist die Implementierung einer Ende-zu-Ende-Verschlüsselung ein Schritt in die richtige Richtung. Hoffentlich folgt der notwendige Rest...

Türsteuerung gibt Zugang preis

Am 01.12.2014 publizierte das RedTeam ein Advisory zur Schwachstelle in der Türsteuerung EntryPass N5200 – über die Konfigurationsoberfläche konnte die Kennung und das Passwort des Administrators in Erfahrung gebracht werden. Die – insbesondere bei der Timeline recht unterhaltsame – Schwachstellenmeldung zeigt, was man nicht tun sollte: So gibt der auf dem System betriebene simple Webserver recht freizügig Informationen preis. Woraus wir lernen können: Auch bei einem physischen Sicherheitssystem darf man die Sicherheit des IT-Anteils nicht ignorieren. Es muss immer das Gesamtsystem betrachtet werden.

Bei Angriffsmöglichkeiten kann man nicht voraussetzen, dass Systeme in einem separierten Management-Netz betrieben werden. Sofern ein System über einen netzseitigen Zugang verfügt, muss der auch entsprechend abgesichert werden. Debug-Meldungen oder sonstige Informationen, die einem Angreifer helfen können, darf das System im Auslieferungszustand nicht mehr ausgeben.

Strafverfolgungspfründe

Der U. S. District Court, S. D. New York hat am 31.10.2014 eine gerichtliche Weisung gegen einen Mobilfunkbetreiber bestätigt, der die Durchsuchung eines Mobiltelefons durch Hilfestellung bei der Entschlüsselung des Speicherinhalts unterstützen sollte. Die Weisung stützt sich auf ein über 225 Jahre altes Gesetz, nach dem ein US-Gericht Dritte zur Mitwirkung verpflichten kann, wenn diese in einer Position sind, in der sie auch als Unbeteiligte den Erfolg einer gerichtlichen Maßnahme verhindern könnten.

Aus dieser Entscheidung könnte abgeleitet werden, dass Mobilfunkbetreiber nach US-Recht verpflichtet sind, sich die Möglichkeit zur Entschlüsselung bei von ihnen vertriebenen Geräten offen zu halten. Das wäre ein weiterer Rückschlag für US-Anbieter, die gerade dabei sind, verlorenes Vertrauen ausländischer Kunden nach dem NSA-Skandal zurückzugewinnen. Jedenfalls lassen die Strafverfolgungsbehörden keine Gelegenheit aus, um zu verhindern, dass Daten ihrem Zugriff entzogen werden.

secorvo
security consulting

Ob Turing das gewollt hätte?

Ohne den Turing-Test durch CAPTCHAs (SSN 2/2008) würden viele Kontakt- und Registrierungsformulare, Foren und Downloadangebote im Internet von Bots überrollt. Allerdings werden CAPTCHAs auch für den Nutzer immer herausfordernder (und nerviger), weil Maschinen die Aufgaben zunehmend besser lösen können als wir (SSN 4/2009).

Wie ein verfrühtes Weihnachtsgeschenk kam am 03.12.2014 eine neue Methode von Google namens No CAPTCHA reCAPTCHA daher. Google berechnet dabei schon vor der Eingabe des CAPTCHA-Codes mithilfe der IP-Adresse, der Verweildauer auf der Seite und der Mausbewegungen im CAPTCHA-Feld, wie wahrscheinlich es ist, dass der Besucher ein Mensch ist. Dieser muss dann keinen Code mehr lösen, sondern nur noch einen Haken setzen. Auf Smartphones funktioniert die Methode mangels Mausbewegungen nicht – hier muss man „lustiges" Tier-Memory spielen.

Doch halt: IP-Adresse übermitteln? Mausbewegungen auswerten? War da nicht etwas mit Datenschutz? Nicht erst „No CAPTCHA", schon der Einsatz des reCAPTCHA-Dienstes bedarf der vorherigen Einwilligung der Seitenbesucher. Schließlich werden dabei personenbezogene Daten an Google übermittelt. reCAPTCHA kann man nicht einmal per Browser-Plugin blockieren. Unterhalb des Radars der meisten Datenschützer hat sich reCAPTCHA massenweise ausgebreitet. Datenschutzkonform und benutzerkompatibel ist einzig eine selbst gehostete CAPTCHA-Lösung.

Internationaler Datenverkehr

Mit ihrem am 26.11.2004 veröffentlichen Arbeitspapier 226 hat die Art. 29-Gruppe ein Verfahren in Kraft gesetzt, das Zuständigkeitskonflikte und bürokratische Hindernisse bei der Verwendung von EU-Standardvertragsklauseln vermeiden soll, wenn bspw. eine internationale Unternehmensgruppe für den konzerninternen Datenverkehr die an sich unveränderlichen Standardvertragsklauseln aufgrund nationalem Recht ergänzt und hierzu eine Genehmigung benötigt. Nun kann die anfragende Stelle eine führende Aufsichtsbehörde vorschlagen, die für alle übrigen Stellen die Rechtskonformität prüft. Alle anderen zuständigen Behörden prüfen nur noch die Voraussetzungen des nationalen Rechts.

Das Papier bekräftigt, dass die Standardvertragsklauseln um weitere Regelungen ergänzt werden können. Auch wenn zunächst nicht viele betroffene Stellen von dem neuen Verfahren Gebrauch machen werden, ist dies eine wichtige Klarstellung.

Secorvo News

Zertifizierter Datenschutzkoordinator

Für Datenschutzbeauftragte gibt es Weiterbildungsangebote wie Sand am Meer. Dünner wird die Luft bei Angeboten für Datenschutzkoordinatoren, die ihrem Datenschutzbeauftragten zuarbeiten. Am 28. bis 29.04.2015 bieten wir die Weiterbildung zum „Geprüften Datenschutzkoordinator im Unternehmen" an. Mit Bestehen der Abschlussprüfung kann der Datenschutzkoordinator anschließend seine Qualifikation mit einem Zertifikat belegen.

Der T.I.S.P. entwickelt sich zu dem am weitest verbreiteten deutschen Personenzertifikat für Informationssicherheit. 700 T.I.S.P.-Absolventen gibt es inzwischen, die sich in einer eigenen Community regelmäßig zum Erfahrungsaustausch treffen. Die nächste Möglichkeit, eine unserer T.I.S.P.-Schulungen zu besuchen, bieten wir Ihnen Mitte März.

Anfang März bringt Sie das Seminar IT-Sicherheit heute in drei Tagen auf den aktuellen Stand – Sie erfahren, was Sie als IT-Sicherheitsverantwortlicher über die aktuelle Sicherheitslage wissen sollten.

Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Krönungsfest

Es ist der höchstdotierte, privat gestiftete Preis Deutschlands: der deutsche IT-Sicherheitspreis, ausgelobt von der Horst Görtz Stiftung und seit 2006 alle zwei Jahre verliehen. Der Preis würdigt mit Preisgeldern in Höhe von insgesamt 200.000 € herausragende deutsche Innovationen in der IT-Sicherheit. Im Jahr 2014 ging der erste Preis über 100.000 € an Herrn Professor Müller-Quade (KASTEL/KIT) und die Karlsruher Firma WIBU-Systems für die Entwicklung der Blurry-Box – einer zukunftsweisenden Lösung für den Softwareschutz, die nicht auf der Geheimhaltung des Verfahrens beruht.

Nicht genug, dass damit Professor Müller-Quade nach seiner Auszeichnung im Jahr 2008 bereits zum zweiten Mal Träger des ersten Preises ist: der KA-IT-Si-Partner WIBU-Systems erhielt die Auszeichnung pünktlich zum 25. Unternehmensjubiläum. Gründe genug für die KA-IT-Si, um Ihnen vorzustellen, was in Karlsruhe möglich ist – und diese Krönung unseres IT-Sicherheitsstandorts bei unserer nächsten KA-IT-Si-Veranstaltung am **15.01.2015** im Informatik-Gebäude des KIT mit Ihnen zu feiern. Anmeldung unter www.ka-it-si.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Januar 2015	
15.01.	Krönungsfest (KA-IT-Si, Karlsruhe)
16.-18.01.	ShmooCon 2015 (The Shmoo Group, Washington/US)
20.-22.01.	Omnicard 2015 (in TIME berlin, Berlin)
Februar 2015	
04.-05.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
24.-25.02.	22. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2015	
03.-05.03.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen & Schutzmechanismen (Secorvo, Karlsruhe)
09.-13.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.03.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)

Fundsache

Im November 2014 wurde auf der CCS 2014 eine Studie zur Aussagekraft von Webseiten-Prüfsiegeln vorgestellt (siehe auch Placebo-Zertifikate, SSN 11/2014). Dabei fanden praktisch alle Prüfverfahren bei einer präparierten Webseite nur einen Bruchteil der Schwachstellen. Auch wurden zahlreiche Webseiten im Netz gefunden, die trotz Prüfsiegel Schwachstellen aufwiesen. Hier wird dem Besucher der Website ein Sicherheitsniveau vorgegaukelt, das eher zu einer Sicherheitsgefährdung aufgrund falschen Vertrauens als zu einem Sicherheitsgewinn führt.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Sven Köhler, Christoph Schäfer.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Januar 2015



Déjà-vu

„Kryptoregulierung“ nannte sich die Debatte vor 20 Jahren, „Verschlüsselungsverbot“ war gemeint. Nun hat der britische Premier diese Büchse der Pandora wieder geöffnet, und ein westlicher Politiker nach dem anderen schiebt sich in seinen Windschatten. Flankierend ruft der Bundesinnenminister nach Vorratsdatenspeicherung, die der Justizminister noch tapfer zu verhindern sucht.

Wie nach 9/11 ziehen nach dem feigen Pariser Mordanschlag nicht nur konservative Politiker reflexartig Ermächtigungen für Strafverfolger und Geheimdienste aus den Schubladen. Damals bescherte es der Welt den „USA Patriot Act“, Rechtsgrundlage der von Edward Snowden aufgedeckten NSA-Überwachungsmaßnahmen.

Keine Frage: Auch wenn die Zahl der Terror-Opfer verglichen mit den Verkehrstoten (in Deutschland: 180 bis 380 – pro Monat) klein wirkt – gegen Morde im Namen totalitärer Überzeugungen muss sich eine Demokratie wehren. Terror will Angst schüren, will offene Gesellschaften zwingen, sich zur Trutzburg zu machen und ihr vermeintlich „totalitäres Antlitz“ zu zeigen – um rückwirkend das eigene Weltbild und Morden zu rechtfertigen. Eine offene Gesellschaft, die auf Terror mit Überwachung reagiert, anlassunabhängig Daten speichert und die Vertraulichkeit der Kommunikation aufhebt, in der vagen Hoffnung, dass sich ein zukünftiger Anschlag verhindern lässt, begeht Selbstmord aus Angst vor dem Tod. Terroristen halten sich nicht an nationale Verschlüsselungsverbote, und die französische Vorratsdatenspeicherung hat den Anschlag auch nicht verhindert.

Für einen Politiker mag es schwer zu akzeptieren sein, dass eine offene Gesellschaft bestimmte Gefahren ertragen muss. Dabei wusste schon Benjamin Franklin 1775: “*They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.*” Leider stimmt aber wohl auch Ingeborg Bachmanns ernüchternde Einsicht: „*Die Geschichte lehrt dauernd. Aber sie findet keine Schüler.*“



Inhalt

Déjà-vu

Security News

Würdiger TrueCrypt-Nachfolger?

Bußgeld für Tippsammler

Umsetzungsdefizit

IT-Grundschutz-Kataloge

DIN-Norm Löschkonzept

Vorwärts, E-Health

Secorvo News

Weiterbildung 2015

Ei des Kolumbus – oder Kuckucksei?

Lesestoff

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Würdiger TrueCrypt-Nachfolger?

Das Ende der beliebten Kryptografie-Software TrueCrypt kam unerwartet und unter nach wie vor unklaren Umständen. Ob man aufgrund der Warnung „*Using TrueCrypt is **N**ot **S**ecure **A**s it may contain unfixed security issues*“ tatsächlich auf eine Einflussnahme der Geheimdienste schließen muss, bleibt Verschwörungstheoretikern überlassen. Mit VeraCrypt der französischen Firma IDRIX wird nun ein auf dem TrueCrypt-Code basierender Nachfolger unter MS-PL als Open-Source-Lösung angeboten. Version 1.0f-1 vom 30.12.2014 besitzt einen „TrueCrypt Mode“, mit dem alte TrueCrypt-Volumen eingebunden werden können.

VeraCrypt macht keinen Hehl aus seiner Herkunft – optisch erinnert es stark an den Vorgänger. Dank einer wesentlich höheren Anzahl an Iterationen beim Passwort-Hash sei es besser gegen Brute-Force-Angriffe geschützt, erläutert der Entwickler.

Kann man VeraCrypt vertrauen? Ein positives Signal ist die Veröffentlichung unter Open-Source-Lizenz, allerdings fehlt bislang eine Code-Analyse, wie es sie zuletzt für TrueCrypt gab (SSN 04/2014).

Bußgeld für Tippsammler

An Kunden zu gelangen kann ein aufwendiges Unterfangen sein. In der Versicherungsbranche setzt man u. a. auf sogenannte Tippgeber, die dem Vertrieb potentielle Neukunden aus dem Freundes- oder Kollegenkreis nennen. Dieser für Branchenfremde eher wundersame Vorgang wird sogar vom Gesetzgeber anerkannt (vgl. BT-Drs. 16/1935, S.17).

Übertrieben hat es allerdings die Debeka. Jahrelang waren Tippgeber eine übliche Praxis, bis sich im Herbst 2013 der rheinland-pfälzische Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) damit beschäftigte. Entgegen offizieller Weisungen hatten Debeka-Mitarbeiter Kontaktdaten potentieller Kunden teilweise entgeltlich erworben, ohne dass diese zuvor eingewilligt hatten. Damit wurden Kundendaten ohne eine gültige Rechtsgrundlage erhoben.

In seiner Pressemitteilung vom 29.12.2014 teilt der LfDI mit, dass die Debeka eine Geldbuße in Höhe von 1,3 Mio. € wegen Verletzung von datenschutzrechtlichen Bestimmungen akzeptiert hat. Außerdem richtet die Debeka für 600.000 € eine Stiftungsprofessur für Datenschutz in Mainz ein. Die Datenschutzaufsichtsbehörde folgt damit ihrem Kurs, bei kleineren Verstößen auf Einsicht zu setzen, bei systematischen allerdings die Bußgeldkeule zu schwingen. Durch den Debeka-Vorfall wurde auch die BaFin aufgeschreckt, die den Versicherungsvertrieb nun künftig stärker regulieren will.

Umsetzungsdefizit

Technischer Datenschutz ist kein neues Konzept, aber noch lange nicht allgemeine Praxis. Anlässlich Art. 23 der geplanten Datenschutz-Grundverordnung, der Datenschutz durch Technik zu einer Ausschreibungsvoraussetzung und Anforderung für Auftragsdatenverarbeiter erhebt, hat die ENISA (*European Union Agency for Network and Information Security*) am 12.01.2015 einen Empfehlungsbericht vorgelegt.

Er soll Datenschutzaufsichtsbehörden und verantwortlichen Stellen als Referenz zum aktuellen Stand der Technik dienen. Dementsprechend enthält der Bericht eine Reihe von datenschutzrelevanten Technikmaßnahmen: von Authentifikationsmethoden über Verschlüsselung und Anonymisierungsdienste bis hin zu Zukunftstechnologien wie homomorpher Verschlüsselung oder *Secure Multi-party Computation*. Er umfasst außerdem eine Auflistung von Datenschutzstrategien, eine Anleitung zur Bewertung von Datenschutzgütesiegeln und Empfehlungen für Gesetzgeber, Standardisierungsgremien, Wissenschaft und Softwarehersteller.

Leider bleiben die Empfehlungen sehr allgemein und unbestimmt in Inhalt und Adressaten. Als Diskussionsgrundlage enthält der Bericht jedoch viele Anregungen.

IT-Grundschutz-Kataloge

Am 19.12.2014 hat das BSI die 14. Ergänzungslieferung der IT-Grundschutz-Kataloge veröffentlicht. Darin stechen vor allem die neuen Bausteine zum Cloud-Computing und für Allgemeine Anwendungen hervor. Damit nimmt sich das BSI wichtiger aktueller Themen in Sicherheitskonzeptionen an. Überarbeitet wurden die Themen Mobilkommunikation und Awareness.

Bisher stehen die Kataloge nur als PDF-Version zum Download zur Verfügung. Eine HTML-Fassung und ein Update der Metadaten für das GSTOOL sind noch nicht verfügbar. Die Prüfgrundlagen für eine Zertifizierung berücksichtigen in der auf der BSI-Seite veröffentlichten Version 2.81 vom 19.02.2014 die 14. Ergänzungslieferung ebenfalls noch nicht. Bei anstehenden BSI-Grundschutz-Zertifizierungen sollte man sie dennoch bereits berücksichtigen.

DIN-Norm Löschkonzept

Ende 2013 starteten die Unternehmen Deutsche Bahn, DATEV, Blancco, Secorvo und Toll Collect ein

gemeinsames Projekt, um die Leitlinie Löschkonzept zu einer DIN-Norm weiterzuentwickeln (SSN 02/2014). Seit dem 09.01.2015 liegt ein Entwurf der Norm 66398 vor und kann auf dem Entwurfsportal des DIN kommentiert werden. Die Norm soll im Herbst 2015 verabschiedet werden. Bereits der Normentwurf gibt wesentliche Hilfestellung für die Entwicklung eigener Löschkonzepte.

Vorwärts, E-Health

Das Bundesgesundheitsministerium hat am 13.01. 2015 einen Referentenentwurf für ein Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) vorgelegt.

Der Gesetzesentwurf schreibt die Einführung der elektronischen Gesundheitskarte als Ersatz für die Krankenversicherungskarte im Sozialgesetzbuch V (SGB V) fest und droht der Gesellschaft für Telematik mit Zahlungssanktionen, wenn sie die Fristen zur Umsetzung der Infrastruktur nicht einhält. Weite Teile des Gesetzes gelten der Ergänzung und Anpassung der Aufgaben der Gesellschaft für Telematik sowie den Verfahrensbestimmungen für Zulassungs- und Schlichtungsverfahren. In den §§ 291f ff SGB V sollen zudem erste Anwendungen wie der elektronische Entlassbrief und elektronische Briefe geregelt werden.

Bestimmungen zur Datensicherheit und zum Datenschutz sind dagegen nur wenig und nur in sehr allgemeiner Form zu finden, was bereits die Kritik des ULD Schleswig-Holstein auf sich gezogen hat. Zu wünschen wäre hier mehr Ausgewogenheit, denn die Sicherheit der mit der elektronischen Gesundheitskarte verbundenen Anwendungen ist ein wesentliches Akzeptanzkriterium.

Secorvo News

Weiterbildung 2015

Die zentralen Bausteine der Informationssicherheit stehen im Mittelpunkt des T.I.S.P. (TeleTrusT Information Security Professional) vom 09.-13.03.2015. Wenn Sie bereits mehrjährige Berufserfahrung im Gebiet IT-Sicherheit, Informationssicherheit oder Datenschutz haben, können Sie Ihre Kenntnisse mit dem T.I.S.P.-Zertifikat bestätigen lassen. Darauf werden Sie von einem Experten-Team in einem fünftägigen Seminar vorbereitet, das zusammen über 200 Jahre Berufserfahrung verfügt. Diese Expertise hilft Ihnen, Ihr Wissen zu festigen und zu vervollständigen.

Wer sich aktiv mit dem Thema PKI in Unternehmen oder Verwaltung beschäftigt und einen produktunabhängigen Überblick sowie vertiefende Antworten sucht, kommt um diese PKI-Schulung nicht herum. Hier lernen Sie das Thema PKI aus vielen verschiedenen Blickwinkeln kennen. Die Referenten wissen aus zahlreichen Realisierungsprojekten, worauf es bei der Konzeption, dem Aufbau und dem Betrieb einer PKI ankommt. Ihre Erfahrung und ihr Wissen haben wir in diesem Seminar gebündelt. Nutzen Sie die Gelegenheit vom 21.-24.04.2015 in Karlsruhe.

Ei des Kolumbus – oder Kuckucksei?

IT-Outsourcing in „die Cloud“ liegt im Trend. Die Anbieter locken mit skalierbaren und anpassungsfähigen Anwendungen und Infrastrukturen. Hard- und Software befinden sich ganz oder teilweise in den Rechenzentren des Anbieters. Auch kurzfristige Anpassungen an den tatsächlichen Bedarf sind oft viel schneller möglich als beim klassischen Outsourcing. Höhere Flexibilität bei geringeren Kosten ist die gewünschte Folge.

Eine solche Lösung ist auch Microsoft Office 365, bei dem die Anwendung aus der Microsoft-Cloud bezogen und Dokumente und E-Mails in Microsoft-Rechenzentren gespeichert werden. Doch wie verträgt sich das mit dem Datenschutz? Auf der kommenden KA-IT-Si Veranstaltung am **19.03. 2015** im CyberForum e.V. werden die datenschutzrechtlichen Hürden und Gestaltungsmöglichkeiten vorgestellt. Anschließend gibt es – wie gewohnt – Gelegenheit zum „Buffet-Networking“. Anmeldung unter www.ka-it-si.de.

Lesestoff

Noch ist es abends früh dunkel – die richtige Jahreszeit, um zu einer guten Lektüre zu greifen. Neben dem neu aufgelegten T.I.S.P.-Buch (als Hardcover oder pdf) – hier finden Sie eine Leseprobe – gibt es auch einige aktuelle Publikationen von Secorvo, die wir Ihnen ans Herz legen, wie z. B. den Beitrag von Dirk Fox über die Hintergründe der NSA-Überwachung von SSL/TLS in Ausgabe 2/2015 der DuD. Eine vollständige Liste unserer Publikationen finden Sie in unserer Publikationsübersicht.

Und auch hören können Sie Secorvo – z. B. Dr. Safuat Hamdy auf dem 14. Deutschen IT-Sicherheitskongress des BSI am 21.05.2015 in Bonn-Bad Godesberg zu Datenschutzaspekten in IPv6.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2015	
04.-05.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
24.-25.02.	22. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2015	
03.-05.03.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen, Schutzmechanismen (Secorvo, Karlsruhe)
09.-13.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.03.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)
April 2015	
14.-15.04.	Datenschutztage 2015 (FFD Forum für Datenschutz, Wiesbaden)
21.-24.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
22.-23.04.	Security Forum 2015 (Hagenberger Kreis, Hagenberg/AT))

Fundsache

Am 17.12.2014 veröffentlichte das BSI den Bericht zur Lage der IT-Sicherheit in Deutschland 2014. Er führt Entwicklungen bei Angreifern und Vorfälle bei Privatanwendern und in der Wirtschaft auf und zeigt Lösungsansätze. Besonders spannend ist die Darstellung eines gezielten Angriffes auf ein Deutsches Stahlwerk, das Opfer einer so genannten *Spear-Phising*-Attacke war. Steuerungskomponenten wurden so manipuliert, dass an einer Hochofenanlage erheblicher Schaden entstand.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Michael Knopp, Christoph Schäfer, Dr. Volker Hammer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2015

Why privacy matters.

Der Amerikaner *Glenn Greenwald*, Jurist, Blogger und seit Juni 2012 Journalist der britischen Tageszeitung The Guardian, bekam als einer der ersten Edward Snowdens Materialien zu Gesicht.

Snowden hatte ihn mit Bedacht gewählt: 2009 war Greenwald mit dem Izzy Award for Independent Journalism ausgezeichnet worden, 2010 erhielt er den Online Journalism Award for Best Commentary für seinen damaligen Blog Salon.com.

Anfang 2014 initiierte er mit finanzieller Unterstützung des Ebay-Gründers *Pierre Omidyar* das Portal „The Intercept", dessen Ziel es ist, „*auf Pressefreiheit zu bestehen und sie gegenüber denjenigen zu verteidigen, die diese verletzen.*"

Am 07.10.2014 hielt Glenn Greenwald eine Rede auf der Konferenz TEDGlobal 2014 in Rio de Janeiro. Sein Titel: „Why privacy matters".

Es ist eine brilliante Rede: Ein Muss für jeden, der meint, Datenschutz sei wohl eher etwas für diejenigen, die etwas zu verbergen haben. Und für alle anderen ebenfalls. Zum Nachlesen existiert eine deutsche Übersetzung.

Es ist eine Rede, bei der sich jeder weitere Kommentar erübrigt.





Inhalt

Why privacy matters.

Security News

ISO-Norm für Datenschutz

Libellen im Kraftwerk

Outsourcing und Berufsgeheimnis

Klare Vorgaben für Cookies gefordert

Insecure by Default

Immer wieder Facebook

Oldie but Goldie

Secorvo News

Ei des Kolumbus oder Kuckucksei?

Kompetenz, wo sie gebraucht wird

Veranstaltungshinweise

secorvo
security consulting

Security News

ISO-Norm für Datenschutz

Am 30.07.2014 wurde die ISO/IEC 27018 als neuer internationaler Standard für den Datenschutz in der Cloud veröffentlicht. Der Standard orientiert sich im Wesentlichen an den Schutz- und Überwachungspflichten des europäischen Datenschutzrechts. Wie das Bundesdatenschutzgesetz fordert er die sorgfältige Auswahl des Dienstleisters. Auch Anforderungen an die Auftragsdatenverarbeitung aus § 11 BDSG sind bereits enthalten; beispielsweise dürfen personenbezogene Daten ausschließlich nach den Vorgaben des Kunden verarbeitet werden und es muss transparent sein, in welchen Ländern die Verarbeitung erfolgt.

Am 16.02.2015 ging Microsoft in die Offensive und gab bekannt, dass das British Standards Institute (BSI) die ISO-27018-Konformität der Cloud-Services Azure, Office 365 und Dynamics CRM Online bestätigt hat. Die Beauftragung eines nach ISO/IEC 27018 zertifizierten Dienstleisters bestätigt – unabhängig von der unklaren Perspektive der EU-Datenschutz-Grundverordnung – zumindest die unternehmerische Sorgfalt bei der Auswahl.

Libellen im Kraftwerk

Schon seit 2013 sind Industrieanlagen der Pharmabranche Ziel der Malware Dragonfly, Warnmeldungen gibt es jedoch erst seit dem vergangenen Jahr. Dragonfly nutzt Spear-Phishing-E-Mails mit viralen Anhängen gefolgt von Malware-Ködern auf Branchen-Webseiten – kombiniert mit infizierten Software-Updates auf Webseiten vertrauter Produkt-Lieferanten wie dem Routerhersteller eWON. In einem Whitepaper vom 09.12.2014 analysiert Joel Langill die Wirksamkeit üblicher Schutzmaßnahmen gegen Dragonfly. Nach bisherigen Erkenntnissen sind Patch-Management, Application-Listing oder VPNs nutzlos. Der Bericht stellt sieben wirksame Techniken vor, die gegen solche Angriffe in der Lieferkette helfen. Zwei der wichtigsten sind:

- Detaillierte Sicherheitsanforderungen an alle Lieferanten, insbesondere bei Fernwartung – Dragonfly attackiert gezielt kleine Dienstleister, die IT-Sicherheit eher ‚pragmatisch' sehen.
- Nutzung von Industrie-Sicherheitsstandards und Isolation durch Netzwerksegmentierung – Dragonfly sucht nach erreichbaren OPC-Servern, die den Datenaustausch zwischen Automatisierungsanwendungen steuern.

Der Angriff zeigt, wie gefährlich es inzwischen ist, „Legacy"-Systeme z. B. im Anlagenbereich von strikten Sicherheitsvorgaben auszunehmen.

Outsourcing und Berufsgeheimnis

Auch Rechtsanwälte, Steuerberater und Ärzte setzen zunehmend Dienstleister ein, um personenbezogene Daten zu verarbeiten. Zu den datenschutzrechtlichen Anforderungen der Auftragsdatenverarbeitung (§ 11 BDSG) kommen hier die strengen Regeln des Berufsgeheimnisses hinzu (§ 203 StGB).

Dennoch finden sich in der Presse regelmäßig Berichte über sensible Daten im Altpapier. Besonders schwer wiegt dies bei Patientendaten wie jüngst in Bayern, wo Röntgenbilder am Straßenrand entdeckt wurden, mit deren Entsorgung ein Krankenhaus einen Dienstleister beauftragt hatte. Die Bayerische Datenschutz-Aufsichtsbehörde äußerte sich am 19.02.2015 unmissverständlich zum Outsourcing im Krankenhaus: Im Regelfall sei das unzulässig. Nach Auffassung der baden-württembergischen Datenschutzaufsicht gibt es nur zwei Lösungen für die Auslagerung der Datenlöschung: Der Dienstleister vernichtet mit einem mobilen Schredder vor Ort oder ein Mitarbeiter des Krankenhauses begleitet den Transport und überwacht die Vernichtung.

Zu beachten ist: Was für Krankenhäuser gilt, müssen auch Rechtsanwälte und Steuerberater beachten. Dienstleister mit der Verarbeitung personenbezogener Daten zu beauftragen ist bei Berufsgeheimnisträgern – wenn überhaupt – nur sehr eingeschränkt zulässig.

Klare Vorgaben für Cookies gefordert

Bereits im Mai 2011 hätte Deutschland die Neufassung der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG („Cookie-Richtlinie") in deutsches Recht umsetzen müssen. Wesentliche Änderung war die Ersetzung der bisherigen Opt-out-Regelung für den Einsatz von Cookies auf Webseiten durch ein Opt-in: „(...) die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, [ist] nur gestattet (...), wenn der betreffende Teilnehmer oder Nutzer (...) seine Einwilligung gegeben hat."

Die Bundesregierung vertritt bisher die Auffassung, dass die Regelungen des § 13 Abs. 1 S. 2 TMG ausreichen. Das sehen die Datenschutz-Aufsichtsbehörden anders: Mit ihrer Entschließung vom 05.02.2015 stellen sie fest, dass Cookies nur mit Einwilligung der Internetnutzer eingesetzt werden dürfen. Im Telemediengesetz sei die Richtlinie nur unzureichend umgesetzt.

secorvo
security consulting

Insecure by Default

Schon am 21.09.2014 wurde berichtet, dass Lenovo Notebooks für Endverbraucher ab Werk mit der Adware Superfish ausliefert. Superfish schleust Werbung in verschlüsselte HTTPS-Verbindungen ein und registriert sich dazu ungefragt im Zertifikatsspeicher von Windows als Root-CA. Der private Schlüssel für das Superfish-Zertifikat liegt dabei quasi ungeschützt auf der Festplatte.

Gefährlicher als die störende Werbung durch Superfish ist die Möglichkeit für Angreifer, damit Man-in-the-Middle-Angriffe auf beliebige HTTPS-Verbindungen durchzuführen. Dafür stellen diese sich mit dem Superfish-Schlüssel Zertifikate für beliebige Domänen aus. Inzwischen konnten derartige Angriffe bei mehr als einem Dutzend verschiedener Malware-Typen beobachtet werden.

Lenovo hat inzwischen angekündigt, künftig nur noch erforderliche Programme vorzuinstallieren. Der Vorfall zeigt jedoch, dass einer Betriebssysteminstallation im Auslieferungszustand besser nicht vertraut werden sollte. Darin findet sich oft ab Werk Zusatzsoftware, die im normalen Betrieb nicht benötigt wird und die Angriffsfläche vergrößert. Gelegentlich erkaufen sich sogar Softwarehersteller ihren Platz in der Standardinstallation. Bei der Beschaffung eines neuen Geräts sollte daher immer zuerst eine Neuinstallation des Betriebssystems durchgeführt werden, die nur die betrieblich benötigten Softwarepakete einschließt.

Immer wieder Facebook

Mit Wirkung zum 30.01.2015 hat Facebook erneut seine Datenschutzrichtlinie, seine Cookie-Richtlinie, die Nutzungsbedingungen sowie weitere Hinweise zum Datenschutz geändert. Die Zustimmung des Nutzers soll ohne ausdrückliche Zustimmung per Login erfolgen. Nach Darstellung von Facebook erleichtert die Änderung das Verständnis der Funktionsweise von Facebook und verbessert die Nutzerkontrolle. Neu eingeführt wurden Lokalisierungsdienste, Einkaufsmöglichkeiten direkt aus Facebook heraus, neue Erläuterungen zu Privatsphäreneinstellungen, eine engere Verknüpfung der Facebook-Dienste sowie die Auswertung von App-Nutzungen. Werbetreibende Dritte sollen Informationen zur Individualisierung von Werbung ohne die Möglichkeit zur Identifizierung des Nutzers erhalten.

Eine Studie im Auftrag der belgischen Datenschutzaufsichtsbehörde kommt zu einem anderen Ergebnis: Bereits die Praxis, die Nutzung von Facebook als Einwilligung zu interpretieren, sei ebenso rechtswidrig wie das Fehlen einer effektiven Opt-out-Möglichkeit. Dasselbe gelte für die Zusammenführung der Daten unterschiedlicher Dienste. Facebook dehne durch die Änderungen seine Datenverwendungen ohne Rechtsgrundlage aus. Am 23.02.2015 hat daher der Bundesverband der Verbraucherzentralen ein Unterlassungsverfahren eingeleitet und Facebook abgemahnt.

Oldie but Goldie

Bereits am 03.11.2014 erschien Version 3.1.1 des bewährten Forensik-Werkzeugs Autopsy. Hinzu gekommen ist die lange ersehnte automatische Identifikation von Dateitypen. Sehr praktisch ist die neue skriptgesteuerte Reporterstellung, die auch für mehrere Festplattenimages übergreifend funktioniert. Dank einer Multi-Thread-Verarbeitung für beliebig viele CPU-Kerne sinkt die Bearbeitungszeit effektiv um die Hälfte. Hilfreichste Neuerung ist die überarbeitete grafische Zeitlinie: Man kann nun ein Analyse-Zeitfenster bis auf Millisekunden festlegen und die Ergebnisse aus allen verfügbaren Metadaten parallel darstellen.

Secorvo News

Ei des Kolumbus oder Kuckucksei?

Kann man das Microsoft-Cloud-Angebot Office 365 Datenschutz konform einsetzen? Welche Hürden sind dabei zu bewältigen? Diese Fragen wird *Christoph Schäfer* auf der kommenden KA-IT-Si Veranstaltung am **19.03.2015** im CyberForum e.V. beantworten. Nach dem Vortrag gibt es Gelegenheit zum „Buffet-Networking". **Anmeldung** unter www.ka-it-si.de (nur noch wenige Plätze!).

Kompetenz, wo sie gebraucht wird

Als Datenschutzbeauftragter in einem großen Unternehmen benötigen Sie Datenschutzkoordinatoren mit solidem Basiswissen im Datenschutz. Unsere zweitägige Schulung „Geprüfter Datenschutzkoordinator im Unternehmen" vom **28. bis 29.04.2015** hilft Ihnen dabei, Ihren Kollegen die erforderlichen Grundkenntnisse zu vermitt eln.

Viele Angriffsszenarien gäbe es gar nicht, wenn bei der Code-Entwicklung Schwachstellen systematisch vermieden würden. Wie man etablierte Verfahren der sicheren Softwareentwicklung in den gesamten Software-Lifecycle einbindet, zeigt die Schulung CPSSE – Certified Professional for Secure Software Engineering vom **04. bis 07.05.2015**.

Die nächste Möglichkeit zur T.I.S.P.-Zertifizierung bieten wir vom **09. bis 13.03.2015**.

Alle Termine und Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/college.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2015	
03.-05.03.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen und Schutzmechanismen (Secorvo, Karlsruhe)
09.-13.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
19.03.	Ei des Kolumbus – oder Kuckucksei? (KA-IT-Si, Karlsruhe)
23.-26.03.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)
April 2015	
14.-15.04.	Datenschutztage 2015 (FFD Forum für Datenschutz, Wiesbaden)
21.-24.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
22.-23.04.	Security Forum 2015 (Hagenberger Kreis, Hagenberg/AT)
23.-24.04.	8. GDD-Fachtagung „Datenschutz International“ (GDD e.V., Berlin)
26.-30.04.	Eurocrypt 2015 (IACR, Sifia/BG)
Mai 2015	
04.-07.05.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
06.-07.05.	16. Datenschutzkongress (EUROFORUM, Berlin)
11.-12.05.	BvD Verbandstag 2015 (BvD e. V., Berlin)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Michael Knopp, Sven Köhler, Christoph Schäfer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2015



Hobbyistensicherheit

Die zentrale Verschlüsselungsinfrastruktur des Internets hängt an 447.247 Programmzeilen von 147 Programmierer-Aktivisten: OpenSSL. Die geschützte Remote-Administration der wahrscheinlich meisten Systeme der Welt basiert auf 64.813 Zeilen C-Code von 92 unabhängigen Entwicklern: OpenSSH. Und die meisten (deutschen) PGP-Verschlüsselungen erledigt die Open-Source-Software GnuPG, entwickelt von 14 enthusiastischen Codern.

Manchmal ist die Abhängigkeit vielleicht nicht offensichtlich, weil sich der Open-Source-Code in einem Produkt „versteckt". Und ja, manche Open-Source-Projekte werden (teil-)finanziert von einem Unterstützer oder erhalten öffentliche Mittel.

Dennoch muss die Situation für jemanden außerhalb der „IT-Szene" ziemlich skurril anmuten. Das dürfte in etwa so wirken, als ob wir die Statik von Brücken durch Hobby-Architekten berechnen, ABS und Airbags von engagierten Bastlern konstruieren und Flugzeuge von Freizeitschraubern warten ließen.

Zwar muss das Ergebnis nicht schlecht sein – im Gegenteil: Wenn viele Engagierte eigeninitiativ und professionell zusammenarbeiten, kann sich das Resultat oft sehen lassen. Zu denken geben sollte uns diese Entwicklung trotzdem: Hat jemand einmal ausgerechnet, wie viel es volkswirtschaftlich kostet, wenn alle Unternehmen, die bspw. TrueCrypt zur Verschlüsselung einsetzen, auf BitLocker wechseln müssen, weil die Initiatoren es nicht weiterführen? Oder wenn eine GPG-Installation durch S/MIME ersetzt werden muss, weil der Hauptentwickler die Code-Pflege aufgibt?

Schließlich hat die Geschichte von OpenSSL gezeigt, dass Open Source nicht dasselbe ist wie „geprüfter" Code – sondern eben nur „prüfbarer" Code. Wäre es nicht angemessen, bei den zentralen Komponenten unserer Sicherheitsinfrastruktur für eine stabile Finanzierung und vor allem regelmäßige Code-Analysen zu sorgen?



Inhalt

Hobbyistensicherheit

Security News

Stromortung

Kompatibilitätsbug

Sozialadäquate Straftat

Angriffsanalyse

Rechts(un)sicherer WLAN-Betrieb

Secorvo News

Sichere Systeme

7. Tag der IT-Sicherheit

„No Blackout"

Veranstaltungshinweise

secorvo
security consulting

Security News

Stromortung

Am 11.02.2015 veröffentlichten vier Forscher der Stanford University und des *National Research and Simulation Center* eine empirische Analyse zur Standortbestimmung über den Stromverbrauch eines Smartphones. Da das Senden und Empfangen von Daten den meisten Strom verbraucht und dieser stark schwankt (abhängig von der Entfernung zum Sendemast und der Signalstärke, die sich durch Hindernisse wie Häuser, Bäume oder Menschen schnell verändert), kann man jedem Ort einen spezifischen Verbrauch zuordnen. In aktuellen Smartphones sind die Strom- und Spannungswerte uneingeschränkt zugänglich; eine App kann diese also zyklisch an einen Server übermitteln, der die Werte mit bereits ausgemessenen Routen korreliert. Die Forscher konnten so innerhalb von zwei Minuten acht von zehn Teilstrecken erkennen.

Für einen flächendeckenden Einsatz erfordert die Technik zwar ausgemessene „Landkarten". Die Sperrung der GPS-Daten im Smartphone lässt sich damit jedoch umgehen. Wegen des geringen Verbrauchs ist ein Verschleiern der Werte durch das Starten vieler Apps keine wirksame Gegenmaßnahme; helfen würde allein eine Ausdehnung des Rechtemanagements auf die Stromverbrauchsdaten.

Kompatibilitätsbug

2010 patchte Microsoft gegen Stuxnet und Fanny – nur leider fehlerhaft. Das belegt die nach Hinweisen von Michael Heerklotz vom Januar initiierte Untersuchung von HP, deren Ergebnisse Dave Weinstein am 10.03.2015 veröffentlichte.

So missbrauchte Stuxnet CPL-Dateien (DLLs mit anderem Namen, also ausführbaren Code), indem er über Icons für Windows-Verknüpfungen (.lnk) eigenen Code aus mitgebrachten CPLs zur Ausführung brachte. Seit dem Patch im Jahr 2010 lädt Microsoft diese Windows-Urgesteine nur noch aus einer CPL-Whitelist. Der Schutz lässt sich allerdings durch geschickte Änderungen des Dateinamens der .lnk-Datei aushebeln: Das Icon wird zusammen mit dem Angriffscode in einen Speicherbereich mit Ausführberechtigung geladen – und Stuxnet ist fünf Jahre nach dem Patch wiederbelebt.

Die kompatibilitätserhaltende Pflege von Architekturschwächen (wie das Laden von Icons in Executable Memory) ist immer wieder ein Einfallstor. Eine ernsthafte Erhöhung des Sicherheitsniveaus erfordert es jedoch, gelegentlich die Rückwärtskompatibilität auf dem Altar der Sicherheit zu opfern.

Sozialadäquate Straftat

In den SSN 2/2015 wiesen wir darauf hin, dass Berufsgeheimnisträger wie Ärzte, Rechtsanwälte und Steuerberater grundsätzlich keine Dienstleister mit der Verarbeitung personenbezogener Daten beauftragen dürfen: Sie müssen die ihnen anvertrauten Geheimnisse schützen (§ 203 Abs. 1 StGB).

Diese (zugegebenermaßen betagte) strafrechtliche Vorschrift empfanden die Anwaltskammern als nicht zeitgemäß und versuchten sie mit dem am 11.11.2014 (sic!) beschlossenen Entwurf zur neuen Berufsordnung (BORA) auszuhebeln: Um künftig Aktenvernichter, Schreib- und Clouddienste einsetzen zu dürfen, soll ein Rechtsanwalt sich nicht mehr strafbar machen, wenn das Outsourcing „im Rahmen der Arbeitsabläufe der Kanzlei einschließlich der Inanspruchnahme von Leistungen Dritter erfolgt und objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz)." Auf Deutsch: Alle schieben ihre Daten in die Cloud – dann muss das der Rechtsanwalt doch auch dürfen.

Dieser eigenmächtigen Strafbefreiung schob der Bundesjustizminister jetzt einen Riegel vor und stellte am 04.03.2015 klar, dass die Berufsordnung das Strafgesetzbuch nicht aufweichen kann. Nicht alles, was technisch machbar ist, darf auch zulässig sein: Schließlich verarbeiten Berufsgeheimnisträger besonders schützenswerte Daten.

Angriffsanalyse

Auf dem USENIX Security Symposium wurden am 21.08.2014 die Ergebnisse einer Analyse gezielter, systematischer Angriffe auf eine China kritische Nichtregierungsorganisation vorgestellt, die Rückschlüsse auf typische Angriffsmethoden erlauben – das dürfte auch der Grund für die Einladung der Autoren als Keynote der diesjährigen 22. DFN-Konferenz gewesen sein.

In der Analyse wurden 1.500 verdächtige E-Mails von ca. 700 unterschiedlichen Absenderadressen untersucht; bei über 1.100 wurde Schadsoftware gefunden. Alle betroffenen E-Mails waren mit für die Empfänger plausiblem individuellen Kontext versehen. Bemerkenswert sind die folgenden Erkenntnisse: Es handelte sich um einen Langzeitangriff, der mindestens von 2009 bis 2013 dauerte und ggf. weiter andauert. Die meisten Empfänger, die Opfer der Angriffe wurden, erhielten erst nach dem Eintritt von Praktikanten in die Organisation infizierte E-Mails. Genutzt wurden keine Zero-Day-Exploits, sondern frei verfügbare Schadsoftware, wobei die Zeitspanne zwischen Veröffentlichung des Exploits und der maliziösen E-Mail meist sehr kurz war. Als „Wirtsdatei" wurden zunächst meist PDF-

Dokumente verwendet, die nach Einführung von Sandboxing in Acrobat Reader (ab 2010) von Microsoft Office-Dokumenten abgelöst wurden.

Daraus können wir Verschiedenes lernen. Erstens: Angreifer haben einen langen Atem. Zweitens: Schnelles Patchen von Sicherheitslücken wird immer wichtiger – „Aufpassen" schützt nicht. Und Drittens: Bei einer Häufung von Schadsoftware-Vorfällen könnte ein gezielter Angriff dahinterstecken – daher ist eine systematische Auswertung wichtig.

Rechts(un)sicherer WLAN-Betrieb

Das Bundesministerium für Wirtschaft und Energie hat am 11.03.2015 einen Gesetzesentwurf für ein zweites Gesetz zur Änderung des Telemediengesetzes vorgelegt. Damit will das Ministerium Rechtssicherheit für WLAN-Anbieter schaffen. Bislang drohen diesen bei missbräuchlicher Nutzung Unterlassungsansprüche (SSN 6/2014). Gleichzeitig will man die Störerhaftung von Plattformanbietern erleichtern, deren Plattformen hauptsächlich für rechtswidrige Handlungen genutzt werden, und das bisherige telemedienrechtliche Haftungsprivileg einschränken.

Diese Ziele soll eine Definitionsergänzung in § 2 TMG für drahtlose lokale Funknetze (= WLAN) ermöglichen. In drei neuen Absätzen des § 8 TMG, dem Haftungsprivileg für Access-Provider, wird klargestellt, dass auch die Störerhaftung ausgeschlossen sein soll. Voraussetzung ist, dass die Anbieter bestimmte Sorgfaltspflichten erfüllen: die Verschlüsselung des Zugangs zum Ausschluss unberechtigter Nutzer und die Beschränkung auf Nutzer, die zuvor erklären, keine Rechtsverletzungen über den Zugang zu begehen. Nicht geschäftsmäßige Anbieter sollen zudem den Zugang auf namentlich bekannte Nutzer beschränken.

Entgegen der in der Rechtsprechung zuletzt erkennbaren Tendenz, das Haftungsprivileg endlich uneingeschränkt auf WLAN-Anbieter anzuwenden, werden nun mit den Sorgfaltspflichten europarechtswidrige, wirkungslose Einschränkungen geschaffen. Erklärungen allein werden Rechtsverletzungen nicht verhindern, das Abmahnrisiko bei einer unzureichenden Umsetzung der Sorgfaltspflichten steigt dagegen. Im Interesse der Rechtssicherheit und einer Verbesserung der WLAN-Verfügbarkeit ist zu hoffen, dass dieser Entwurf gar nicht erst den Bundestag erreicht.

Secorvo News

Sichere Systeme

Für die Entwicklung sicherer Systeme genügt es nicht, nur die Sicherheit der einzelnen Komponenten zu betrachten – in deren Zusammenspiel und an der Schnittstelle zum Benutzer können unerwartet neue Risiken entstehen. Wie sich auch in komplexen Systemen Security by Design erreichen lässt, erfahren Sie auf unserem Seminar T.E.S.S. – Sichere Systeme dank System Security Engineering vom 14. bis 19.06.2015 mit anschließender Zertifizierung als T.E.S.S. (TeleTrusT Engineer for System Security).

Der T.I.S.P., das deutsche Personenzertifikat für Informationssicherheit, umfasst alle grundlegenden Themenbereiche der Informationssicherheit. In unseren T.I.S.P. Schulungen erhalten Sie in fünf Tagen einen kompakten Überblick – und vorab unser T.I.S.P.-Begleitbuch zur Vorbereitung. Für die Schulung vom 22. bis 26.06.2015 gibt es noch wenige freie Plätze. Die nächste Möglichkeit zur Zertifizierung bieten wir im September und November. Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/college.

7. Tag der IT-Sicherheit

Der Tag der IT-Sicherheit am **19.05.2015** in Karlsruhe, eine Kooperationsveranstaltung der KA-IT-Si mit der IHK Karlsruhe, dem CyberForum und KASTEL, beschäftigt sich mit aktuellen IT-Sicherheitsherausforderungen für Unternehmen. Das Landesamt für Verfassungsschutz Baden-Württemberg informiert in einer Keynote über die aktuelle Bedrohungslage. Es folgen Fachvorträge zu den Themen Netzwerksicherheit, Datenschutz und Mobile Computing. Die Veranstaltung schließt mit einem Live-Hacking, das Sicherheitslücken von Webseiten aufzeigt. Zwischendurch gibt es Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern. Wir freuen uns auf Ihre Anmeldung!

„No Blackout"

Am **12. und 13.05.2015** veranstaltet Secorvo anlässlich der bevorstehenden Verabschiedung des IT-Sicherheitsgesetzes und der daraus folgenden Verpflichtungen von Betreibern kritischer Infrastrukturen das Symposium „No Blackout – IT-Sicherheit für die Energieversorgung" in der Buhlschen Mühle in Ettlingen. Die Veranstaltung richtet sich nicht nur an Unternehmen und Institutionen aus dem Bereich der kritischen Infrastrukturen – sie bietet wertvolle Informationen für alle Unternehmen, die den Aufbau eines ISMS planen oder vorbereiten. Unter anderem werden die Stadtwerke Ettlingen über den „fx-Hack" und die Folgen berichten, und wir werden etwas über die IT-Sicherheit in Kernkraftwerken erfahren. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2015	
14.-15.04.	Datenschutztage 2015 (FFD Forum für Datenschutz, Wiesbaden)
21.-24.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
22.-23.04.	Security Forum 2015 (Hagenberger Kreis, Hagenberg/AT)
23.-24.04.	8. GDD-Fachtagung "Datenschutz International" (GDD e.V., Berlin)
26.-30.04.	Eurocrypt 2015 (IACR, Sofia/BG)
Mai 2015	
04.-07.05.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
06.-07.05.	16. Datenschutzkongress (EUROFORUM, Berlin)
11.-12.05.	BvD Verbandstag 2015 (BvD e. V., Berlin)
12.-13.05.	No Blackout – Symposium IT-Sicherheit für die Energieversorgung (Secorvo, Ettlingen)
18.-20.05.	IMF 2015 (Fraunhofer IAO, Magdeburg)
18.-21.05.	OWASP AppSec EU 2015 (OWASP Foundation, Amsterdam/NL)
19.-21.05.	14. Deutscher IT-Sicherheitskongress (BSI, Bonn)
19.05.	7. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
20.-22.05.	Entwicklertag 2015 (VKSI, ObjektForum, Karlsruhe)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Michael Knopp, Sven Köhler, Christoph Schäfer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2015



Maßlos

Angenommen, wir besäßen ein riesiges Stück Papier mit einer Materialstärke von 0,09 mm. Wie oft müssten wir dieses Papier falten, um den Abstand zwischen Erde und Mond (ca. 384.400 km) zu überbrücken? Den Rechenweg kennen wir aus der Schule:

$$2^n \cdot 0{,}09 \text{ mm} = 384.400 \text{ km},$$
$$\text{also: } n = \log_2 (42{,}71 \cdot 10^{11}) \approx 42.$$

Ein überraschend kleiner Wert, den wir – Douglas-Adams-Fans ausgeschlossen – eher nicht erwartet hätten. Die kleine Rechnung zeigt, wie schwer wir uns exponentielles Wachstum vorstellen können.

Und das hat Folgen. Im Januar 1997 lobte die Firma RSA eine *Crypto Challenge* aus: Eine mit RC5 und einem 56 bit langen Schlüssel verschlüsselte Nachricht sollte durch eine Brute-Force-Attacke entschlüsselt werden. Das gelang einem riesigen Netzwerk von Freiwilligen, die die Leerlaufzeiten ihrer PCs für die Schlüsselsuche zur Verfügung stellten, in 270 Tagen. Einer dieser Freiwilligen war ein Student, den ich betreute. Nachdem der Schlüssel gefunden war, erklärte er mir freudestrahlend, jetzt wolle er mit den Institutsrechnern an der RC5-64 bit-Challenge teilnehmen. Als ich ihn fragte, wer ihm denn ein so langes Studium bezahle, sah er mich mit großen Augen an – und ich musste ihm vorrechnen, dass die Challenge die 2^8-fache Rechenleistung benötigt, seine 4.000 Teams ohne schnellere Rechner fast 190 Jahre suchen müssten.

So verleitet uns unsere mangelnde Vorstellungskraft, es bei Schlüssellängen ständig zu übertreiben. Denn ein 256 bit-AES-Schlüssel ist nicht doppelt, sondern 2^{128}-mal so sicher wie ein 128 bit-Key. Das ist, als wolle man ein Haus mit einer gepanzerten Tür dadurch sicherer machen, dass man nicht eine zweite, sondern gleich $3{,}4 \cdot 10^{38}$ zusätzliche Türen montiert. Die würden übrigens nicht in unser Universum passen – das hat lediglich einen Durchmesser von 93 Milliarden Lichtjahren (etwa $8{,}8 \cdot 10^{26}$ m), wir benötigten also 387 Milliarden weitere Universen gleicher Größe dafür.



Inhalt

Maßlos

Security News

Nächster Persilschein

Car to go

Ende des Passworts?

XP lebt!

Secorvo News

Symposium „No Blackout“

7. Tag der IT-Sicherheit

Mit Brief und Siegel

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Nächster Persilschein

Gerade ein Jahr ist es her, dass Microsoft einen vermeintlichen Persilschein der europäischen Datenschutz-Aufsichtsbehörden (Art.-29-Gruppe) für Microsoft Office 365 erhielt (SSN 04/2014). Nun hat auch Amazon den Datenschutz als Schlüssel zum europäischen Markt entdeckt und am 06.03.2015 ein ähnliches Dokument der luxemburgischen Datenschutzaufsicht (CNPD), stellvertretend für die Art.-29-Gruppe, für seinen Cloud-Service AWS erhalten. Wie zuvor Microsoft verkündet Amazon seitdem vollmundig, AWS sei damit datenschutzkonform einsetzbar. Tatsächlich schreibt die CNPD genau das Gegenteil: Sie habe lediglich gemäß dem Cloud-Leitfaden der Art.-29-Gruppe die Vertragsstruktur geprüft und will das positive Prüfergebnis gerade nicht als Freigabe für AWS verstanden wissen.

Derweil kämpfen die amerikanischen Cloud-Anbieter weiter um den europäischen und insbesondere den deutschen Markt und setzen dabei zunehmend auf nationale Niederlassungen, wie den AWS Marketplace in Frankfurt. Doch die augenscheinlich lokal angebotenen Dienste sind weiterhin in die globale Infrastruktur des Anbieters eingebunden. Cloud-Willige sollten daher nicht den Fehler machen, sich ohne eine gründliche (datenschutz-) rechtliche und (sicherheits-)technische Prüfung auf die Marketing-Aussagen der Anbieter zu verlassen.

Car to go

Das Keyless-System PKES entriegelt Fahrzeugtüren automatisch, wenn der Besitzer naht. Oder auch ein geschickter Dieb: Am 06.04.2015 musste der Reporter Nik Bilton zusehen, wie zwei Teenager mit seinem Toyota Prius davonfuhren. Wahrscheinlich nutzten die beiden einen simplen Signalverstärker, der die Reichweite der Kommunikation zwischen Token und Fahrzeug vergrößerte.

Der Fehler liegt nicht im verwendeten kryptografischen Protokoll - denn Kryptografie hilft nicht gegen diese Art von Angriffen. Ein weiteres Beispiel dafür, dass mancher Komfortgewinn nur auf Kosten der Sicherheit erhältlich ist.

Zur Prävention können betroffene Autobesitzer ihr Token mit Schutzhüllen vor Funksignalen abschirmen – oder besser gleich wieder auf herkömmliche Schlüssel mit Knopfdruckentriegelung umsteigen.

Ende des Passworts?

Die unter anderem von Paypal initiierte FIDO-Alliance, der inzwischen weitere Größen wie Alibaba oder die Bank of America beigetreten sind, engagiert sich neben der 2-Faktor-Authentifikation (U2F, siehe SSN 10/2014) verstärkt für biometrische Authentifikationsverfahren (Fingerabdruck-, Herzrhythmus- und Venenerkennung) und hat am 09.12.2014 Version 1.0 ihres Universal Authentication Framework (UAF) veröffentlicht.

Doch Biometrie hat bekannte Schwächen. Jüngst zeigten das der Vortrag von starbug auf dem 31. Chaos Communication Congress am 27.12.2014, der u. a. über Kameras in Mobiltelefonen biometrische Merkmale ausspähte, und der Hack des iPhone-Fingerabdrucksensors von Ben Schlabs, dem es im September 2014 gelang, den Sensor mit einem Holzleim-Fingerimitat zu täuschen.

Ein grundsätzliches Problem ist, dass sich biometrische Merkmale, wenn sie einmal gestohlen wurden, nicht einfach wie ein Passwort ändern lassen – lediglich der Fingerabdruck erlaubt bis zu neun Wechsel. Das wiegt umso schwerer, als dieselben biometrischen Merkmale unvermeidlich für die Authentifikation in zahlreichen unterschiedlichen Anwendungen zum Einsatz kommen werden.

Mit Passwörtern werden wir daher wohl noch eine Weile leben und sollten uns mit Verfahren beschäftigen, die zu sichereren Passwörtern führen. So lassen sich Anwender möglicherweise zu Wahl stärkerer Passwörter bewegen, wenn sie von Passwort-Managern unterstützt werden. Und Anwendungen könnten die Stärke eines gewählten Passworts mit Passwort-Metern bei der Eingabe messen und zu schwache Passwörter zurückweisen.

XP lebt!

Totgesagte leben länger. Dies belegen Anfragen der Grünen und der Piratenpartei zum Einsatz von Windows XP in der Berliner Stadtverwaltung anlässlich des bevorstehenden Ablaufs der teuer bezahlten Supportverlängerung von Microsoft: Ab April 2015 werden keine Aktualisierungen mehr geliefert. Tatsächlich ist Berlin nicht die einzige Stadtverwaltung, bei der ältere Anwendungen die Ablösung von Windows XP bisher verhindert haben. Auch werden noch eine Vielzahl von Geldautomaten unter Windows XP betrieben. Wie groß aber ist die Gefährdung durch Windows XP wirklich?

Werden neu entdeckte Sicherheitslücken von XP nicht mehr behoben, steigt das Risiko, dass Schadsoftware durch Ausnutzung dieser Lücken Systeme befällt. Dagegen hilft eine strikte Entkopplung der produktiven Anwendungen von „Malwarezugängen“ wie dem Internet, den lokalen Datenschnittstellen (vulgo USB-Anschlüsse) und dem Einfallstor E-Mail-Anhang.

Realisieren lässt sich das, indem man z. B. den Internet- und E-Mail-Zugang über einen Terminalserver bereitstellt oder, noch besser, die alte Software in eine virtuelle Maschine mit XP verfrachtet – und diese auf aktuellen Windows-Clients betreibt.

Dass Abschalten keine Lösung, sondern „friendly fire" ist, dürfte auch dem Berliner Datenschutzbeauftragten Dix klar sein. Mit einer besonnenen und differenzierten Analyse lassen sich Lösungen finden, XP-abhängige Anwendungen mindestens für eine Übergangszeit und mit vertretbaren Komforteinbußen für die Benutzer weiter zu betreiben, ohne damit einen Sicherheits-Gau zu riskieren.

Secorvo News

Symposium „No Blackout"

Anlässlich der bevorstehenden Verabschiedung des IT-Sicherheitsgesetzes und der daraus folgenden Verpflichtungen von Betreibern kritischer Infrastrukturen veranstaltet Secorvo am **12.** und **13.05.2015** das Symposium „No Blackout – IT-Sicherheit für die Energieversorgung" in der Buhlschen Mühle in Ettlingen.



Die Veranstaltung richtet sich nicht nur an Unternehmen und Institutionen aus dem Bereich der kritischen Infrastrukturen – sie bietet wertvolle Erfahrungen für alle Firmen, die den Aufbau eines Information Security Managements (ISMS) planen oder bereits vorbereiten.

Unter anderem werden die Stadtwerke Ettlingen über den „fx-Hack" und die Folgen berichten, und wir werden etwas über die IT-Sicherheit in Kernkraftwerken erfahren. Gelegenheit zur Diskussion bieten das gemeinsame Dinner in der Villa Hartmaier's am 12.05. und die Networking-Pausen.

Wir freuen uns auf Ihre Teilnahme.

7. Tag der IT-Sicherheit

Beim 7. Tag der IT-Sicherheit am **19.05.2015**, einer Kooperationsveranstaltung der KA-IT-Si mit der IHK Karlsruhe, dem CyberForum und KASTEL, informiert das Landesamt für Verfassungsschutz über die aktuelle Bedrohungslage und die Risiken „Mensch" und „Technik". Es folgen Fachvorträge zu den Themen Netzwerksicherheit, Datenschutz und Mobile Computing. Das Programm schließt mit einem Live-Hacking, in dem gezeigt wird, welche Sicherheitsschwächen zahlreiche Webanwendungen aufweisen.

Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern bieten die „Networking-Pausen". Wir freuen uns auf Ihre Anmeldung.

Mit Brief und Siegel

Seit vielen Jahren setzt Secorvo College auf Seminare, bei denen die Teilnehmer ihre Qualifikation durch eine anschließende Prüfung und ein Zertifikat nachweisen können.

Dazu zählt insbesondere der T.I.S.P. (TeleTrusT Information Security Professional), ein inzwischen deutschlandweit anerkanntes Expertenzertifikat für Informationssicherheit. In unseren T.I.S.P.-Schulungen erhalten Sie in fünf Tagen einen kompakten Überblick zu allem, was in der Informationssicherheit zählt – unterstützt vom T.I.S.P.-Buch „Zentrale Bausteine der Informationssicherheit". Auf dem Seminar vom **22.** bis **26.06.2015** gibt es noch wenige Plätze; weitere Gelegenheiten zur Zertifizierung Ihrer Expertise bieten wir im September (**21.–25.09.2015**) und November (**23.–27.11.2015**) in unseren Seminarräumen in Karlsruhe.



Die Zertifikatsschulung T.E.S.S. – Sichere Systeme dank System Security Engineering zeigt Wege auf, wie ganze Systeme mit allen Komponenten, Schnittstellen und Prozessen mit angemessener Sicherheit gestaltet werden können. Der T.E.S.S. (TeleTrusT Engineer for System Security) steht für interdisziplinäre Sicherheitskompetenz. Termine: **14.–19.06.2015** und **10.–13.11.2015** in Karlsruhe.

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/college.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2015	
06.-07.05.	16. Datenschutzkongress (EUROFORUM, Berlin)
12.-13-05.	Symposium „No Blackout“ – IT-Sicherheit für die Energieversorgung (Secorvo, Karlsruhe)
18.-21.05.	OWASP AppSec EU 2015 (OWASP Foundation, Amsterdam/NL)
18.-20.05.	IMF 2015 (Fraunhofer IAO, Magdeburg)
19.-21.05.	14. Deutscher IT-Sicherheitskongress (BSI, Bonn)
19.05.	7. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si; Karlsruhe)
20.-22.05.	Entwicklertag 2015 (VKSI, GI, ObjektForum; Karlsruhe)
26.-28.05.	IFIP SEC 2015 (IFIP, Hamburg)
Juni 2015	
08.-12.06.	Audit Challenge 2015 (Frankfurt School of Finance & Management, Frankfurt)
15.-16.06.	DuD 2015 (COMPUTAS, Berlin)

Fundsache

Am 02.04.2015 wurden vom Open Crypto Audit Project die Ergebnisse des TrueCrypt-Audits (v7.1a) veröffentlicht. Mängelfrei ist die Software nicht, aber Hintertüren oder einfach ausnutzbare Angriffsmöglichkeiten wurden nicht gefunden. Trotz der Einstellung der Weiterentwicklung spricht also derzeit nichts gegen die Nutzung dieser Version – oder auf TrueCrypt aufbauender Lösungen wie VeraCrypt.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Sven Köhler, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Mai 2015



Wir regulieren uns zu Tode

Nicht immer kommt die Bürokratie so unübersehbar daher wie beim Mindestlohngesetz. Dokumentationspflichten, Erklärungen gegenüber Auftraggebern und Verpflichtungen von Auftragnehmern – 99% aller Unternehmen werden wegen einzelner schwarzer Schafe in kollektive Misstrauenshaft genommen.

Ganz Ähnliches ereilt Deutschland in Folge des Sarbanes-Oxley-Act: Die Skandale bei Enron und Worldcom hatten 2002 in den USA eine Welle der Compliance-Regulierung losgetreten. Seitdem sickern regulatorische Kontrollen unternehmerischen Wohlverhaltens in deutsche Unternehmen ein. Wirtschaftsprüfer stellen in wachsendem Umfang auch Anforderungen an den sicheren IT-Betrieb. Mit teilweise skurrilen Resultaten: Keine Prüfung, in der nicht für zentrale IT-Systeme ein regelmäßiger Passwortwechsel spätestens alle 90 Tage gefordert wird. Von dem eigentlichen Zweck (Begrenzung des Schadens, sollte ein Passwort kompromittiert sein) hat sich diese Regelung längst befreit – denn Benutzer wählen Passwörter, denen sie eine einfache Bildungsregel mitgeben, wie z. B. eine Ziffer am Ende. Ein Angreifer kennt daher mit einem Passwort auch alle folgenden – und wir quälen alle 90 Tage eine wahrscheinlich 8stellige Zahl von IT-Nutzern mit einem Sinn entleerten Ritual, das sogar die Passwortkomplexität senkt. Ähnliches könnte uns nun mit dem IT-Sicherheitsgesetz bevorstehen – und auch die Vorratsdatenspeicherung wird nicht ohne Auswirkungen auf die Compliance-Anforderungen in Unternehmen bleiben (siehe die Beiträge in diesen SSN).

Manchmal ist es unvermeidlich, dass politisch oder gesellschaftlich gewünschtes Verhalten gesetzlich erzwungen wird. Die durch Detailregulierung entstehenden Bürokratiekosten dürften jedoch – bei aller Sympathie für die IT-Sicherheit – die verhinderten Schäden um ein Vielfaches übersteigen. Wer in erster Linie wirtschaftlichen Schaden von Unternehmen abwenden will, sollte die IT-Sicherheit daher besser der Selbstregulierung und Haftung überlassen.



Inhalt

Wir regulieren uns zu Tode

Security News

Das BAG und die Einwilligung

Seiteneffekt der Vorratsspeicherung

Wirkungen von Datensicherheit

Schriftform bei Mitarbeiterfotos

Security-Adventure

Secorvo News

Kompetenz darf sich auszahlen

Mehr Sicherheit im Mittelstand

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Das BAG und die Einwilligung

Dass die Einwilligung nur in speziellen Ausnahmefällen als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten taugt ist herrschende Meinung unter Datenschützern.

Das Bundesarbeitsgericht hat sich nun in einem Urteil vom 11.12.2014 – eher beiläufig – zu dieser Frage geäußert. So gebe der Arbeitnehmer mit Eingehen des Arbeitsvertrags nicht seine Persönlichkeitsrechte auf. Eine Benachteiligung aufgrund einer Einwilligungsverweigerung stelle einen groben arbeitgeberseitigen Nebenpflichtverstoß und einen Verstoß gegen das Maßregelungsverbot aus § 612a BGB (Verbot der Benachteiligungen wegen einer zulässigen Rechteausübung) dar. Arbeitnehmer könnten sich auch im Arbeitsverhältnis frei entscheiden, wie sie ihr Grundrecht auf informationelle Selbstbestimmung ausüben.

Eine Revolution steht trotzdem nicht bevor: Zwar stellt das BAG auch die Widerruflichkeit einer Einwilligung unter den Vorbehalt einer Interessensabwägung. Es verleiht damit aber der Einwilligung trotzdem nicht die praktisch notwendige Stabilität.

Zudem sind an der Argumentation des BAG Zweifel angebracht: Bereits die Befürchtung, der Arbeitgeber könne aufgrund der Verweigerung benachteiligen, ohne dass der Zusammenhang nachweisbar ist, kann die Freiwilligkeit einer Einwilligung im Arbeitsverhältnis erheblich einschränken. Der Verweis auf späteren Rechtsschutz ist sehr formal und verkürzt den Schutz der Informationellen Selbstbestimmung erheblich.

Seiteneffekt der Vorratsspeicherung

Am 27.05.2015 hat das Bundeskabinett den Gesetzentwurf zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten – kurz: die Vorratsdatendatenspeicherung – beschlossen. Die Diskussion über die Verfassungsmäßigkeit des neuen Anlaufs ist nun in vollem Gange.

Aus Sicht der Informationssicherheit ist jedoch von Interesse, wie die Bundesregierung die Mahnung des Bundesverfassungsgerichts umgesetzt hat, den Schutz der Daten zu regeln. Der Entwurf kommt dieser Anforderung in den vorgeschlagenen §§ 113d ff TKG nach. Vorgesehen sind – in Ergänzung zu § 109 TKG – u. a. der Einsatz eines „besonders sicheren Verschlüsselungsverfahrens“, die Speicherung in getrennten Speichereinrichtungen, das „Vier-Augen-Prinzip“ für den Zugriff und eine Zugriffsprotokollierung von einem Jahr über Zeitpunkt, Akteure, Zweck und Art des Zugriffs.

Die Bundesnetzagentur soll in Abstimmung mit dem BSI und der Bundesdatenschutzbeauftragten einen ergänzenden Anforderungskatalog erstellen. Das Sicherheitskonzept der Provider nach § 109 Abs. 4 TKG ist entsprechend zu ergänzen. Ein mangelnder Schutz soll Geldstrafen bis zu 500.000 € nach sich ziehen.

Sollte der Entwurf Gesetz werden, könnte dies weit reichende Auswirkungen auf andere Verarbeitungen besonders schutzwürdiger Daten haben: Die Sicherheitsvorgaben setzen hier einen neuen Maßstab. Mit Spannung darf man daher den Anforderungskatalog der BNetzA erwarten – vor allem in Bezug auf die in § 113b Abs. 8 TKG n.F. geforderte irreversible Löschung oder die Kriterien für ein „besonders sicheres Verschlüsselungsverfahren“.

Wirkungen von Datensicherheit

Häufig sind es die Nebenfolgen, der die wahre Bedeutung eines Urteils ausmachen. So auch bei einem Urteil des Landesarbeitsgerichts Schleswig-Holstein vom 04.03.2015, das die Aufhebung einer Kündigung bestätigt, die gegen ein Betriebsratsmitglied wegen des Verstoßes gegen die Verschwiegenheitspflicht ausgesprochen worden war. Das Betriebsratsmitglied hatte Rechtsanwaltsrechnungen zu betriebsverfassungsrechtlichen und individualarbeitsrechtlichen Beratungen an den betroffenen Betriebsrat eines verbundenen Unternehmens weitergegeben.

Das Landesarbeitsgericht sah hierin keinen die fristlose Kündigung rechtfertigenden Verstoß. Denn die Zugriffsrechte des Gekündigten waren nicht eingeschränkt und es fehlte eine Kennzeichnung des Geheimhaltungsbedarfs an den Dokumenten.

Das Urteil verdeutlicht die rechtliche Bedeutung von IT-Sicherheitsmaßnahmen: Sie begründen bereits durch ihre Existenz rechtlichen Schutz und erzeugen auch rechtliche Wirkungen. Aus diesem Grund sollte selbst auf überwindbare technische und organisatorische Maßnahmen und eine Geheimhaltungsklassifizierung nicht verzichtet werden.

Schriftform bei Mitarbeiterfotos

Wollen Arbeitgeber Fotos oder Videos ihrer Mitarbeiter veröffentlichen, bedarf dies nach § 22 Kunsturhebergesetz (KUG) in der Regel der Einwilligung der Arbeitnehmer. Das Gesetz sieht für diese Einwilligung keine besondere Form vor. Tatsächlich setzen Unternehmen oft auf ein „lautes Nicken“ – die für einen Werksausweis angefertigten Fotos werden so oft wie selbstverständlich in das elektro-

nische Telefonverzeichnis aufgenommen und auf die Webseite gestellt.

Das Bundesarbeitsgericht (BAG) hat nun mit Urteil vom 11.12.2014 (Az. 8 AZR 1010/13) schärfer als die Forderung des KUG entschieden, dass eine ausdrückliche – also in der Regel schriftliche – Einwilligung der betroffenen Arbeitnehmer erforderlich ist. Anlass war ein Werbefilm im Internet, in dem Mitarbeiter einige Sekunden lang gezeigt wurden. Gleichzeitig stellte das BAG fest, dass eine formal korrekte Einwilligung nicht automatisch mit Beendigung des Arbeitsverhältnisses erlischt, sondern der Widerruf vielmehr eines plausiblen Grundes bedarf – zumindest dann, wenn nicht die Person des Mitarbeiters im Vordergrund steht.

Für die Fotos auf Werksausweisen wird man auch weiterhin von überwiegenden Sicherheitsinteressen des Unternehmens ausgehen können. In den meisten anderen Fällen der Veröffentlichung müssen Unternehmen schriftliche – und zweckbezogene – Einwilligungen einholen. Dies gilt für das Internet gleichermaßen wie für das Intranet. Eine unspezifische Generaleinwilligung in Arbeitsverträgen scheidet aus – solche Klauseln scheitern meist am AGB-Recht.

Security-Adventure

Die Spieler von „Gezielter Angriff – Das Spiel", einem am 05.05.2015 veröffentlichten kostenlosen Online-Lernspiel des japanischen IT-Sicherheitsanbieters Trend Micro, schlüpfen in die Rolle des CIOs der fiktiven Firma „The Fugle". Er hat ein beschränktes Budget und muss im Spiel das Geld in sinnvolle und angesichts der aktuellen Risiken angemessene Projekte investieren.

Seine Entscheidungen beeinflussen den weiteren Verlauf der Spiels, bis es schließlich zu einem gezielten Angriff kommt. Spieler, die den Angriff nicht mehr verhindern können, erhalten eine Analyse ihrer Handlungsschritte und Hinweise, wie sie das Spiel beim nächsten Mal in die richtige Richtung lenken können.

Ein interessanter Ansatz, um die Sensibilität für IT-Sicherheit zu steigern und zugleich ein gesundes Verständnis für angemessene Schutzmaßnahmen zu vermitteln. Das Spiel ist kostenlos, die Spieler müssen keine persönlichen Daten preisgeben.

Secorvo News

Kompetenz darf sich auszahlen

In diesen Tagen wird das 750ste T.I.S.P.-Zertifikat ausgestellt. Es belegt neben der mindestens dreijährigen Berufserfahrung im Gebiet IT-Sicherheit vertiefte Kenntnisse in allen relevanten Teilgebieten der Informationssicherheit – von rechtlichen Anforderungen über Public Key Infrastrukturen bis zur Sicherheit mobiler Endgeräte.

In unseren fünftägigen T.I.S.P. Schulungen erhalten Sie einen kompakten Überblick über alle für die Zertifizierung relevanten Wissensgebiete. Zur Vorbereitung schicken wir Ihnen vorab das von uns verfasste 700seitige Begleitbuch zum T.I.S.P. („Zentrale Bausteine der Informationssicherheit", 2. Auflage 2014).

2015 geben wir Ihnen noch drei Mal die Gelegenheit das T.I.S.P.-Zertifikat zu erwerben: im Juni (**22.–26.06.**), September (**21.–25.09.**) und November (**23.–27.11.**). Sichern Sie sich Ihren Platz!



Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Mehr Sicherheit im Mittelstand

Über 100 Verantwortliche für Datenschutz und IT-Sicherheit aus Unternehmen der TechnologieRegion Karlsruhe folgten am 19.05.2015 den Praxisberichten und Expertenvorträgen auf dem 7. Tag der IT-Sicherheit in Karlsruhe. Wer die Veranstaltung verpasst haben sollte, findet die Pressemitteilung und die Vortragsunterlagen (zu den Themen Risiko Mensch und Technik, Aktuelle Entwicklungen zu ‚Privacy by Design', Sicherheit im Always-On, Designprinzipien für sichere Systeme, Intrusion Prevention Systeme) ab sofort auf http://www.tag-der-it-sicherheit.de.

Das nächste Event der Karlsruher IT-Sicherheitsinitiative findet statt am **16.07.2015** im Panoramasaal der IHK Karlsruhe. Dort wird Dominik Schadow über Java-Security sprechen – wer ‚Java' sagt, sollte auch ‚sichere Softwareentwicklung' meinen …

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2015	
08.-12.06.	Audit Challenge 2015 (Frankfurt School of Finance & Management, Frankfurt)
15.-16.06.	DuD 2015 (COMPUTAS Gisela Geuhs GmbH, Berlin)
19.06.	Workshop: Social Media Security (Fachgruppe SECMGT der Gesellschaft für Informatik e.V., Frankfurt)
22.-26.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)>
August 2015	
01.-06.08.	Blackhat USA 2015 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 23 (DEFCON, Las Vegas/US)
09.-13.08.	15th Annual DFRWS Conference 2015 (DFRWS, Philadelphia/US)
12.-14.08.	24th USENIX Security Symposium (Usenix, Washington D.C./US)
16.-20.08.	Crypto 2015 (IACR, Santa Barbara/US)
31.08.	Sommerakademie (ULD, Kiel)

Fundsache

Am 12.01.2015 hat die ENISA einen 78seitigen Report „Privacy and Data Protection by Design" veröffentlicht. Darin versuchen die Autoren, die rechtlichen Anforderungen und technischen Möglichkeiten in Überdeckung zu bringen. Lesenswert sind die „Eight Privacy by Design Strategies" und der profunde Überblick über aktuelle Privacy Enhancement Technologies. 211 Referenzen belegen die breite fachliche Abdeckung.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Juni 2015



Von Medizinern lernen

Dass eine gesetzliche Immunität nicht vor Trojanerangriffen schützt mussten jüngst auch die Abgeordneten des Deutschen Bundestages schmerzlich erfahren. Und sie sind in guter Gesellschaft: Die Zahl der Fälle, in denen Angreifer über gut gemachte E-Mail-Anhänge und unveröffentlichte Sicherheitslücken (Zero-Day-Attacken) in Unternehmen eindringen, nehmen nachweislich zu.

Dabei sind die bekannten Fälle möglicherweise nur die Spitze eines (großen) Eisbergs: Wie im Bundestag bleiben die Angriffe häufig lange unentdeckt. Denn komplexe Angriffssoftware kümmert sich auch um den eigenen Schutz: Mit herkömmlichen Tools ist sie meist nicht aufzuspüren, und wenn die Aktivitäten des Trojaners unterhalb der Wahrnehmungsschwelle des Benutzers bleiben, schöpft dieser auch keinen Verdacht.

Gegen Angriffe dieser Art ist unser etabliertes Instrumentarium – ein Sicherheitskonzept plus präventive Schutzsysteme – schnell mit seinem Latein am Ende. Da hilft auch kein ‚fingerpointing' auf das Risiko vor dem Bildschirm – denn bei einem sorgfältig vorbereiteten, gezielten Angriff ist ‚Aufpassen' keine adäquate Schutzmethode. Wenn schon der Virenscanner die Schadsoftware nicht erkennen kann, wie soll dies dann dem Anwender glücken?

Vielleicht müssen wir angesichts dieser Herausforderungen den Beruf des Informations-Sicherheitsbeauftragten neu denken. Denn es geht uns inzwischen ähnlich wie den Medizinern: Auch wenn wir die Zusammenhänge immer besser verstehen, werden Krankheiten komplexer, Therapien spezialisierter, entwickeln Viren Resistenzen gegen bislang wirksame Medikamente und suchen sich neue Infektionswege. Neue Medikamente haben wiederum unbekannte Nebenwirkungen – damit steigt die Unübersichtlichkeit. Mediziner haben darauf mit Diversifizierung und Spezialisierung reagiert. Dabei haben sie gegenüber uns Technikern einen uneinholbaren Vorteil: Ihre Patienten heilen meist von selbst. Auch trotz der Therapie.



Inhalt

Von Medizinern lernen

Security News

Der Chirurg

Der Internist

Der Psychologe

Der Labordiagnostiker

Der Notarzt

Der Anästhesist

Der Pathologe

Das Gesundheitsamt

Secorvo News

Secorvo ist ‚Top Consultant'

Wer ‚Java' sagt, sollte auch sichere Softwareentwicklung meinen.

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Der Chirurg

Der unvermeidliche ‚Trade-off' zwischen erzielbarer Sicherheit und Benutzerakzeptanz kann gelegentlich den Chirurgen erfordern. Denn manchmal geht es nicht ohne operativen Eingriff.

So benötigen Trojaner einen Kommunikationsweg, um von einem Endsystem aus mit dem Angreifer zu kommunizieren. Schneidet man das Unternehmensnetz in mehrere Teilnetze, so kann man die externe und interne Kommunikation entkoppeln. Das Surfen im Internet lässt sich beispielsweise über einen Terminalserver mit Browser realisieren, während das Endsystem nur auf das interne Netz zugreifen kann. Hat der Browser eine Malware eingefangen, kann diese nicht auf interne Daten zugreifen. Der Download von Daten aus dem Internet funktioniert dann allerdings nicht mehr ganz so bequem über einen Quarantänebereich.

Der Internist

Die aktuellen Infektionswege zwingen zu einer genaueren Beschäftigung mit den inneren Organen. So können durch eine Separierung von Anwendungen deren Daten vor anderen, möglicherweise infizierten ‚Organen' geschützt werden. Technisch realisierbar ist so etwas über Virtualisierungslösungen wie Qubes OS oder Docker. Dabei läuft jede Anwendung in einem eigenen Kontext, damit bei einem Sicherheitsproblem nur die jeweilige virtuelle Plattform betroffen ist, nicht aber das Gesamtsystem oder weitere Anwendungen. Der Datenaustausch zwischen diesen Plattformen sollte restriktiv gehandhabt werden.

Leider ist dieser hochinteressante Ansatz ab Werk bisher nur für eine Handvoll Anwendungen wie Firefox, Thunderbird und Libreoffice verfügbar. Für eigene Anwendungen muss ggf. eine Windows-VM etabliert werden.

Der Infektionsschutz kann durch die Innere Medizin erheblich gesteigert werden. Risiken und Nebenwirkungen sollten jedoch mit den betroffenen Benutzern abgestimmt werden.

Der Psychologe

Der Psychologe kümmert sich um den Menschen, darum, was dieser denkt und fühlt. Ihn interessieren weniger technische Lösungen sondern Maßnahmen, die auf das Verhalten der Menschen zielen. Er greift da ein, wo es in ungesunder Weise von der gesetzten Norm abweicht.

Eines seiner Instrumente ist die Durchführung wirksamer Awareness-Kampagnen, die mit Wahrnehmungs- und Verhaltensgewohnheiten brechen und einprägsam wesentliche Kernbotschaften vermitteln. Statistiken und Messungen helfen ihm, den Erfolg seiner Maßnahmen zu überprüfen.

Der Labordiagnostiker

Die Labordiagnostik untersucht Proben auf Befunde und versucht, aus den Ergebnissen zusammen mit der Bewertung anderer Symptome eine Diagnose zu erstellen. Auch in der Informationssicherheit sollte man die Diagnose nicht allein auf Symptome wie Anzeichen für Schwächen oder Berichte über Vorfälle stützen. Ein Labordiagnostiker solle regelmäßig Proben analysieren, um Infektionsgefahren frühzeitig zu erkennen. Die Ergebnisse von Schwachstellenscans und Penetrationstest können Handlungsbedarf aufzeigen.

Wie in der Medizin sind auch hier Erfahrung und die richtigen Werkzeuge der Schlüssel zur zutreffenden Diagnose. Konkrete Ansätze findet man z. B. bei PCI, beim BSI, beim NIST sowie im OWASP OTG und OWASP ASVS.

Der Notarzt

Gelegentlich sind akut lebensrettende Maßnahmen für die Versorgung eines Notfallpatienten erforderlich. Treten eine Störung des Bewusstseins, der Atmung, des Kreislaufes oder Lähmungen, Verbrennungen, Vergiftungen, Schuss-, Stich- oder Hiebverletzungen lebenswichtiger Organe auf, sollte spätestens 10 bis 15 Minuten nach Eingang des Notrufs der Notarzt seinen Einsatzort erreichen. Kommt er zu spät, können auch Fachwissen und Reanimation dem Notfallpatienten meist nicht mehr helfen.

Zwar ist auch der Notarzt der Informationstechnik gelegentlich von einem Fehlalarm betroffen. Oft aber stößt er auf zunächst unerklärliche Effekte auf der Ebene der Betriebssysteme oder im Netzwerkverkehr, die Symptome einer getarnten Schadsoftware sein können.

Die Auswertung von zusammengeführten Logdaten und Netflows bringt ihn, manchmal mit Unterstützung des »*Labodiagnostikers* oder, wenn er zu spät gekommen ist, des »*Pathologen*, auf die Spur des Krankheitsbilds und erlaubt ihm eine Einschätzung, wie kritisch der Grad der Verletzung bzw. der Infektion für das einzelne System und die gesamte Infrastruktur ist. Wird er zu spät gerufen, lassen sich betroffene Infrastrukturbereiche nicht mehr isolieren und es bleibt ihm nur, der IT eine Totenbescheinigung auszustellen.

secorvo
security consulting

Der Anästhesist

Der Anästhesist sorgt dafür, dass die Vitalfunktionen des Patienten während operativer und diagnostischer Eingriffe aufrechterhalten werden. Ein medizinischer Eingriff ist eine Krise – und der Anästhesist ihr Manager. Egal ob sich ein Hackerangriff, ein Systemausfall oder eine sonstige Krise im Unternehmen ereignet: es bedarf eines Krisenmanagers, der den Überblick und den Puls des Unternehmens im Auge behält, der mit allen Beteiligten in Kontakt steht und sie bei Bedarf beruhigt. Das gilt gleichermaßen für interne Beteiligte wie für interessierte Dritte, etwa die Presse.

Vor allem aber muss er den Patienten im Blick behalten, damit der Eingriff, die Säuberung der IT-Systeme und der Tausch von Hard- und Software, trotz des Zeitdrucks in geordneten Bahnen verläuft.

Der Anästhesist muss sich in vielen Disziplinen wenigstens grundsätzlich auskennen, er muss Situationen einschätzen, entscheiden und moderieren können. Vor allem aber muss er für Ruhe und Gelassenheit sorgen, damit der Patient die Operation gut übersteht.

Der Pathologe

Auch nach einer erfolgreichen (Not-) Operation gibt es noch offene Fragen. Wie konnte es dazu kommen? Was waren die Ursachen? Wie lässt sich so etwas in Zukunft vermeiden?

Der Pathologe unterstützt die Bewertung und Behandlung von Notfällen und Infektionen durch die Analyse von Gewebeproben (Biopsie) und Obduktionen. Er untersucht sowohl funktionierende IT-Systeme, bei denen Auffälligkeiten festgestellt wurden, als auch Systeme, die ohne erkennbaren Grund ihre Funktionen eingestellt haben.

Dabei gewinnt er Metadaten aus Hauptspeicherabzügen und Festplattenduplikationen und wertet diese zielgerichtet aus. Kann er die Infektion eines Systems feststellen, veranlasst er Quarantänemaßnahmen zur Eingrenzung der Ansteckungsgefahr. Sollte es zu einem Abfluss von Vitaldaten gekommen sein, werden die Nachweise so dokumentiert, dass sie im Streitfall gerichtsverwertbar sind.

Das Gesundheitsamt

Die Gesundheitsämter wachen über Hygiene und Epidemien. Eine wesentliche Säule sind Meldepflichten, die auch in der IT-Sicherheit langsam Einzug in Gesetze halten. Beispiele sind § 109a TKG, § 42a BDSG, § 15a TMG oder § 83a SGB X. Hinzu kommt die Einführung von Meldepflichten in dem vor der Verabschiedung stehenden IT-Sicherheitsgesetz: § 8b Abs. 4 BSIG-E wird künftig die Betreiber kritischer Infrastrukturen zur Meldung verpflichten.

Empfänger der Meldungen sind die Datenschutzaufsichtsbehörden, die Bundesnetzagentur und künftig das Bundesamt für Sicherheit in der Informationstechnik (BSI). Ähnlich den Datenschutzaufsichtsbehörden kann auch das BSI bald Auflagen zur Beseitigung von Sicherheitsmängeln erteilen.

Damit entsteht eine staatliche, auf Informationssicherheit bezogene Aufsicht. Im Gesundheitswesen wurde mit den Gesundheitsämtern der Grundstein für eine erfolgreiche Epidemiebekämpfung gelegt.

Secorvo News

Secorvo ist ‚Top Consultant'

Am vergangenen Freitag, den 26.06.2015, wurde Secorvo in Essen als eines der besten deutschen Beratungsunternehmen für den Mittelstand ausgezeichnet. Das Urteil der Jury ist das Ergebnis einer Bewertung der Professionalität von Secorvo in elf Dimensionen durch zehn mittelständischen Referenzkunden, die wissenschaftlich ausgewertet wurde. Die Auszeichnung überreichte Bundespräsident a. D. Christian Wulff.



Wer ‚Java' sagt, sollte auch sichere Softwareentwicklung meinen.

Die Sicherheit von Java-Webanwendungen hatte lange Zeit einen guten Ruf. Tatsächlich ist Java jedoch nicht sicherer oder unsicherer als andere Programmiersprachen. Spätestens mit den zahlreichen Java-Sicherheitsproblemen der vergangenen Jahre hat sich diese Erkenntnis herumgesprochen. Auf dem nächsten KA-IT-Si-Event am **16.07.2015** stellt Dominik Schadow (BridgingIT) in seinem Vortrag Sichere Webanwendungen mit Java typische Fallstricke bei der Planung, Entwicklung und Wartung von Java-Webanwendungen vor und zeigt, wie man diesen wirkungsvoll in allen Phasen eines Entwicklungsprojekts zu Leibe rücken kann (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2015	
16.07.	Wer 'Java' sagt, sollte auch sichere Softwareentwicklung meinen. (KA-IT-Si, Karlsruhe)
August 2015	
01.-06.08.	Blackhat USA 2015 (Blackhat, Las Vegas/US)
06.-09.08.	DEFCON 23 (DEFCON, Las Vegas/US)
09.-13.08.	15th Annual DFRWS Conference 2015 (DFRWS, Philadelphia/US)
12.-14.08.	24th USENIX Security Symposium (Usenix, Washington D.C./US)
16.-20.08.	Crypto 2015 (IACR, Santa Barbara/US)
31.08.	Sommerakademie (ULD, Kiel)
September 2015	
08.-09.09.	D•A•CH Security (Gemeinsame Arbeitskonferenz GI OCG BITKOM SI TeleTrusT, Sankt Augustin)
15.-17.09.	Future Security 2015 (Fraunhofer VVS, Berlin)
17.09.	Informationstag "Elektronische Signatur" 2015 (TeleTrust, Berlin)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Wer schon immer wissen wollte wie Gedankenlesen funktioniert - im folgenden 2,5minütigen Video wird dieses Mysterium aufgelöst.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Christoph Schäfer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2015



… denn sie wissen nicht, was sie tun.

Siebzig Jahre ist es her, dass James Dean in kürzester Zeit die unbekümmerte Ungezügeltheit der Jugend salonfähig machte. Daran konnten auch die Umstände seines frühen Todes nichts ändern. Und sein Vermächtnis wirkt offenbar bis heute fort.

So ist es in den vergangenen 20 Jahren endlich Schritt für Schritt gelungen, Sicherheit als eine wesentliche Eigenschaft eines IT-Systems zu verankern. Kaum ein Anbieter, der sich der Frage der Sicherheit eines neuen IT-Produkts nicht widmen würde – und sei es auf den letzten Metern vor der Produktivschaltung. Das ist das Ergebnis eines mühsamen, oft von unangenehmen (und vermeidbaren) Lernerfahrungen begleiteten Prozesses.

Doch kaum ist es so weit, konterkariert das „Internet der Dinge" diese Entwicklung auf erschreckende Weise: Elektrische Skateboards lassen sich via Bluetooth unter fremde Kontrolle bringen, kontaktlose „Smart-Keys" schalten das Fahrzeug einfach aus, wenn Mitfahrer sie während der Fahrt aus dem Fenster werfen. Ein Automobilhersteller liefert Autos mit Internet-Zugang, die sich während der Fahrt von unberechtigten Dritten steuern und manipulieren lassen – und bittet anschließend seine Kunden, einen Patch über das Internet herunterzuladen und via USB-Stick zu installieren (siehe diese SSN). Schließlich kommt ein 13.000 US$ teures Präzisionsgewehr auf den Markt, bei dem Unberechtigte die Zieleinrichtung via WLAN umkonfigurieren können.

In Fragen der Sicherheit scheint ungezügelte, von Kompetenz unbelastete Produktentwicklung im Internet der Dinge wieder „En Vogue" zu sein – ungeachtet der um ein Vielfaches größeren Gefahren, die dabei für Leben und Gesundheit drohen. Wir können nur hoffen, dass die Lernkurve diesmal steiler und kürzer ausfällt.



Inhalt

… denn sie wissen nicht, was sie tun.

Security News

Mit Daten bezahlen

Clipper reloaded

Ferngesteuert in den Graben

Sozialadäquanz als Erlaubnistatbestand?

Weisungsfreiheit externer DSBs

Einjährige Hackerin

Side-Channel in der Cloud

Secorvo News

Secure Coding

T.I.S.P., PKI und aktuelle Fragen

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Mit Daten bezahlen

Was lange von Datenschützern befürchtet wurde, wird nun wahr: Ab 2016 werden unsere Gesundheitsdaten zur Währung. Die Generali plant die Einführung ihres Tarifs „Vitality“ in 2016. Per Smartphone-App können Versicherte Fitnessdaten an Generali übermitteln und werden für einen gesunden Lebensstil mit Rabatten belohnt. Derweil hat Apple am 16.07.2015 ein Verfahren zum Patent angemeldet, mit dem Nutzern eines Smartphones oder Tablets nur dann bestimmte Werbeanzeigen eingeblendet werden, wenn sie sich die beworbenen Produkte oder Dienste auch leisten können. Festgestellt wird das anhand von Bank- oder Prepaid-Guthaben.

Noch sind solche Angebote die Ausnahme, und nur eine Minderheit von freiwilligen „First Movern“ wird sie nutzen. Irgendwann aber wird sich das Blatt wenden. Wer seine Daten dann nicht als Zahlungsmittel einsetzt, wird unter Rechtfertigungsdruck geraten. Mit Freiwilligkeit hat die Datenpreisgabe dann nichts mehr zu tun.

Clipper reloaded

Vor gut 22 Jahren, am 16.04.1993, löste die US-Regierung mit einer Pressemitteilung zum Clipper-Chip eine heftige Debatte über Verschlüsselung aus. Sie plante damals die Einführung einer Telefonie-Verschlüsselung mit einer Zugriffsmöglichkeit für die Strafverfolgungsbehörden. Die öffentliche Diskussion mündete schließlich 1997 in einer öffentlichen Stellungnahme führender Kryptologen mit dem Titel „*The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*“, die dazu beitrug, dass in den USA und Europa die Regulierung von Verschlüsselung aufgegeben wurde.

Aber Geschichte wiederholt sich. Begehrlichkeiten von Ermittlungsbehörden, wie sie von FBI-Direktor James B. Comey am 16.10.2014 ausgesprochen wurden, haben eine Kryptodebatte 2.0 losgetreten. Daher haben nun die Autoren der Stellungnahme von 1997 erneut Position bezogen. In ihrem Papier „*Keys Under Doormats*“ vom 06.07.2015 machen sie deutlich, dass Zugriffsmöglichkeiten für Strafverfolgungsbehörden auf verschlüsselte Daten die Fortschritte bei der Sicherheit im Internet konterkarieren: durch höhere Komplexität, zentrale Angriffspunkte und Hintertüren, die von Dritten ausgenutzt werden können. Es ist zu hoffen, dass das Papier den Gegnern offener Kryptografie den Wind genauso aus den Segeln nehmen wird wie die Stellungnahme 19 Jahre zuvor.

Ferngesteuert in den Graben

Chris Valasek und Charlie Miller sorgten am 21.07.2015 mit der Veröffentlichung eines Hacks, den sie auf der diesjährigen BlackHat vorstellen werden, bei Autofahrern für Gänsehaut: Es gelang ihnen, mittels einer Schwachstelle im Uconnect-Bordsystem über das Internet direkt auf Fahrzeuge verschiedener Marken des Konzerns Fiat-Chrysler (unter anderen Jeep, Fiat und Alfa Romeo) zuzugreifen. So konnten sie bei einem gekaperten Jeep Cherokee nicht nur die Bordelektronik (Klimaanlage, Radio) fernsteuern, sondern bekamen auch sicherheitskritische Komponenten unter ihre Kontrolle: Sie konnten Hupen, Bremsen deaktivieren und in die Lenkung eingreifen. Auch beim Umgang mit der Schwachstelle schwächelte Chrysler – und bot über die Uconnect-Webseite ein Executable zum Download für die Installation via USB-Stick an.

Die Schwachstelle ist kein Einzelfall, wie Valasek und Miller bereits 2014 in einer 100seitigen Studie belegten. Sie beweist aber überdeutlich, dass durch die für die Vernetzung von Auto und Smartphone erforderliche Anbindung an das Internet neue Bedrohungen entstehen – und sich auch traditionelle Industriezweige ernsthaft mit Security Engineering befassen sollten.

Sozialadäquanz als Erlaubnistatbestand?

Schon in den SSN 3/2015 berichteten wir über die geplante Neufassung von § 2 BORA (Berufsordnung der Rechtsanwälte), die das Outsourcing bei Berufsgeheimnisträgern legalisieren sollte. Der Bundesjustizminister hatte den Beschluss mit Verweis auf die mangelnde Regelungsbefugnis am 04.03.2015 aufgehoben. Auf Intervention der Bundesrechtsanwaltskammer wurde die Aufhebung am 31.03.2015 wieder rückgängig gemacht und die Neuregelung trat am 01.07.2015 in Kraft.

Damit ist die Inanspruchnahme von Leistungen Dritter nun auch bei Gefahr einer möglichen Offenbarung von geheimen Inhalten zulässig, wenn sie „objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz)“. Bisher machte sich ein Berufsgeheimnisträger durch unbefugte Offenbarungen strafbar, wenn er bspw. externe IT-Dienstleistungen in Anspruch nahm, bei denen er mit eigenen Mitteln einen unberechtigten Zugriff auf die Daten kaum verhindern konnte.

Bei allem Verständnis für das Dilemma: Die Argumentation der Rechtsanwaltskammer ist angesichts des hohen Schutzgutes gefährlich. Soll ein ungenügender Schutz, der üblich wird, künftig als Legitimationsgrundlage taugen?

Weisungsfreiheit externer DSBs

Das Landesarbeitsgericht Düsseldorf hat in einem jüngst veröffentlichten Urteil vom 04.03.2015 wichtige Standpunkte zur Stellung eines in einem Drittunternehmen angestellten, persönlich bestellten externen Datenschutzbeauftragten ausgeführt. Darunter sind für externe Datenschutzbeauftragte die folgenden Aussagen besonders interessant:

Die arbeitsvertragliche Weisungsgebundenheit des zum externen DSB persönlich bestellten Unternehmensmitarbeiters steht der Weisungsfreiheit gegenüber der verantwortlichen Stelle nicht entgegen. Auch das Benachteiligungsverbot betrifft nur das Vertragsverhältnis zur verantwortlichen Stelle. Eine persönliche Bestellung darf allerdings dem Angestellten eines dritten Unternehmens nicht aufgedrängt werden, es sei denn, dies ist Teil der arbeitsvertraglichen Leistung.

Tatsächlich ist die BDSG-konforme Bestellung eines externen Datenschutzbeauftragten unter Experten umstritten. Durch diese Entscheidung wird die Bestellung von Angestellten aufgewertet – ein bislang eher kritisch betrachteter Weg. Zu empfehlen ist er wegen des Auseinanderfallens von Bestellung und Leistungsvertrag dennoch nicht.

Einjährige Hackerin

Am 18.07.2015 gelang einem einjährigen Mädchen ein unfreiwilliger Hack des VW Passat ihrer Mutter: Es warf auf der A1 den Schlüsselbund mitsamt dem Smart-Key des Passat aus dem Fenster. Sofort schaltete sich der Motor aus – die Mutter konnte den Wagen glücklicherweise noch unfallfrei auf den Standstreifen lenken.

Offenbar ist der Hersteller hier bei der Bedrohungsanalyse zu kurz gesprungen. Bequemlichkeit sollte besser nicht vor Sicherheit gehen, schon gar nicht, wenn dadurch Leib und Leben in Gefahr geraten können. Auch bei Automobilzulieferern sollte man besser Security Engineering praktizieren.

Side-Channel in der Cloud

Auf der diesjährigen Recon stellte Sophia D'Antoine am 19.06.2015 einen sehr interessanten Side-Channel Angriff auf virtuelle Maschinen (VM) vor. VMs nutzen Hardware-Ressourcen gemeinsam; die virtuellen Instanzen und die darauf verarbeiteten Daten werden über einen Hypervisor getrennt. D'Antoines Angriff liest über den gemeinsamen Zugriff zweier VMs auf die Level-3-Caches des Prozessors Daten der VMs untereinander aus. Yuval Yarom und Katrina Falkner zeigten bereits am 05.07.2013 in „aFLUSH+Reload: A High Resolution, Low Noise, L3 Cache Side-Channel Attack", wie von einer Angreifer-VM aus z. B. auf den privaten PGP-Schlüssel in einer zweiten VM zugegriffen werden kann.

Wer vertrauliche Daten in der Cloud verarbeitet sollte nicht nur seinen Provider, sondern auch seine unmittelbaren Nachbarn auf Vertrauenswürdigkeit prüfen: Auch Hardware sollte man besser nicht unbesehen mit jedermann teilen.

Secorvo News

Secure Coding

Kaum ein Angriff, der zu seiner Durchführung nicht auf eine Software-Schwachstelle angewiesen wäre. Daher gilt: Wer das Übel an der Wurzel packen möchte, muss dafür sorgen, dass Software sicherer wird. Seit einigen Jahren engagiert sich Secorvo deshalb für sichere Software-Entwicklung und unterstützt Unternehmen mit entsprechenden Trainings.

Neben dem Seminar „Certified Professional for Secure Software Engineering" (CPSSE) sind daraus nun zwei Seminare speziell für Softwareentwickler entstanden: Für Java- und für C/C#-Entwickler bietet Secorvo College ab Oktober zwei Schulungen, die vermitteln, wie Sicherheit „programmiert" werden kann. Java Security findet statt am 13.-16.10.2015, und Secure Coding C/C# bieten wir an am 01.-03.12.2015.

T.I.S.P., PKI und aktuelle Fragen

Ende September (21.-25.09.2015) und Ende November (23.-27.11.2015) können Sie Ihre Kenntnisse und Erfahrungen mit dem T.I.S.P.-Zertifikat krönen – beim „Seminar zum Buch".

Schon einige hundert Teilnehmer haben sich mit unserem laufend aktualisierten Hands-on-Seminar „PKI – Grundlagen, Vertiefung, Realisierung" mit CAs, CRLs und OCSP vertraut gemacht. Die nächste Gelegenheit für die Teilnahme an diesem PKI-Steilkurs bietet sich Ihnen am 20.-23.10.2015 (schnelle Buchung empfohlen).

Mit der Neuauflage unseres Seminars IT-Sicherheit heute – das Schlaglicht auf die Informationssicherheit setzen wir auf aktuelle Themen mit hoher Relevanz für die Praxis – und auf eine Kombination auf konzentrierter Wissensvermittlung, Erfahrungsaustausch und Diskussion. Nächster Termin: 29.09.-01.10.2015.

Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/seminare.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2015	
01.-06.08.	Blackhat USA 2015 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 23 (DEFCON, Las Vegas/US)
09.-13.08.	15th Annual DFRWS Conference 2015 (DFRWS, Philadelphia/US)
12.-14.08.	24th USENIX Security Symposium (Usenix, Washington D.C./US)
16.-20.08.	Crypto 2015 (IACR, Santa Barbara/US)
31.08.	Sommerakademie (ULD, Kiel)
September 2015	
08.-09.09.	D·A·CH Security (Gemeinsame Arbeitskonferenz GI OCG BITKOM SI TeleTrusT, Sankt Augustin)
15.-17.09.	Future Security 2015 (Fraunhofer VVS, Berlin)
17.09.	3. Deutscher Rechenzentrumstag (proRZ Rechenzentrumsbau GmbH, Freiburg)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
21.-22.09.	OWASP AppSec USA 2015 (OWASP Foundation, San Fransisco/CA)

Fundsache

Am 23.07.2015 veröffentlichte Google die Ergebnisse der Studie *Comparing Expert and Non-Expert Security Practices*. Die Befragung von über 500 Experten und Laien zeigt Aufklärungsbedarf: Während Experten Software-Updates für die wichtigste Maßnahme halten, setzen Laien auf Antivirus-Software – bei Experten nicht unter den fünf wichtigsten.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

August 2015



Das bislang beste Windows?

Was ein unaufgefordert erschienenes hartnäckiges Windows-Symbol wochenlang angekündigt hatte, stand am 29.07.2015 endlich zum Download bereit: Windows 10. Microsoft hat von Apple gelernt: Upgrades verteilen sich einfach besser, wenn sie nichts kosten. Und, man muss es Microsoft lassen, das Upgrade klappt schnell und problemlos. Bei Windows 8 fühlt es sich eher wie ein Update an, bei dem der nervige Metro-Screen abgeschaltet wird.

Nachdem Microsoft sich mit Windows 8 – einer komplett am Bedarf von Windows-Nutzern vorbeigegangenen Entwicklung – eine blutige Nase geholt hatte, sollte nun alles besser werden. Und eigentlich hatte man bisher das Gefühl, Microsoft hätte im Rahmen von Office 365 gelernt, dass – zumindest in Europa und speziell in Deutschland – der Datenschutz ein entscheidendes Kriterium ist.

Die Ernüchterung folgt nach der Installation, denn die nächste Stunde benötigt man dafür, die Datensammelwut – inklusive der Vergabe einer eindeutigen Werbe-ID – in unzähligen Einstellungen zu begrenzen. Vollständig abstellen lässt sie sich nicht. Dass man zur Installation ein Microsoft-Live-Konto benötigt, daran hatten sich Windows 8-Nutzer schon gewöhnt. Man konnte (und kann) anschließend immerhin den Offline-Modus aktivieren. Karl Klammers Nachfolgerin heißt nicht Siri, sondern Cortana und sammelt alles, was sie zu lesen oder hören bekommt.

Überflüssig zu erwähnen, dass ein Aufschrei zur Datensammelwut folgte. In Russland prüft der Generalbundesanwalt bereits Anzeigen. Microsofts Selbstwahrnehmung ist hingegen eine andere – und natürlich ist man unheimlich transparent.

Microsoft scheint das Prinzip „Lernen durch Schmerzen“ fest in seinen Entwicklungsprozessen verankert zu haben. Das bislang beste Windows? Funktional mag das stimmen, dennoch bleibt XP ungeschlagen. Vielleicht lernen sie es ja noch ...



Inhalt

Das bislang beste Windows?

Security News

Websites im Fokus

Automatisierbare Bedrohungen

Experten und Laien

Recht auf Vergessen? Vergiss es...

Kali 2.0

Pseudonyme Nutzung

Secorvo News

Für Kurzentschlossene

Eine kurze Geschichte der Überwachung

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Websites im Fokus

Bereits im Juni haben die Datenschutzaufsichtsbehörden von Hamburg, Bayern und Baden-Württemberg bekanntgegeben, gezielt Webportale auf Datenschutz und Datensicherheit zu prüfen. Derzeit prüfen die Aufsichtsbehörden die Datensicherheit noch auf der Grundlage von § 13 Abs. 4 TMG anhand von Fragebögen.

Nun sind die gesetzlichen Sicherheitspflichten aus dem TMG durch das am 25.07.2015 in Kraft getretene IT-Sicherheitsgesetz verschärft worden. Es ergänzt § 13 TMG um weitere Pflichten: Geschäftsmäßige Anbieter von Telemedien haben nun technisch-organisatorische Maßnahmen zu ergreifen, um unerlaubte Zugriffe auf die genutzten technischen Einrichtungen zu verhindern. Außerdem sind die Angebote gegen Störungen, auch durch Angriffe, und unbefugte Zugriffe auf personenbezogene Daten nach dem Stand der Technik zu schützen. Eine Maßnahme hierzu sollen anerkannte Verschlüsselungsverfahren sein. Bei Verstößen können die Datenschutz-Aufsichtsbehörden Bußgelder von bis zu 50.000 € verhängen.

Bei Vorfällen wie dem Ashley Madison Hack müssen deutsche Anbieter künftig neben allem anderen ein Ordnungswidrigkeitsverfahren wegen unzureichender Sicherheitsmaßnahmen fürchten. Dabei werden sich dokumentierte Sicherheits-Maßnahmen und Sicherheitskonzepte auszahlen. Damit steigt der Druck auf Anbieter, sich systematisch mit Sicherheitsfragen auseinanderzusetzen. Der pauschale Verweis des Gesetzes auf Verschlüsselungstechnik wirkt allerdings ein wenig naiv.

Automatisierbare Bedrohungen

Am 31.07.2015 stellte Colin Watson das OWASP-Projekt „OWASP Automated Threat Handbook v1.00“ vor. Mit diesem Handbook will die Projektgruppe auf relevante, automatisierbare Bedrohungen von Webanwendungen hinweisen, die bisher höchstens am Rande betrachtet wurden. Wir empfehlen dieses Dokument jedem Entwickler, um geeignete Schutzmechanismen gegen solche weniger bekannten Bedrohungen zu implementieren. Entscheidern und Architekten sei zumindest ein Blick in die zweiseitige Zusammenfassung angeraten.

Experten und Laien

Google-Mitarbeiter publizierten am 23.07.2015 die Ergebnisse einer Studie, in der vergleichend untersucht wurde, welche IT-Sicherheitsmaßnahmen 230 befragte Security-Experten für wirksam halten und an welche Maßnahmen 290 interviewte Laien glauben. Von den zahlreichen detaillierten Ergebnissen der Studie überrascht vor allem die Erkenntnis, dass nur der „Umgang mit Passwörtern“ bei beiden Gruppen zu den fünf wirkungsvollsten Sicherheitsmaßnahmen zählt. Während Laien an die Wirksamkeit von Virenschutz glauben, setzen Experten darauf, ihre Systeme auf einem möglichst aktuellen Stand zu halten. Statt eines regelmäßigen Passwort-Wechsels bevorzugen Experten komplexe und einmalige Passwörter, die sicher aufbewahrt werden, oder Mehrfaktorauthentifizierung. Und nur Laien glauben daran, dass man einer Webseite ihre Vertrauenswürdigkeit ansehen kann.

Die Ergebnisse machen deutlich, dass eine verbesserte Aufklärung von Laien über wirksame IT-Sicherheitsmaßnahmen notwendig ist, wenn man nicht immer mehr Jessicas riskieren will.

Recht auf Vergessen? Vergiss es...

Das so genannte „Recht auf Vergessen“, das der Europäische Gerichtshof in seiner Google Spain-Entscheidung vom 13.05.2014 (SSN 5/2014) geprägt hat, bleibt weiter umstritten. Eine Anordnung der französischen Datenschutzaufsichtsbehörde CNIL vom 12.06.2015, beantragte Sperrungen weltweit auf alle Google-Domains zu erstrecken, beantwortete Google am 30.07.2015 in einem Blog-Beitrag: Das durch den EuGH formulierte „Recht auf Vergessen“ sei auf Europa beschränkt. Es sei keinem Land erlaubt, zu bestimmen, was in einem anderen Land zugänglich gemacht werde. Ansonsten drohe das restriktivste nationale Recht weltweit zum Maßstab der Freiheit im Internet zu werden. Dass Google dabei staatliche Zensurbestrebungen und Daten- oder Persönlichkeitsschutz in einen Topf wirft, zeigt deutlich das andauernde Unverständnis für europäisches Recht.

Derweil hat das OLG Hamburg über die Löschpflicht der Anbieter der Ursprungsseiten entschieden. Es bejaht einen Unterlassungs-Anspruch auch gegen den veröffentlichenden Website-Anbieter. Hintergrund war die Berichterstattung über ein eingestelltes Strafverfahren auf der Seite einer Tageszeitung. Da jedoch auch die Pressefreiheit der Beklagten zu berücksichtigen war, beschränkt sich der Anspruch in Fortsetzung der Google Spain-Rechtsprechung darauf, dass der Anbieter die Auffindbarkeit durch Suchmaschinen anhand des Namens verhindert.

Selbst wenn es gelänge, die Rechtsauffassungen dies- und jenseits des Atlantik anzugleichen, zeigt die OLG-Entscheidung, wie stark beim „Recht auf Vergessen“ das Persönlichkeitsrecht mit anderen Rechten wie bspw. der Pressefreiheit kollidieren kann. Das letzte Wort ist bei diesem Thema sicher noch lange nicht gesprochen.

Kali 2.0

Am 11.08.2015 erschien die rundum erneuerte Version 2.0 der *Penetration Testing Destribution Kali Linux*. Seit dem Schritt von Backtrack zu Kali Linux im Jahr 2013 konnte die Distribution ihre Stellung als de facto-Standard für Penetrationstests noch weiter ausbauen. Die neue Version bringt neben etlichen aktualisierten Tools, die das Herz eines jeden Testers höher schlagen lassen, auch einen Linux Kernel der Version 4.0 und diverse grafische Benutzerumgebungen mit.

Ab dieser Version erscheint Kali als Rolling-Release mit ständig aktuellen Paketen auf Basis von Debian Testing. Neben den typischen Plattformen stehen auch Versionen für ARM, die mobile Penetration Testing Plattform Nethunter und spezielle Images für den RaspberryPi 2 bereit. Ein Blick auf die neue Version lohnt also auf jeden Fall.

Pseudonyme Nutzung

Der Streit um die Klarnamenpflicht bei Facebook geht mit einer Anordnung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Prof. Dr. Johannes Caspar, vom 28.07.2015 in eine neue Runde. Darin wird Facebook Ireland Ltd. erneut verpflichtet, die pseudonyme Nutzung seines Dienstes zuzulassen und Sperrungen pseudonymer Accounts aufzuheben. Außerdem wird Facebook untersagt, Ausweiskopien zur Identitätsbestätigung zu verlangen. Anlass ist die Beschwerde einer Nutzerin, die von Facebook zur Angabe ihres echten Namens unter Vorlage einer Personalausweiskopie aufgefordert wurde und deren gesperrtes Profil Facebook gegen ihren Willen auf den Klarnamen umgestellt hatte, allerdings ohne das Profil freizuschalten.

Die Anordnung folgt in den Fußstapfen der im April 2013 durch das OVG Schleswig-Holstein kassierten Anordnung des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein. Caspar beruft sich erneut auf § 13 Abs. 6 TMG und bzgl. des Personalausweises auf § 20 Abs. 2 PAuswG. Durch die Google Spain-Entscheidung des EuGH vom 13.05.2014 (SSN 5/2014) ist das Hauptargument des OVG-Urteils von 2013 jedoch entfallen: Aufgrund der wirtschaftlichen Tätigkeit der in Hamburg niedergelassenen Facebook Germany GmbH kommt nun sehr wohl deutsches Datenschutzrecht zur Anwendung. Die Erfolgsaussichten von Caspers erneuter Anordnung sind damit erheblich gestiegen.

Secorvo News

Für Kurzentschlossene

Nutzen Sie noch im September die Möglichkeit, Ihre Erfahrungen und Kenntnisse zu vertiefen und mit einem Zertifikat zu krönen: Die T.I.S.P.-Schulung (**21.–25.09.2015**) bereitet auf die anschließende T.I.S.P.-Prüfung am 26.09.2015 vor und hilft, durch einen umfassenden Einblick in alle Gebiete der Informationssicherheit verbliebene Wissenslücken zu schließen. Zur Vorbereitung erhalten Sie nach Ihrer Anmeldung das Begleitbuch „Zentrale Bausteine der Informationssicherheit".

Der ständigen Weiterentwicklung des Themas IT-Sicherheit trägt das Seminar IT-Sicherheit heute (**29.09.–01.10.2015**) mit der Behandlung aktueller Fragestellungen Rechnung. Hier erfahren Sie das Wesentliche über die aktuellen Entwicklungen und Bedrohungen und lernen Best Practice-Vorgehensweisen kennen, mit denen Sie Ihr Unternehmen wirksam schützen können.

Alle Termine und das komplette Seminarangebot finden Sie unter www.secorvo.de/college.

Eine kurze Geschichte der Überwachung

Im Rahmen der Ausstellung „Globale Überwachung und Zensur" des ZKM | Zentrum für Kunst und Medientechnologie Karlsruhe geben Prof. Dr. Müller-Quade und Dirk Fox am **08.10.2015 um 18 Uhr** im Vortragssaal des ZKM | Karlsruhe einen Rück- und Ausblick auf die Geschichte und Entwicklung geheimdienstlicher Überwachung. Zur Einstimmung bietet das ZKM | Karlsruhe ab 17 Uhr für interessierte Teilnehmer eine Führung durch die Ausstellung an. Da die Zahl der Plätze beschränkt ist, bitten wir um rechtzeitige Anmeldung.

Führung und Vortragsveranstaltung finden auf Einladung des ZKM | Karlsruhe in Zusammenarbeit mit dem KIT und der Karlsruher IT-Sicherheitsinitiative statt. Sie sind **kostenfrei** – und setzen auch keine Fachkenntnisse voraus. Bringen Sie also gerne interessierte Freunde, Kollegen und Bekannte mit!

Im Anschluss an den Vortrag haben Sie die Möglichkeit, den Abend gemütlich im „mint - bistro.café.bar.catering" im Foyer des ZKM ausklingen zu lassen.



Weitere Informationen und die Möglichkeit zur Anmeldung zur Führung finden Sie auf www.ka-it-si.de. Wir freuen uns auf Ihr Kommen!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2015	
08.-09.09.	D•A•CH Security (Gemeinsame Arbeitskonferenz GI OCG BITKOM SI TeleTrusT, Sankt Augustin)
15.-17.09.	Future Security 2015 (Fraunhofer VVS, Berlin)
17.09.	3. Deutscher Rechenzentrumstag (proRZ Rechenzentrumsbau GmbH, Freiburg)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
21.-22.09.	OWASP AppSec USA 2015 (OWASP Foundation, San Fransisco/CA)
29.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
29.09.-01.10.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen & Schutzmechanismen (Secorvo, Karlsruhe)
Oktober 2015	
06.-08.10.	it-sa 2015 (NürnbergMesse GmbH, Nürnberg)>
12.-16.10.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Denver/USA)
13.-15.10.	15. IDACON 2015 (WEKA-Akademie, München)
13.-16.10.	Java Security (Secorvo, Karlsruhe)

Fundsache

Auf der diesjährigen 23. Konferenz DefCon präsentierten am 08.08.2015 Dan Petro und Oscar Salazar, wie sich die „Smart Safes" Galileo des Herstellers Brink mit einem USB-Stick öffnen lassen. Auch hier hätte die Empfehlung „Schuster, bleib' bei deinem Leisten" geholfen.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick, Kai Jendrian, Michael Knopp, Christoph Schäfer (Editorial).

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2015



Eingebettetes Vertrauen

Kaum ein Gerät, das heute nicht von Software gesteuert wird. Die wenigen verbliebenen rein mechanischen Lösungen (wie batteriefreie Armbanduhren) genießen bereits Kult-Status.

Zwar wissen wir, dass Software fehlerhaft sein kann. Aber Fehler fallen auf: Abweichendes Systemverhalten zeigt sich bei Tests, und bei unspezifischen Fehlern stürzt das System meist ab. Daher ist unser Vertrauen in ursprünglich mechanische, aber zunehmend von Software gesteuerte Geräte meist unbeeinträchtigt geblieben. In der Regel ist das auch vernünftig: Eine Waschmaschine, die zu heiß wäscht, erkennen wir an eingelaufener Wäsche. Eine Uhr, die die falsche Zeit anzeigt, erkennen wir beim Vergleich mit anderen Zeitanzeigen. Und ein Auto, bei dem die Motorsteuerung schwächelt, erkennen wir am Fahrverhalten.

Allerdings gibt es auch Systeme, bei denen Fehler weniger offensichtlich sind und eine Überprüfung schwierig ist. Wie sollten wir die Korrektheit eines Taxameters prüfen? Oder die des Kilometerzählers im Gebrauchtwagen? Und wie sollten wir bei einem Spielautomaten feststellen, dass das Gerät auch die gesetzlich vorgeschriebene Menge an Gewinnausschüttungen einhält? Genau aus diesen Gründen hat das Bundesverfassungsgericht 2009 dem Einsatz von Wahlcomputern bei Bundestagswahlen einen Riegel vorgeschoben.

Üblicherweise werden solche Geräte unabhängig geprüft. Aber wie gut kann eine solche Prüfung sein, deren Umfang weit unter dem einer „Common Criteria"-Zertifizierung liegt? Prüft der Prüfer den Source-Code? Und was ist, wenn Schadcode über die Programmierumgebung in den ausführbaren Code gelangt (siehe diese SSN)?

Die Entwicklung effizienter Verfahren, mit denen die Vertrauenswürdigkeit solcher Systeme sichergestellt und transparent gemacht werden kann, wird eine große Herausforderung der Zukunft sein.



Inhalt

Eingebettetes Vertrauen

Security News

Komplexität killt Sperrbildschirm

Kamera-Attrappen

Passworttipps der Spione

DIN-Norm Löschkonzept

Der Geist im iPhone

Finger in die Wunde

Datenschutzniveau der USA

Secorvo News

Eine kurze Geschichte der Überwachung

Softwaresicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Komplexität killt Sperrbildschirm

Ein YouTube-Video vom 20.09.2015 legte eine gravierende Schwachstelle der neuen Version 9 von Apples iOS offen: Sie ermöglicht es, den Sperrbildschirm zu umgehen und auf Kontakte und Bilder zuzugreifen. Dabei werden lediglich auf dem Sperrbildschirm verfügbare Funktionen wie der Sprachassistent Siri und die eingebaute Uhr verwendet.

Diese Verwundbarkeit reiht sich ein in zahlreiche gleichartige Schwachstellen, beispielsweise für iOS 7, Android 5 oder Windows 8. Die Ursache aller dieser Schwachstellen liegt darin, dass der Sperrbildschirm um immer mehr Funktionen erweitert wird. Wenn man aber erlaubt, dass ausgewählte Aktionen schnell und bequem durchgeführt werden können, ohne das Gerät zu entsperren, so vergrößert man zugleich die Angriffsfläche. Hersteller sollten den Sperrbildschirm nicht weiter als Platz zum Abladen von Apps oder als Schnellstartseite missverstehen, sondern als ein essentielles Sicherheitsfeature, das man besser nicht aufweicht.

Kamera-Attrappen

Nach einer kürzlich veröffentlichten Entscheidung des Landesarbeitsgerichts (LAG) Mecklenburg-Vorpommern vom 12.11.2014 (Az. 3 TaBV 5/14) unterliegt das Anbringen von Kamera-Attrappen im Außenbereich nicht der Mitbestimmung des Betriebsrats. In seiner grammatischen Auslegung des § 87 Abs. 1 Nr. 6 BetrVG stellt das LAG fest, dass eine Attrappe nicht zur Überwachung der Arbeitnehmer geeignet ist. Dass auch die Vorschriften des Bundesdatenschutzgesetzes (BDSG) keine Anwendung finden, hat der Bundesgerichtshof in einem Nachbarschaftsstreit bereits am 16.03.2010 entschieden (Az. VI ZR 176/09). Allerdings bestätigte er gleichzeitig, dass dennoch ein „Überwachungsdruck“ und damit ein Eingriff in das allgemeine Persönlichkeitsrecht vorliegen kann. Folglich kann ein zivilrechtlicher Unterlassungsanspruch gemäß §§ 1004, 823 BGB geltend gemacht und damit die Beseitigung der Kamera-Attrappe verlangt werden.

Anders als Datenschutzaufsichtsbehörden teilweise behaupten sind Attrappen demnach nicht wie echte Kameras zu behandeln. Unzulässig können sie im Einzelfall dennoch sein.

Passworttipps der Spione

Am 08.09.2015 hat der englische Geheimdienst GHCQ Hinweise zum Umgang mit Passwörtern veröffentlicht. Auch wenn man nach den Skandalen um die Geheimdienste einem solchen Dokument erst mal skeptisch gegenüber stehen mag, finden sich dort doch sinnvolle und angemessene, wenn auch nicht sonderlich überraschende Hinweise zum Umgang mit Passwörtern – gut dargestellt auf 13 Seiten. Anscheinend beschäftigen sich einige Mitarbeiter des GHCQ auch mit für die Sicherheit wertvollen Tätigkeiten.

DIN-Norm Löschkonzept

Der zuständige Arbeitskreis des DIN verabschiedete am 10.09.2015 eine weiterentwickelte Fassung der Leitlinie Löschkonzept als DIN-Norm 66398 – passend zur DIN 66399, die die Vernichtung von Datenträgern regelt. Seit Ende 2013 hatten die Deutsche Bahn, DATEV, Blancco, Secorvo und Toll Collect an diesem Projekt gearbeitet (siehe SSN 2/2014 und SSN 1/2015). Die neue DIN 66398 hilft bei der Entwicklung passender Löschkonzepte, insbesondere für personenbezogene Daten. Sie beschreibt die Elemente eines Löschkonzepts und stellt dar, wie mit Hilfe von Löschklassen Löschregeln für unterschiedliche Datenarten festgelegt werden können. Die Norm wird voraussichtlich Ende November im Beuth-Verlag erscheinen; eine englische Übersetzung ist geplant.

Für den Datenschutz ist die neue Norm ein großer Gewinn: Sie kann helfen, das Vollzugsdefizit beim Löschen personenbezogener Daten abzubauen.

Der Geist im iPhone

Am 20.09.2015 gestand die Firma Apple einen erfolgreichen Angriff auf den Appstore ein. Eine bisher unbekannte Anzahl von Apps (FireEye spricht von über 4000) ist durch Verwendung einer modifizierten XCode-Entwicklungsumgebung mit Schadsoftware infiziert worden. Apple arbeitet an der Bereinigung. Der Vorfall zeigt, dass selbst ein stark reguliertes Anwendungsökosystem anfällig für Angriffe sein kann. Dass modifizierte Compiler ein Sicherheitsproblem sein können, hat Ken Thompson schon 1984 in seinem berühmten Artikel „Reflections on Trusting Trust“ angesprochen. Sollten Software-Entwicklungswerkzeuge zum Einfallstor für Schadsoftware werden, wird dies die Entwicklung sicherer Software vor ganz neue Herausforderungen stellen.

Finger in die Wunde

Die Auftragsdatenverarbeitung (ADV) ist eines der wichtigsten Instrumente des Datenschutzes, wenn es um das Outsourcing der Verarbeitung personenbezogener Daten geht. Braucht man hierfür normalerweise einen Erlaubnistatbestand, ermöglicht es die gesetzliche Fiktion der ADV, diese durch einen Vertrag zu ersetzen. Dadurch wird der Auftragnehmer datenschutzrechtlich zum Teil des Auftrag-

gebers (verantwortliche Stelle), sodass keine – erlaubnispflichtige – Datenübermittlung an einen Dritten vorliegt.

Mit einer Pressemitteilung vom 20.08.2015 und einem Bußgeldbescheid in fünfstelliger Höhe legte das Bayerisches Landesamt für Datenschutzaufsicht (BayLDA) den Finger tief in die Wunde der praktischen Umsetzung: Oft machen es sich Auftraggeber allzu leicht und verwenden ADV-Vertragsmuster aus dem Internet, ohne dass diese auf den konkreten Fall angepasst werden. So sollte man beispielsweise mit einem Aktenvernichtungsunternehmen keine Rückgabe der Datenträger nach Erfüllung des Auftrags vereinbaren.

Insbesondere mangelt es häufig an konkret vereinbarten technischen und organisatorischen (Sicherheits-) Maßnahmen (TOM) – stattdessen werden nur allgemeine Floskeln angeführt oder eine Ankreuz-Liste beigefügt, die meist nur geringe Aussagekraft besitzt. Eine individuelle Vereinbarung und Prüfung der Auftragnehmer ist aber unumgänglich, um als Auftraggeber den gesetzlichen Aufsichts- und Kontrollpflichten zu genügen.

Datenschutzniveau der USA

Wir erinnern uns: Der österreichische Datenschutz-Aktivist Max Schrems hatte gegen die irische Datenschutzaufsichtsbehörde wegen der Speicherung der Daten europäischer Facebook-Nutzer in den USA und die damit einhergehende Überwachung durch US-Behörden vor dem irischen High Court geklagt. Dieser hatte unter Berufung auf die Safe Harbor-Entscheidung der EU-Kommission die Prüfung der Beschwerde abgelehnt. Im daraufhin von Max Schrems eingeleiteten Verfahren gegen den irischen Data Protection Commissioner hat der EuGH nun nach Ansicht des Generalanwalts zu prüfen, ob die Kommissionsentscheidung die nationalen Aufsichtsbehörden an eigenen Maßnahmen und Prüfungen hindert und ob unter Anwendung der Safe-Harbor-Grundsätze von einem angemessenen Datenschutzniveau in den USA ausgegangen werden kann. Angesichts der nicht bestrittenen massiven und nicht zielgerichteten Überwachungspraxis sowie des fehlenden gerichtlichen Rechtsschutzes wird letzteres von Generalanwalt Bot in seinen Schlussanträgen vom 23.09.2015 verneint.

Folgt man dieser Begründung steht jedoch nicht nur das Safe-Harbor-Abkommen auf dem Prüfstand, sondern indirekt auch die Wirksamkeit der Standardvertragsklauseln. Denn die staatliche Überwachungspraxis kann auch durch diese nicht ausgeschlossen werden. Bezogen auf deutsche Unternehmen wäre die Folge, dass Datenübermittlungen in die USA nur noch mit Genehmigung der Aufsichtsbehörden, mit Einwilligung des Betroffenen oder in den Ausnahmefällen aus § 4c Abs. 1 BDSG zulässig blieben. Für die betroffenen Unternehmen würde das zu gravierenden Problemen führen, da ein Großteil der Datenverarbeitungen mit US-Unternehmen faktisch rechtswidrig wären.

Secorvo News

Eine kurze Geschichte der Überwachung

Im Rahmen der Ausstellung GLOBAL CONTROL AND CENSORSHIP. Weltweite Überwachung und Zensur des ZKM | Zentrum für Kunst und Medientechnologie Karlsruhe geben Prof. Dr. Müller-Quade (Karlsruher Institut für Technologie) und Dirk Fox (Secorvo) am **08.10.2015** um **18 Uhr** im Vortragssaal des ZKM | Karlsruhe einen Rück- und Ausblick auf die Geschichte und Entwicklung geheimdienstlicher Überwachung.

Zur Einstimmung bietet das ZKM | Karlsruhe ab 17 Uhr für interessierte Teilnehmer eine Führung durch die Ausstellung an. Da die Zahl der Plätze beschränkt ist, bitten wir um rechtzeitige Anmeldung zur Führung – eine Anmeldung zur Veranstaltung ist nicht erforderlich. Führung und Vortragsveranstaltung finden auf Einladung des ZKM Karlsruhe in Zusammenarbeit mit dem KIT und der KA-IT-Si statt. Sie sind kostenfrei und setzen auch keine Fachkenntnisse voraus. Bringen Sie also gerne interessierte Freunde, Kollegen und Bekannte mit!

Im Anschluss an den Vortrag haben Sie die Möglichkeit, den Abend gemütlich im „mint – bistro.café.bar.catering“ im Foyer des ZKM ausklingen zu lassen.

Softwaresicherheit

Sicherheitsrelevante Schwachstellen in Software lassen sich durch systematisches Vorgehen bei der Softwareentwicklung vermeiden. Mit zwei Seminaren führen wir in die Sichere Softwareentwicklung (CPSSE, **16.–19.11.2015**) und das System Security Engineering (T.E.S.S., **09.–11.11.2015**) ein und bieten Ihnen anschließend die Möglichkeit, sich als *Certified Professional for Secure Software Engineering* (CPSSE) bzw. als *TeleTrusT Engineer for System Security* (T.E.S.S.) zu zertifizieren.

Alle weiteren Seminarangebote und den Seminarkalender für 2016 finden Sie jetzt auf unserer Webseite.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2015	
06.-08.10.	it-sa 2015 (NürnbergMesse GmbH, Nürnberg)
08.10.	Eine kurze Geschichte der Überwachung (KA-IT-Si, Karlsruhe)
12.-16.10.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Denver/USA)
13.-15.10.	15. IDACON 2015 (WEKA-Akademie, München)
20.-23.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
21.10.	Swiss Cyber Storm 6 (Swiss Cyber Storm Association)
November 2015	
02.-03.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
10.-11.11.	ISSE 2015 (TeleTrusT e.V./eema, Berlin)
10.-13.11.	T.E.S.S. - Sichere Systeme dank System Security Engineering (Secorvo, Karlsruhe)
10.-13.11.	Blackhat Europe 2015 (Blackhat, Amsterdam/NL)
16.-19.11.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
23.-27.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)

Fundsache

Das BSI hat eine FAQ zum IT-Sicherheitsgesetz veröffentlicht, in der der Geltungsbereich des Gesetzes präzisiert und die Verpflichtungen der betroffenen Unternehmen zusammengefasst werden.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Oktober 2015



Datenschutzdomino

Elf Jahre lang, von 1998 bis 2009, fand jährlich der Domino-Day statt. Seine Spannung bezog er aus der Ungewissheit, wie viele Steine der erste Stein zum Fallen bringen würde.

Dieselbe Spannung befällt nun Unternehmen und Datenschützer angesichts des Realitäts-checks für Safe Harbor durch den EuGH. Allein bewirkt dieser erste gefallene Stein wenig, stehen doch u. a. mit Standardvertrags-klauseln und Corporate Binding Rules noch andere Wege für die rechtskonforme Übermittlung personen-bezogener Daten an US-Unternehmen bereit.

Doch die nächsten Steine wackeln. Die im Urteil festgestellten Schutzlücken gegenüber staatlicher Datenerhebung können auch Standardvertragsklauseln nicht beheben. Selbst die Einwilligung des Betroffenen wird, mangels Transparenz, als unwirksam angesehen. Solche Defizite sind nicht auf die USA beschränkt – die Urteilsfolgen werden es langfristig auch nicht sein. Andere Bausteine wie die Auf-tragsdatenverarbeitung bspw. im Konzern oder in der Cloud könnten bei konsequenter vergleichbarer Spruchpraxis wanken – hier hat der Auftraggeber häufig weder die Weisungshoheit noch effektive Kontrollmöglichkeiten.

Das Datenschutzrecht hat ein Problem mit der Schutzgewährleistung bei der kooperativen, vor allem internationalen Datenverarbeitung. Instrumente wie Safe Harbor versprachen Rechtssicherheit; die reale Umsetzung des europäischen Datenschutzes war jedoch schon lange und erkennbar reine Fiktion. Da kann auch ein auf die Schnelle verabschiedetes US-Gesetz nicht helfen.

Informationelle Selbstbestimmung durch Isolation der Daten in der EU ist unrealistisch. Laissez faire allerdings auch keine Lösung.

Beim Domino Day entstanden aus den umgefallenen Steinen neue Bilder. Genauso braucht das Datenschutzrecht neue Instrumente, die einen effektiven Schutz personenbezogener Daten nicht untergraben.



Inhalt

Datenschutzdomino

Security News

Chrome will weniger verwirren

Still und Heimlich

DANE ist RFC 7672

Audit Fails

Threat Modelling Tool 2016

Secorvo News

Ritterschlag

T.I.S.P., CPSSE und mehr...

Globale Überwachung

Eat, Sleep, Pwn, Repeat

Veranstaltungshinweise

secorvo
security consulting

Security News

Chrome will weniger verwirren

Am 13.10.2015 hat Google in einem Blogpost angekündigt, mit Wechsel von der Version 45 auf 46 die Darstellung von HTTPS-Verbindungen in Chrome, die die Überprüfung nicht vollständig bestehen, zu vereinfachen. Das bisherige gelbe Symbol, mit dem auf kleinere Probleme bei einer HTTPS-Verbindung hingewiesen wurde, fällt weg. Dieser Status wird zukünftig mit dem Status „HTTP“ gleichgesetzt. Dadurch reduziert Google die Anzeige auf drei Status.

Das ist aus unserer Sicht ein begrüßenswerter Ansatz, denn bisher konnte die Vermutung aufkommen, dass HTTPS mit kleineren Problemen (gelb) unsicherer sei als reines HTTP (keine Farbe). Für Benutzer ist es schon schwierig genug, HTTPS zu verstehen – daher ist jeder Gewinn an Klarheit bei der Darstellung ein Gewinn für die Sicherheit.

Still und Heimlich

Mit dem eilig verabschiedeten neuen Gesetz zur Vorratsdatenspeicherung – offiziell Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten – ist, kaum wahrgenommen, auch ein neuer Straftatbestand der „Datenhehlerei“ im Strafrecht (§ 202d StGB) eingeführt worden.

Danach soll bestraft werden, wer sich oder Dritten Daten verschafft, verbreitet oder zugänglich macht, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat. Ausgenommen sind lediglich Handlungen, die ausschließlich der Erfüllung beruflicher Pflichten dienen. Laut Entwurfsbegründung sollen so Lücken im Schutz vor dem Handel mit illegal erlangten Daten geschlossen werden.

Befürchtet wird jedoch, dass der Tatbestand auch Whistleblower oder Blogger erfasst, die Informationen veröffentlichen, ohne deren illegale Beschaffung ausschließen zu können. Die subjektiven Voraussetzungen schränken den Straftatbestand jedoch ein, denn es muss eine Bereicherungs- oder Schädigungsabsicht vorliegen. Journalisten sind nur dann ausgenommen, wenn ihr Status anerkannt wird – das dürfte mindestens zu Verunsicherung führen. Dabei drängt sich tatsächlich der Eindruck auf, dies könnte angesichts zahlreicher Leaks das primäre Ziel der Regelung sein.

DANE ist RFC 7672

Mit der Standardisierung von DANE for SMTP als RFC 7672 hat die Internet Engineering Task Force (IETF) im vergleichsweise kurzen Zeitraum von nur zwei Jahren einen neuen Standard für den sicheren E-Mail-Transport geschaffen. Auch das BSI fordert mittlerweile in seiner technischen Richtlinie Sicherer E-Mail-Transport den Einsatz von DANE.

Im Gegensatz zur Ende-zu-Ende-Verschlüsselung (wie S/MIME oder PGP) zielt DANE darauf ab, einen sicheren Transport zwischen den Mailservern mittels SSL/TLS zu gewährleisten. Hierzu publizieren die E-Mail-Server einen über DNSSEC gesicherten Eintrag mit dem Fingerprint ihres X.509 Zertifikats. Der sendende E-Mail-Server kann diesen Fingerprint zum Schutz vor manipulierten Zertifikaten beim Verbindungsaufbau prüfen.

Der schnellen Verbreitung von DANE steht derzeit noch entgegen, dass alle beteiligten E-Mail-Server für DANE konfiguriert sein müssen und das noch nicht sehr weit verbreitete DNSSEC-Protokoll benötigen.

Audit Fails

Am 07.10.2015 veröffentlichte Guido Vranken gleich acht Schwachstellen, die er bei seiner Analyse des Quellcodes der freien SSL/TLS Bibliothek ARM mbed TLS / PolarSSL gefunden hatte. Damit lässt sich PolarSSL teilweise sogar über das Netzwerk angreifen. Die Ursache sind überwiegend Buffer-Overflows auf Stack und Heap – typische Fehler der 90er Jahre des vergangenen Jahrhunderts. Pikant wird diese Entdeckung vor dem Hintergrund, dass PolarSSL im Auftrag des niederländischen Geheimdienstes AIVD durch die Firma Fox-IT einem Code-Audit unterzogen wurde, bei dem diese Schwachstellen nicht gefunden wurden.

Der Fall weist eine gewisse Ähnlichkeit zu Truecrypt auf: Forscher des Google-Projekts Zero veröffentlichten am 18.09.2015 eine kritische Schwachstelle von Truecrypt (Incorrect Impersonation Token Handling EoP), die bei der Prüfung im Rahmen des Open Crypto Audit Project (siehe SSN 04/2015) offenbar nicht aufgefallen war. Ein Fehler im Truecrypt-Treiber ermöglicht den unberechtigten Zugriff auf Truecrypt-Container anderer Nutzer auf derselben Maschine. Auch wenn die Schwachstelle nur unter bestimmten Voraussetzungen ausgenutzt werden kann, ist ein Umstieg auf Alternativen wie den Truecrypt-Nachfolger Veracrypt (Fehler gefixt) oder Ciphershed zu empfehlen.

Auch ein Code-Audit ist keine Garantie für die Abwesenheit von Schwachstellen. Denn erstens kann aufgrund der Komplexität heutiger Anwendungen meistens nur ein Teil intensiv durchleuchtet werden; das sollte von den Auditoren sauber dokumentiert werden. Und zweitens ist trotz der

Unterstützung durch ausgefeilte Tools am Ende immer der Auditor gefragt. Dabei kann leicht der eine oder andere kleine Fehler übersehen werden – mit fatalen Folgen für die Sicherheit des Produkts.

Threat Modelling Tool 2016

Am 07.10.2015 hat Microsoft eine verbesserte Version des Microsoft Threat Modelling Tool angekündigt. Das Tool hat sich in der Praxis für die Erstellung von Bedrohungsmodellen bewährt, hatte aber bisher einige Schwächen bei der Anpassung der Vorlagen für Modelle. Wir begrüßen es sehr, dass Microsoft sich genau dieser Punkte angenommen hat und mit der neuen Version einen Template-Editor liefert, auf den wir sehr gespannt sind. Bedrohungsmodelle sind ein wichtiger Teil von Sicherheitsanalysen. Nach unserer Erfahrung lohnt es, das (kostenlose) Werkzeug für die Durchführung von Bedrohungsanalysen in Betracht zu ziehen.

Secorvo News

Ritterschlag

Mit der zunehmenden Sensibilität für IT-Sicherheit wachsen Penetrationstester wie Pilze aus dem Boden. Wenn ein Penetrationstest keine relevanten Schwachstellen findet, liegt das daher manchmal nicht nur an der Absicherung.

Mit dem Zertifikat „Offensive Security Certified Professional“ (OSCP) haben die Urheber von Kali-Linux und der Exploit-DB vor knapp fünf Jahren eine Qualifikation für Pentester geschaffen, die es in sich hat: Nach intensiven Live-Hacking-Lektionen über mehrere Monate (von der Informationssammlung über die Nutzung von Exploit-Code bis zur Übernahme von Windows-Domänen) folgt eine praktische Prüfung, in der die Kandidaten innerhalb von 24 Stunden in einer Laborumgebung ein vorgegebenes Hacking-Ziel erreichen und anschließend dokumentieren müssen.

Im Oktober haben **Dr. Safuat Hamdy** und **André Domnick** diese derzeit anerkannteste Pentester-Zertifizierung bestanden – ein Ritterschlag.

T.I.S.P., CPSSE und mehr...

Zwei Gelegenheiten zur Zertifizierung Ihrer Qualifikation bietet Secorvo College noch in diesem Jahr: Ein CPSSE- (**16.–19.11.2015**) und ein T.I.S.P.-Seminar (**23.–27.11.2015**) mit anschließender Zertifikatsprüfung.

Im kommenden Jahr bieten wir wieder zahlreiche interessante und lehrreiche Schulungen an. Neu im Programm ist der D'Day – Datenschutz Deep Impact, der sich an Datenschutzbeauftrage richtet: Ausgewähltes aktuelles Erfahrungswissen, konzentriert an einem Tag. Die erste Gelegenheit für eine Teilnahme bietet sich am **25.02.2016**.

Den Schwerpunkt Sichere Software- und Systementwicklung haben wir ausgebaut. Mit den Seminaren Java Security und Secure Coding C/C++ vertiefen wir die Sicherheitsaspekte von der Projektierung bis zum Coding. Das Seminar spricht nicht nur Entwickler, sondern alle Beteiligte im Lifecycle der Softwareentwicklung an.

Auch die Zertifikatsseminare T.I.S.P., T.E.S.S. und CPSSE bieten wir im kommenden Jahr zu mehreren Gelegenheiten an, ebenso das Seminar IT-Sicherheit heute – praxisnah, zielsicher, kompakt mit den neuesten Entwicklungen in Informationssicherheit und Datenschutz. Am **26.–28.01.2016** können Sie sich auf den neusten Stand bringen lassen.

Globale Überwachung

Beim KA-IT-Si-Event „Eine kurze Geschichte der Überwachung“ am 08.10.2015 füllten knapp 200 Teilnehmer das Medientheater des ZKM | Karlsruhe. Den ersten 80 angemeldeten Teilnehmern konnten wir eine Sonderführung durch die sehr empfehlenswerte Ausstellung "GLOBALE: GLOBAL CONTROL AND CENSORSHIP. Weltweite Überwachung und Zensur" anbieten. Zahlreiche Exponate bieten einen interessanten Einblick in digitale Überwachung und Zensur, wie beispielsweise ein Live-Ticker der aktuell in China gesperrten Websites, eine Visualisierung aller gerade eingeschalteten Smartphones im ZKM (und der von diesen gesuchten WLANs) und eine Wand voller „Überwachungsmonitore“, die Live-Bilder von im Internet frei erreichbaren Webcams zeigen. Die Ausstellung kann noch **bis zum 01.05.2016** besucht werden. (Museums-) Eintritt: 10 €; freitags von 14-18 Uhr ist der Eintritt frei.

Eat, Sleep, Pwn, Repeat

Sicherheitslücken in Protokollen, Systemen und Anwendungen sind die zentrale Ursache erfolgreicher Angriffe auf moderne IT-Systeme. Dennoch gibt es nur wenige Möglichkeiten, tiefergehendes Wissen in diesem Bereich zu erlernen. Capture-The-Flag-Wettbewerbe (CTF) bieten dafür einen spielerischen Rahmen. Dabei treten über den Zeitraum eines Wochenendes mehrere Teams gegeneinander an und lösen anspruchsvolle Aufgaben aus den Bereichen Binary Exploitation, Kryptologie, Reverse Engineering, Web-Sicherheit und Forensik.

Beim nächsten KA-IT-Si-Event am **03.12.2015, 18 Uhr** berichten **Samuel Groß** und **Niklas Baumstark** (KITCTF Team) von ihren Erfahrungen und stellen ausgewählte Beispiele von Aufgaben aus CTFs vor (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2015	
02.-03.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
10.-13.11.	T.E.S.S. – Sichere Systeme dank System Security Engineering (Secorvo, Karlsruhe)
10.-11.11.	ISSE 2015 (TeleTrust e.V./eema, Berlin)
10.-13.11.	Blackhat Europe 2015 (Blackhat, Amsterdam/NL)
12.-13.11.	Smart Energy 2015 (Fachhochschule Dortmund)
16.-19.11.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
17.-20.11.	DeepSec ISDC 2015 (DeepSec GmbH, Wien/AT)
19.-20.11.	39. Datenschutzfachtagung (DAFTA) (GDD, Köln)
23.-27.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
24.-25.11.	3. DFN-Konferenz "Datenschutz" (DFN-Cert Services GmbH, Hamburg)
25.-26.11.	Die Zukunft der IT im Digital Business (Management Circle AG, München)
30.11.-01.12.	IsSec/ZertiFA 2015 (COMPUTAS Gisela Geuhs GmbH, Berlin)
Dezember 2015	
03.12.	Eat, Sleep, Pwn, Repeat, (KA-IT-Si, Karlsruhe)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp (Editorial).

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

November 2015



Geschäftsmodell Ohnmacht

Wir wissen: So genannte „Soziale“ Netzwerke und Kommunikationsdienste sammeln zu viele Nutzerdaten, in den meisten Fällen ohne (europäische) Rechtsgrundlage und damit rechtswidrig. Jetzt wissen wir auch, dass alle deutschen Verbraucher es wissen: In einer Ende Oktober veröffentlichten Emnid-Studie im Auftrag des Bundesverbands der Verbraucherzentralen (vzbv) haben dieser Aussage 84% der Befragten beigepflichtet. Und sie machen sich Sorgen – 63% weil sie nicht wissen, wer ihre persönlichen Daten nutzt. Allerdings glauben 75% der Befragten, dass ein „vorsichtiger Umgang mit persönlichen Daten“ wirkungsvoll schützt: Wer sich eingehender mit dem Thema beschäftigt wird wohl eher zu den 22% gehören, die „Aufpassen“ für wirkungslos halten.

Immer mehr Menschen sind jedoch skeptisch, dass Maßnahmen zur Eindämmung der Datensammelei fruchten: So wären 51% (!) aller Befragten bereit, für Datenschutz und Werbefreiheit im Internet zu bezahlen – vor zwei Jahren lag deren Anteil erst bei 35%. Und das nicht zu knapp: 54% dieser Personengruppe ist Datenschutz bis zu 5 € im Monat wert, ein Drittel würde eine noch höhere Gebühr akzeptieren.

Das klingt nach einem viel versprechenden Geschäftsmodell: Daten sammeln, um sich anschließend das selektive Löschen vergolden zu lassen. Das Modell lässt sich verallgemeinern: Wie wäre es mit einem monatlichen Entgelt an Einbrecher, damit sie die Wohnung unangetastet lassen (Art. 13 GG)? Oder einer Gebühr, damit die Polizei öffentliche Versammlungen zulässt (Art. 8 GG)? Denkbar wäre auch, die Gleichheit vor dem Gesetz durch eine monatliche Gerichtsabgabe sicherzustellen (Art. 3 GG).

Warum also nicht gleich eine monatliche Menschenrechts-Abgabe? Klingt verrückt? Jedenfalls nicht für die Verbraucher, wenn es um die freie Entfaltung der Persönlichkeit geht (Art. 2 GG). So weit kann Ohnmacht den Menschen bringen.



Inhalt

Geschäftsmodell Ohnmacht

Security News

Bad Barcode

Zweckbindung der Meldebehörde

OWASP ASVS 3.0

Secure Messaging reloaded

Deserialisierung

Einer geht noch ...

Nmap 7 wird volljährig

Secorvo News

Hacking pur

Seminare 2016

24 Tage, 24 Krypto-Rätsel

Veranstaltungshinweise

Security News

Bad Barcode

Der am 11.11.2015 von Hyperchem Ma auf der PacSec in Tokyo vorgestellte Angriff mit dem griffigen Namen BadBarcode zeigt, wie verbreitet Designfehler beim Umgang mit Benutzereingaben auch bei etablierten Funktionen sind. Der Angriff nutzt aus, dass viele Barcode-Leser als Tastatur (HID) via USB angebunden sind und auch nicht als ASCII darstellbare Steuerzeichen ungefiltert als Tastaturangaben an das System weiterleiten. Da das Betriebssystem nicht zwischen einer Tastatur und einem solchen HID-Barcode-Scanner unterscheiden kann, kann ein Angreifer via Barcode eine Kommandozeile im Kontext des Benutzers öffnen und beliebige Befehle ausführen. Den Forschern gelang es mittels eines präparierten Amazon Kindle derartige Angriffe auch automatisiert durchzuführen. Aufgrund der weiten Verbreitung von Barcode-Scannern (Kassensystem, Hochregallager etc.) sind die konkreten Auswirkungen dieser Design-Schwachstelle schwer abzusehen - und vor allem schwer zu verhindern.

Zweckbindung der Meldebehörde

Am 01.11.2015 trat das bereits am 03.05.2013 beschlossene Bundesmeldegesetz (BMG) in Kraft, das die Landesmeldegesetze ersetzt. Datenschutzrechtlich relevante Änderungen ergeben sich vor allem für die gewerbliche Nutzung und Auskünfte zum Zweck der Werbung und des Adresshandels (§ 44 BMG). So sind Auskünfte nur noch möglich, wenn der Betroffene generell gegenüber der Meldebehörde oder gegenüber dem Anfragenden eingewilligt hat. Eine Prüfung müssen die Meldebehörden immerhin stichprobenartig durchführen. Gegenüber der bisherigen Widerspruchslösung hat sich damit die Position der Betroffenen aus Datenschutzsicht verbessert. Bemerkenswert ist, dass das BMG auf strenge Zweckbindung setzt: Der Zweck ist bei Auskunftsverlangen zu benennen und nach Zweckerreichung sind die Daten zu löschen. Verletzungen der Zweckbindung werden als Ordnungswidrigkeit mit Geldbußen bis zu 50.000 € sanktioniert.

OWASP ASVS 3.0

OWASP veröffentlichte am 09.10.2015 den Application Security Verification Standard (ASVS) in der Version 3.0. Der ASVS ist eine Sammlung von Anforderungen zur systematischen Prüfung der Sicherheitsmaßnahmen in Webanwendungen. In der Praxis hat sich dieser Standard sowohl als Grundlage für Audits als auch für die Ausgestaltung von Sicherheitsmechanismen in Anwendungen bewährt. In der neuen Version wurden Anforderungen an die Konfiguration und Web-Services ergänzt. Neben weiteren Aufräumarbeiten erhielt der Standard Verweise auf passende Cheat Sheets, die Hilfestellungen bei der Umsetzung bieten. Wir empfehlen den Standard wärmstens allen Prüfern und Entwicklern von Webanwendungen.

Secure Messaging reloaded

Zwar werben Dienste wie iMessage oder WhatsApp mit (teilweiser) Absicherung durch Verschlüsselung – letztlich muss man bei beiden Diensten aber dem Betreiber vertrauen, da es sich nicht um eine Ende-zu-Ende-Verschlüsselung handelt.

Messenger mit echter Ende-zu-Ende-Verschlüsselung sind Threema, Signal und Jabber mit OTR. In einem am 02.11.2015 veröffentlichten Auditbericht hat die Schweizer Security AG die Sicherheitsfunktionen von Threema für gut befunden; Threema dokumentiert seine Sicherheitsmechanismen in einem detaillierten Whitepaper und beschreibt, wie man die Verschlüsselung validieren kann. Am selben Tag hat Open Whisper Systems die Veröffentlichung seiner quelloffenen Lösung für Android verkündet, die schon länger für iOS verfügbar ist. Und schon am 05.11.2014 haben Sicherheitsexperten der Ruhr Universität Bochum das Ergebnis ihrer Untersuchung der Sicherheit von TextSecure publiziert, dem Vorgänger von Signal. Eine Alternative zu Messengern mit Store-and-Forward ist Jabber mit dem Off-the-Record-Protokoll (OTR).

Deserialisierung

Am 06.11.2015 sorgte eine Zero-Day-Schwachstelle in der verbreiteten Java-Bibiothek Commons Collections für Schlagzeilen: Viele Server (z. B. WebLogic, WebSphere, JBoss und Jenkins) sind von ihr betroffen. Die Lücke und das Werkzeug „ysoserial" zu ihrer Ausnutzung wurden bereits Ende Januar 2015 auf der OWASP AppSec Konferenz vorgestellt.

Ursache der Schwachstelle ist die ungesicherte Verwendung der Java-Deserialisierung – ein Problem, das nicht spezifisch für Java ist: Für die Kommunikation mit Java-Anwendungen werden Objekte als Bytefolge abgespeichert und übertragen, die ein Angreifer modifizieren kann – indem er beispielsweise ausführbaren Code hinzufügt. Ein Empfänger (im Fall der Bibliothek Commons Collections ein Server), der die Bytefolge nicht sorgfältig überprüft, generiert bei der Deserialisierung Java-Objekte, bei denen es im schlimmsten Fall zur Ausführung des vom Angreifer eingespielten Programmcodes kommt.

Das Apache Commons Team arbeitet daran, die Deserialisierung mit der verwundbaren Klasse

InvokerTransformer zu unterbinden. Die Hersteller Oracle, Red Hat und Jenkins haben Patches angekündigt bzw. Workarounds bereitgestellt. Bis zur Verfügbarkeit der Patches sollten Administratoren die Klasse *InvokerTransformer* manuell aus allen commons-collections-Jar-Files entfernen.

Einer geht noch …

Spätestens seit dem EuGH-Urteil zu Safe Harbor vom 06.10.2015 sind gesetzlich angeordnete oder erlaubte Weitergaben personenbezogener Daten ohne ausreichende Transparenz und Rechtsschutz in den USA konfliktgeladen. Mit dem Cybersecurity Information Sharing Act of 2015 (CISA) befindet sich nun ein weiteres US-Gesetz in der Endphase des Gesetzgebungsprozesses, das Unternehmen die Weitergabe von personenbezogenen Daten zum Austausch über IT-Security-Bedrohungen gestattet.

Das Gesetz verpflichtet die Sicherheitsbehörden, Berichte und Strategien z. B. für kritische Infrastrukturen oder den Gesundheitssektor zu erstellen und Unternehmen zur Verfügung zu stellen. Die entscheidenden Art. 104, 105 regeln, sehr unbestimmt, die Erlaubnis zum Informationsaustausch zwischen Unternehmen. Die auszutauschenden „Cyber threat indicators" dürfen ausdrücklich auch personenbezogene Daten enthalten. Richtlinien für den Umgang mit diesen Daten sollen erst nach Beschluss des Gesetzes festgelegt werden.

Auch wenn die Ziele legitim sind, Privacy behandelt und sogar eine Art Zweckbindung geregelt wird: Für ein angemessenes Datenschutzniveau fehlen weiter die Transparenz für Betroffene und der Rechtsschutz. Zudem wird auch diese Erlaubnis über vertraglichen Einschränkungen des Datenumgangs mit europäischen Datenexporteuren stehen.

Nmap 7 wird volljährig

Am 19.11.2015 wurde Nmap 7 veröffentlicht – dreieinhalb Jahre nach dem letzten Release und mehr als 18 Jahre seit der ersten Version. Die Verbesserungen betreffen vor allem die Erweiterung der Skript-Bibliothek: Hier wurden u. a. viele Schwachstellen-Scans, Skripte für Webanwendungen und SSL/TLS sowie für eine detaillierte Informationsbeschaffung ergänzt. Außerdem gibt es Verbesserungen bei der IPv6-Unterstützung und bei der Performanz; auch die Datenbank zur System- und Diensterkennung ist kräftig gewachsen.

Mittlerweile ist Nmap 7 auch als Paket für viele Betriebssystem-Distributionen verfügbar, so dass es unmittelbar genutzt werden kann.

Secorvo News

Hacking pur

Auf dem KA-IT-Si-Event „Eat, Sleep, Pwn, Repeat" am **03.12.2015** im Fraunhofer IOSB berichten Samuel Groß und Niklas Baumstark (KITCTF) von ihren Erfahrungen aus Capture-The-Flag-Wettbewerben (CTF). Dabei treten mehrere Teams über ein Wochenende gegeneinander an und müssen anspruchsvolle Aufgaben aus den Bereichen Binary Exploitation, Kryptologie, Reverse Engineering, Web-Sicherheit und Forensik lösen.

Nach dem Vortrag gibt es – wie immer – die Gelegenheit zum „Buffet-Networking". Anmeldung unter www.ka-it-si.de.

Seminare 2016

Gleich zum Jahresanfang bietet Secorvo College zwei spannende Veranstaltungen: Aktuelle Entwicklungen und Fragestellungen in der Informationssicherheit beleuchtet das Dreitagesseminar IT-Sicherheit heute (**26.–28.01.2016**). Die Veranstaltung D'Day – Datenschutz Deep Impact vertieft am **25.02.2016** ausgewählte und aktuelle Themen des Datenschutzes. Das nächste T.I.S.P.-Seminar findet vom **29.02.** bis **04.03.2016** statt. Details und weitere Seminare finden Sie auf unserer Webseite.



24 Tage, 24 Krypto-Rätsel

Um Schülerinnen und Schüler spielerisch an die Kryptologie heranzuführen, startet die KA-IT-Si dieses Jahr gemeinsam mit der Pädagogische Hochschule Karlsruhe das Adventsrätsel „Krypto im Advent". Daran können Schülerinnen und Schüler der Klassen 3 bis 7 teilnehmen; den Siegern winken zahlreiche Sachpreise. Auch ältere Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2015	
03.12.	Eat, Sleep, Pwn, Repeat (KA-IT-Si, Karlsruhe)
Januar 2016	
15.-17.01.	ShmooCon 2016 (The Shmoo Group, Washington/US)
19.-21.01.	Omnicard 2016 (in TIME berlin, Berlin)
26.-28.01.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
Februar 2016	
09.-10.02.	23. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
17.-18.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)>
25.02.	D'Day – Datenschutz Deep Impact (Secorvo, Karlsruhe)
29.02.-04.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
März 2016	
07.-11.03.	Audit Challenge 2016 (Frankfurt School of Finance & Management, Frankfurt)
08.-11.03.	Java Security (Secorvo, Karlsruhe)
14.-15.03.	9. GDD-Fachtagung "Datenschutz International" (Gesellschaft für Datenschutz und Datensicherung e.V., Berlin)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, André Domnick, Dr. Safuat Hamdy, Kai Jendrian, Michael Knopp.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Dezember 2015



Würdelos

Sie werden es vernommen haben: „In Zeiten, in denen nahezu alle Bereiche von Wirtschaft und Gesellschaft digitalisiert werden, muss das Konzept der Datensparsamkeit überdacht werden." (Bitkom-Präsident Thorsten Dirks am 20.07.2015). Und: Datenschutz dürfe „nicht die Oberhand über die wirtschaftliche Verarbeitung gewinnen" (Angela Merkel, Bundeskanzlerin, am 02.11.2015). Die „Minimierung [der Verarbeitung personenbezogener Daten] als oberstes Ziel ist das Gegenteil des Geschäftsmodells von Big Data" (Sigmar Gabriel, Stellvertreter der Bundeskanzlerin, am 19.11.2015).

Kaum hat der letzte Politiker verstanden, dass Informationstechnik zum Wirtschaftsfaktor geworden ist und das Silicon Valley die Nase vorn hat (beides seit der Einführung des Apple II im Jahr 1977 absehbar), ertönt der Ruf nach ungehemmter Datenverarbeitung.

Sind „Informationelle Selbstbestimmung" und „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten" (Volkszählungsurteil des BVerfG, 1983) Konzepte von gestern? Weil amerikanische Internet-Konzerne wie Google, Amazon oder Facebook unsere Persönlichkeitsrechte mit Füßen treten, indem sie (europa-)rechtswidrig Nutzungsdaten unbegrenzt speichern und so ihre Geschäftsmodelle optimieren? Wie frei ist ein Leben, in dem Bewegungsprofile (SmartPhone), Internet-Nutzung (GoogleAnalytics), Kommunikation (WhatsApp, Skype, GMail), Vitaldaten (AppleWatch), TV-Konsum (SmartTV) und Fahrverhalten (iCar) unbegrenzt protokolliert werden?

Was ist das für ein Staat, dessen Repräsentanten ungerügt die Säge an Grundrechte anlegen? Würden wir auch unser Strafrecht ‚modernisieren', wenn Körperverletzung in Mode käme? „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt." (Grundgesetz Artikel 1, Absatz 1). Lesen bildet.



Inhalt

Würdelos

Security News

SmartToys mit Schwachstellen

Mode und Recht

Freie Zertifikate für alle

TLS-Chaos

Secorvo News

Ich bereue immer noch nichts

Spotlight: D'Day

T.I.S.P. und Java Security

Wer druckt, der bleibt

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

SmartToys mit Schwachstellen

Interaktive, netzfähige SmartToys erfreuen zur Weihnachtszeit nicht nur Kinder, sondern auch Hacker und Datendiebe: Anfang November griffen sie auf die Datenbanken des Lernspielzeug-Anbieters VTech zu. Bei dem am 14.11.2015 entdeckten Einbruch wurden Kontodaten von rund 4,8 Millionen Kunden und Profile von 6,3 Millionen Kindern erbeutet. Sie enthalten Namen, Geschlecht, E-Mail-Adressen, Geburtsdaten, verschlüsselte Passwörter, Sicherheitsabfragen und Antworten zur Kennwortwiederherstellung, IP-Adressen sowie Postanschriften und Download-Chroniken. Auf der Webseite „Have I been pwned?“ des Sicherheitsforschers Troy Hunt können VTech-Kunden prüfen, ob auch ihre Daten den Hackern in die Hände gefallen sind. VTech hat eine ausführliche, regelmäßig aktualisierte FAQ zum Vorfall veröffentlicht. Die betroffenen Webseiten sind derzeit wegen eines gründlichen Security Assessments außer Betrieb.

Auch bei „Hello Barbie“, der interaktiven Barbie-Puppe, die sich in Echtzeit unterhalten kann, wurden – erneut – Schwachstellen in der App und in der Server-Konfiguration gefunden. Die Puppe schickt Tonaufzeichnungen via WLAN zur Beantwortung in die Cloud – und speichert sie dort für zwei Jahre. Dafür erhielt sie im Oktober den Negativ-Preis „Big Brother Awards Austria“.

Mode und Recht

Der Bundesgerichtshof hat mit zwei Urteilen vom 26.11.2015 die Internetsperre wiederbelebt – diesmal zum Schutz von Urheberrechten: Wenn gegen den Störer oder Host-Provider nicht vorgegangen werden kann, soll der Access-Provider auf Grundlage der Störerhaftung zur Sperrung rechtsverletzender Seiten verpflichtet werden können.

Die GEMA hatte gegen die Deutsche Telekom auf Unterlassen der Zugangsvermittlung geklagt, da über Telekom-Zugänge die Urheberrechte verletzenden Seiten „3dl.am“ und „goldesel.to“ erreichbar waren. Das Vorgehen gegen Seitenbetreiber und Host-Provider gelang wegen falscher Adressen nicht. Zwar scheiterte die GEMA vor dem BGH, weil weitere Anstrengungen gegen die Verursacher hätten nachgewiesen werden müssen; den Anspruch bejahte der BGH aber grundsätzlich, da ein adäquat-kausaler Tatbeitrag des Access-Providers bestehe. Umgehungsmöglichkeiten stünden der Verhältnismäßigkeit nicht entgegen.

Die Idee der Internetsperre galt eigentlich seit dem gescheiterten Zugangserschwerungsgesetz von 2010 als tot. Aber offenbar haben Recht und Schlaghosen eines gemeinsam: beide können eine modische Wiederauferstehung erleben. Von der Entscheidung sind alle Unternehmen betroffen, die Internet-Zugänge für die Öffentlichkeit bereitstellen. Dabei verursacht die Prüfung von Sperranforderungen Aufwand – denn irrtümliches Sperren kann als wettbewerbswidrige Handlung gelten.

Freie Zertifikate für alle

Am 03.12.2015 begann die CA Let's Enrypt mit der weitgehend automatischen Bereitstellung kostenloser TLS-DV-Zertifikaten im Testbetrieb. Die Initiative Internet Security Research Group (ISRG) finanziert den Betrieb der CA mit Hilfe von Sponsoren. Jeder Interessierte kann mit Hilfe des auf Github bereitgestellten Clients Zertifikate installieren oder erneuern.

Der Client implementiert den aktuellen Draft des geplanten IETF-Standard ACME. In Praxistest gelang es, Apache manuell zu konfigurieren und Zertifikate automatisiert per Webroot-Challenge zu beantragen oder zu verlängern. Automatische Konfigurationsänderungen von Apache schlugen jedoch fehl.

Die automatische Bereitstellung und Verlängerung freier TLS-DV-Zertifikate ist sehr zu begrüßen; sie wird die Verbreitung verschlüsselter Services befördern. Allerdings weist die aktuelle Implementierung noch Schwächen auf: Im Standalone-Modus muss kurzzeitig der eigentliche Webserver heruntergefahren werden – das ist nicht für alle Anbieter eine Option. Auch werden sich viele Betreiber scheuen, die Client-Software als root laufen zu lassen, was erforderlich ist, um Konfigurationsdateien anzupassen oder einen Service auf Port 80 zu starten. Nicht zuletzt dürfte die Nutzung von HTTP Public Key Pinning zu Problemen in der Praxis führen, da Let's Encrypt zur Zeit noch bei jeder Verlängerung das Schlüsselpaar erneuert.

Für Privatpersonen oder kleine Unternehmen, denen die manuelle Verwaltung von Zertifikaten eine Last ist, bietet Let's Encrypt schon heute eine Erleichterung. Man darf aber nicht zu viel erwarten: Ohne ein solides Verständnis der Funktionsweise von TLS ist es derzeit noch eine Herausforderung, die Software in Betrieb zu nehmen.

TLS-Chaos

Anders als gelegentlich kolportiert herrscht keineswegs ein Mangel an sicheren kryptografischen Verfahren – wohl aber an deren korrektem Einsatz in der Praxis. Dies bestätigen erneut zwei aktuelle Vorfälle.

Am 23.11.2015 hatte auf der Diskussionsplattform reddit ein Benutzer namens „robotercowboy“ berichtet, dass auf seinem XPS-Notebook von Dell die eDellRoot-CA als vertrauenswürdige Stammzertifizierungsstelle im Windows Zertifikatspeicher installiert sei. Der harmlose Hinweis wurde zum Skandal, als bekannt wurde, dass Dell nicht nur sein eigenes Root-CA-Zertifkat, sondern gleich auch den zugehörigen geheimen Schlüssel vorinstalliert hatte. Damit konnte jedermann Zertifikate für beliebige Namen ausstellen, die von Dell-Systemen als vertrauenswürdig akzeptiert wurden. Nicht der erste Fall dieser Art: Lenovo leistete sich Ähnliches erst Anfang 2015.

Andere kompromittieren in voller Absicht: Am 30.11.2015 forderte Kazakhtelecom ihre Kunden unter dem Vorwand der Internetsicherheit und mit Verweis auf die Gesetzgebung dazu auf, ein neues „national security certificate“ auf ihren Geräten zu installieren – das dem kasachischen Staat letztlich das unbemerkte Aufbrechen von TLS-Verbindungen seiner Bürger ermöglicht.

Doch auch bei anderen TLS-Protokollen (POP3S, IMAPS, SMTPS, IRCS) sieht es düster aus. Das zeigt eine am 02.11.2015 publizierte Untersuchung von Forschern der Universitäten Sydney, Berkeley und München, in der der gesamte IPv4-Adressraum analysiert und mehr als 110 Mio. TLS-Verbindungen ausgewertet wurden. Nur bei rund 31 % aller SMTP-Server war eine Verbindung mittels STARTTLS möglich, und von diesen Servern setzten nur rund 30 % ein vertrauenswürdiges X.509-Zertifikat ein. Bei (je nach Dienst) bis zu 30 % der Server war das Zertifikat abgelaufen, und 10-20 % der TLS-Verbindungen waren mit RC4 verschlüsselt.

Secorvo News

Ich bereue immer noch nichts

Wer das Snowden-Theaterstück „Ich bereue nichts“ des Badischen Staatstheaters Karlsruhe noch nicht gesehen hat, kann das am **29.01.2016** und **05.02.2016** nachholen. Der Darsteller Thomas Halle wurde am 30.03.2015 bei der Woche junger Schauspieler in Bensheim für seine schauspielerische Leistung in diesem Stück mit dem Günther-Rühle-Preis ausgezeichnet.

Am **29.01.2016** gestaltet Secorvo ab 19:30 Uhr das Rahmenprogramm: Christoph Schäfer führt in das Stück ein („NSA: Der Skandal im Zeitraffer“), und Kai Jendrian geht im anschließenden Publikumsgespräch auf die Möglichkeiten des Selbstschutzes ein. Beide Experten stehen anschließend für Fragen zur Verfügung. Sichern Sie sich jetzt eine Platzkarte!

Spotlight: D'Day

Das eintägige Seminar D´Day – Datenschutz Deep Impact für Datenschutzbeauftragte am 25.02.2016 wird aktuelle Herausforderungen im Datenschutz diskutieren und bewerten. Nach einer einführenden Betrachtung von Dirk Fox über vermeintliche und tatsächliche Datenschutz-Highlights diskutiert Karin Schuler mit Ihnen Aufbau und Gestaltung einer Datenschutz-Stellungnahme. Michael Knopp und Christoph Schäfer zeigen Fallstricke und Lösungswege beim Cloud-Outsourcing auf. Über die Möglichkeiten der Ausgestaltung eines Security Information and Event Managements (SIEM) berichtet Dr. Safuat Hamdy; Michael Knopp übernimmt die datenschutzrechtliche Einordnung. Abschließend stellt Ihnen Dr. Volker Hammer (Editor der DIN 66398) vor, wie Sie das systematische Löschen personenbezogener Daten in den Griff bekommen.

T.I.S.P. und Java Security

Unsere erste T.I.S.P.-Schulung im neuen Jahr – vom **29.02. bis 04.03.2016** – lädt Sie ein, Ihre Berufserfahrung und Qualifikation im Gebiet Informationssicherheit durch ein T.I.S.P.-Zertifikat bestätigen zu lassen. Zur Vorbereitung erhalten Sie vorab unser T.I.S.P.-Begleitbuch.

Dass viele Bedrohungen durch sicher programmierte Software erst gar nicht entstehen würden, muss an dieser Stelle nicht betont werden. Wie Sie das in Java erreichen, erfahren Sie in unserer „Hands-On“-Schulung Java Security vom **08. bis 11.03.2016**.

Alle Seminarangebote mit detaillierter Beschreibung finden Sie auf unseren Webseiten.

Wer druckt, der bleibt

Drucker und Kopierer sind heute keine dummen Ausgabegeräte mehr, sondern haben sich zu smarten Netzwerkteilnehmern gemausert. Mit ihnen werden tagtäglich personenbezogene und vertrauliche Informationen gedruckt, kopiert, gescannt und gelegentlich auch gefaxt. Damit sind sie ein Angriffsziel für Innen- und Außentäter – nicht nur Geräte mit Festplatte.

Beim nächsten KA-IT-Si-Event am **02.02.2016** um 18 Uhr zeigt Hendrik Herberger (MODOX – Modern Documents GmbH) in den Räumen des CyberForum e.V. die Gefährdungslage auf und gibt konkrete Empfehlungen, wie sich bestehende Risiken minimieren lassen. Anschließend haben Sie wie gewohnt die Gelegenheit zum „Buffet-Networking“. Anmeldung unter www.ka-it-si.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Januar 2016	
15.-17.01.	ShmooCon 2016 (The Shmoo Group, Washington/US)
19.-21.01.	OmniSecure 2016 (inTIME, Berlin)
Februar 2016	
09.-10.02.	23. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
17.-18.02.	25. SIT-SmartCard Workshop (SIT, Darmstadt)
25.02.	D'Day – Datenschutz Deep Impact (Secorvo, Karlsruhe)
29.02.-04.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
März 2016	
07.-11.03.	Audit Challenge 2016 (Frankfurt School of Finance & Management, Frankfurt)
08.-11.03.	Java Security (Secorvo, Karlsruhe)
14.-15.03.	9. GDD-Fachtagung "Datenschutz International" (GDD e.V., Berlin)
29.03.-01.04.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)

Fundsache

Mozilla hat Ende November in Hamburg die Bedrohung unserer Privatsphäre durch Internet-Konzerne mit einem Glashaus-Experiment veranschaulicht – dokumentiert in einem Youtube-Video.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, André Domnick, Kai Jendrian, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2016



Next Big Thing

Während Experten noch darüber streiten, was genau unter „Industrie 4.0“ zu verstehen ist, rauscht bereits die nächste große „IT-Sau“ auf das Dorf zu: das „Internet of Things“, kurz: IoT. Zwar ist die Idee nicht mehr ganz frisch: Sie basiert auf einem Aufsatz von Mark Weiser aus dem Jahr 1991 und dem „Ubiquitous computing“ – der Erwartung, dass die Miniaturisierung von Computern diese allgegenwärtig machen wird. Im Automobil ist das bereits Realität: Hunderte Steuerungs- und Diagnosesysteme sind darin verbaut. Dank des mit IPv6 ins Unvorstellbare (genauer: auf $3{,}4 \cdot 10^{38}$) vergrößerten Adressbereichs kann nun jedes Staubkorn auf unserem Planeten eine IP-Adresse erhalten – erst recht die immer kompakteren und leistungsfähigeren Miniaturrechner. Ausgestattet mit Sensoren vermessen diese nun unsere Welt: Das Einschalten von Geräten verrät unser Nutzungsverhalten, die Senderwahl im TV unsere Vorlieben, der Kühlschrank erlernt unsere Ernährungsgewohnheiten, die Armbanduhr erhebt unsere Vitaldaten, das Gaspedal erkennt unseren Fahrstil, den der Bordcomputer mit dem Ortsinformationen korreliert.

Damit sind Dienste möglich, die unsere Vorstellungskraft (noch) übersteigen: Nach intensiver Gerätenutzung könnten uns Neugeräte angeboten, das abendliche TV-Programm passgenau zusammengestellt, Nahrungsmittel geliefert, bevor der Vorrat zur Neige geht, Medikamente bei Bedarf automatisch zugestellt, Rasen und Falschparken direkt an die zuständigen Behörden gemeldet, Versicherungsprämien aus dem tatsächlichen Risiko (Zigaretten? Alkohol? Blutdruck? Riskanter Fahrstil?) berechnet und Verhaltensoptimierungen via App empfohlen (und deren Einhaltung überprüft) werden.

Derweil einigten sich die Datenschutzaufsichtsbehörden mit dem VDA am 26.01.2016, dass „... die bei der KfZ-Nutzung anfallenden Daten (...) jedenfalls dann personenbezogen (...) sind, wenn eine Verknüpfung mit (...) dem KfZ-Kennzeichen vorliegt“.



Inhalt

Next Big Thing

Security News

Firewalls mit Hintertür

Abmahnrecht für Verbände

OpenSSH-Schwäche

Freunde finden

Cross Device Tracking

Secorvo News

Wer druckt, der bleibt

Das T.I.S.P.-Zertifkat

Das T.E.S.S.-Zertifikat

PKI für Experten

Krypto im Advent

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Firewalls mit Hintertür

Nachdem kurz vor Weihnachten Netzwerkgeräte von Juniper mit gleich zwei Hintertüren (sowohl im SSH-Zugang als auch im Zufallszahlengenerator für VPN-Verbindungen) für Aufsehen sorgten, zog am 12.01.2016 der bekannte Firewall-Hersteller Fortinet nach. Ein fest kodiertes „Managementpasswort" erlaubte es Angreifern jahrelang, sich per SSH an Fortigate-Firewalls anzumelden. Die Schwachstellen sind zwar behoben, ein ungutes Gefühl in der Magengegend bleibt jedoch. Beide Fälle zeigen, dass Netzwerkgeräte und Appliances kein uneingeschränktes Vertrauen verdienen.

Bei Penetrationstests entdecken wir in Netzwerkgeräten häufig vom Internet erreichbare Management-Zugänge wie SSH oder Web-Schnittstellen. Begründet wird der Zugang oft damit, dass so eine schnelle Remote-Fehlerbehebung ermöglicht werden solle – schließlich würden sichere Passwörter, Anmeldemechanismen und Protokolle eingesetzt. Die entdeckten Hintertüren sollten Anlass sein, solche Zugänge auf den Prüfstand zu stellen.

Abmahnrecht für Verbände

Bislang konnten Datenschutz-Verstöße in erster Linie von Betroffenen abgemahnt werden. Teilweise wurde dieses Recht auch Mitbewerbern zugesprochen. Mit dem am 17.12.2015 beschlossenen „Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts" kommen registrierte Verbände hinzu. Das UKlaG und das BGB werden angepasst.

Künftig können beispielsweise Verbraucherschutzzentralen per Unterlassungsklage gegen Unternehmen vorgehen, die aus ihrer Sicht Datenschutzverstöße mit Verbraucherbezug begehen. Während die meisten Datenschutz-Aufsichtsbehörden eher auf Einsicht von Unternehmen setzen, dürften Verbände weniger Beißhemmungen und vor allem mehr (personelle) Kapazitäten haben.

Besonders Betreiber von Web-Shops dürften die Auswirkungen spüren. Bisher konnten fehlende oder falsche Klauseln in AGB und Datenschutzerklärungen abgemahnt werden; nun kommen tatsächliche Datenverarbeitungen hinzu. Die Verbände werden sich Vorgänge wie Bonitätsprüfungen oder Retargeting vermutlich sehr genau anschauen. Unternehmen sollten das Gesetz zum Anlass nehmen, ihre Web-Shop-Prozesse von ihrem betrieblichen Datenschutzbeauftragten überprüfen zu lassen.

OpenSSH-Schwäche

Für das weit verbreitete OpenSSH Projekt begann das neue Jahr am 14.01.2016 mit einer gravierenden Client-Schwachstelle (CVE-2016-0777). Sie ermöglicht es, unter Ausnutzung der (experimentellen) Roaming-Funktionalität mit einem manipulierten Server-Dienst bei einer Authentisierung mit privatem Schlüssel diesen auszulesen. Damit können sich Angreifer, die einen Server übernehmen konnten, die Schlüssel der Administratoren verschaffen. Da letztere oft das gleiche Schlüsselpaar für eine große Anzahl von Servern nutzen, erhalten die Angreifer so die Credentials für alle diese Server.

Gegen derartige Angriffe können sich Nutzer durch das Deaktivieren des Roaming Supports oder durch das Einspielen eines gepatchten SSH-Clients schützen. Eine präventive Maßnahme wäre die Verwendung eines Schlüsselpaars pro Zielsystem oder der Einsatz von Smartcards gewesen.

Wie bei Heartbleed hatte hier eine Schwachstelle in einer praktisch nicht genutzten, experimentellen Funktion gravierende Auswirkungen auf die Sicherheit des gesamten Systems. Vor allem bei derart sicherheitskritischen Werkzeugen sollte man sich auf den Grundsatz besinnen: Weniger ist mehr!

Freunde finden

Der Bundesgerichtshof hat am 14.01.2016 die Funktion „Freunde finden" von Facebook für rechtswidrig erklärt und damit das Berufungsurteil des Kammergerichts Berlin vom 24.01.2014 bestätigt. Facebook verschickte über diese Funktion mittels der aus den Adressbüchern neu registrierter Nutzer ermittelten E-Mail-Adressen automatisch Einladungen zur Registrierung auch an Nicht-Mitglieder des Netzwerks. Der Verbraucherzentrale Bundesverband (VZBV) war 2010 hiergegen vorgegangen. Der BGH hat nun bestätigt, dass darin eine unzulässige, belästigende Werbung i. S. von § 7 Abs. 1 und 2 Nr. 3 UWG sowie eine Täuschung der Nutzer über die Verwendung ihrer Adressbuchdaten gelegen habe. Das Ergebnis der Revision ist wenig überraschend. Die Praxis, Adressbuchdaten ungefragt zu nutzen, hat Facebook inzwischen längst aufgegeben.

Zahlreiche weitere Soziale Netzwerke, z. B. auch Xing, bieten den Nutzern ähnliche Funktionen, um Einladungen an ihre Adressbuchkontakte zu verschicken. Nach den Kriterien des bestätigten Berufungsurteils führt die bloße technische Hilfestellung durch den Netzwerkanbieter jedoch nicht zu unerlaubter Werbung. Offen ist allerdings noch, wie der BGH automatisch generierte Erinnerungen an eine solche Einladung bewertet.

Cross Device Tracking

Dass smarte Software „nach Hause telefoniert“, um ihren Hersteller mit Nutzungsdaten zu versorgen, ist nicht neu. Neu ist, dass besonders smarte Software über Device-Grenzen via Ultraschall miteinander kommuniziert – und so ihr Wissen über das Nutzungsverhalten an PC, Smartphone, Tablet und TV verknüpfen kann. Am 16.10.2015 hatte das Center for Democracy and Technology (CDT) in einem öffentlichen Brief an die US-amerikanische Federal Trade Commission zu diesem seit mindestens Mitte 2014 bekannten Verfahren Stellung genommen.

Marktführer ist demnach die indische Firma SilverPush, die für das menschliche Ohr nicht wahrnehmbare Tonsequenzen in TV- und Browser-Werbung einblendet, die von einem in bereits mehr als 67 Apps versteckten SDK empfangen und ausgewertet werden können. Angeblich kontrolliert SilverPush auf diese Weise schon mehr als 18 Mio. Smartphones – und erfährt so, wie lange eine Anzeige oder eine TV-Werbung sichtbar ist oder ob sie weggeklickt wird. Offenbar gehören auch Google, Nestle und McDonalds zu den über 150 Kunden von SilverPush, wie Jai Vardhan am 11.11.2015 berichtete.

Tatsächlich entzieht sich diese Art des Trackings jeder technischen Gegenmaßnahme – und ist zudem nicht ohne weiteres feststellbar. Wer sich davor schützen will, dem bleibt nur, das Mikrofon seines Smartphones abzukleben – oder die „Aus“-Taste zu suchen (und zu betätigen).

Secorvo News

Wer druckt, der bleibt

Bei unserem kommenden KA-IT-Si-Event am **02.02.2016** (ausnahmsweise einem **Dienstag**) wird Ihnen Hendrik Herberger (Modox - Modern Documents GmbH) in seinem Vortrag „Übersehen und unterschätzt - Live Hacking von Druckern“ die Gefährdung Ihrer Daten durch moderne Drucker und Kopierer aufzeigen und konkrete Empfehlungen geben, wie sich diese Risiken minimieren lassen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Anmeldung unter www.ka-it-si.de.

Das T.I.S.P.-Zertifkat

Am 29.02.2016 startet die erste T.I.S.P.-Schulung 2016. Sie schließt mit der Prüfung zum T.I.S.P.-Zertifikat ab. Die Schulung gibt Ihnen einen umfassenden und themenübergreifenden Überblick über die wichtigsten Gebiete der Informationssicherheit. Vorab erhalten Sie zur Vorbereitung das Begleitbuch „Zentrale Bausteine der Informationssicherheit“. Mehr als 800 IT-Sicherheitsexperten belegen ihre Qualifikation bereits mit dem anerkannten T.I.S.P.-Zertifikat. Termin: **29.02.-04.03.2016** in Karlsruhe. Es gibt nur noch wenige freie Plätze.

Das T.E.S.S.-Zertifikat

System Security Engineering betrachtet die Sicherheit komplexer Systeme. Diese hängt nicht nur von den Sicherheitseigenschaften der beteiligten Komponenten, sondern auch von deren Zusammenwirken und den verwendeten Schnittstellen und Protokollen ab. In der Schulung T.E.S.S. lernen Sie das Zusammenspiel aller Faktoren so zu gestalten, dass das resultierende Gesamtsystem Ihren Sicherheitsanforderungen genügt. Mit dem Erwerb des T.E.S.S.-Zertifikats (TeleTrusT Engineer System Security) dokumentieren Sie Ihre Qualifikation. Termin: **04.-07.04.2016** in Karlsruhe

PKI für Experten

Wer für die Konzeption, den Aufbau oder Betrieb einer PKI zuständig ist, sei unser Praxis-Seminar-Klassiker wärmstens ans Herz gelegt. Fast 300 positive Teilnehmerbewertungen belegen, dass die Expertise und Erfahrung aus 19 Jahren PKI-Praxis ankommt. Termin: **19.-22.04.2016** in Karlsruhe

Detailbeschreibungen unserer Seminarangebote und die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite.

Krypto im Advent



In Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe realisierten wir den interaktiven Online-Adventskalender „Krypto im Advent“. Mehr als 1.100 Schülerinnen und Schülern der Klassen 3 bis 7 machten sich im Dezember 2015 täglich an die Lösung einer Knobelaufgabe aus der Welt der Kryptologie. Dabei gab es zahlreiche gesponserte Sachpreise zu gewinnen. Aufgrund der großen und begeisterten Resonanz werden wir das Adventsrätsel auch 2016 anbieten. Zum Üben gibt es alle Aufgaben aus dem vergangenen Jahr (und die Lösungen) zum Download.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2016	
02.02.	Wer druckt, der bleibt (KA-IT-Si, Karlsruhe)
09.-10.02.	23. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
17.-18.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)>
29.02.-04.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
März 2016	
08.-11.03.	Java Security (Secorvo, Karlsruhe)
21.-24.03.	1st IEEE European Symposium on Security and Privacy (IEEE, Saarbrücken)
29.03.-01.04.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)
April 2016	
04.-07.04.	T.E.S.S. - TeleTrusT Engineer System Security (Secorvo, Karlsruhe)
11.-14.04.	CPSSE - Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe)
19.-22.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)

Fundsache

Der Informatiker Carsten Eilers hat am 28.01.2016 ein (kostenfreies) E-Book veröffentlicht, in dem er alle 2015 bekannt gewordenen Router-Schwachstellen zusammengefasst hat. Eine hilfreiche Checkliste.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Februar 2016



Trägheitsprinzip

Das Trägheitsprinzip ist ein zentrales Axiom der Physik *Sir Isaac Newtons* (1642-1726), auch bekannt als das im Jahr 1687 publizierte „Erste Newtonsche Gesetz". Formuliert wurde es bereits im Jahr 1638 von *Galileo Galilei* (1564-1641): Jeder Körper behält seinen Ruhe- oder Bewegungszustand bei, solange keine auf ihn einwirkende Kraft ihn zur Änderung dieses Zustands zwingt.

Wie wir heute wissen, lassen sich mit diesem Prinzip nicht nur die Bewegungen der Himmelskörper erklären, sondern auch das Verhalten von elektromagnetischen Feldern. Verfolgt man aufmerksam die Nachrichten, kann man sich außerdem des Eindrucks nicht erwehren, dass auch das menschliche Verhalten diesem Prinzip gehorcht.

Wie anders ließe es sich auch erklären, dass nach einer Analyse von 35 Millionen Authentifikationsdaten durch das Hasso-Plattner-Institut im Jahr 2015 das meistgenutzte Passwort der Welt „123456" lautet? Dass gut 15 Jahre nach dem I-Love-You-Virus noch immer angeklickte E-Mail-Anhänge das Haupteinfallstor für Schadsoftware sind? Dass auch heute noch Mitarbeiter ihre Rechner am Arbeitsplatz in der Regel ohne Aktivierung einer Zugangssperre verlassen? Dass Mitarbeiter sich mit Händen und Füßen gegen den Entzug von Administratorrechten für ihren lokalen Rechner wehren?

Sicherheit könnte viel einfacher sein – etwas mehr Einsicht bei den „Gurtmuffeln" des 21. Jahrhunderts vorausgesetzt. Derweil üben sich die Verantwortlichen in Selbsttäuschung: Nach dem am 17.11.2015 veröffentlichten „Cyber Security Report" des Instituts für Demoskopie Allensbach (im Auftrag der Deutschen Telekom) halten die befragten Führungskräfte deutscher Unternehmen das Schadensrisiko durch einen Hackerangriff für eher gering (60 %) und sehen ihr Unternehmen „so gut wie möglich vorbereitet" (60 %).

Offenbar müssen wohl auch hier erst externe Kräfte einwirken, damit sich der Zustand ändert.



Inhalt

Trägheitsprinzip

Security News

Und Krypto funktioniert doch …

Minimierung per Verordnung

Arbeitnehmerkontrolle

Transparenz ist Pflicht

Grünes Licht für Cookie-Opt-out

Grenzen der Werbeflut

Secorvo News

Call for Paper für die T.I.S.P.-Community

Das CPSSE-Zertifikat

PKI für die Praxis

Dumm. Dümmer. DAU?

Save the Date: APP #4

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Und Krypto funktioniert doch ...

... zumindest bei aktuellen Erpressungs-Trojanern (*Ransomware*) wie Teslacrypt. Ließen sich von Teslacrypt 2 verschlüsselte Dateien noch mit dem TeslaDecoder wiederherstellen, weil der verwendete AES-Schlüssel rekonstruierbar im Header der Datei versteckt wurde, ist dies bei dem am 12.01.2016 in Umlauf gebrachten Teslacrypt 3 nicht mehr möglich. Auch ältere Erpressungs-Trojaner wie Cryptowall (seit 01.11.2014 bekannt) setzen inzwischen so gute kryptographische Verfahren ein, dass das FBI empfiehlt, die erpresste Summe zu zahlen.

Gegen derartige Angriffe hilft eine Kombination aus technischen und Sensibilisierungs-Maßnahmen für die Benutzer. Werden E-Mail-Anhänge abgefangen oder solche mit Schadsoftware gar nicht erst geöffnet, wird damit die Infektion unterbunden – das ist wirkungsvoller als ein Virenschutz, der neue Varianten der Trojaner ohnehin zunächst nicht erkennt. Um den Schaden einer Infektion zu begrenzen helfen restriktive Berechtigungen, sodass nur wenige (Benutzer-) Dateien und nicht komplette Netzlaufwerke unerwünscht verschlüsselt werden. Und eine angepasste und strikte Backup-Strategie hilft im Fall der Fälle bei der Wiederherstellung der Daten.

Minimierung per Verordnung

Das Bundesinnenministerium hat am 13.01.2016 einen Referentenentwurf der Verordnung (BSI-KritisV) zum am 25.07.2015 in Kraft getretenen IT-Sicherheitsgesetz vorgelegt, der insbesondere näher festlegt, welche Anlagen als kritische Infrastrukturen gelten und damit dem Gesetz unterfallen.

Der Entwurf zählt die Anlagenkategorien aus den Bereichen Energie, Wasserversorgung, Telekommunikation und Ernährung auf und umfasst einen Anhang mit branchenspezifischen Schwellenwerten. Beispielsweise fallen Stromerzeugungsanlagen ab 420 MW installierter Leistung und Serverfarmen mit im Jahresdurchschnitt mindestens 25.000 laufenden Instanzen unter die Regelungen.

Der Aspekt des Gefährdungspotentials für die öffentliche Sicherheit (§ 2 Abs. 10 Nr. 2 BSI-Gesetz) wird dabei vollständig ausgeblendet. Auch die im Gesetzestext enthaltenen Sektoren Gesundheit, Transport und Verkehr oder Finanz- und Versicherungswesen sind (bis Ende 2016) ausgespart. Nach der Begründung sind in Deutschland insgesamt 650 Anlagen betroffen, deren Betreiber jährlich mit einem Aufwand von sieben Vorfallsmeldungen à 660 Euro pro Anlage rechnen müssen. In der Gesetzesbegründung war noch von 2000 Betreibern und einem nicht quantifizierbaren Aufwand für die Maßnahmenumsetzung die Rede. Offenbar ist ein ISMS in Deutschland zurzeit günstig zu haben.

Arbeitnehmerkontrolle

Das Landesarbeitsgericht Berlin-Brandenburg hat am 14.01.2016 entschieden, dass Arbeitgeber die Internetnutzung ihrer Mitarbeiter – auch bei in Pausen ausnahmsweise gestatteter privater Nutzung – ohne Einwilligung der Betroffenen anhand der Browserprotokollierung überprüfen dürfen. Die Protokolle haben zudem Beweiskraft im Streit über eine außerordentliche Kündigung wegen exzessiver Internetnutzung.

Die Datenschutz-Aufsichtsbehörden sehen dies v. a. bei erlaubter Privatnutzung kritischer und haben ihre Einschätzung gerade erst in einer am 30.01. 2016 veröffentlichten Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz dargestellt.

Das Landesarbeitsgericht Berlin-Brandenburg hat bereits im Jahr 2011 vertreten, dass der Arbeitgeber selbst bei erlaubter Privatnutzung nicht zum Telekommunikationsdiensteanbieter wird. Ob dieses jüngste Urteil in ähnlicher Weise rechtliche Streitstände vertieft, wird jedoch erst die Urteilsbegründung verraten.

Transparenz ist Pflicht

Fast jede Webseite verfügt heute über eine Anbieterkennzeichnung gem. § 5 TMG, meist zu finden unter dem Link „Impressum“. Eine korrekte Datenschutzerklärung nach § 13 TMG fällt vielen Seitenbetreibern schon viel schwerer. Dabei hatte das OLG Hamburg bereits im Juli 2013 entschieden, dass fehlende oder fehlerhafte Datenschutzerklärungen einen abmahnfähigen Wettbewerbsverstoß darstellen.

Dieser Entscheidung folgt das LG Köln mit seinem Beschluss vom 26.11.2015 und erließ eine entsprechende einstweilige Verfügung gegen einen Webseitenbetreiber. Unter anderem wurde auf der Seite das Remarketing-Tool Google Adwords eingesetzt. Webseitenbetreiber sollten den Beschluss als Ermahnung nehmen, ihre Datenschutzerklärung auf Aktualität und Vollständigkeit zu überprüfen – oder umgehend eine zu erstellen.

Grünes Licht für Cookie-Opt-out

Das OLG Frankfurt hat am 17.12.2015 entschieden, dass eine Opt-out-Möglichkeit beim Einsatz eines Webanalyse-Dienstes ausreicht. In dem Urteil über die Klage eines Verbraucherschutzverbands ging es um eine Gewinnspiel-Einwilligung, die aufgrund

undifferenzierter Verlinkung auf 59 Kooperationspartner nicht rechtswirksam war.

„Nebenbei" beantwortet das Urteil jedoch die Frage, ob die so genannte Cookie-Richtlinie der EU und deren Vorgabe zur Einwilligung beim Einsatz von Cookies in Deutschland unmittelbar anwendbar ist. Diese Frage ist seit Jahren heiß diskutiert und umstritten. Das OLG hat nun klargestellt, dass die entsprechenden datenschutzrechtlichen Vorschriften keine Einwilligung (in Gestalt eines Opt-in-Verfahrens) vorschreiben. Die Zustimmung gilt als erteilt, wenn der Nutzer einen bereits gesetzten Haken nicht entfernt (Opt-out-Verfahren).

Grenzen der Werbeflut

In seiner Urteilsbegründung zu der bereits am 15.12.2015 ergangenen Entscheidung über Werbung in Eingangsbestätigungs-E-Mails ist der Bundesgerichtshof (BGH) auf die Reichweite der von ihm angenommenen Persönlichkeitsrechtsverletzung eingegangen. Im verhandelten Fall hatte der Kläger auf einen Werbewiderspruch eine automatische Eingangsbestätigungs-E-Mail mit Werbeinhalt erhalten. Der § 7 UWG war in diesem Fall nicht anwendbar, da es sich beim Kläger um einen Verbraucher, nicht um einen Wettbewerber handelte. Ein elektronisches Postfach sei jedoch Teil der Privatsphäre, das allgemeine Persönlichkeitsrecht vermittle das Recht „in Ruhe gelassen zu werden".

Ob das Einwilligungserfordernis aus Art. 13 Abs. 1 der EU-Datenschutzrichtlinie für elektronische Kommunikation bei Verstößen stets zu einem Eingriff in das Persönlichkeitsrecht mit resultierendem Unterlassungsanspruch führt, ließ der BGH jedoch offen. Dies gelte jedenfalls regelmäßig für einen Werbewiderspruch.

Werbezusätze in E-Mails dürfen nach dieser Rechtsprechung nur noch bei Einwilligung oder bei bestehender Geschäftsbeziehung eingesetzt werden – vom E-Mail-Server automatisch angehängte Marketing-Footer können zukünftig teuer werden.

Secorvo News

Call for Paper für die T.I.S.P.-Community

Vom **10. bis 11.11.2016** treffen sich in Frankfurt Absolventen des T.I.S.P.-Zertifikats auf dem „10. T.I.S.P. Community Meeting" zum Erfahrungsaustausch. Von TeleTrusT wurde ein Call for Paper für diese Veranstaltung veröffentlicht: Bis zum 18.04. 2016 können Sie Beitragsvorschläge einreichen.

Das CPSSE-Zertifikat

Werden bei der Entwicklung von Software-Sicherheitsanforderungen systematisch berücksichtigt, dann ist das nicht nur ein wichtiger Schritt zu einer höheren Softwarequalität, sondern auch ein Gewinn für die IT-Sicherheit aller Kunden. Wie das gelingt, zeigt die Schulung zum Certified Professional for Secure Software Engineering (CPSSE) vom **11. bis 14.04.2016** in Karlsruhe. Ein Teilnehmer schrieb uns dazu: „*Secure Software Engineering: alles andere als nur Theorie: Informatives und interaktives Seminar mit einem sehr guten Verhältnis von Theorie und Praxis.*"

PKI für die Praxis

Über 300 PKI-Experten haben sich bisher auf einem unserer PKI-Seminare mit aktuellem Know-how versorgt. Eine Teilnehmerstimme: „*Das gesamte Seminar war beeindruckend strukturiert aufgebaut und umfasste alle wesentlichen Themen wie Grundlagen, Standards und praktische Umsetzung. Unter kompetenter Begleitung durch spezialisierte Dozenten hat mich der abschließende Workshop für die schrittweise Vorgehensweise sensibilisiert [...]. Eine wohltuende Atmosphäre um das Seminar [...].*" Die nächste PKI-Schulung, die Expertise und Erfahrung aus 20 Jahren aktiver Gestaltung von PKIs bündelt, findet vom **19. bis 22.04.2016** in Karlsruhe statt.

Detaillierte Seminarinhalte, weitere Angebote und die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite.

Dumm. Dümmer. DAU?

In der IT gilt die alte Weisheit, stets den „Dümmsten Anzunehmenden User" (DAU) im Blick zu behalten. Doch was heißt das eigentlich? Und warum verhält sich der DAU so „dumm"? Und was kann man daraus lernen?

In seinem Vortrag „Psychologie der Sicherheit: Ist der DAU wirklich dumm?" beim nächsten KA-IT-Si-Event am **21.04.2016** um 18 Uhr erläutert Christoph Schäfer (Secorvo Security Consulting GmbH), wie Entscheidungsprozesse im menschlichen Gehirn ablaufen und welchen systematischen Fehlern Menschen bei der Entscheidungsfindung unterliegen.

Dabei wird deutlich, welche Bedeutung dem „Faktor Mensch" in der IT-Sicherheit zukommt – und was man daraus lernen sollte. Anschließend haben Sie wie gewohnt die Gelegenheit zum „Buffet-Networking". Anmeldung unter www.ka-it-si.de.

Save the Date: APP #4

Merken Sie sich bereits den 29.04.2016 vor – den Termin unserer vierten Anti-Prism-Party im Karlsruher ZKM.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2016	
14.-15.03.	9. GDD-Fachtagung „Datenschutz International“ (Gesellschaft für Datenschutz und Datensicherung e.V., Berlin)
21.-24.03.	1st IEEE European Symposium on Security and Privacy (IEEE, Saarbrücken)
April 2016	
04.-07.04.	T.E.S.S. - TeleTrusT Engineer System Security (Secorvo, Karlsruhe)
11.-14.04.	CPSSE - Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe)
19.-22.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
21.04.	Dumm. Dümmer. DAU? (KA-IT-Si, Karlsruhe)
27.-28.04.	17. Datenschutzkongress (EUROFORUM, Berlin)
29.04.	Anti-Prism-Party 4. Staffel (KA-IT-Si, Karlsruhe)
Mai 2016	
30.05.-01.06.	IFIP SEC 2016 (IFIP, Hamburg)

Fundsache

Am 28.01.2016 hat der Rat der Europäischen Union die deutschsprachige Fassung der am 15.12.2016 beschlossenen Datenschutz-Grundverordnung veröffentlicht, die die EU-Richtlinie aus dem Jahr 1995 ablöst.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2016



Rettungsleck

Vor einigen Jahren nahmen wir an einer Wildwasser-Fahrt im Schlauchboot teil. Als mein Blick bei der Einweisung auf die Boote fiel, staunte ich nicht schlecht: im Boden klaffte jeweils ein großes Loch. „Damit das Wasser herauslaufen kann", erläuterte uns der Bootsführer grinsend. Kaum im Wasser klärte sich das vermeintliche Wunder: Der Auftrieb der Luftkammern hielt das Boot so weit über der Wasseroberfläche, dass das hereinschwappende Wasser tatsächlich durch das Loch ablief – ohne Loch hätte das Boot tief und schwerfällig im Wasser gelegen.

An dieses Erlebnis musste ich am 09.03.2016 denken, als ein Verschlüsselungstrojaner unter Verwendung der Ransomware EDA2 die Runde machte. Dessen Autor Utku Sen hatte eine Entschlüsselungs-Hintertür in EDA2 eingebaut, die eine Rekonstruktion der Schlüssel ermöglichte – etwa 700 Betroffene kamen daher ohne Lösegeldzahlung wieder an ihre unerwünscht verschlüsselten Daten.

Das klingt nach einem guten Argument für das FBI, das derzeit von Apple den Einbau von Entschlüsselungs-Hintertüren in iPhones fordert. Aber wie beim Loch im Wildwasser-Schlauchboot gilt auch hier: Nicht jede Speziallösung eignet sich als generelles Konzept. Denn nachweislich ist ein Loch im Rumpf normalerweise kein wirksamer Sinkschutz.

Ein Verschlüsselungsverfahren ist nur dann ein sicheres Verfahren, wenn es keine Hintertür besitzt. Solche Verschlüsselungsverfahren sind bei einem Ransomware-Angriff zweifellos unerfreulich – sie sind jedoch nicht die Ursache des Problems. Auch die „Klick-nicht-auf-den-Anhang"-Empfehlung nimmt allein den Auslöser ins Visier. Der Schaden von Ransomware ist hingegen meist deshalb so groß, weil die betroffenen Benutzer Schreibrechte auf zu vielen Daten besitzen – und die zugehörigen Backups zu alt sind für eine verlustarme Wiederherstellung. Hier stecken die eigentlichen Hausaufgaben.



Inhalt

Rettungsleck

Security News

DROWN-Angriff: ein SSL-Krimi

Quadratur des Kreises

Hackers Contest

No-Spy-Klausel

Datenschutz via Kartellrecht

Secorvo News

CfP T.I.S.P. Community Meeting

PKI für Praktiker

CPSSE-Zertifikat

T.I.S.P.-Zertifikat

Anti-Prism-Party #4

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

DROWN-Angriff: ein SSL-Krimi

Der von einer Gruppe von Sicherheitsexperten am 01.03.2016 publizierte jüngste Angriff auf TLS/SSL (DROWN – *Decrypting RSA using Obsolete and Weakened eNcryption*) liest sich wie ein Krimi: Eine Gemengelage aus Crypto War-Relikten, Protokoll-Designfehlern, fehlerhafter Konfiguration und Bugs. Er basiert auf der verbreiteten, aber irrigen Annahme, dass es ungefährlich sei, wenn ein Server das „ausgestorbene" Protokoll SSLv2 nicht deaktiviert. Anfang März 2016 unterstützten allein sechs Millionen HTTPS-Server SSLv2. Anfällig für DROWN sind weitere Millionen Server, die andere SSL-basierte Protokolle nutzen oder mit einem SSLv2 unterstützenden Server das Zertifikat teilen.

DROWN nutzt die schwachen Export-Chiffren von SSLv2 aus den 90er Jahren mit nur 40 bit langen symmetrischen Schlüsseln (RC2 bzw. RC4) für einen *Chosen-Ciphertext*-Angriff, um den Sitzungsschlüssel einer mitgeschnittenen TLS-Verbindung zu berechnen und damit die Daten nachträglich zu entschlüsseln. Kryptographisch basiert DROWN auf dem *Padding Oracle*-Angriff von Daniel Bleichenbacher aus dem Jahr 1989.

Um einen HTTPS-Server vor DROWN zu schützen, reicht das Entfernen der Export-Chiffren in der Serverkonfiguration nicht aus: Es müssen SSLv2 serverseitig deaktiviert und aktuelle TLS/SSL-Bibliotheken (z. B. für OpenSSL) eingespielt werden.

Zum Testen der Verwundbarkeit eines HTTPS-Servers bietet die Webseite „The DROWN Attack" ein Check Tool und eine wunderbare FAQ.

Quadratur des Kreises

Nach erfolgloser Abmahnung hat die Verbraucherzentrale Nordrhein-Westfalen am 29.02.2016 Microsoft vor dem LG München I (AZ. 12 O 909/16) auf Unterlassung verklagt. Grund ist die nach Auffassung der Verbraucherzentrale schwer verständliche und unklare Datenschutzerklärung zu Windows 10, auf deren Grundlage jeder Windows-Nutzer in zahlreiche Datenübertragungen einwilligen soll.

Die Datenschutzerklärung von Microsoft differenziert nach Diensten und verlinkt jeweils auf unterschiedliche Informationsquellen. Dabei ist für den Nutzer kaum zu erkennen, welche Datenkategorien zu welchen Zwecken unter welchen Umständen erhoben und verarbeitet werden. Andererseits handelt es sich bei Windows 10 um ein komplexes System von verschiedensten Diensten und Funktionen; sämtliche hierbei anfallenden Datenerhebungen in einer kurzen, hervorgehobenen Erklärung darzustellen und dabei alle einwilligungsrelevanten Informationen zu vermitteln dürfte der Quadratur des Kreises gleichkommen.

Auch wenn ein gesteigerter Sanktionsdruck bezüglich der Verarbeitungstransparenz wünschenswert ist, so ist in diesem konkreten Fall jedoch auch zu hoffen, dass er nicht zum Auftakt einer Abmahnwelle wird, die auf konfligierenden Gesetzesanforderungen fußt und auch bemühte Anbieter erfasst.

Hackers Contest

Im Rahmen der von TippingPoint im Jahr 2005 gegründeten Zero Day Initiative, die Security-Forscher mit Preisgeldern für gefundene Schwachstellen belohnt, fand am 16. und 17.03.2016 der Pwn2Own-Contest 2016 in Vancouver statt. Dabei lobten HP und Trend Micro hohe Preise für diejenigen aus, denen es gelingen sollte, Systeme über die aktuellen Versionen von Google Chrome, Microsoft Edge, Adobe Flash oder Apple Safari mittels *Zero Day Exploits* zu übernehmen. Die Teilnehmer deckten insgesamt 21 kritische Sicherheitslücken auf – und reisten mit Prämien in Höhe von insgesamt 460.000 $ ab. Allein 145.000 $ strich der erfolgreichste Teilnehmer, der Südkoreaner Jung Hoon Lee ein: Ihm gelang die Übernahme von Google Chrome in weniger als zwei Minuten. Schon im vergangenen Jahr war er als Sieger aus dem Contest hervorgegangen und mit einer Gesamtprämie in Höhe von 225.000 $ zurückgekehrt.

Der Wettbewerb zeigt den Herstellern jährlich die Grenzen ihrer Softwareentwicklung auf – und macht eindrucksvoll deutlich, dass es, allen Anstrengungen zum Trotz, mit deren Qualität noch längst nicht zum Besten bestellt ist.

No-Spy-Klausel

Am 16.03.2016 hat der IT-Planungsrat – das zentrale Gremium zur Koordination der Informationstechnik zwischen Bund und Ländern nach Art. 91c GG – in ihre Standard-Beschaffungsverträge die Zusicherung des Auftragnehmers aufgenommen, dass erworbene Hardware „frei von Funktionen ist, die die Integrität, Vertraulichkeit und Verfügbarkeit der Hardware, anderer Hardware und/oder Software oder von Daten gefährden". Eine entsprechende Formulierung hatte der IT-Planungsrat bereits am 16.07.2015 in die Vertragsbedingungen für die Beschaffung und Pflege von Standardsoftware aufgenommen.

Ein wichtiger Schritt um Softwarehersteller dazu zu bewegen, Sicherheitsaspekten eine höhere Priorität einzuräumen.

Datenschutz via Kartellrecht

Am 02.03.2016 teilte das Bundeskartellamt mit, dass ein Verfahren gegen Facebook Inc., Facebook Ltd. und Facebook Germany GmbH wegen „Konditionenmissbrauchs" eingeleitet wurde: Es bestehe ein Anfangsverdacht, dass Facebook seine marktbeherrschende Stellung auf dem Gebiet der sozialen Netzwerke zur Durchsetzung rechtswidriger Datenschutzklauseln verwendet. Anlass ist die Einwilligung in die Datenverarbeitung bei der Nutzerregistrierung, die sich auf die als Fragenkatalog gestalteten Datenschutzrichtlinien bezieht. Darin wird nur sehr ungenau beschrieben, welche Daten in welchem Umfang verarbeitet und an Dritte weitergegeben werden.

Das Kartellamt kann nach eigener Auffassung selbständig datenschutzrechtliche Verstöße feststellen und Anordnungen zur Beseitigung oder Bußgelder von bis zu 10% des Jahresumsatzes verhängen.

Ob es tatsächlich zu einem Bußgeld kommt und dieses auch einen anschließenden Rechtsstreit übersteht, ist noch eine offene Frage. Im Erfolgsfall ist der Ansatz jedoch angesichts der Sanktionsmöglichkeiten des Kartellamtes (§ 32 ff GWB) ein starkes Druckmittel, Transparenz und die Einhaltung von Datenschutzgrenzen bei großen, internationalen Anbietern zu erzwingen. Voraussetzung dafür ist jedoch eine sorgfältige Marktdefinition, um deren marktbeherrschende Stellung bei bestimmten Angeboten nachzuweisen.

Secorvo News

CfP T.I.S.P. Community Meeting

In Frankfurt treffen sich vom **10. bis 11.11.2016** 150 IT-Sicherheitsexperten der deutschen Wirtschaft zum Erfahrungsaustausch beim 10. *T.I.S.P. Community Meeting*. Noch bis zum 18.04.2016 können Vortragsvorschläge eingereicht werden.

PKI für Praktiker

Unsere PKI-Schulung vom **19. bis 22.04.2016** bündelt die Expertise und Erfahrung aus 19 Jahren aktiver Gestaltung von Public Key-Infrastrukturen. Hier die Einschätzung eines der über 300 Teilnehmer: „*Das PKI-Seminar bei Secorvo hat mir durch seine thematische Breite bei gleichzeitig gut durchdachter Struktur alle notwendigen Kenntnisse und Werkzeuge an die Hand gegeben, die mich in die Lage versetzen, auch künftigen PKI-Anforderungen unserer Organisation zu begegnen.*" Wir freuen uns, Sie auf dem Seminar zu begrüßen (Anmeldung).

CPSSE-Zertifikat

Auf unserer Schulung zum Certified Professional for Secure Software Engineering (CPSSE) vom **11. bis 14.04.2016** in Karlsruhe lernen Sie, wie Sie bereits bei der Code-Entwicklung Schwachstellen gezielt vermeiden. Dazu eine Teilnehmerstimme: „*Ich kann das Seminar nur weiterempfehlen. Hervorheben möchte ich neben der Kompetenz der Vortragenden die angenehme und inspirierende Atmosphäre und die dadurch ermöglichten Diskussionen, die wesentlich zum Verständnis der Problematik beitragen und motivieren, sich weiter mit dem Thema auseinanderzusetzen.*" Wir freuen uns auf Ihre Anmeldung.

T.I.S.P.-Zertifikat

Vom **06. bis 10.06.2016** gibt Ihnen die Schulung zum T.I.S.P. einen umfassenden und themenübergreifenden Überblick über die aktuell wichtigsten Gebiete der Informationssicherheit. Mit der anschließenden Prüfung können Sie das anerkannte T.I.S.P.-Zertifikat erwerben und damit Ihr Expertenwissen dokumentieren.

Anti-Prism-Party #4

Zum Abschluss der Ausstellung „Global Control and Censorship" des ZKM | Karlsruhe lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL) und dem CyberForum e.V. am **Freitag, 29.04.2016 ab 16 Uhr** zur 4. Staffel der Anti-Prism-Party (Eintritt frei).

Dort zeigen Experten, wie Sie sich vor Ausspähung im Internet schützen können. Es gibt Live-Vorführungen zu den Themen „Sicheres Surfen", „Sicher kommunizieren" und „Sichere Kommunikation im Karlsruher Public WLAN". Vertiefte IT-Kenntnisse sind nicht erforderlich, um den anschaulichen Vorführungen folgen zu können. Sie können sich von Experten individuell beraten lassen und die Erläuterungen im Workshop „E-Mail-Verschlüsselung" direkt am eigenen Laptop umsetzen. Derweil werden Ihre Kinder in der Spion-Schule von der Pädagogischen Hochschule Karlsruhe zu Verschlüsselungsexperten ausgebildet.

Um 18:30 Uhr schließt die Veranstaltung mit einem offenen Diskussionsforum unter Mitwirkung des Datenschutz-Aktivisten Malte Spitz. Nähere Informationen und das Programm zur 4. Staffel der Karlsruher Anti-Prism-Party finden Sie auf der Webseite www.anti-prism-party.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2016	
04.-07.04.	T.E.S.S. - TeleTrusT Engineer System Security (Secorvo, Karlsruhe)
05.04.	Security Sells (CyberForum, Karlsruhe)
11.-14.04.	CPSSE - Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe)
19.-22.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
21.04.	Dumm. Dümmer. DAU? (KA-IT-Si, Karlsruhe)
27.-28.04.	17. Datenschutzkongress (EUROFORUM, Berlin)
29.04.	Anti-Prism-Party 4. Staffel (KA-IT-Si, Karlsruhe)
Mai 2016	
30.05.-01.06.	IFIP SEC 2016 (IFIP, Hamburg)
Juni 2016	
06.-10.06.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
13.-14.06.	DuD 2016 (Computas, Berlin)
22.06.	8. Tag der IT-Sicherheit (KA-IT-Si, Karlsruhe)

Fundsache

Das Nationale IT-Lagezentrum des BSI hat angesichts der zunehmenden Verbreitung von Ransomware am 11.03.2016 ein Dokument mit Empfehlungen zur Prävention und Reaktion herausgegeben. Inhaltlich wenig Überraschendes, aber eine gute Zusammenfassung.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, Michael Knopp.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2016



Time is money

Die ungebremste Beschleunigung unserer Arbeitswelt, die inzwischen sogar unser Privatleben vereinnahmt, beklagen wir nicht erst seit der Verbreitung des Smartphones (nanu, da ist ja ein „Aus"-Knopf?!). Sie erfasst nun auch die dunkle Seite des Internet: Cyber-Angriffe werden zum stressigen Unterfangen. Die internationale Kooperation und die Nachrüstung von Strafverfolgungsbehörden, Richtern und Staatsanwälten in Sachen IT-Know-How beginnen offenbar Früchte zu tragen. Wer eine Attacke startet, muss heute mit koordinierter und energischer Gegenwehr rechnen: Maliziöse Systeme werden vom Netz getrennt, kriminelle Gruppen ausgehoben.

Zwar lässt sich mit *flux networks*, in denen durch schnelle Änderungen der IP-Konfigurationen das Abkoppeln der Angriffssysteme erschwert wird, etwas Zeit gewinnen – doch wie im echten Leben gilt es nun auch im virtuellen Raum, den kriminellen Zugriff möglichst kurz zu halten. Oft bleibt nur ein Zeitfenster von wenigen Stunden, manchmal sogar Minuten, um von einem Phishing-, Verschlüsselungs- oder DoS-Angriff zu profitieren. Während der Vorbereitungsaufwand für einen erfolgreichen Angriff steigt, sinkt mit der Verkleinerung des Zeitfensters dessen Profitabilität.

Sicherlich darf man trotzdem in naher Zukunft nicht darauf hoffen, dass blanke Not die Cracker zu Gutmenschen mutieren lässt. Denn noch finden sie ausreichend Nahrung: Lange nicht jedes Unternehmen hat seine Hausaufgaben ordentlich gemacht. Und ist erst der gesamte Fileserver verschlüsselt, steigt die Zahlungsbereitschaft meist mit Lichtgeschwindigkeit.

Sollte die Entwicklung so weitergehen, könnte sich dennoch am Horizont ein wenig Licht abzeichnen. Vielleicht genügt es ja eines Tages, nicht jede ankommende E-Mail sofort zu öffnen.

Das wäre zugleich ein kleiner Beitrag zur Entschleunigung – der vielleicht auch einfach mal so gut tun würde.



Inhalt

Time is money

Security News

Anti-Ransomware

Volksverschlüsselung über Nacht

Paranoia als Sorgfaltspflicht?

Forensische Jagd

Standardisiertes Löschen

Durch Wiederholung richtig?

Datenschutzgrundverordnung

Secorvo News

Zertifikat für Experten

Auslaufmodell Datenschutz?

Save the date - 8. Tag der IT-Sicherheit

Veranstaltungshinweise

secorvo
security consulting

Security News

Anti-Ransomware

Fast täglich tauchen neue, immer ausgeklügeltere Varianten von Verschlüsselungstrojanern (*Ransomware*) auf – auch in kritischen Infrastrukturen, wie heise.de am 18.02.2016 berichtete. Anti-Viren-Programme helfen nicht dagegen: Die Schadsoftware wird oft erst Tage später erkannt.

Was lässt sich dagegen tun? Neben einem Backup, das im Katastrophenfall die Wiederherstellung unzugänglich verschlüsselter Daten erlaubt, erreicht man nachhaltigen Schutz nur durch einen zurückhaltenden Umgang mit Schreib- und Ausführungsrechten. Will man den Schaden für Dateien auf Fileservern begrenzen, benötigt man ein differenziertes und restriktives Rechte- und Rollenkonzept, das Benutzern nur die Schreibzugriffe einräumt, die sie tatsächlich benötigen. Auch sollten Anwender nie mit administrativen Rechten auf externe Daten (Webseiten, E-Mail-Anhänge, USB-Stick-Inhalte) zugreifen.

Zusätzlich ist zu empfehlen, via AppLocker über Gruppenrichtlinien einzuschränken, welche Dateien ausgeführt werden dürfen, und das Aktivieren von Ransomware auf allen Systemen zu unterbinden. Auch eine Einschränkung von Skriptsprachen wie Powershell oder CScript sollte in Betracht gezogen werden. Zum Schutz vor Office-Makros bietet sich auch die Verwendung vertrauenswürdiger Speicherorte an. Nicht zuletzt sollten die Anwender mit geeigneten Security Awareness-Maßnahmen für die Risiken sensibilisiert werden, damit sie in Zweifelsfällen fragen, bevor sie eine Schadsoftware aktivieren.

Volksverschlüsselung über Nacht

Am 05.04.2016 poppte in WhatsApp-Chats auf Millionen Smartphones die Nachricht auf: Ab sofort seien alle Nachrichten und Anrufe mit dem Gesprächspartner Ende-zu-Ende verschlüsselt.

Bei aller berechtigter Kritik an WhatsApp muss man vor dieser Maßnahme den Hut ziehen. Unter der Annahme, dass die Implementierung der Verschlüsselung ordentlich erfolgt ist (derzeit gibt es keinen Grund etwas Anderes anzunehmen – sie basiert auf dem anerkannten TextSecure-Protokoll), wurde über Nacht ein immenser Gewinn für die Privatsphäre von Millionen Menschen geschaffen. Die Umsetzung ist unkompliziert: Schlüsselerstellung und -austausch erfolgen automatisch. Zusätzlich kann eine Sicherheitsnummer (QR-Code) abgeglichen werden, um den Gegenüber zu authentifizieren. Diese Funktion ist allerdings stiefmütterlich platziert – offenbar sind die Entwickler zu der (realistischen?) Einschätzung gelangt, dass die Authentifizierung die User ohnehin nicht interessiert.

Allerdings fallen nach wie vor Metadaten zuhauf an (wer kommuniziert wann mit wem?). Und weiterhin synchronisiert WhatsApp automatisch das Adressbuch – im Unternehmensumfeld in der Regel ohne Rechtsgrundlage. Daher sollten Unternehmen nicht dem Irrglauben verfallen, die geschäftliche Nutzung von WhatsApp sei durch die Verschlüsselung unbedenklich geworden.

Paranoia als Sorgfaltspflicht?

Geht es nach der Rechtsprechung steigt die Awareness der Durchschnittsnutzer offenbar stetig. Das Amtsgericht Frankfurt a. M. hat mit Urteil vom 24.03.2016 das Hereinfallen auf eine Phishing-Mail, die zur Mitteilung der Telefon-Banking-PIN verleitete, als grobe Fahrlässigkeit gewertet. Verschiedene Instanzgerichte und 2012 auch der Bundesgerichtshof haben die Herausgabe von TANs und PINs bereits als vom Nutzer zu verantworten qualifiziert, wenn die Bank zuvor auf die Gefahren durch Phishing hingewiesen und klargestellt hat, dass sie zu bestimmten Verhaltensweisen nicht auffordern wird. Bis Oktober 2009 haftete der Bankkunde bereits bei einfacher Fahrlässigkeit, danach wurde § 675v Abs. 2 BGB auf grobe Fahrlässigkeit beschränkt. Sie liegt vor, wenn die erforderliche Sorgfalt in besonders schwerem Maß verletzt wird und selbst naheliegende Überlegungen nicht angestellt werden. Angesichts der steigenden Qualität der Angriffe darf man jedoch bezweifeln, dass vom Durchschnittsnutzer generell erwartet werden kann, eine Phishing-Mail zu erkennen.

Forensische Jagd

Das Google Rapid Response Framework (GRR) ist ein bewährtes forensisches Werkzeug für die Analyse von Apple-, Windows- und Linux-Systemen. Im aktuellen Release 3.1 vom 16.04.2016 wurde die Möglichkeit ausgebaut, eine umfassende Jagd (*hunt*) über eine Gruppe von Zielsystemen durchzuführen, um die Existenz eines spezifischen Artefakts zu prüfen und optional auch Gegenmaßnahmen einzuleiten. Unter der Haube des GRR wurde die forensische Echtzeitanalyse in das am 05.04.2016 fertig gestellte Rekall V1.5 integriert, das jetzt auf den Capstone Disassembler umgestellt hat und dadurch ein sehr viel weiter gehendes Bild über die Ablaufstrukturen von Programmfunktionen liefert als das, was man bisher von einem forensischen *Incident Tool Framework* erwarten durfte. Wer GRR testen möchte, dem seien der aktuelle Docker Build oder die pre-build Binaries empfohlen. *Happy Hunting*!

Standardisiertes Löschen

Die „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ ist am 08.04.2016 als DIN 66398 erschienen und kann nun beim Beuth Verlag bezogen werden. Die Weiterentwicklung der Leitlinie Löschkonzept zu einer DIN-Norm wurde seit Ende 2013 von den Unternehmen Deutsche Bahn, Blancco, DATEV, Secorvo und Toll Collect gefördert (SSN 2/2014, SSN 1/2015 und SSN 9/2015). Ein großer Schritt für den Datenschutz: Nun gibt es einen Standard für die Festlegung von Löschfristen.

Durch Wiederholung richtig?

Das Landesarbeitsgericht Berlin-Brandenburg hat anlässlich eines Falls exzessiver Internetnutzung eines Arbeitnehmers sein Urteil von 2011 bekräftigt und die Stellung des Arbeitgebers als Telekommunikationsanbieter verneint. So sei der Arbeitnehmer bei erlaubter Privatnutzung kein Dritter, und es läge keine Erbringung von Telekommunikationsdiensten vor (§ 3 Nr. 10 TKG). Die Zulässigkeit der Auswertung des Browserverlaufsprotokolls stützt das Gericht auf § 32 BDSG. Die Speicherung sei zur Missbrauchskontrolle zulässig. Da der Arbeitnehmer das Protokoll beliebig löschen kann, ist allerdings bereits die Eignung fraglich.

Insgesamt überzeugt die Begründung des Gerichts auch bei dieser neuen Entscheidung nicht, da sich das Urteil weder argumentativ mit der Dritteigenschaft von Arbeitnehmern noch vollständig mit der datenschutzrechtlichen Qualifizierung von Browserverlaufsdaten auseinandersetzt. Unternehmen sollten daher auch weiterhin bei erlaubter Privatnutzung die Pflichten eines Telekommunikationsdiensteanbieters erfüllen.

Datenschutzgrundverordnung

Am 14.04.2016 hat als letzte Instanz auch das Europäische Parlament die Datenschutzgrundverordnung verabschiedet, die damit nach Veröffentlichung im Europäischen Amtsblatt in Kraft tritt und ab Mitte 2018 europaweit gelten wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich bereits am 07.04.2016 mit der Anpassung der deutschen Datenschutzgesetze auseinandergesetzt. Die Datenschutzbeauftragten fordern u. a. die Einführung eines Beschäftigtendatenschutzgesetzes (oder die Beibehaltung von § 32 BDSG), Beschränkungen für Gesundheitsdaten, die Normierung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit und die Beibehaltung des § 4f Abs. 1 BDSG zur Bestellpflicht eines bDSB.

Die Erklärung macht deutlich, dass auch mit der Grundverordnung noch lange keine Klarheit über die 2018 eintretende Rechtslage und die zu erwartenden Auswirkungen für Unternehmen besteht.

Secorvo News

Zertifikat für Experten

Wir können Ihnen noch einige wenige freie Plätze auf dem kommenden T.I.S.P.-Seminar vom **06. bis 10.06.2016** anbieten. Mit Ihrer Anmeldung erhalten Sie das T.I.S.P.-Begleitbuch zur Vorbereitung. Die nächste Gelegenheit zur Zertifizierung bieten wir dann erst wieder im November – der frühe Vogel bekommt den Platz …

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Auslaufmodell Datenschutz?

Zum Abschluss der Ausstellung "Global Control and Censorship“ lädt die KA-IT-Si zusammen mit dem ZKM | Karlsruhe, KASTEL und dem CyberForum e.V. am **Freitag, 29. April 2016 ab 16 Uhr** zur größten Anti-Prism-Party Europas (4. Staffel) ins ZKM (Eintritt frei). Experten zeigen in Live-Vorführungen und an Beratungsständen, wie Sie sich vor Ausspähungen im Internet schützen können; begleitet von Führungen durch die Ausstellung. Derweil können sich Ihre Kinder in der Spion-Schule der Pädagogischen Hochschule Karlsruhe zum Verschlüsselungsexperten ausbilden lassen.

Gibt es überhaupt Chancen, der allgegenwärtigen Überwachung zu entgehen? Ist das Konzept „Datenschutz“ gar ein Auslaufmodell? Diese Fragen möchten wir um **18:30 Uhr** im Medientheater des ZKM mit Ihnen und dem Datenschutz-Aktivisten Malte Spitz in einer Publikumsdiskussion erörtern.

Programm: https://www.anti-prism-party.de

Save the date - 8. Tag der IT-Sicherheit

Auf dem „Tag der IT-Sicherheit“, einer Veranstaltung von KA-IT-Si, IHK Karlsruhe und CyberForum, zeigen wir einmal jährlich aktuelle IT-Sicherheitsbedrohungen für Unternehmen auf und informieren über Präventionsmöglichkeiten. Unser diesjähriger *Keynote Speaker* ist Tobias Schrödel, IT-Sicherheitsexperte und erster Comedyhacker. Das Programm finden Sie auf unserer Webseite. Merken Sie sich den **22.06.2016, 14 Uhr** schon jetzt in Ihrem Terminkalender vor.

Wir empfehlen eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2016	
08.-12.05.	Eurocrypt 2016 (IACR, Sofia/BG)
30.05.-01.06.	IFIP SEC 2016 (IFIP, Hamburg)
Juni 2016	
06.-10.06.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.06.	IT-Sicherheitsrisiken managen: Hürden und Möglichkeiten (Fachgruppe SECMGT der GI, Frankfurt)
10.-11.06.	AREA41 Security Conference (DC4131 DEFCON Switzerland, Zürich/CH)
13.-14.06.	DuD 2016 (Computas, Berlin)
15.-17.06.	Entwicklertag 2016 (VKSI, GI, ObjektForum, Karlsruhe)
22.06.	8. Tag der IT-Sicherheit (KA-IT-Si, Karlsruhe)
27.06.-01.07.	OWASP AppSec EU 2016 (OWASP Foundation, Rom/I)
Juli 2016	
30.07.-04.08.	Blackhat USA 2016 (Blackhat, Las Vegas/US)
August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Dr. Volker Hammer, Kai Jendrian, Michael Knopp, Christoph Schäfer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Mai 2016



Vom Aushalten

Ein Login ohne Passwort? Eine EC-Karte ohne Geheimnummer? Online-Banking ohne PIN/TAN? Informationstechnik ohne Schutzmaßnahmen ist heute undenkbar.

Beim Zugriff auf Daten von Kriminellen wird aus dem Schutz jedoch ein Ermittlungshindernis. Am 21.04.2016 gestand Direktor James Comey der Washington Post, dass das Knacken des Smartphones des San-Bernardino-Mörders dem FBI über 1,3 Mio. US$ wert war – mit einem Programm, das eine Schwachstelle im iOS ausnutzte, die nur beim iPhone 5c funktionierte. Da selbst das FBI (Etat: 8,7 Mrd. US$) Hacks auf alle Smartphone-Modelle (sofern überhaupt möglich) nicht bezahlen könne, fordert Comey von den Herstellern direkten Datenzugriff. Wie könnte das funktionieren? Zwei Ansätze gibt es dafür: Entweder durch eine Hintertür in der Software oder durch Hinterlegung der kryptografischen Schlüssel.

Beide Ansätze sind keine gute Idee. Informationen über Hintertüren verbreiten sich rasch – die Listen der BIOS-Master-Passwörter zur Umgehung des Bootschutzes sind legendär. Das weiß auch das FBI: Seit Mitte 2015 kursieren 3D-Druckvorlagen der sieben Master-Schlüssel für TSA-Kofferschlösser, die angeblich nur Zollbeamten zugänglich sind. Auch gelingen immer wieder Angriffe auf hinterlegte Schlüssel – wie die Kompromittierung des SecureID-Root-Keys von RSA vor fünf Jahren (SSN 03/2011). Der 1993 von der Clinton-Regierung entwickelte *Escrowed Encryption Standard*, nach dem die Verschlüsselungsschlüssel verschlüsselt mitgesendet bzw. -gespeichert werden sollten, scheiterte an einem Protokollfehler. Die Erfahrung lehrt: Sichere Verschlüsselung muss frei von Hintertüren sein – und Schlüssel dürfen nicht zentral gespeichert werden.

Wenn wir die Sicherheit unserer Informationstechnik insgesamt nicht aufs Spiel setzen wollen, bleibt uns daher nur, es auszuhalten, dass auch Kriminelle Daten so verschlüsseln können, dass kein Strafverfolger darauf zugreifen kann.



Inhalt

Vom Aushalten

Security News

Wette auf fallende Kurse

Kritische Anlagen

Ad-hoc-Meldung

Spionagetools statt Gold

Investition im Keksmarkt

Haftung bleibt

Secorvo News

Aktuelle Entwicklungen

T.I.S.P.

8. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Wette auf fallende Kurse

In letzter Zeit häufen sich wieder Meldungen zu Schwachstellen in Sicherheitssoftware: Betroffen waren u. a. Virenschutzprogramme von Symantec, (16.05.2016), SSL-Proxies von Jugendschutzfiltern mehrerer Hersteller (20.12.2015) und die Management-Software von Lenovo (26.04.2016). Diese Programme sollen die Sicherheit verbessern – schaffen aber durch Schwachstellen selbst neue Angriffspunkte.

Generell gilt: Ganz gleich, welche Art von Software man einsetzt, immer erhöht man dadurch die Wahrscheinlichkeit von Schwachstellen. Bei Sicherheitssoftware stellen sie meist eine besondere Gefahr dar, da diese oft mit privilegierten Rechten arbeitet. So mancher Benutzer wiegt sich daher mit solchen Programmen in trügerischer Sicherheit.

Schon vor zwei Jahren berichteten wir über Schwachstellen, die man sich durch den Einsatz von Virenschutz- und Monitoring-Agenten erst einhandelt (SSN 05/2014). Manchmal ist weniger mehr: Ein wenig Awareness dafür, worauf man bei der Internetnutzung achten sollte, ist womöglich eine bessere Investition als ein technischer Filter – der neue Viren ohnehin erstmal nicht erkennt und zudem womöglich Schwachstellen enthält.

Das dabei gesparte Geld sollte man vielleicht Gewinn bringend auf fallende Aktienkurse ausgewählter Hersteller von Sicherheitssoftware setzen.

Kritische Anlagen

Weitgehend unverändert ist der Referentenentwurf der ersten Verordnung zum Anwendungsbereich des IT-Sicherheitsgesetzes am 03.05.2016 in Kraft getreten. Ergänzt wurde die Behandlung von miteinander verbundenen kritischen Anlagen. Das Prinzip, den Versorgungsgrad als Maß für die Kritikalität einer Anlage heranzuziehen (SSN 02/2016), ist geblieben – die Gefährdung der öffentlichen Sicherheit durch Fehlfunktion einer Anlage bleibt bei der Einstufung weiterhin ausgeblendet.

Die Verordnung zu den Sektoren Finanzen, Transport, Verkehr und Gesundheit soll Anfang 2017 folgen. Zur Unterstützung der Entwicklung branchenspezifischer Sicherheitsstandards hat das BSI im Dezember eine Orientierungshilfe publiziert; bisher wurde jedoch noch kein Standard veröffentlicht.

Die Umsetzungsfrist für die Betreiber von in den Anhängen der Verordnung benannten Infrastrukturen läuft bis zum 03.05.2018. Bis dahin sind Investitionen in Anbieter rund um ISM-Systeme sicher keine schlechte Kapitalanlage.

Ad-hoc-Meldung

Am 03.05.2016 wurde gleich eine Handvoll schwerer Schwachstellen in der beliebten Bildbearbeitungssoftware ImageMagick veröffentlicht. Brisant sind diese Schwachstellen nicht nur wegen der Möglichkeit, beliebigen Code ausführen zu können, sondern auch, weil der ImageMagick-Code in zahlreichen Bibliotheken verwendet wird, ohne dass dies den Entwicklern bekannt sein dürfte: Nicht nur dort, wo ImageMagick draufsteht, ist ImageMagick drin.

Wer Anteile an ImageMagick hält, sollte sie nicht gleich abstoßen – denn bekanntlich ist auch schlechte Publicity gute Publicity. Aber man sollte den Fall zum Anlass nehmen, neben einem funktionierenden Patch-Management dafür zu sorgen, dass die in der Entwicklungsabteilung verwendeten (Open-Source-) Bibliotheken inventarisiert und der Umgang mit dazu veröffentlichten Schwachstellen geregelt wird.

Spionagetools statt Gold

Spätestens seit der Veröffentlichung der Panama Papers sind kreative neue Möglichkeiten der Geldanlage gefragt. Die Bundesnetzagentur will helfen und sagte am 25.04.2016 Spionagekameras den Kampf an: Seitdem ist es verboten, WLAN-Kameras anzubieten oder zu besitzen, die in Alltagsgegenständen wie beispielsweise Kugelschreibern oder Rauchmeldern versteckt sind. Die BNetzA geht gegen Hersteller, Verkäufer und Käufer vor und verlangt die Vernichtung der Gegenstände – nach eigenen Angaben bisher in rund 70 Fällen.

Nicht bekannt ist, ob auch Organisierte Kriminalität und Nachrichtendienste zu den Betroffenen zählen – und warum andere „hilfreiche" Tools wie sendende Keylogger oder spionierende Hotspots nicht unter den Bann fallen.

Dennoch ist jetzt der richtige Zeitpunkt, um schnell noch in Restbestände von Spionagekameras zu investieren und diese vom benachbarten Ausland über einschlägige, nicht-deutsche Online-Shopping-Plattformen zu vertreiben.

Investition im Keksmarkt

Cookies sind ein geliebtes Feindbild des Datenschutzes – kein Grund allerdings, Investitionen im Keksmarkt zu reduzieren. Denn die am 24.05.2016 in Kraft getretene Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, DSGVO) bringt keineswegs die vielerorts erhoffte Klarheit.

Während der Bundesinnenminister mehr Flexibilität fordert, da personenbezogene Daten schließlich „nicht um ihrer selbst willen schützenswert“ seien, weisen Experten auf strukturelle Probleme der DSGVO hin, u. a. ihre Unterkomplexität. Es bleibt eine große Unsicherheit, denn die in zwei Jahren unmittelbar geltenden Regelungen enthalten eine Vielzahl von Öffnungsklauseln. Manche stellen einen konkreten Handlungsauftrag an den nationalen Gesetzgeber: Das BDSG wird durch ein Nachfolgegesetz ersetzt werden müssen. Umgekehrt werden viele Regelungen, die Datenverarbeitungen bisher legitimieren, aufgrund fehlender Öffnungsklauseln schlicht wegfallen, so z. B. Teile des § 28 BDSG zur werblichen Nutzung personenbezogener Daten.

Da viele Datenschützer den Besuch eines der unzähligen Seminarangebote zur DSGVO einer Lektüre der 187-seitigen Broschüre der BfDI vorziehen dürften, ist in den nächsten Monaten mit einem Anstieg des Kekskonsums zu rechnen – Cookies hin oder her. Wer sich die Seminarkosten angesichts der herrschenden Unklarheit über die finale Rechtslage spart, sollte daher über eine Aufstockung seiner Investitionen im Keksmarkt nachdenken.

Haftung bleibt

Folgt man der Euphorie der Medien, ist die Störerhaftung für offene WLANs schon so gut wie begraben. Tatsächlich hat sich die Bundesregierung am 10.05.2016 auf eine Entschärfung eines vom September 2015 stammenden Gesetzesentwurfs zur Änderung des Telemediengesetzes geeinigt.

§ 8 Abs. 4 des ursprünglichen Entwurfs sah verschiedene Pflichten für Anbieter von WLAN-Hotspots vor. Diese sollen nun entfallen und Anbieter offener WLANs vollständig Zugangsanbietern gleichgestellt werden, die bereits heute nach § 8 TMG ein Haftungsprivileg genießen. Ursache des Sinneswandels ist unter anderem der Schlussantrag des Generalanwalts am EuGH vom 16.03.2016, der diese Gleichstellung auf Basis von Art. 12 der E-Commerce-Richtlinie vornimmt.

Der Schlussantrag lässt jedoch genau wie das BGH-Urteil vom 26.11.2015 den Weg zu Sperranordnungen offen. Die Rechtsprechung wendet das Haftungsprivileg zudem bislang nicht auf zukunftsgerichtete Unterlassungsansprüche an. Daran ändert auch die neue Einigung nichts. Der Schlussantrag kommt allerdings zu dem Ergebnis, dass Anbietern keine Abmahnkosten auferlegt werden dürfen. Von einer Abschaffung der Störerhaftung kann also kaum die Rede sein.

Investitionen in Musik- und Filmverlage sollte man daher nicht gleich abstoßen – hingegen lohnt es weiterhin, in Anbieter von Sperrsoftware und auf Urheberrechtsfragen spezialisierte Rechtsberatungen zu setzen.

Secorvo News

Aktuelle Entwicklungen

Auch die Informationssicherheit wird von der Schnelllebigkeit technischer Entwicklungen nicht verschont. Auf dem Seminar „IT-Sicherheit heute“ (**27.-29.09.2016**) greifen wir aktuelle Entwicklungen und neue Themen auf, um eine Hilfestellung beim Nachjustieren von Sicherheitskonzepten und Schutzmaßnahmen zu bieten. Das Programm des Seminars wird ständig aktualisiert.

T.I.S.P.

Anfang des Jahres 2017 dürfte die 1.000er-Marke fallen – so viele IT-Sicherheitsexperten haben inzwischen das T.I.S.P.-Zertifikat zum Nachweis ihrer fachlichen Qualifikation erworben. Der Erfolg des T.I.S.P. lässt sich nicht nur an der großen Nachfrage ablesen, sondern auch an der Bedeutung, die Stellenanzeigen im Bereich der IT- und Informationssicherheit dem Zertifikat einräumen.

Wer das T.I.S.P.-Seminar bei Secorvo besucht, erhält zur Vorbereitung das Begleitbuch zum T.I.S.P., ein 700seitiges Lehr- und Lernbuch sowie Nachschlagewerk zu den zentralen Themen der Informationssicherheit. Das nächste T.I.S.P.-Seminar mit freien Plätzen findet vom **21. bis 25.11.2016** statt. Programm und Online-Anmeldung unter https://www.secorvo.de/college.

8. Tag der IT-Sicherheit

Der Karlsruher Tag der IT-Sicherheit, den die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) in Zusammenarbeit mit dem CyberForum e.V. und der IHK Karlsruhe austrägt, beschäftigt sich in diesem Jahr zum achten Mal mit aktuellen IT-Sicherheitsherausforderungen für Unternehmen. Er macht deutlich, wie wichtig ein professioneller Umgang mit den Themen IT-Sicherheit und Datenschutz ist und informiert über Präventionsmöglichkeiten. Diesjähriger Keynote Speaker ist Tobias Schrödel, IT-Sicherheitsexperte und erster „Comedyhacker“. Die Fachvorträge beschäftigen sich u. a. mit den Themen Cybercrime und Industrial Security im Produktionsumfeld. Das Programm schließt mit einem Live-Hacking und bietet Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern.

Die Veranstaltung findet am **22.06.2016** im Saal Baden der IHK Karlsruhe statt. Das Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2016	
06.-10.06.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.06.	IT-Sicherheitsrisiken managen: Hürden und Möglichkeiten (Fachgruppe SECMGT der GI, Frankfurt)
10.-11.06.	AREA41 Security Conference (DC4131 DEFCON Switzerland, Zürich/CH)
13.-14.06.	DuD 2016 (Computas, Berlin)
15.-17.06.	Entwicklertag 2016 (VKSI, GI, ObjektForum, Karlsruhe)
22.06.	8. Tag der IT-Sicherheit (KA-IT-Si, Karlsruhe)
27.06.-01.07.	OWASP AppSec EU 2016 (OWASP Foundation, Rom/I)
Juli 2016	
30.07.-04.08.	Blackhat USA 2016 (Blackhat, Las Vegas/US)
August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)

Fundsache

Der Landesbeauftragte für den Datenschutz Baden-Württemberg hat am 22.04.2016 einen 27-seitigen Leitfaden für Datenschutzeinstellungen bei Windows 10 herausgegeben, der empfehlenswerte Grundkonfigurationen Schritt für Schritt erläutert.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Juni 2016



Glückliche Sklaven

Während sich der von der Safe-Harbor-Entscheidung des EuGH vom 06.10.2016 aufgewirbelte Staub langsam legt, die ersten Aufsichtsbehörden Bußgeld-Bescheide verschicken und sich die EU beeilt, via Privacy Shield-Abkommen eine neue Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA zu zimmern, erreicht die heimliche Überwachung neue Dimensionen.

Anfang der 2000er Jahre schossen sich Datenschützer auf die Nutzung von Cookies als Tracking-Instrument ein. Darauf reagierte die EU am 25.11.2009 mit der Verabschiedung einer (wenig universellen) „Cookie-Richtlinie“, die eine Einwilligung der Benutzer fordert. Sie ist bis heute in vielen EU-Staaten nicht umgesetzt; Verstöße werden nicht geahndet. Derweil wichen Google & Co. auf andere, weit ergiebigere Methoden zur Gewinnung von Internet-Nutzungsdaten aus: Mit „kostenlosen“ Service-Angeboten spannten sie Webseitenbetreiber vor ihren Karren. Mit Erfolg: Das Webseiten-Analysetool Google Analytics erreichte einen Marktanteil von über 90%, bevor es in den Fokus von Datenschützern geriet, denen die Datensammelei von Marketingabteilungen ohnehin ein Dorn im Auge war.

Während sich Datenschützer an Google Analytics und Social Media Plugins festbissen, zündeten Google & Co. ein Feuerwerk an Angeboten für Webentwickler, die diese bereitwillig in ihren Code einbetteten. Kaum eine Webseite, die kein Javascript- oder CSS-Framework und keinen Web-Font nachlädt – und dabei die Nutzerdaten bei Facebook, Google oder Twitter abliefert. Schließlich erfand Google die Safe Browsing-API, die jeden Seitenaufruf anhand einer Google-Blacklist auf enthaltene Schadsoftware prüft. Inzwischen Teil von Firefox, Safari und Chrome meldet die API jeden Webseitenaufruf von einer Milliarde Nutzern an Google. Microsoft wollte da nicht zurückstehen führte im IE8 den SmartScreen-Filter ein. Ein genialer Coup. Denn die erbittertsten Feinde der Freiheit sind bekanntlich die glücklichen Sklaven.



Inhalt

Glückliche Sklaven

Security News

Heimlich, still und leise

Versteckter Tracing Code

Smart Spy

Unsichere Updates

Seitenkanäle im PC

Secorvo News

IT-Sicherheit heute

Who is who?

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Heimlich, still und leise

Google Analytics und Social-Media-Plugins sind immer wieder für eine Aufregung gut – wie zuletzt anlässlich der Bußgeldbescheide der Datenschutz-Aufsichtsbehörde Hamburg vom 06.06.2016. Technisch sind beide inzwischen Nebenkriegsschauplätze der großflächigen Erhebung von Metadaten. Die erfolgt mittlerweile – heimlich, still und leise – durch Web-Entwickler-Tools, die sich bisher weitgehend der Wahrnehmung von Datenschützern und Aufsichtsbehörden entziehen:

Bootstrap: Das von Twitter angebotene CSS-Framework erfreut sich großer Beliebtheit bei Webseitenbetreibern. Wird es jedoch nicht auf dem eigenen Server installiert, bekommt Twitter beim Online-Download die Nutzerdaten (IP-Adresse, besuchte Webseite und Zugriffszeitpunkt) frei Haus.

jQuery/Ajax: Eine Webseite zu finden, die ohne den Einsatz der freien JavaScript-Bibliothek auskommt, gleicht schon fast einem Wunder. Werden dabei die jQuery-Bibliotheken von Google nachgeladen, erhält Google die Nutzerdaten.

AngularJS: Genauso verhält es sich mit Googles JavaScript-Webframework. Eine lokale Installation ist aus Datenschutzgründen anzuraten, doch welcher Webdesigner macht das schon?

React: Facebook bietet mit React eine Alternative zu Angular – ein Webframework, das beim Nachladen die Nutzerdaten an Facebook übermittelt.

Web-Fonts: Annähernd jede moderne Webseite nutzt Web-Fonts von Google oder Adobe. In der Regel werden die Fonts dabei erst beim Seitenbesuch nachgeladen. Dabei wäre eine lokale Installation der Fonts problemlos möglich.

Kartendienste: Beliebt ist es auch, auf der Kontakt-Seite die Kartendienste von Google oder Bing Maps einzubinden. Auch hier liefert man dem Anbieter die Nutzungsdaten seiner Seitenbesucher. Mangels einer ähnlichen Lösung wie für die Social-Media-Plugins würde hingegen ein Link zum Kartendienst genügen – sofern man nicht gleich auf die freie Alternative OpenStreetMap setzen möchte.

No CAPTCHA reCAPTCHA: In den SSN 12/2014 berichteten wir über die Google-Version des Turing-Tests, bei der die IP-Adresse übermittelt und Mausbewegungen ausgewertet werden. Zumindest die DENIC setzt nach harscher Kritik im Netz inzwischen wieder auf eine alternative Lösung.

Viele Webseiten-Entwickler erliegen heute den Verlockungen kostenfreier Frameworks, Schriften etc. Die Übermittlung der Nutzungsdaten der Webseitenbesucher in die USA ist nach der Entscheidung des EuGH (SSN 10/2015) jedoch ohne einen Vertrag nach EU-Standardvertragsklauseln oder eine wirksame Einwilligung der Betroffenen rechtswidrig. Zumindest eine lokale Installation der Dienste ist daher geboten – auch wenn man sich anschließend selbst um das Patching kümmern muss.

Versteckter Tracing Code

Dank eines Beitrags im Diskussionsforum reddit wurde am 10.05.2016 bekannt, dass der C++-Compiler von Visual Studio 2015 ungefragt *Tracing Code* in kompilierte Anwendungen einbaut. Dabei handelt es sich um Telemetriedaten wie bestimmte Events und Zeitstempel, die an die Systemkomponente ETW (*Event Tracing for Windows*) weitergeleitet werden. Daraufhin sah sich Microsoft zu einer Stellungnahme gezwungen, in der angekündigt wurde, diese Funktion mit dem nächsten Update zu entfernen.

Auch wenn diese Daten nur lokal auf dem System gespeichert werden und nicht unmittelbar abfließen, ist es schon bedenklich, dass derartige Funktionen im Verborgenen injiziert werden. Schließlich ist es nahezu unmöglich nachzuvollziehen, ob das kompilierte Programm tatsächlich nur die gewünschte Funktionalität enthält. Beim Vertrauen in die eigesetzten Werkzeuge ist besondere Vorsicht geboten, wie schon Ken Thompson in seinem 1984 erschienenen Paper „Reflections on Trusting Trust“ aufzeigte.

Smart Spy

Groß war die Aufregung, als heise am 25.01.2014 SmartTVs als potentielle Spione im Wohnzimmer entlarvte. Über den Datendienst HbbTV können TV-Sender den Fernseher anweisen, eine bestimmte URL abzurufen – und zwar genau dann, wenn man den Sender einschaltet: Der Zählpixel der TV-Welt, mit dem sich das Fernsehverhalten der Nutzer protokollieren lässt. Eine senderübergreifende Auswertungsmöglichkeit mit Google Analytics versteht sich von selbst – Cookies finden nicht nur im PC, sondern auch im Fernseher Verwendung.

Neben den TV-Sendern lassen sich inzwischen auch die Hersteller smarter Fernsehgeräte mit Daten über den Nutzer beglücken. In einem Musterklageverfahren gegen die deutsche Samsung-Tochter konnte nun die Verbraucherzentrale Nordrhein-Westfalen am 10.06.2016 einen kleinen Sieg beim Landgericht Frankfurt am Main erringen (Az. 2-03 O 364/15): Auch wenn man die AGB und die über 56 Bildschirmseiten lange Datenschutzerklärung gele-

sen und abgelehnt hat, übermittelt ein Samsung-SmartTV die IP-Adresse des Nutzers an Samsung.

Das LG akzeptierte die Datenschutzbestimmungen wegen ihrer Länge und Unübersichtlichkeit nicht als wirksame Einwilligung. Da die Datenübermittlung jedoch nicht an die beklagte deutsche Samsung-Tochter, sondern an die Muttergesellschaft erfolgt, muss Samsung Deutschland nur seine AGB nachbessern. „Ob die Datenübermittlung in der konkreten Art und Weise rechtmäßig war, hatte die Kammer (...) nicht zu entscheiden" – schließlich gilt das BDSG nicht für Südkorea.

Unsichere Updates

Automatische Updates von Software beugen der Ausnutzung von Schwachstellen in veralteten und verwundbaren Programm-Versionen vor und stellen damit eine immer wieder empfohlene Schutzmaßnahme dar. Allerdings setzen viele Software-Hersteller ihre Nutzer durch automatische Update-Mechanismen unnötigen Gefahren aus, wenn der sensitive Update-Prozess über unverschlüsselte HTTP-Verbindungen erfolgt. So geschehen z. B. bei Intels Driver Update Utility (19.01.2016), ebenso bei Dell (23.11.2015) und bei Lenovo (31.05.2015). Sogar Sicherheitssoftware wie Keepass 2 (02.03.2016) ist verwundbar.

Erfolgt der Download nicht über TLS, können Angreifer mit einem Man-in-the-Middle-Angriff die übermittelten Updates *on the fly* mit Schadsoftware „anreichern". Die dafür benötigten Werkzeuge sind frei im Web verfügbar. Für die Nutzer ist die Manipulation eines Updates praktisch nicht zu erkennen. Wirksam schützen kann man sich davor nur, indem man unverschlüsselte Updates ausschließlich im eigenen, vertrauenswürdigen Netz zulässt.

Seitenkanäle im PC

Angriffe über so genannte Seitenkanäle, also nicht intendierte Informationswege wie das physische Verhalten eines Systems (Zeit, Stromverbrauch oder Arbeitsgeräusche), sind nichts grundsätzlich Neues. So wurden in der Vergangenheit Funker an der „Handschrift" ihrer Morsezeichen identifiziert oder Inhalte von Röhrenmonitoren über deren elektromagnetische Abstrahlung rekonstruiert.

Neu ist, dass über die Auswertung des Stromverbrauchs, des elektromagnetischen Felds oder der Geräuschentwicklung nicht nur geheime Schlüssel einer SmartCard (Paul Kocher, 1996), sondern auch aus einem modernen PC gewonnen werden können. Das belegen Daniel Genkin, Lev Pachmanov, Itamar Pipman, Adi Shamir und Eran Tromer in ihrem am 04.06.2016 in der Juni-Ausgabe der Communications of the ACM erschienenen Beitrag am Beispiel von Angriffen auf GnuPG – zwar unter optimierten Bedingungen, aber mit preiswertem Equipment aus gut 10 m Entfernung.

Will man Krypto-Software wirksam vor solchen Seitenkanalangriffen schützen, führt kein Weg an den bei Krypto-Hardware bereits üblichen Schutzmechanismen wie „Blinding" vorbei. Eine neue Herausforderung für Softwareentwickler.

Secorvo News

IT-Sicherheit heute

Für das Herbstseminar „IT-Sicherheit heute" sind noch letzte Plätze frei. Vom **27. bis 29.09.2016** bringen wir Sie auf den aktuellen Stand in den Bereichen Informationssicherheit, IT-Sicherheit und Datenschutz.

Neben Themen wie dem IT-Sicherheitsgesetz und der EU-Datenschutz-Grundverordnung stehen aktuelle Bedrohungen im Fokus: Gleich zu Seminarbeginn schlüpfen Sie in die Rolle von Angreifer und Verteidiger. Am dritten Seminartag (Hacking Day) zeigen Ihnen unsere Experten in Live-Hacks Angriffe mit Ransomware und PowerShell. Auch klassische Angriffsmethoden wie Spoofing und Man-in-the-Middle werden vorgestellt und es wird auf die Sicherheitslücken von Web-Anwendungen eingegangen. Zum Abschluss des Seminares dürfen Sie selbst Hand anlegen: Im WebGoat-Workshop nähern Sie sich Schritt für Schritt der Web-Security.

Wichtig für alle T.I.S.P.-Absolventen: Das Seminar wird als Weiterbildung für die Re-Zertifizierung anerkannt. Wir freuen uns auf Ihre Anmeldung.

Who is who?

Bei der Anmeldung an Ihrem Arbeitsplatzrechner müssen Sie sich authentisieren, d. h. Ihre Identität gegenüber dem System nachweisen. Das erfolgt heute in den meisten Fällen über die Eingabe Ihres Passworts.

Doch sind Passwörter noch zeitgemäß? Immer mehr Unternehmen setzen auf eine Zwei-Faktor-Authentifizierung (2FA). Bei unserer kommenden KA-IT-Si-Veranstaltung am **14.07.2016**, diesmal in den Räumen der Nexus Technology GmbH in Ettlingen, stellen Petra Barzin (Secorvo), Sandra Bialinski und Michael Leuchtner (Nexus) vor, welche 2FA-Alternativen es gibt und welche Stärken und Schwächen diese Lösungen besitzen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Weitere Infos und die Möglichkeit zur Anmeldung auf www.ka-it-si.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2016	
14.07.	Who is who? (KA-IT-Si, Karlsruhe)
30.07.-04.08.	Blackhat USA 2016 (Blackhat, Las Vegas/US)
August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)
10.-12.08.	25th USENIX Security Symposium (Usenix, Austin/US)
14.-18.08.	Crypto 2016 (IACR, Santa Barbara/US)
September 2016	
07.-08.09.	Annual Privacy Forum 2016 (ENISA, EC DG Connect, Goethe Universität, Frankfurt)
13.-15.09.	Future Security 2016 (Fraunhofer VVS, Berlin))
19.09.	Sommerakademie (ULD Schleswig-Holstein, Kiel)
26.-27.09.	D • A • CH Security (Gemeinsame Arbeitskonferenz von GI, OCG, BITKOM, SI, TeleTrusT, Klagenfurt)
27.-29.09.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)

Fundsache

Wer angesichts der zahlreichen Passwort-Leaks auf einen Passwort-Manager umsteigen will, dem sei dieser am 22.06.2016 veröffentlichte ausführliche Vergleich der wichtigsten Lösungen empfohlen.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2016



Wir täuschen uns vielleicht

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, (...) kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden“ (Volkszählungsurteil vom 15.12.1983). Wie wahr. Man stelle sich vor, ein Gesprächspartner kenne alle irgendwo über uns gespeicherten Daten: Die bargeldlosen Zahlungen mit Datum/Uhrzeit, die Bewegungsmuster, die das Navi übermittelt, die Schlüsselworte, nach denen wir gegoogelt und die Webseiten, die wir je besucht haben. Wir trösten uns damit, dass diese Daten ohne Weiteres nicht zugänglich sind. Und täuschen uns vielleicht.

Unseren Namen erfährt man über die Fahrzeughalterauskunft, die Adresse über das Einwohnermeldeamt und die Teilnahme an einer Sportveranstaltung über die Ergebnislisten im Internet. Wir trösten uns damit, dass selbst öffentlich zugängliche Daten in der Regel nur mit höherem Aufwand zu erfahren sind, den wohl kaum jemand auf sich nimmt. Und täuschen uns vielleicht.

Denn es gibt Menschen, die sich den Aufwand leisten – um zum Beispiel (Privat-)Insolvenzen über eine App in Google Maps sichtbar zu machen. Oder um zu zeigen, welcher Arzt unseres Vertrauens Zahlungen von Pharmaunternehmen erhält. Diese Apps ließen sich rechtskonform aufwerten, indem man die Vorstandstätigkeiten in Vereinen, die veröffentlichungspflichtigen Leitungsfunktionen in Unternehmen, die Jahresgehälter und Pensionsverpflichtungen von AG-Vorständen und Aufsichtsräten sowie die von ihnen verkauften Aktien ergänzte. Dazu die Einblendung eines aktuellen Fotos aus Facebook, die Angabe des Hochzeitstags aus der Bestellung des Aufgebots und Verweise auf die nächsten Verwandten z. B. aus einer Online-Traueranzeige. Wir trösten uns damit, dass der Gesetzgeber dem schon einen Riegel vorschieben wird. Und täuschen uns vielleicht.



Inhalt

Wir täuschen uns vielleicht

Security News

Malware Virenschutz

Ganz klein gelandet

PKI unter Zeitdruck

Gut gemeint

Stand der Technik

Datenschutz-Workaround

Lawful Access

Secorvo News

Spätsommerseminar

Penetrationstests

Encryption as a Service (EaaS)

Veranstaltungshinweise

secorvo
security consulting

Security News

Malware Virenschutz

Wie erneut ein aktueller Fall vom 28.06.2016 zeigt (siehe SSN 5/2014), verstecken sich auch in Virenschutzprodukten (diesmal: Symantec) Schwachstellen. Virenschutzsoftware muss man daher inzwischen auch als eine potentielle Gefährdung ansehen, zumal Angreifer über solche Schwachstellen privilegierte Rechte erhalten. Hinzu kommt, dass neue Schadprogramme erst mit mehreren Tagen Verzögerung erkannt und Heuristiken von geschickten Angreifern umgangen werden.

Werden Datenträger konsequent auf Viren geprüft und erfolgt die Datenübermittlung über zentrale Content Filter, sollte man daher darüber nachdenken, auf Fat-Clients und Servern ganz auf Virenschutz zu verzichten.

Wem die Virenfreiheit von Systemen zu bestimmten Zeitpunkten wichtig ist, sollte einen (schreibgeschützten und Firmware-signierten) „Virenschutz-Stick" z. B. mit dem vom heise-Verlag veröffentlichten Desinfec't verwenden, um damit stichprobenhafte Prüfungen durchzuführen.

Ganz klein gelandet

Am 17.06.2016 hat das zweite Gesetz zur Änderung des Telemediengesetzes den Bundesrat passiert. Die Änderungen nach fast 12-monatigem Gesetzgebungsverfahren und noch längerer Vordiskussion umfassen eine WLAN-Definition und § 8 Abs. 3, der klarstellt, dass Anbieter öffentlicher WLANs dem Haftungsprivileg für Access-Provider unterfallen. Ein geplanter Abs. 4, der auch Unterlassungsansprüche ausschließen sollte, wurde nicht aufgenommen.

Hotels und Anbieter von Gäste-WLANs oder Hotspots müssen nun keine Erklärungen ihrer Nutzer mehr einholen und auch keinen verschlüsselten Zugang anbieten. Abmahnungen wegen Rechtsverletzungen der Nutzer können den Anbieter jedoch weiter treffen, denn nach bisheriger Rechtsprechung sind diese vom Haftungsprivileg nicht umfasst. Dem steht nur die unverbindliche Gesetzesbegründung entgegen. Unsicherheit wird weiter die Frage schaffen, was ein zur Unterlassung verpflichteter Anbieter denn tun soll, um erneute Rechtsverstöße über sein WLAN zu verhindern.

PKI unter Zeitdruck

Erfolge erschaffen bekanntlich Neider - und finden oft Nachahmer. So veröffentlichte die israelische Firma StartCom Ltd. am 06.06.2016 ihr Produkt StartEncrypt, das viele Ähnlichkeiten mit dem sehr erfolgreichen Projekt LetsEncrypt aufweist. Kurz darauf wurden allerdings gravierende Sicherheitsprobleme aufgedeckt, sodass der Service am 04.07.2016 wieder eingestellt wurde – vorübergehend, wie es heißt, da man aus Zeitdruck nicht ausreichend getestet habe. Ein für ein Sicherheitsunternehmen besonders peinliches Eingeständnis.

Gut gemeint

Die Volksverschlüsselungs-Software, die die Fraunhofer Gesellschaft mit Unterstützung der Deutschen Telekom am 29.06.2016 in der aktuellen Version zum Download bereit gestellt hat, um Ende-zu-Ende E-Mail-Verschlüsselung auf Grundlage von S/MIME und PGP mit kostenlosen Zertifikaten für private Endanwender tauglich zu machen, ist gar keine Verschlüsselungslösung – sie kümmert sich allein um die Erzeugung und Einbindung des Public-Private-Schlüsselpaars.

Keine ganz neue Idee: Schon Anfang der 2000er Jahre hatte TC Trustcenter kostenlose S/MIME- und PGP-Zertifikate für Privatnutzer im Angebot.

Vor allem aber kombiniert sie die Nachteile offener und geschlossener PKIs: den aufwändigen Registrierungsprozess einer jedermann offenstehenden PKI mit der Beschränkung auf „mitspielende" Kommunikationspartner wie bei einer geschlossenen PKI.

Vielleicht sollte man lieber die vereinfachte Benutzerschnittstelle der Open-Source Volksverschlüsselungs-App mit einem Open-Source E-Mail-Client wie bspw. Thunderbird kombinieren – und auf die ebenfalls kostenlosen E-Mail-Zertifikate öffentlicher Trust Center wie Comodo oder StartCom zurückgreifen.

Stand der Technik

In Gesetzten und Verträgen wird von IT-Sicherheitsmaßnahmen häufig die Erfüllung eines „Stands der Technik" gefordert. Doch welche Maßnahmen genügen diesem Kriterium? Dieser Fragestellung hat sich der TeleTrusT-Arbeitskreis Stand der Technik angenommen. Am 26.05.2016 legte er eine "Handreichung zum Stand der Technik" im Sinne des IT-Sicherheitsgesetzes vor, die im Detail aufzeigt, welche Produkte und Technologien als etabliert betrachtet werden können.

Das mit viel Engagement erstellte Dokument bietet eine recht vollständige Aufstellung und erscheint nur in einzelnen Bereichen (wie den konkreten Anforderungen an sichere Softwareentwicklung oder die Sicherheit von Web-Applikationen) ergänzungswürdig, während das Thema „Datendiode" etwas überbewertet erscheint. Dennoch eine klare Leseempfehlung.

Datenschutz-Workaround

Die Europäische Kommission hat am 12.07.2016 ihre hoch umstrittene Angemessenheitsentscheidung (Art. 25 Abs. 6 Datenschutz-Richtlinie) zur Datenübermittlung in die USA auf Basis des sog. *EU-US Privacy Shield* erlassen. Diese Antwort auf die Safe-Harbor-Entscheidung des EuGH besteht aus mehreren Regelungsdokumenten, die die EU-Kommission mit verschiedenen US-Ministerien ausgehandelt hat, darunter Datenverarbeitungsprinzipien, Schiedsverfahren, Betroffenenrechte und ein erläuternder Anhang zur Datenschutz-Rechtslage in den USA. Zentraler Mechanismus ist weiter die freiwillige Selbstzertifizierung der US-Unternehmen, die personenbezogene Daten importieren; sie unterliegt staatlicher Aufsicht und Verstöße sollen sanktioniert werden.

Die Entscheidungsbegründung geht nur auf Basis der US-Darstellungen auf die Überwachungs- und Rechtsschutzpraxis ein; eine vom EuGH geforderte eigenständige Prüfung der objektiven Rechtslage ist kaum erkennbar. Auch der Privacy Shield dürfte daher vor dem EuGH landen und der Prüfung mit hoher Wahrscheinlichkeit nicht standhalten. Wer als Rechtsgrundlage seines Datenverkehrs in die USA gerade erst Verträge mit Standardvertragsklauseln abgeschlossen hat, sollte es erst einmal dabei belassen. Allerdings werden auch diese Gegenstand eines EuGH-Verfahrens.

Lawful Access

Wie ein Damokles-Schwert schwebte seit zwei Jahren ein Gerichtsverfahren vor einem New Yorker Bezirksgericht über den US-amerikanischen Cloud-Anbietern: Die US-Regierung hatte im Rahmen eines Drogenermittlungsverfahrens eine Verfügung gegen Microsoft erwirkt, um an Daten eines E-Mail-Accounts zu gelangen, die im Microsoft-Rechenzentrum in Irland gespeichert sind. Microsoft wehrte sich mit allen juristischen Mitteln. Unterstützung erfuhren sie dabei nicht nur von anderen IT-Giganten wie AT&T, Apple, Cisco und Verizon und Bürgerrechtsorganisationen wie der Electronic Frontier Foundation (EFF) als Amicus Curiae – auch die irische Regierung schaltete sich ein. Die umstrittene Verfügung wurde nun am 14.07.2016 durch ein Bundesberufungsgericht aufgehoben. Der Stored Communications Act (SCA) von 1986, auf den sie gestützt wurde, sei im Gegenteil dazu da, Daten vor dem Zugriff des Staates zu schützen, und dies gelte auch für ausländische Server eines US-Unternehmens.

Der Microsoft-Chefjurist Brad Smith äußerte sich frenetisch. Gewonnen ist jedoch lediglich ein Kampf in der großen Schlacht um die Datenhoheit. Eine große Hürde für amerikanische SaaS-Anbieter ist aus dem Weg geräumt – aber FBI & Co. werden zweifellos weiter nach kreativen juristischen Wegen für den Datenzugriff suchen.

Secorvo News

Spätsommerseminar

Unser rundum erneuertes Seminar „IT-Sicherheit heute“ (**27.–29.09.2016**) erfreut sich großer Nachfrage – damit sind interessante Diskussionen und ein lebhafter Erfahrungsaustausch schon garantiert. Das Programm reicht von aktuellen Rechtsthemen wie dem IT-Sicherheitsgesetz oder der Datenschutz-Grundverordnung der EU bis zu einem „Hacking Day“ mit WebGoat-Workshop.

Schnell Entschlossene bekommen noch einen Platz (Programm und Online-Anmeldung).

Penetrationstests

Das Angebot von Penetrationstests erfordert eine ständige Weiterentwicklung, da sich Angriffsmethoden und Tools permanent verändern. Daher haben sich unsere Pentester der renommierten OSCP-Zertifizierung unterzogen, unseren Pentest-Werkzeugkasten weiter ausgebaut sowie typische Leistungspakete (wie die Untersuchung von Webanwendungen, der DMZ-Systeme oder des WLAN-Zugangs) geschnürt, die den Leistungsumfang transparenter machen.

Durch standardisierte Arbeitsabläufe und die Ergänzung von Einzelanalysen konnten wir die Aussagekraft unserer Berichte weiter verbessern – was den Mehrwert der Penetrationstests nochmal deutlich erhöht. Eine Übersicht unseres Pentest-Leistungsangebots finden Sie in unserem neuen Produktflyer.

Encryption as a Service (EaaS)

Wie real ist die Gefahr, sich mit einer Ransomware zu infizieren? Welche Infektionswege verwenden die Angreifer? Wie arbeitet ein solcher Verschlüsselungstrojaner? Und welche Schutzmaßnahmen helfen dagegen?

Auf diese Fragen gibt auf dem nächsten KA-IT-Si-Event am **22.09.2016** der Vortrag von Tobias Häcker (Leitwerk AG) Antworten. Er wirft einen Blick hinter die Kulissen moderner Ransomware, beleuchtet deren Funktionsweise und stellt Abwehrmaßnahmen vor. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" – mit Blick über die Dächer von Karlsruhe. Wir freuen uns auf Ihre Anmeldung.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)
10.-12.08.	25th USENIX Security Symposium (Usenix, Austin/US)
14.-18.08.	Crypto 2016 (IACR, Santa Barbara/US)
September 2016	
07.-08.09.	Annual Privacy Forum 2016 (ENISA, EC DG Connect, Goethe Universität, mobile business, Frankfurt)
13.-15.09.	Future Security 2016 (Fraunhofer VVS, Berlin))
19.09.	Sommerakademie des ULD Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel)
22.09.	EaaS – Encryption as a Service (KA-IT-Si, Karlsruhe)
26.-27.09.	D • A • CH Security (Gemeinsame Arbeitskonferenz GI, OCG, BITKOM, SI, TeleTrusT, Klagenfurt)
27.-29.09.	IT-Sicherheit heute - praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
Oktober 2016	
04.-07.10.	Java Security (Secorvo, Karlsruhe)
11.-14.10.	OWASP AppSec USA 2016 (OWASP Foundation, Washington DC/US)
18.-20.10.	it-sa 2016 (NürnbergMesse GmbH)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2016



Digitalisierung 5.0

Die Welt wird digital. Das ist nicht neu – auch wenn es einige Menschen erst jetzt zu bemerken scheinen. Rechner bestimmen schon seit Jahrzehnten unser Leben, und vieles bekämen wir ohne sie nicht mehr hin. Vielleicht bewundern wir deshalb Michelangelos David oder Leonardos Mona Lisa, obwohl jeder mit 3D-Drucker und Smartphone selbst perfekte Abbilder der Wirklichkeit erzeugen kann.

Vor einigen Jahren hat jedoch eine neue Phase begonnen, die weit über das „Internet der Dinge“ und „Industrie 4.0“ hinausweist. Ich will sie „Digitalisierung 5.0“ nennen. Es ist eine Phase der Selbstbezüglichkeit: Computer beginnen, sich selbst zu gestalten. Und es ist die IT-Sicherheit, die diese Entwicklung befeuert. So akzeptieren wir (wenn auch nicht immer klaglos), dass unsere Rechner sich via Virenscanner ständig selbst untersuchen, eigenständig die Signaturdatenbank aktualisieren und unsere E-Mails von Spam befreien. Programm- und Betriebssystem-Updates erfolgen inzwischen ohne Freigabe der Benutzer, die Suche nach Programmfehlern übernehmen automatisierte Prozesse und Tools – nicht nur bei Softwareentwicklern, sondern auch als Cloud-Service. Längst arbeiten Angreifer mit Systemen, die systematisch Exploits durchprobieren, kombinieren – und die Zielsysteme sogar auf noch unbekannte Schwachstellen abklopfen. Die Antwort heißt IDS oder SIEM: die automatische Analyse von Netzverkehr und Log-Dateien auf Angriffsspuren.

Nicht mehr lange, und unsere Rechner nehmen sich in Quarantäne, säubern sich gegenseitig von Schadsoftware und setzen sich neu auf. Sie werden ihre Erfahrungen anderen Rechnern über Wissensdatenbanken zugänglich machen, ihre Leistungen womöglich in selbst „geschürften“ Bitcoin bezahlen und die robustesten Kollegen zu Entscheidern wählen. Nutzen könnte man sie wahrscheinlich nicht mehr – wozu aber auch: Schließlich brauchen die Rechner uns, damit wir gelegentlich defekte Festplatten ersetzen oder das RAM erweitern.



Inhalt

Digitalisierung 5.0

Security News

Abgehörte Tastaturen

Leitfaden zum EU-U.S. Privacy Shield

IT-Grundschutz-Modernisierung

Vorratsdatenspeicherung revisited

BSI-Zertifizierung nach TR

Wir haben Ihren PC aktualisiert

Secorvo News

PKI Check-up

Fast ausgebucht

Zertifikate

Cloud Encryption

Veranstaltungshinweise

secorvo
security consulting

Security News

Abgehörte Tastaturen

In ihrer Veröffentlichung zum KeySniffer-Hack vom 27.07.2016 zeigen die Forscher von Bastille, was sich mit Angriffen wie MouseJack und Keysweeper bereits abzeichnete: Zahlreiche kabellose Tastaturen und Mäuse bekannter Hersteller wie HP oder Toshiba aber auch Logitech und Microsoft sind für das Abhören oder die Injektion von Tastatureingaben anfällig. Angreifer können so an Passwörter oder Kreditkartennummern gelangen oder sogar das Zielsystem übernehmen.

Die Schwachstelle liegt bei den Herstellern der betroffenen Geräte, die eigene Übertragungsprotokolle und Sicherheitsmechanismen entwickelten anstatt auf bewährte Standards zu setzen. Mit einer Behebung der Schwachstelle ist eher nicht zu rechnen, da ein Einspielen neuer Firmware in die Dongles und Eingabegeräte nicht möglich ist oder der Aufwand von den Herstellern als zu hoch eingeschätzt wird.

Grundsätzlich sind kabelgebundene Tastaturen und Mäuse kabellosen Geräten vorzuziehen. Muss es dennoch eine kabellose Variante sein, so sollte man auf den Bluetooth-Standard setzen, der ein sicheres Kommunikationsprotokoll verwendet, das Authentifikation und Verschlüsselung umfasst.

Leitfaden zum EU-U.S. Privacy Shield

Seit dem 01.08.2016 liegt der EU-U.S. Privacy Shield als Garantie angemessenen Datenschutzes für U.S.-Unternehmen vor. Begleitend hat die EU-Kommission einen Leitfaden für Betroffene zu den Rechten aus den Privacy Shield Principles veröffentlicht.

Darin werden die Verpflichtungen von Privacy-Shield-Unternehmen, die diesbezüglichen Betroffenenrechte, die Beschwerderechte, die möglichen Adressaten sowie der für den gesamten EU-U.S.-Datenverkehr anwendbare Ombudsmann-Mechanismus ausführlich erläutert.

Eine Beschwerde kann an die verarbeitende U.S.-Gesellschaft, an eine von dieser einzusetzenden unabhängigen Beschwerdestelle und an die nationale Aufsichtsbehörde beim Department of Commerce oder der Federal Trade Commission gerichtet werden. Arbeitnehmer können sich stets an die nationale Aufsichtsbehörde wenden.

Scheitert eine Beschwerde, kann ein Schiedsverfahren verlangt werden. Dieses findet in den USA statt. Es besteht aber ein Recht auf Hilfestellung durch die nationale Aufsichtsbehörde, die Möglichkeit, per Videokonferenz teilzunehmen und ein Recht auf kostenlose Übersetzungen. Die Kosten werden von einem Fonds getragen.

Der vorerst nur in englischer Sprache verfügbare Leitfaden bietet datenschutzkundigen Betroffenen eine gelungene Übersicht über die grundsätzlichen Möglichkeiten. Er dokumentiert aber auch, dass der praktische Nutzen des Privacy Shields für einen einzelnen Betroffenen nur sehr schwer realisierbar sein dürfte.

IT-Grundschutz-Modernisierung

Am 08.08.2016 hat das BSI den Entwurf für einen modernisierten Baustein der IT-Grundschutzkataloge veröffentlicht. Ein weiterer Baustein folgte am 09.08.2016. Die wesentliche Neuerung ist, dass bei den modernisierten Bausteinen deutlich zwischen einem Anforderungsteil und sogenannten Umsetzungshinweisen unterschieden wird. Letztere weisen einen höheren Detaillierungsgrad auf als die eigentlichen Bausteine und ähneln den bisherigen Katalogen, stellen jedoch nur noch eine Möglichkeit zur Umsetzung dar.

Die neuen Bausteine stellen nun in kompakter Form die Vorgaben zusammen. Auf eine umfassende Gefährdungsdarstellung wurde verzichtet; die wesentlichen Maßnahmen, die aus Grundschutz-Sicht umgesetzt werden müssen, sind übersichtlich auf wenigen Seiten aufgeführt. Aus unserer Sicht eine deutliche Flexibilisierung und der richtige Weg, um die Umsetzung von IT-Grundschutz in der Praxis handhabbarer zu machen.

Vorratsdatenspeicherung revisited

Der Generalanwalt am Europäischen Gerichtshof hat am 19.07.2016 seine Schlussanträge in zwei verbundenen Rechtssachen zu nationalen Vorratsdatenspeicherungsregelungen gestellt.

Bereits 2014 hat der EuGH im Verfahren Digital Rights Ireland Ltd die Richtlinie zur Vorratsdatenspeicherung für ungültig erklärt. Die deutsche Umsetzung in § 113a ff. TKG a.F. war zuvor schon vom Bundesverfassungsgericht für verfassungswidrig erklärt worden (seit Dezember 2015 ist eine bis 2017 umzusetzende Nachfolgeregelung in Kraft).

In seinen Schlussanträgen leitet der Generalanwalt aus der Grundrechtscharta der Europäischen Union strenge Anforderungen an nationale Pflichten zur Vorratsdatenspeicherung ab. Sie dürfe nur der Bekämpfung schwerer Kriminalität dienen und müsse hierfür absolut notwendig sein. Die Anforderungen an den Schutz der Daten des vorausgegangenen Urteils müssten erfüllt und die mit der Vorratsdatenspeicherung verbundenen Gefahren dürften nicht unverhältnismäßig zu ihrem Nutzen sein.

Sollte der EuGH dem Antrag folgen, bleibt eine verfassungsgemäße Vorratsdatenspeicherung möglich. Der Nachweis der Verhältnismäßigkeit vor nationalen Gerichten wird aber angesichts vorliegender Studien schwierig. Den Vorschlägen des deutschen Innenministeriums, die Vorratsdatenspeicherung zu reanimieren und auf Telemedien auszudehnen, dürfte das Urteil jedoch einen Dämpfer setzen.

BSI-Zertifizierung nach TR

Mit der ISO 27001-Zertifizierung auf Basis von IT-Grundschutz darf man die am 12.08.2016 vorgestellte Zertifizierung nach TR in Verbindung mit ISO 27001 nicht verwechseln: Hier geht es, aufbauend auf einer ISMS-Zertifizierung nach ISO 27001, um die Zertifizierung konkreter, in den Technischen Richtlinien (TR) des BSI definierten Maßnahmen für ganz bestimmte Einsatzzwecke. In Vorbereitung ist derzeit eine Zertifizierung nach TR-03108 Secure E-Mail Transport für E-Mail-Provider.

Wir haben Ihren PC aktualisiert

Seit dem 02.08.2016 verteilt Microsoft das drei Gigabyte große Anniversary Update, mit dem die Strategie des „Windows as a Service" fortgesetzt wird: Jeder Windows-Nutzer soll stets die aktuellste Version des Betriebssystems verwenden – Apple lässt grüßen. Home-User können diesen „Service" nicht verweigern.

Neben einigen optischen und funktionalen Anpassungen sowie dem nachhaltigen Aushebeln von Secure Boot, holt das Thema Datenschutz mal wieder Microsoft ein (vgl. SSN 8/2015). Die US-Bürgerrechtsorganisation EFF sowie die französische Datenschutzaufsicht CNIL kritisieren Microsoft deutlich. Im Zentrum steht das Windows-Assistenzsystem Cortana, das nun zur Standardsuche in Windows 10 wird – bislang konnte man es deaktivieren. Cortana ist sehr kommunikativ: Es überträgt zahlreiche persönliche Informationen an Microsoft, darunter den Standort, Text-, Sprach- und Touch-Eingaben, Webseitenbesuche sowie Nutzungsstatistiken. Details zu den übertragenen Telemetriedaten sind bisher nicht bekannt. Firmenkunden können Cortana immerhin per GPO abschalten, Home-User müssen dafür zu regedit greifen. Da wünscht man sich glatt Karl Klammer zurück – der war zwar nervig, aber wenigstens verschwiegen.

Nach erfolgreichem Update wird man von seinem aufgefrischten Windows mit „Hallo. Wir haben Ihren PC aktualisiert." begrüßt. Besser lässt sich der Hoheitsverlust über den eigenen Rechner nicht zusammenfassen - Realsatire as a Service.

Secorvo News

PKI Check-up

In den vergangenen Jahren haben viele Unternehmen und Organisationen interne Public-Key-Infrastrukturen (PKI) aufgebaut. Viele Betreiber fragen sich jedoch, ob ihre PKI noch angemessen sicher, praxistauglich und für künftige Herausforderungen gerüstet ist. Als Abhilfe hat Secorvo daher einen PKI Check-up entwickelt, der PKI-Prozesse, -Architektur und -Dokumentation an bewährten Best Practices und Standards misst, bewertet und Optimierungspotenzial aufzeigt.

Fast ausgebucht

Noch drei letzte freie Plätze gibt es auf unserem rundum erneuerten Seminar „IT-Sicherheit heute" (**27.–29.09.2016**). Das Programm reicht von aktuellen Rechtsthemen wie dem IT-Sicherheitsgesetz und der Datenschutz-Grundverordnung bis zu einem „Hacking Day" mit WebGoat-Workshop – und ist als Weiterbildung zur T.I.S.P.-Re-Zertifizierung anerkannt. Schnell Entschlossene erwischen noch einen Platz (Programm und Online-Anmeldung).

Zertifikate

Im November (**21.–25.11.2016**) bieten wir die nächste Möglichkeit zur T.I.S.P.-Zertifizierung. Nach Ihrer Anmeldung erhalten Sie, frühzeitig vor Seminarbeginn, unser T.I.S.P.-Buch zur Vorbereitung: ein systematischer Zugang zur Informationssicherheit in 26 Kapiteln auf 700 Seiten, verfasst von Experten für Experten.

Software-Architekten und -Entwickler bereiten wir im Oktober (**24.–27.10.2016**) auf die Zertifizierung zum *Certified Professional for Secure Software Engineering* (CPSSE) vor. Auch hier empfehlen wir eine frühzeitige Anmeldung.

Cloud Encryption

Wie real ist die Gefahr, sich mit einer „Ransomware" zu infizieren? Welche Infektionswege verwenden die Angreifer? Wie arbeitet ein solcher Verschlüsselungstrojaner? Und welche technischen und organisatorischen Schutzmaßnahmen wirken dagegen? Auf diese Fragen gibt am **22.09.2016** ab 18 Uhr Tobias Häcker (Leitwerk AG) im Rahmen des nächsten KA-IT-Si-Events im Panoramasaal der IHK Karlsruhe Antworten und wirft einen Blick hinter die Kulissen aktueller Erpressungstrojaner. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" – mit Blick über die Dächer von Karlsruhe.

Wir freuen uns auf Ihre Anmeldung.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2016	
07.-08.09.	Annual Privacy Forum 2016 (ENISA, EC DG Connect, Goethe Universität, mobile business, Frankfurt)
19.09.	Sommerakademie des ULD Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel)
22.09.	EaaS – Encryption as a Service (KA-IT-Si, Karlsruhe)
26.-27.09.	D • A • CH Security (Gemeinsame Arbeitskonferenz GI, OCG, BITKOM, SI, TeleTrusT, Klagenfurt/AT)
26.-30.09.	Informatik 2016 (Gesellschaft für Informatik, Klagenfurt/AT)
27.-29.09.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
Oktober 2016	
04.10.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
11.-14.10.	OWASP AppSec USA 2016 (OWASP Foundation, Washington DC/US)
18.-20.10.	it-sa 2016 (NürnbergMesse GmbH)
19.10.	Swiss Cyber Storm 6 (Swiss Cyber Storm Association, Luzern/CH)
24.-27.10.	CPSSE – Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.-28.10.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Wien/AT)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2016



Die Tür

Wer in den vergangenen Jahren die Nachrichten verfolgt, dem drängt sich leicht der Eindruck auf, dass gegen alle diese Cracks – ob in staatlichem Auftrag, aus krimineller Motivation oder schlichtem Spieltrieb – einfach kein Kraut gewachsen ist. Warum also überhaupt diesen ganzen Aufwand treiben? Wieso nicht einfach alle Daten in die billigste Cloud verlegen, jede hilfreiche App auf das preisgünstigste Smartphone laden – und das gesparte Geld statt in Schutzmaßnahmen in Aktien investieren? Wenn der Datengau ohnehin früher oder später jeden trifft, dann hat man bis dahin wenigstens am Vermögen gearbeitet... So ähnlich klang kürzlich der Fatalismus zwischen den Zeilen eines Gesprächspartners, dem der Schreck über einige von mir vorgestellten Angriffswege noch anzusehen war.

Da kam mir eine Geschichte in Sinn, die schon einige Jahre zurückliegt. Bei unseren Nachbarn war eingebrochen worden – am hellichten Tag, mit nicht mehr als einem langen Schraubenzieher als Hebel. Es wurde wenig entwendet, aber der Schock saß tief.

Unvermeidlich unterzog ich unsere Haustür einem kritischen Blick – und musste feststellen, dass auch sie einem solchen Angriff nicht standgehalten hätte. Also holte ich mir Rat bei einem erfahrenen Kriminalisten. Der besah sich die Tür und beäugte mich amüsiert, als ich ihn fragte, was ich tun müsste, um so einen Einbruch zu verhindern. Falsche Frage, meinte er: „Es geht nicht darum, *ob* jemand einbrechen kann – sondern *wie lange* er dafür braucht." Genau das sei der Punkt. Jede Tür ließe sich öffnen – oft mit überraschend wenig Aufwand, und wenn es sein muss, mit schwerem Gerät. Entscheidend sei der Aufwand: Je mehr Zeit ein Einbrecher benötige und je mehr Lärm er verursache, desto größer sei die Entdeckungsgefahr. Wie bei der IT-Sicherheit: Je aufwändiger und langwieriger ein Angriff, desto höher Kosten und Risiko. Darum helfen Schutzmaßnahmen – gegen Einbrecher ebenso wie gegen Cracker.



Inhalt

Die Tür

Security News

Flüsterangriff auf Smartphones

Hacker-Stecker

WLAN-Haftung

IoT-Krypto-Camouflage

OPM-Hack

Smart-Meter-Regulierung

Secorvo News

Von und für Experten

Live Hacking

IT-Grundschutz-Zertifizierung

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Flüsterangriff auf Smartphones

Auf dem diesjährigen 25th USENIX Security Symposium wurde am 11.08.2016 ein unkonventioneller Angriff auf Smartphones vorgestellt: Ein Smartphone mit aktivierter Spracherkennung lässt sich von für ein menschliches Ohr unverständlichen Sprachbefehlen steuern. Denn die Geräuschfilterung ist erstaunlicherweise so gut, dass ein Smartphone manche Befehle wie "Öffne URL xyz" erkennt und ausführt, während der Besitzer dies aufgrund von Umgebungsgeräuschen nicht mitbekommt. Bei Tests wurde ein verschleiertes "OK Google" zu 95% vom Smartphone, aber nur von 22% der Probanden verstanden.

Einige Beispiele solcher „Hidden Voice Commands" für Android-Smartphones haben die Autoren auf ihrer Webseite zusammengestellt. Dort finden sich auch Tests, bei denen den Forschern Details zum Spracherkennungssystem vorlagen. Wer sicher gehen möchte, dass sein Smartphone keine Fremdsteuerung ermöglicht, sollte die Sprachsteuerung deaktivieren – oder zumindest so konfigurieren, dass sie im gesperrten Zustand nicht reagiert.

Hacker-Stecker

Ein einheitlicher Micro-USB-Stecker ist bei Smartphones (bis auf wenige Ausnahmen) mittlerweile Standard – und ab 2017 gesetzlich vorgeschrieben. Neben dem Laden des Akkus und dem Datenaustausch mit einem Computer bietet der Anschluss dank OTG meist nahezu die gleichen Möglichkeiten wie jeder USB-Port eines Computers. Durch den immer größeren Funktionsumfang der Schnittstelle entstehen jedoch auch neue Angriffsflächen, wie Brian Markus auf der Hacking-Konferenz DEF Con vom 04. bis 07.08.2016 demonstrierte. Bei seinem als „VideoJacking" bezeichneten Angriff wird ein externer Monitor oder ein Aufnahmegerät über einen Splitter mit dem Ladekabel verbunden. Darüber kann das auf dem Smartphone angezeigte Bild gespiegelt und abgegriffen werden. Betroffen sind alle mit dem Feature *Mobile High-Definition Link* (MHL) ausgestatteten Smartphones.

Für einen Nutzer ist grundsätzlich nicht ersichtlich, ob das über den Micro-USB-Port angeschlossene Gerät auch das ist, was es zu sein vorgibt. Fremde Ladegeräte sollten daher gar nicht oder nur mit einer dazwischen gesteckten Datenaustauschsperre (wie z. B. dem USB-Kondom) genutzt werden.

WLAN-Haftung

Der rechtliche Rahmen für Hotspots und Gäste-WLANs ist seit langem umstritten und mit großer Unsicherheit behaftet. Nach dem Vorstoß des deutschen Gesetzgebers (siehe SSN 7/2016) hat nun der EuGH am 15.09. 2016 sein Urteil im Fall Tobias McFadden ./. Sony Music verkündet. Der Beklagte hatte in seinen Verkaufsräumen ein ungesichertes WLAN betrieben und sich anlässlich einer Abmahnung von Sony wegen einer Urheberrechtsverletzung auf Art. 12 der Richtlinie 2000/31/EG und deren deutsche Umsetzung in § 8 TMG (das „Providerprivileg") berufen. Der EuGH hat nun entschieden, dass eine Schadensersatzhaftung des Anbieters gegen die Richtlinie verstoße und von dem Anbieter keine über die Richtlinie hinaus gehenden Maßnahmen verlangt werden dürften. Der Anbieter könne aber auf Unterlassung in Anspruch genommen werden und müsse hierfür die Kosten tragen. Er dürfe zum Schutz des WLANs durch ein Passwort und zur Nutzeridentifikation verpflichtet werden.

Die (ohnehin voreilige) Euphorie über den neuen § 8 Abs. 3 TMG dürfte damit verflogen sein. Die Richtlinie lässt die Störerhaftung in Art. 12 Abs. 3 ausdrücklich zu, das Urteil ist daher nachvollziehbar. Passwortschutz und Identifikation alleine reichen jedoch zur Umsetzung des Unterlassungsanspruchs nicht aus, daher hat das Urteil nicht zur Klarheit über die tatsächlichen Pflichten des Anbieters beigetragen – ein weiteres in der langen Reihe unglücklicher WLAN-Entscheidungen.

IoT-Krypto-Camouflage

Am 06.09.2016 veröffentlichte das Unternehmen SEC Consult eine Untersuchung der Sicherheit der Implementierung kryptographischer Verfahren in IoT-Geräten. Schon im November 2015 war SEC Consult in eine Studie zu dem Ergebnis gekommen, dass die Verwendung von privaten Schlüsseln in verbreiteten Geräten bei weitem nicht dem Stand der Technik entspricht. Die aktuellen Ergebnisse legen nahe, dass sich die Situation in den vergangenen neun Monaten eher verschlimmert hat. Vielfach erlauben falsch verwendete Schlüssel und Zertifikate Zugriff auf Geräte oder vertrauliche Informationen. Betroffene Schlüssel und Zertifikate wurden inzwischen auf Github veröffentlicht; darunter finden sich auch einige Schlüssel von AVM Fritzboxen. Auf die offizielle Meldung des US CERTs reagierte offenbar bisher fast keines der betroffenen Unternehmen. Der Kauf von billiger Kryptographie kann die Nutzer also teuer zu stehen kommen.

OPM-Hack

Fast wie ein Krimi lesen sich die 217 Seiten des am 07.09.2016 veröffentlichten offiziellen Untersuchungsberichts mit dem prägnanten Titel „The OPM

Data Breach: How the Government Jeopardized Our National Security for More than a Generation“ zu den Angriffen auf das *U.S. Office of Personnel Management* (OPM) in den Jahren 2014 und 2015, bei denen sehr persönliche Daten aus Sicherheitsüberprüfungen, darunter auch Fingerabdrücke, von mehr als 21,5 Millionen Amerikanern entwendet wurden. Das OPM war Ende 2014 als die Behörde mit den schwächsten Authentifikationsverfahren gerügt worden und betrieb zentrale Server (die später kompromittiert wurden) vorschriftswidrig ohne Security Assessment. Bereits im März 2014 war das OPM vom US-CERT auf einen Hackerangriff hingewiesen worden; die Aktivitäten des Hackers wurden vom OPM jedoch lediglich über zwei Monate beobachtet. Mangelhafte Schutzmaßnahmen, unvollständige Logs und unangemessene Reaktionen sieht der Bericht als Ursachen des (verhinderbaren) Datenabzugs. Ein abschreckendes Beispiel für falsche Prioritätensetzung beim Umgang mit Informationssicherheit.

Smart-Meter-Regulierung

Am 01.09.2016 ist das am 08.07.2016 vom Bundesrat verabschiedete Gesetz zur Digitalisierung der Energiewende im Bundesgesetzblatt veröffentlicht worden und am 02.09.2016 in Kraft getreten. Kernstück ist das ‚Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen‘ (Messstellenbetriebsgesetz – MsbG). Es regelt den Übergang zu modernen Messstellen in zukünftigen Energienetzen.

Technische Vorgaben an die Datensicherheit werden in den §§ 19 ff. MsbG geregelt. Konkrete Anforderungen an Interoperabilität und Anbindungssicherheit vor allem der Smart-Meter-Gateways finden sich in bereits vorliegenden technischen Richtlinien. Die Erfüllung der Anforderungen durch die Geräte ist mit einer Zertifizierung nachzuweisen. Nicht den Anforderungen entsprechende Geräte dürfen nur noch bis Ende 2016 verbaut und anschließend maximal acht Jahre genutzt werden.

Die Datenerhebung und –verarbeitung wird umfangreich in 25 Paragraphen (§§ 49 ff. MsbG) geregelt, darunter finden sich auch Löschpflichten und sogar konkrete Löschfristen. Die aus Datenschutz- und Datensicherheitsanforderungen resultierenden Umsetzungspflichten sind komplex und umfangreich; sie werden von Herstellern und Betreibern mehr als einen Blick über den Tellerrand erfordern, um den Zertifizierungsanforderungen genügen zu können.

Secorvo News

Von und für Experten

Vierzig Jahre liegt die wegweisende Veröffentlichung von Whitfield Diffie und Martin E. Hellman („New Directions in Cryptography“) inzwischen zurück – und noch immer sind Aufbau und Betrieb einer PKI eine Herausforderung. Wie so oft liegt der Teufel in den Details – Zertifikatsgültigkeiten, Key Usage, Prozesse und Policies sind geeignet festzulegen und umzusetzen. Wie das geht, zeigen wir in Theorie und Praxis auf unserem PKI-Seminar vom **14. bis 17.11.2016** (Programm und Anmeldung).

Bis Mitte des Jahres 2016 wurden 850 T.I.S.P.-Zertifikate ausgestellt. Sofern Sie drei Jahre Berufserfahrung im Gebiet Informationssicherheit mitbringen, können Sie noch in diesem Jahr Teil dieser schnell wachsenden Experten-Community der *Information Security Professionals* werden: Vom **21. bis 25.11.2016** findet in Karlsruhe die nächste T.I.S.P.-Schulung mit anschließender Zertifikatsprüfung statt, durchgeführt von den Autoren des T.I.S.P.-Buchs (detaillierte Agenda und Online-Anmeldung).

Live Hacking

Kaum etwas ist wirkungsvoller als die Anschauung – das gilt auch für die IT-Sicherheit. Daher haben wir in den vergangenen Monaten zahlreiche Live-Hacking-Vorführungen entwickelt, die verbreite Einfallstore zeigen. Alle Live Hacks kommen ohne „Hokuspokus“ wie Spezialversionen einer anfälligen Soft- oder Hardware aus; gezeigt wird, was ohne größere Investitionen in die Ausrüstung heute möglich ist. Wenn Sie einen solchen Live Hack buchen möchten, nehmen Sie bitte mit uns Kontakt auf.

IT-Grundschutz-Zertifizierung

Zertifizierung eines großen Rechenzentrums – nach IT-Grundschutz? Kann das mit vertretbarem Aufwand und in überschaubarer Zeit funktionieren? Sascha Grund, IT Compliance Manager der Globalways AG, stellt auf dem kommenden KA-IT-Si Event am **10.11.2016, 18 Uhr** in den Räumen des CyberForum e.V. vor, dass und wie das geht – und gibt praktische Tipps zur Umsetzung.

Im Anschluss an den Vortrag haben Sie wie gewohnt die Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Anmeldung und weitere Informationen unter www.ka-it-si.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2016	
04.10.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
11.-14.10.	OWASP AppSec USA 2016 (OWASP Foundation, Washington DC/US)
18.-20.10.	it-sa 2016 (NürnbergMesse GmbH)
19.10.	Swiss Cyber Storm 6 (Swiss Cyber Storm Association, Luzern/CH)
26.-28.10.	IDACON 2016 (WEKA-Akademie, München)
November 2016	
01.-04.11.	Black Hat Europe 2016 (Blackhat, London/UK)
08.-11.11.	DeepSec In-Depth Security Conference 2016 Europe (DeepSec, Wien/AT)
10.11.	IT-Grundschutz-Zertifizierung (KA-IT-Si, Karlsruhe)
10.-11.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
14.-17.11.	PKI (Secorvo, Karlsruhe)
17.-18.11.	40. DAFTA (GDD, Köln)
21.-25.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Die 40seitige Publikation „Offenes Geheimnis – Mythen und Fakten zu Überwachung und digitaler Selbstverteidigung“ der Rosa Luxemburg Stiftung gibt eine Übersicht über Hintergründe und Schutzmöglichkeiten für Endanwender.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Oktober 2016



Freiwillige Cyberwehr

Es ist kein guter Stil, Salz in offene Wunden zu streuen. DIE ZEIT und netzpolitik.org haben sich bereits ausführlich über die freiwillige Cyberwehr ausgelassen, und via Twitter wurde das BSI mit Spott übergossen. Doch das Thema ist zu wichtig, um es unkommentiert zu lassen. Worum also geht es?

Bereits Anfang Juni 2016 wurde bekannt, dass das BSI ein 20-köpfiges „Mobile Incident Response Team" aufbauen will, das ab 2017 Betreiber kritischer Infrastrukturen bei einem IT-Sicherheitsvorfall unterstützen soll. So weit, so gut. Offenbar bekam das BSI nun jedoch Respekt vor der eigenen Courage und entwarf rasch eine Kooperationsvereinbarung für eine „freiwillige Cyberwehr", die Anfang Oktober publik wurde. Das Konzept: Kooperierende Unternehmen stellen eigene Fachkräfte für IT-Sicherheit ab, die bei einem IT-Sicherheitsvorfall der „Cyberwehr" des BSI unterstellt werden und bis zu drei Tage Soforthilfe leisten. Die Unternehmen sichern ein vom BSI abrufbares Einsatzkontingent von jeweils bis zu 20 Personentagen jährlich (zuzüglich Reisekosten, Übungen und Fortbildungen) zu – unentgeltlich, versteht sich – und besetzen eine rund um die Uhr erreichbare Kontaktstelle für die Alarmierung.

Eine wenig beruhigende Vorstellung: IT-Sicherheitsvorfälle in kritischen Infrastrukturen werden zukünftig von einer bunten, auf Zuruf zusammengetrommelten Truppe freiwilliger Cybercops unter BSI-Leitung bekämpft. Sieht man einmal von der Frage ab, ob Unternehmen bereit sein werden, ihre hoch bezahlten Fachkräfte für solche Einsätze abzustellen – professionell klingt das nicht.

Wollte man Schäden wirksam begrenzen und den Umgang mit Vorfällen professionalisieren, müsste den immer ausgefeilteren Angriffsmethoden eine intensiv trainierte, hoch kompetente und eingespielte schnelle Eingreiftruppe gegenüberstehen. Wer schon einmal eine IT-Notfallübung durchgeführt hat, weiß, dass es dabei mit drei Tagen „Schlauch draufhalten" nicht getan ist. SEKs sind schließlich auch keine spontan einberufenen Grisu-Teams.



Inhalt

Freiwillige Cyberwehr
Security News
Risikomanagement erneuert
Datenübermittlung auf der Kippe
Unendliche Geschichte
6. Deutscher IT-Sicherheitspreis
Microsoft Edge-VM
Secorvo News
Das Standard-ADV-Modell
T.I.S.P.-Zertifikat
Mit Brief und Siegel
Krypto im Advent 2016
Veranstaltungshinweise
Fundsache

secorvo
security consulting

Security News

Risikomanagement erneuert

Am 19.10.2016 hat das BSI die "Community Draft"-Version des neuen Risikomanagement-Standards 200-3 veröffentlicht. Die reichlich formale und in der Praxis selten hilfreiche Vorgehensweise des Vorgängers 100-3 wurde erheblich überarbeitet.

Zum einen wurden die noch als Ergänzung zum 100-3 definierten ‚Elementaren Gefährdungen' nun als wesentliche Komponente für Risikoanalysen integriert, ein für die Praxis durchaus sinnvoller Schritt. Zum anderen ist nun ein kompletter Prozess für das Risikomanagement von Informationssicherheitsrisiken beschrieben. Und der rockt. Praxistauglich, pragmatisch und, wenn man noch die Beispiele kürzt und den nicht wirklich belastbaren Begriff der Eintrittswahrscheinlichkeit durch eine (subjektive) Wahrscheinlichkeitseinschätzung ersetzt, ein wirklich brauchbares Grundlagenwerk. Ein kleiner Schritt in der Versionsnummer, aber ein großer Schritt in Richtung praktikablen IT-Grundschutzes.

Datenübermittlung auf der Kippe

Wer glaubt, mit dem EU-U.S. Privacy Shield (SSN 07/2016, 08/2016) sei der Datentransfer außerhalb der EU wieder in trockenen Tüchern, der wiegt sich in trügerischer Sicherheit. Nach dem erfolgreichen Vorgehen gegen Facebooks Datenübermittlung auf Basis von Safe Harbor hat Max Schrems im Mai 2016 auch die Prüfung EU-Standardvertragsklauseln bei der zuständigen irischen Datenschutzbeauftragten (DPC) initiiert. Diese Klauseln dienen als Rechtsgrundlage einer Datenübermittlung in jedes Drittland (nicht nur den USA) und werden vielerorts als „bessere Alternative" zu Safe Harbor verstanden. Am 28.09.2016 informierte die DPC über den Verfahrensstand: Nach ihrer Überzeugung verstoßen die Klauseln gegen europäisches Recht, denn EU-Bürgern stehen in den USA keine wirksamen Rechtsbehelfe zur Verfügung. Die Argumentation stützt sich auf die Entscheidungsgründe im Safe-Harbor-Urteil des EuGH.

Anfang 2017 wird der Austausch mit dem High Court abgeschlossen sein – und dieser kann kaum etwas anderes tun, als die Frage nach der Rechtmäßigkeit der Klauseln dem EuGH vorzulegen. Folgt dieser seinen eigenen Argumenten, wird er die Standardvertragsklauseln für unwirksam erklären. Damit bliebe für die Datenübermittlung in die USA nur noch der Privacy Shield, den die europäischen Datenschutz-Aufsichtsbehörden zunächst auf ein Jahr befristet beobachten wollen, um dann zu entscheiden, ob sie ihn als rechtmäßig ansehen.

Unendliche Geschichte

Mit seinem Urteil in Sachen Breyer ./. BRD hat der EuGH dem alten Streit um den Personenbezug der IP-Adresse am 19.10.2016 ein neues Kapitel hinzugefügt. Einerseits wird der Personenbezug dynamischer IP-Adressen erneut bejaht, wenn auch nicht uneingeschränkt. Daneben wurde die Frage, ob die Protokollierung von Webseitenzugriffen zu Sicherheitszwecken zulässig ist, gegen die in Deutschland herrschende Meinung entschieden: Nach Auffassung des EuGH ist sie regelmäßig erlaubt.

An der IP-Adresse entzündet sich immer wieder der Streit um ein objektives oder relatives Verständnis der Personenbeziehbarkeit: Reicht es, dass ein Dritter den Betroffenen ermitteln kann oder muss dies dem Dateninhaber selbst möglich sein?

Der EuGH sieht die Personenbeziehbarkeit auch gegeben, wenn der Dateninhaber die Zuordnung nicht allein vornehmen kann, aber die rechtliche Möglichkeit hat, die Zuordnungsdaten zu erlangen. Das ist im Umkehrschluss ein Brückenschlag zur „relativen Theorie". Außerdem stünde die RL 95/46/EG einer Regelung entgegen, die eine Datenverarbeitung ohne jegliche Abwägungsmöglichkeit kategorisch verbiete. Beide Aussagen gehen deutlich über das Telemediengesetz hinaus. Mit der Öffnung zur relativen Theorie sind beispielsweise Pseudonyme rechtlich neu zu bewerten. Die neue Entscheidungslage hat jedoch ein Verfallsdatum, denn mit der Datenschutz-Grundverordnung entfallen ab Mai 2018 wesentliche Teile der Wortlautargumente des EuGH – und der Streit wird wohl von vorne beginnen.

6. Deutscher IT-Sicherheitspreis

Der „Deutsche IT-Sicherheitspreis", gestiftet von Dr. Horst Görtz, dem Gründer des ersten großen deutschen IT-Sicherheitsunternehmens, zeichnet seit 2006 alle zwei Jahre drei herausragende Entwicklungen im Gebiet der IT-Sicherheit aus. Mit einem Preisgeld von insgesamt 200.000 € ist dies einer der höchsten privat gestifteten Preise in Deutschland. Am 06.10.2016 wurden in Darmstadt die diesjährigen Gewinner ausgezeichnet. Den ersten Preis erhielt die Analysesoftware Harvester der Forschungsgruppe um Professor Eric Bodden, die eine Schadsoftwareerkennung auch in obfuskierten Android-Apps erlaubt. Preis zwei ging an die Plattform Octopus zur Schwachstellensuche der Forschungsgruppe um Professor Konrad Rieck, die mit Methoden des Pattern Matching und des maschinellen Lernens beeindruckende Analyseerfolge mit einer Minimalzahl an „False Positives" vorweisen kann. Ein deutliches Signal, welcher Stellenwert der

Bekämpfung von Schadsoftware und Schwachstellen inzwischen eingeräumt wird – und welche überraschende Fortschritte in diesem Bereich noch möglich sind.

Microsoft Edge-VM

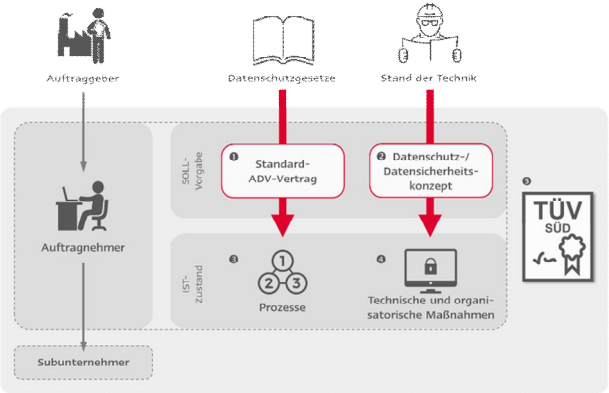
Microsoft plant, den Microsoft-Internetbrowser Edge in der nächsten Version von Windows 10 in eine virtuelle Umgebung zu verfrachten. Die *Windows Defender Application Guard* genannte Technologie startet beim Aufruf von nicht vertrauenswürdigen Seiten eine schlanke virtuelle Windows-Instanz, in welcher der Browser selbst bei infizierten Webseiten Angriffsmöglichkeiten auf das eigentliche Betriebssystem und die Benutzerdaten unterbindet. Im Intranet wird Edge „ganz normal" gestartet und kann auch auf die internen Daten zugreifen. Ein viel versprechender Ansatz, den Zugriff auf Webseiten sicherer zu machen.

Secorvo News

Das Standard-ADV-Modell

Wie lassen sich Auftragsdatenverarbeiter systematisch und kontinuierlich, zugleich aber effizient und effektiv auf die wirksame Umsetzung geeigneter technischer und organisatorischer Maßnahmen (TOM) zum Schutz der verarbeiteten personenbezogenen Daten prüfen? Die Verantwortung für die Verarbeitung liegt beim Auftraggeber: Er muss regelmäßig prüfen, ob geeignete Maßnahmen zu deren Schutz getroffen wurden und die gesetzlichen Anforderungen erfüllt sind.

Eine Zertifizierung kann aufwändige Einzelprüfungen durch ein standardisiertes Verfahren ersetzen. Doch warum hat sich bisher kein Standard etabliert? Genau mit dieser Frage haben sich Secorvo und der TÜV SÜD beschäftigt. Daraus ist das Standard-ADV-Modell mit Zertifizierung entstanden, das Auftragnehmer von Auftragsdatenverarbeitungen beim Nachweis der Eignung und Angemessenheit der getroffenen Maßnahmen gegenüber ihren Auftraggebern mit dem Prüfzeichen und Zertifikat „Zertifizierte Auftragsdatenverarbeitung" unterstützt. Mit einer nach wenigen Monaten bereits zweistelligen Zahl erfolgreicher Zertifizierungen könnte das Konzept ein Erfolgsmodell werden.



Eine ausführliche Darstellung des Modells und des Zertifizierungsverfahrens haben Christoph Schäfer und Dirk Fox in Ausgabe 11/2016 der Fachzeitschrift DuD veröffentlicht.

T.I.S.P.-Zertifikat

Eine letzte Möglichkeit, Ihre Kenntnisse und Qualifikation in der Informationssicherheit noch in diesem Jahr zu zertifizieren, bieten wir mit unserem T.I.S.P.-Seminar im November (**21.–25.11.2016**). Das Begleitbuch erhalten Sie zur Vorbereitung auf das Seminar unmittelbar nach Eingang Ihrer Anmeldung. Programm und Online-Anmeldung sowie die Termine und Seminarangebote für 2017 finden Sie unter www.secorvo.de/seminare.

Mit Brief und Siegel

Zertifizierung eines großen Rechenzentrums – nach IT-Grundschutz? Kann das mit vertretbarem Aufwand und in überschaubarer Zeit funktionieren?

Der Globalways AG ist das mit einem pragmatischen Ansatz bei der Vorbereitung und Umsetzung der IT-Grundschutzmaßnahmen auf effiziente Weise gelungen. Die Erfahrungen, Herausforderungen und „Lessons Learned" im Zertifizierungsprozess, von der Vorbereitung bis zum Zertifikat, stellt der CISO Sascha Grund bei unserer nächsten KA-IT-Si Veranstaltung am **10.11.2016, 18 Uhr** vor. Dabei wird vor allem auf das Zusammenspiel der eingesetzten Werkzeuge und deren Verwendung im Informationsverbund eingegangen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Die Möglichkeit zur Anmeldung finden Sie unter www.ka-it-si.de.

Krypto im Advent 2016

Nach dem großen Erfolg im Advent 2015 bietet die KA-IT-Si gemeinsam mit der Pädagogischen Hochschule Karlsruhe im Dezember 2016 wieder den interaktiven Online-Adventskalender „Krypto im Advent" an, bei dem Schülerinnen und Schüler die Welt der Verschlüsselung und Geheimsprachen kennenlernen und tolle Preise gewinnen können. Auch ältere, an Ver- und Entschlüsselungsverfahren Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2016	
01.-04.11.	Black Hat Europe 2016 (Blackhat, London/UK)
08.-11.11.	DeepSec In-Depth Security Conference 2016 Europe (DeepSec, Wien/AT)
10.11.	Mit Brief und Siegel (KA-IT-Si, Karlsruhe)
10.-11.11.	T.I.S.P. Community Meeting (TeleTrusT, Frankfurt am Main)
17.-18.11.	40. DAFTA (GDD, Köln)
21.-25.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
21.-22.11.	6. Handelsblatt Jahrestagung - Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
29.-30.11.	5. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Hamburg)
Januar 2017	
13.-15.01.	ShmooCon 2017 (Shmoo Group, Washington/US)
16.-18.01.	OmniSecure 2017 (inTime, Berlin)
23.-25.01.	AppSec Cali 2017 (OWASP Foundation, CA/US)

Fundsache

Valerie Tischbein hat am 22.08.2016 auf Netzpolitik.org eine Übersicht der von Facebook erhobenen 98 Datentypen zur Schaltung zielgenauer Werbung und den korrespondieren Datenschutzeinstellungen veröffentlicht, basierend auf einer Analyse der Washington Post.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Michael Knopp, Christoph Schäfer.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

November 2016



Reichtum

Zuerst verwirren sich die Worte.
Dann verwirren sich die Begriffe.
Und schließlich verwirren sich die Sachen.
(Chinesische Weisheit)

Oft beginnt es mit ungenauen Begriffen. Wenn wir „Datenschutz" sagen, meinen wir „Schutz der Persönlichkeitsrechte". Gesprächspartner verstehen aber meist „Schutz der Daten" – und assoziieren unvermeidlich „IT-Sicherheit". Eine wichtige Ursache für das verbreitete Unverständnis, dem Datenschützer begegnen – geschuldet einer irreführenden Bezeichnung.

Schlimmer noch als ungenaue Begriffe sind falsche Metaphern. Das hat viel damit zu tun, dass unser Gehirn „in Bildern denkt": Assoziationen bilden wir nicht in Gestalt abstrakter Begriffe, sondern als visuelle Vorstellungen. Eine starke Veranschaulichung überlagert daher alle denkbaren Bedeutungsnuancen mit unseren damit verbundenen Emotionen und Vorurteilen. Daher sind Metaphern starke argumentative Waffen: Sie fokussieren, vereinfachen und können wahre Bedeutungen sogar überdecken oder verdrängen.

Manchmal jedoch schlägt eine solche argumentative Metapher unerwartet zurück. So sprechen wir seit Jahren von Daten als neuer „Währung", mit denen wir unentgeltliche Leistungen im Internet bezahlen. Der Friedenspreisträger des deutschen Buchhandels von 2014, Jaron Lanier, schlägt sogar vor, dass Nutzer für die Preisgabe ihrer Nutzungsdaten ein Entgelt erhalten. Gar keine schlechte Idee, Daten einen Wert beizumessen, oder? Zweifellos steigt damit ihre Schutzwürdigkeit – wollen wir nicht genau das?

Tatsächlich aber untergräbt die Währungs-Metapher den Wesensgehalt des Datenschutzes. Was macht man mit einer Währung? Man versucht, möglichst viel davon zu akkumulieren. Das Ergebnis ist Reichtum – das Gegenteil von (Daten-) Sparsamkeit (war das nicht die Tugend von Armen und Geizigen?). Kein Wunder, dass Verkehrsminister Dobrint nach „Datenreichtum" ruft – und Datenschützer zurückrudern. Hätten wir bloß diese Metapher verhindert.



Inhalt

Reichtum

Security News

Attacks are getting better...

AppSec Practice

Poison Pi

Engineering Reversed

Privacy Leaks

Orientierungssuche

Secorvo News

ISMS-Verstärkung

IT-Sicherheit in der Produktion

24 Krypto-Rätsel

Veranstaltungshinweise

secorvo
security consulting

Security News

Attacks are getting better...

... oder wie man mit einer Sonnenbrille zu George Clooney wird: Am 27.10.2016 haben Forscher der Carnegie Mellon University auf der 23rd ACM Conference on Computer and Communications Security vorgestellt, wie sich Gesichtserkennungssysteme in die Irre leiten lassen. In ihrem Vortrag zeigten sie anschaulich, wie sie von theoretischen Überlegungen zu Schwächen in Gesichtserkennungssystemen zu praktischen Angriffen kamen, die die Eignung solcher Systeme als Sicherheitsmaßnahme zweifelhaft erscheinen lassen: Es gelang ihnen – wenn auch unter Laborbedingungen – durch die Verwendung spezieller Brillen Gesichtserkennungssystemen vorzutäuschen, sie seien eine beliebige andere Person, die das System kennt. Mit dem Einsatz von Gesichtserkennungssystemen in Hochsicherheitsbereichen sollte man sich also noch zurückhalten.

AppSec Practice

Am 03.11.2016 veröffentlichte die Firma Veracode eine Studie mit dem Titel *How IT Professionals are approaching AppSec today*. Die Erkenntnisse der Umfrage unter über 300 Verantwortlichen für Softwaresicherheit sind womöglich nicht überraschend, aber dennoch erschreckend: Als Hauptgründe für unzureichende Sicherheit von Softwarelösungen wurden externer und interner Druck sowie die wachsende Komplexität angegeben. Häufig würden Schutzmaßnahmen verwendet, die erwiesenermaßen nicht optimal sind. Dass dies auch praktische Konsequenzen hat, zeigen beispielsweise die im *Verizon 2016 Data Breach Investigation Report* vom 19.05.2016 dokumentierten Fälle.

Leider beschränkt sich der Bericht auf die Problembeschreibung und zeigt keine konkreten Auswege auf. Wir empfehlen die Beachtung konstruktiver Hilfestellungen wie beispielsweise die des OWASP oder aktueller Publikationen wie des CSA-Whitepapers zur Absicherung von IoT-Devices.

Poison Pi

Je leistungsfähiger Microcontroller-Boards wie der Raspberry Pi werden, desto mehr eignen sie sich auch als preiswertes Angriffs-Tool. Der amerikanische Sicherheitsforscher Samy Kamkar veröffentlichte am 16.11.2016 ein auf einem 5 US$ teuren Raspberry Pi Zero implementiertes, Streichholzschachtel großes Angriffswerkzeug (PoisonTap), das sich (sogar gegenüber einem mit Passwort gesperrten PC) als lokales USB-Ethernet ausgibt und den gesamten Netzverkehr über den Raspberry Pi umleitet. Als „Man-in-the-Middle" kann es Login-Daten mitschneiden, Schadsoftware unterschieben, Daten abfließen lassen oder verfälschen – mehr als einen freien USB-Anschluss in einem laufenden PC mit offenem Browser benötigt es dafür nicht.

Neben einer regelmäßigen Überprüfung der USB-Anschlüsse am PC kann man Client-seitig wenig tun – ein gestarteter Browser genügt PoisonTap. Webserver-seitig hilft HTTPS *Strict Transport Security* (HSTS, RFC 6797), da es HTTPS-Verbindungen erzwingt, die PoisonTap nur unter Inkaufnahme einer TLS-Fehlermeldung aufbrechen kann.

Engineering Reversed

Der reinen Lehre zufolge sollten für neue Kryptoprotokolle zunächst die genauen Sicherheitsziele festgelegt, dann die Verfahren formal definiert und ihre Sicherheit analysiert werden, bevor man sie implementiert und unter das Volk bringt. Beim Kryptoprotokoll des Messengers Signal ist diese Reihenfolge gehörig durcheinander gekommen: Seine wesentlichen Elemente wurden bereits in den Messenger-Anwendungen von WhatsApp, Facebook & Co. genutzt, bevor eine unabhängige Forschergruppe aus England, Australien und Kanada in einer am 01.11.2016 veröffentlichten Analyse das Protokoll und seine Anforderungen formalisiert und basierend auf einer bereits vor 15 Jahren etablierten formalen Beweismethodik untersucht hat.

Für ihre Analyse mussten die Forscher sogar Details aus dem Open Source Quellcode rekonstruieren. Inzwischen wäre das nicht mehr notwendig, denn zwischen dem 20.10. und 20.11.2016 haben die Signal-Autoren schließlich selbst das Protokoll und die Sicherheitseigenschaften in drei Teilen dokumentiert. Die gute Nachricht für eine Milliarde Messenger-Nutzer: Das Protokoll wurde in der formalen Analyse für gut befunden. Auch, wenn das Vorgehen nicht empfohlen werden kann – ob das Protokoll nach Lehrbuch entworfen wurde, interessierte am Ende niemanden mehr.

Privacy Leaks

Greenpeace und der Spiegel veröffentlichten am 25.11.2016 verschiedene Verhandlungsdokumente des internationalen Abkommens über den freien Handel mit Dienstleistungen (*Trade in Services Agreement* – TiSA). Den vorliegenden Dokumenten nach wird dieses geheim verhandelte Abkommen europäisches Datenschutzrecht tangieren. So fordert das „Non-Paper on data flows", Beschränkungen für den Datenfluss auch personenbezogener Daten nicht zuzulassen, wenn dadurch Dienstleistungsanbieter ungerechtfertigt diskriminiert werden. Immerhin enthält der Entwurf eine Ausnahmeklausel für Maßnahmen zum Datenschutz

(Art. I-9 (c) (ii)), und der Annex zum E-Commerce sieht die Berücksichtigung nationalen Verbraucherschutzrechts vor. Allerdings darf kein Vertragsstaat als Bedingung für den Marktzugang die Nutzung von Rechenzentren im eigenen Territorium verlangen – das beißt sich mit geltendem Datenschutzrecht.

Zwar sind die Entwürfe noch deutlich von einer Endfassung entfernt, doch enthalten die Regelungsvorschläge zahlreiche Konfliktpunkte mit den gerade erst neu erlassenen europaweiten Datenschutzbestimmungen.

Orientierungssuche

Die Übermittlung personenbezogener Daten ins außereuropäische Ausland beschäftigt derzeit die Datenschutz-Aufsichtsbehörden: Die Behörden der Länder Bayern, Berlin, Bremen, Hamburg, Niedersachsen, NRW, Rheinland-Pfalz, Saarland und Sachsen-Anhalt haben am 03.11.2016 in Pressemitteilungen bekannt gegeben, 500 zufällig ausgewählte Unternehmen verbindlich zur Beantwortung eines diesbezüglichen Fragebogens auffordern zu wollen. Darin wird u. a. nach Übermittlungen in die USA und weitere Drittstaaten, nach der Rechtsgrundlage (u. a. auch Safe Harbor), nach der Überprüfung der tatsächlichen Privacy-Shield-Unterwerfung und nach typischen Auslagerungen oder Cloud-Diensten mit außereuropäischem Bezug gefragt. Zum weiteren Vorgehen machten die Aufsichtsbehörden hingegen keine Angaben.

Nun ist wenig gegen Versuche der Aufsichtsbehörden einzuwenden, einen Überblick über die Praxis der Datenübermittlung zu gewinnen. Dass den Unternehmen bei den Angaben zahlreich Gelegenheit gegeben wird, sich diverser Datenschutzverstöße selbst zu bezichtigen, hinterlässt jedoch einen schlechten Beigeschmack – während die Aufsichtsbehörden an anderer Stelle ihre Unsicherheit bei der Beurteilung der derzeitigen Rechtslage betonen.

Secorvo News

ISMS-Verstärkung

Angesichts der wachsenden Bedeutung, die Unternehmen inzwischen dem systematischen Umgang mit Informationssicherheit beimessen, haben wir uns um Verstärkung bemüht: Seit dem 01.11.2016 zählt Fabian Ebner zum Secorvo-Team. Er bringt neben praktischer Erfahrung einen Bachelor-Abschluss in Unternehmens- und IT-Sicherheit mit – und damit ein breites Grundlagenwissen über alle Gebiete der Informationssicherheit hinweg.

Ebenfalls im November hat Stefan Gora die Qualifikation eines ISO 27001:2013-Lead-Auditors erlangt – als vierter im Secorvo-Team.

IT-Sicherheit in der Produktion

Am **08.12.2016** führen wir in Kooperation mit der Innovationsallianz Karlsruhe unsere letzte KA-IT-Si-Veranstaltung in diesem Jahr zum Thema „IT-Sicherheit in der Produktion“ durch.

Als besonderes „Schmankerl“ starten wir diesmal mit einer Führung durch das IT-Sicherheitslabor des Fraunhofer IOSB. Im Anschluss zeigt das Fraunhofer ISI das wachsende Gefährdungspotential durch Industrie 4.0 und stellt Handlungsvorschläge zur Verbesserung der IT-Sicherheit vor. Das IOSB präsentiert das „Smart Factory Web“, eine Verbindung von Modellfabriken in Südkorea und Deutschland.

Schließlich gewährt die Firma HOMAG einen Einblick in das nationale Referenzprojekt zur IT-Sicherheit für „Industrie 4.0“. Im Anschluss an die Fachvorträge haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking". Die Möglichkeit zur Anmeldung finden Sie unter www.ka-it-si.de.



24 Krypto-Rätsel

Am 1. Dezember beginnt unser diesjähriges Adventsrätsel „Krypto im Advent“ für Schülerinnen und Schüler der Klassen 3-9. Der in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe entwickelte interaktive Adventskalender entführt in die Welt der Verschlüsselung und Geheimsprachen. Diesmal gilt es, drei Spione zu stoppen, die es auf die Weihnachtsgeschenke abgesehen haben... Wer alle Aufgaben richtig beantwortet, kann einen der zahlreichen, von unseren Sponsoren beigesteuerten Preise gewinnen.

Auch ältere, an der Kryptologie Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2016	
08.12.	IT-Sicherheit in der Produktion (KA-IT-Si, Innovationsallianz, Karlsruhe)
16.12.	Sicherheit oder Datenschutz: Ein falscher Gegensatz? (GFT, ZKM, GI Karlsruhe)
Januar 2017	
13.-15.01.	ShmooCon 2017 (The Shmoo Group, Washington/US)
16.-18.01.	Omnisecure 2017 (in TIME berlin, Berlin)
23.-25.01.	AppSec Cali 2017 (OWASP Foundation, Californien, US)
Februar 2017	
14.-15.02.	24. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2017	
06.-10.03.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.-16.03.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Überlingen)
27.-30.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Christoph Schäfer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Dezember 2016



Bescherung

Jahr für Jahr überrascht uns das Weihnachtsfest – kaum sind die warmen Tage Vergangenheit, müssen wir uns schon über passende Geschenke Gedanken machen. In diesem Jahr liegen die Festtage – wenigstens für Arbeitnehmer – besonders unpraktisch, und in der gefühlten Monatsmitte mahnt bereits der vierte Advent zur Eile.

Um Ihnen ein wenig aus der Verlegenheit zu helfen, haben wir Ihnen in dieser Weihnachtsausgabe der Security News einige aktuelle Geschenkempfehlungen zusammengestellt. Da sollte für jeden Geschmack und Bedarf etwas dabei sein.

Damit auch Sie nicht zu kurz kommen, wagen wir anlässlich des nahenden Jahresendes sogar einen Blick in die Glaskugel. Das vermeiden wir üblicherweise, um nicht weitere Prognosen in die Welt zu setzen, die niemand braucht – und über die man im Rückblick lächeln müsste, würde man sich die Mühe machen, sie ein oder zwei Jahre später auf ihren Wahrheitsgehalt zu prüfen.

Allerdings waren die Trends in Informationssicherheit und Datenschutz selten so deutlich erkennbar. So haben uns die erfolgreichen Ransomware-Angriffe sehr anschaulich demonstriert, dass saubere Backup-Prozesse und systematische Berechtigungsvergaben wichtiger sind als aktuelle Virenscanner. Nicht im Perimeter-Schutz liegt die Zukunft der Informationssicherheit, sondern in systematischen Risikoanalysen, konsequenter Schadensbegrenzung und wirksamen Incident-Response-Konzepten. Wir müssen lernen, mit Angriffen umzugehen, anstatt uns darauf zu konzentrieren, sie zu verhindern. Daher wird die professionelle Organisation der Informationssicherheit – vulgo: ISMS – signifikant an Bedeutung gewinnen.

Eine ähnliche Entwicklung ist im Datenschutz erkennbar. Hier sind jedoch nicht reale Schäden der Antrieb, sondern die (EU-)Gesetzgebung. Zertifikate und eine professionelle Organisation des Datenschutzes sind auch hier die Zukunft – das „DSMS“ lässt grüßen.



Inhalt

Bescherung

Security News

Für Schnäppchenjäger

Für Ungeduldige

Für Tablet-Fans

Für Vergessliche

Für Entwickler

Für die Jüngsten

Für Fans von Ausgefallenem

Für Scherzhafte

Für Schneeliebhaber

Secorvo News

T.I.S.P.- und T.P.S.S.E.-Zertifizierung

Wenn der Vorstand zweimal klingelt …

Veranstaltungshinweise

secorvo
security consulting

Security News

Für Schnäppchenjäger

Wer den Cent beim Weihnachtseinkauf gerne mehrmals umdreht, sollte einen Blick auf aktuelle Billig-Handys werfen. Trotz des günstigen Preises kommen sie mit kostenloser Zusatzsoftware auf den Gabentisch, die eine vollumfängliche Überwachung und heimliche Software-Updates ermöglicht. Zwar ist dieses Schnäppchen nicht ganz neu (schon 2014 haben Hersteller mit einer ähnlichen kostenlosen Dreingabe Kunden zu begeistern versucht) – aber ohne Zweifel effektvoll. Könnte von einem aufmerksamen Beschenkten allerdings, nicht ganz zu Unrecht, als Danaer-Geschenk verstanden werden.

Für Ungeduldige

Pünktlich zum ersten Advent hat das Bundesministerium des Inneren am 23.11.2016 den deutschen Unternehmen und Datenschützern mit dem neuen BDSG-Entwurf ein verfrühtes Präsent beschert. Angesichts der guten Wirtschaftslage geriet der Entwurf auch nicht knauserig: Er macht nicht nur Datenverarbeitern Geschenke, sondern spendiert ganze 79 Paragraphen – 65% mehr als das noch geltende BDSG. Darin bleiben die bisherige Bestellpflicht für betriebliche Datenschutzbeauftragte, die Regelung des § 32 BDSG für Beschäftigtendaten, der bisherige § 5 BDSG zum Datengeheimnis und die Strafvorschrift des § 44 BDSG erhalten. Die Betroffenenrechte aus Art. 12 ff DS-GVO werden hingegen über Art. 14 Abs. 5 DS-GVO hinaus eingeschränkt.

Allerdings ist auch bei diesem Entwurf fraglich, ob er die Öffnungsklauseln der DS-GVO nicht etwas sehr großzügig auslegt. Auch die zahlreichen Textwiederholungen, inzwischen ausgewiesen und reduziert, sind europarechtlich problematisch. Wer sich für dieses Geschenk entscheidet, sollte mit einem Umtausch rechnen.

Für Tablet-Fans

Kann man sich etwas Exotischeres vorstellen als ein nordkoreanisches High-Tech-Gerät? Nach dem Erfolg des Red Star OS erscheint in diesem Jahr, pünktlich zum Fest, das passende Tablet Woolim auf dem europäischen Markt. Dass das Gerät es in sich hat, werden Niklaus Schiess und Florian Grunow auf dem diesjährigen Hacker-Kongress 33c3 vom 27. bis 30.12.2016 demonstrieren. Der Funktionsumfang geht weit über den herkömmlicher Tablets hinaus: So gewährleistet das Woolim, dass die Beschenkten (und ihre Geheimdienste) nie mehr rätseln müssen, woher geteilte Bilder stammen oder wer subversive Nachrichten verfasst hat. Zur Steigerung des Benutzerkomforts nehmen außerdem intelligente Filtermechanismen dem Anwender die Entscheidung ab, welche Medien er konsumiert oder verbreitet.

Für Vergessliche

Passcodes können schon nervig sein – vor allem, wenn sich die Zeichenfolge nicht so recht im Gedächtnis einprägen will. Wer vergesslichen Zeitgenossen eine Freude machen möchte, der sollte einen Link auf das Youtube-DIY-Video vom 18.11.2016 verschenken. Darin wird gezeigt, wie sich der Passcode jedes iPhones und iPads – von iOS 8 bis iOS 10.2 – dank Siri mit wenigen Schritten umgehen lässt. Post-It-Anbietern könnte diese kleine Freundesgabe glatt das Geschäft vermasseln, sofern Apple nicht schnell Abhilfe schafft.

Für Entwickler

Sicherheitslücken in Software sind das Haupteinfallstor erfolgreicher Angriffe. Da liegt es nahe, befreundete Entwickler an Weihnachten z. B. mit einem Gutschein für ein T.P.S.S.E.-Seminar zu beglücken (siehe unten). Aber es geht auch billiger: So hat Google am 19.12.2016 eine neue Testsuite für Kryptoalgorithmen publiziert. Bisher konnte die Toolsammlung bereits über 40 Bugs in verschiedenen Implementierungen aufdecken.

Für die Jüngsten

Seit dem 06.12.2016 gibt es Produktinnovationen im Spielwarenbereich, die im Zeitalter des Internet of Things unter dem Weihnachtsbaum nicht fehlen dürfen: *My Friend Cayla* und *Hello Barbie* für Mädchen und der coole *i-Que Robot* für Jungs. Um immer die passende Antwort parat zu haben, senden diese smarten Toys die mit dem eingebauten Mikrofon aufgenommene Sprache direkt in die Cloud eines amerikanischen Unternehmens. Man darf sicher davon ausgehen, dass der Vorbehalt in den Nutzungsbedingungen für die Verwendung und Weitergabe der Sprachdaten ausschließlich der Verbesserung des Angebots dient. Bedenken könnten einen vielleicht hinsichtlich des Vokabulars beschleichen – das Unternehmen stammt nämlich aus dem Verteidigungssektor.

Für Fans von Ausgefallenem

Wer etwas Ausgefallenes für seine Liebsten sucht, der sollte auf bewährte Router der Deutschen Telekom zurückgreifen. Am Wochenende des 27.11.2016 fand eine beeindruckende Produktdemonstration statt, bei der fast eine Million Router den Dienst quittierten und die betroffenen Haushalte vom Netz der Telekom und dem Internet

trennten. Zwar hatte die Telekom noch Glück im Unglück, da die Ausfälle lediglich ein Kollateralschaden des eigentlichen Angriffs waren. Aber vielleicht sollte man dem Router unter dem Baum sicherheitshalber doch lieber eine eigene Firewall zur Seite stellen.

Für Scherzhafte

Mit ein wenig Unterhaltung wartet das Landgericht (LG) Hamburg zum Jahresende auf. Am 18.11.2016 hat es – in inhaltlicher Überdehnung eines EuGH-Urteils – eine einstweilige Verfügung wegen eines urheberrechtswidrig verwendeten Fotos auf einer Homepage beschlossen. Nur war in dem seither viel diskutierten Fall nicht der Website-Betreiber Antragsgegner, sondern ein Anbieter, der lediglich auf die Webseite eines Dritten mit diesem Foto verlinkt hat. Das LG Hamburg vertritt nun die Auffassung, dass ein auf eine Webseite verlinkender Anbieter diese zuvor auf die Rechtmäßigkeit ihrer Inhalte prüfen muss – ansonsten nähme er Verstöße bewusst in Kauf oder handele fahrlässig.

Damit hat das Landgericht zahlreichen Website-Anbietern Kopfzerbrechen bereitet. Der Heise-Verlag bat daher das LG Hamburg am 12.12.2016 vor der Verlinkung des Urteils um eine verbindliche Aussage zur Rechtskonformität seiner Website – die zu erklären das LG in einem amüsanten Schriftwechsel ablehnte. Hier eröffnet sich nun eine Vielzahl an Geschenkoptionen – von der Rechtskonformitätserklärung für Verlinkungen auf die eigene Webseite über täglich durchzuführende Prüfschritte bei allen verlinkten Webseiten bis hin zur Abmahnung Dritter wegen Urheberrechtsverstößen auf von jenen verlinkten Seiten.

Für Schneeliebhaber

Passend zum Fest liefern die Ransomware-Schmieden zwei neue Geschenke aus. Die Petya-Variante Goldeneye befreit Personaler von dem Problem unspezifischer Malware-Mails. Um dem Empfänger die Entscheidung (öffnen oder nicht öffnen?) zu erleichtern gibt sich Goldeneye als Bewerbung auf eine tatsächlich ausgeschriebene Stelle des Unternehmens aus. Welcher Personaler würde ein solches Geschenk nicht auspacken?

Eine noch kreativere Verbreitungsvariante hat Popcorn Time auf Lager. Dieser neue Ransomware-Strang stellt die kostenlose Entschlüsselung der eigenen Daten in Aussicht, wenn man seine Freunde infiziert: Entweder zahlt man 1.0 Bitcoin oder man verteilt den Trojaner an mindestens zwei Personen weiter. Wenn schon der Schnee an Weihnachten ausbleibt, sorgt man damit wenigstens für ein hübsches Schneeballsystem.

Secorvo News

T.I.S.P.- und T.P.S.S.E.-Zertifizierung

Schon bald können 1.000 deutsche Informationssicherheitsexperten ihre Kenntnisse und Erfahrungen mit einem T.I.S.P.-Zertifikat belegen. Wenn Sie auch zu diesem wachsenden Kreis von Experten zählen möchten, haben Sie vom **06. bis 10.03.2017** die Gelegenheit, Ihre Kompetenz zertifizieren zu lassen. Das einwöchige T.I.S.P.-Seminar und das Begleitbuch bereiten Sie perfekt auf die Prüfung vor.

Aber auch T.I.S.P.-Absolventen kommen im März auf ihre Kosten: Vom **14. bis 16.03.2017** bietet das Seminar „IT-Sicherheit heute“ die Gelegenheit, Ihre für die Rezertifizierung erforderliche fachliche Weiterbildung nachzuweisen.

Schließlich kommen auch Entwickler und Systemdesigner auf ihre Kosten: Das Seminar T.P.S.S.E. bereitet Sie vom **27. bis 30.03.2017** systematisch auf die Prüfung als zertifizierter Professional für sicheres Software-Engineering vor – hier lernen Sie, wie sich Security by Design in der Praxis umsetzen lässt.

Weitere Seminarangebote und die Möglichkeit zur Anmeldung finden Sie unter www.secorvo.de/seminare.

Wenn der Vorstand zweimal klingelt …

Seit einem guten Jahr gehören auch deutsche Unternehmen zu den Opfern der als „CFO Fraud“ oder „Fake President Fraud“ bekannt gewordenen Social-Engineering-Angriffe. Dabei erhalten gezielt ausgewählte Mitarbeiter mittelständischer oder großer Unternehmen E-Mails und Anrufe, die vermeintlich von der Unternehmensleitung stammen oder von ihr initiiert wurden. Unter der Vortäuschung streng vertraulicher Akquisitionen werden die Mitarbeiter dazu gebracht, große Zahlungen unter Umgehung interner Prozesse auszulösen.

Auf der Jahresauftaktveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) berichten Dr. Boris Hemkemeier und Ronny Wolf von der Commerzbank AG am **02.02.2017** über diese und andere aktuelle Cybercrimeangriffe gegen Unternehmen und zeigen, wie man sich dagegen schützen kann.

Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Januar 2017	
13.-15.01.	ShmooCon 2017 (The Shmoo Group, Washington/US)
16.-18.01.	Omnisecure 2017 (in TIME berlin, Berlin)
23.-25.01.	AppSec Cali 2017 (OWASP Foundation, Californien, US)
Februar 2017	
02.02.	Wenn der Vorstand zweimal klingelt ... (KA-IT-Si, Karlsruhe)
14.-15.02.	24. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
15.-16.02.	27. Smart Card Workshop (Fraunhofer SIT, Darmstadt)
März 2017	
06.-10.03.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.-16.03.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Überlingen)
27.-30.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Michael Knopp, Christoph Schäfer.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Januar 2017



Wie wirklich ist die Wirklichkeit?

Vor vierzig Jahren veröffentlichte Paul Watzlawick (1921-2007) sein wegweisendes Werk über die Relativität menschlicher Wahrnehmung. Darin belegt er überzeugend, dass unsere Weltsicht nie objektiv, sondern das Ergebnis von Kommunikation und (subjektiver) Interpretation ist. Neben kulturellen und sozialen Prägungen spielen dabei auch Phänomene wie sich selbst erfüllende Prophezeiungen eine Rolle. So wird unsere Wahrnehmung durch unsere eigene Weltsicht gefiltert: Konforme Erfahrungen werden als Beleg, widersprechende als die Regel bestätigende Ausnahme interpretiert.

Diese Einsicht müsste uns eigentlich skeptisch gegenüber unseren eigenen und tolerant gegenüber den Überzeugungen anderer stimmen. Stattdessen treibt uns eine unerschütterliche Wahrheitssehnsucht dazu, meist wenige Beispiele als Beweis für allgemeine Urteile zu akzeptieren: „Schau' Dir das einmal an. Da sieht man mal wieder, dass ...". Dabei dürfte nicht nur Mathematikern klar sein, dass man die Aussage „Jede Zahl ist eine Primzahl" nicht dadurch beweisen kann, dass man 3, 5, 7 und 11 als Beleg heranzieht.

In der von Blogs, Twitter und Facebook geprägten Meinungsöffentlichkeit finden wir heute unzählige solcher Belege für jedes unserer (Vor-)Urteile, die darüber zu Gewissheiten reifen. Darunter sind auch zahlreiche Falschbehauptungen („4 ist eine Primzahl"), die ebenfalls die eine oder andere Weltsicht zur Wahrheit veredeln. Keine guten Voraussetzungen für Selbstbescheidung und Toleranz.

Da passt es, dass Sprachlog.de am 31.01.2017 „Fake News" zum Anglizismus des Jahres 2016 gekürt hat. Würden wir wenigstens nur solche Behauptungen als „möglicherweise wahr" akzeptieren, deren Herkunft belegt ist, würden es „stille Post" und gezielte Falschmeldungen schwerer haben. Wäre das nicht mal eine wirklich großartige Aufgabe für digitale Signaturen?



Inhalt

Wie wirklich ist die Wirklichkeit?

Security News

Datenbank als Geisel

Überfällige Regulierung

Volatility 2.6

Der letzte Vorhang

Noch eine Verordnung

Secorvo News

Enkeltrick für Fortgeschrittene

Ihr Weg zum Zertifikat

Save the Date

Veranstaltungshinweise

secorvo
security consulting

Security News

Datenbank als Geisel

Im vergangenen Jahr machte Ransomware einen Großteil der Neuinfektionen mit Schadsoftware aus. Nach und nach erweiterten die Angreifer ihren Fokus und nahmen Unternehmen (vor allem deren Personalabteilungen) mit individualisierten E-Mails ins Visier. Jüngster Trend: Seit Anfang Januar sind über das Internet erreichbare mongoDB-Datenbanken von Verschlüsselungsangriffen betroffen. Eine neue Angriffswelle vom 12.01.2017 zielt dabei auf Installationen der Suchmaschine Elasticsearch. Die Angreifer verschlüsseln die Datenbankinhalte und fordern Lösegeld in Bitcoins. Nach Analysen des Sicherheitsforschers Niall Merrigan sind ihnen schon zehntausende Installationen zum Opfer gefallen.

Schutz vor den Angriffen bietet das Blockieren des Internet-Zugriffs auf die Datenbank. Außerdem sollten die Empfehlungen der Hersteller zur Zugriffskontrolle und sicheren Konfiguration umgesetzt werden. Und wie bei anderer Ransomware gilt auch hier: Regelmäßige Backups ermöglichen die Wiederherstellung der Daten, falls es doch zu einer Infektion kommen sollte.

Überfällige Regulierung

Die IT-Dienstleister von Berufsgeheimnisträgern wie Ärzten und Rechtsanwälten hadern schon lange mit der Strafbarkeit des (in der Praxis nicht auszuschließenden) Einblicks in die von ihnen verarbeiteten geheimen Daten. Nach Jahrzehnten der Rechtsunsicherheit hat sich nun die Bundesregierung mit einem Referentenentwurf vom 15.12.2016 der Überarbeitung des § 203 StGB angenommen.

Die Begründung des Entwurfs belegt (ohne es auszusprechen), dass sich die Mehrheit der Berufsgeheimnisträger seit Jahren durch die Inanspruchnahme von IT-Dienstleistungen strafbar macht. Die Gesetzesänderung sieht nun vor, dass der bisherige Gehilfenkreis um erforderliche Mitwirkende erweitert wird; dem Geheimnisträger fällt die Aufgabe zu, die Mitwirkenden sorgfältig auszuwählen, zu überwachen und zum Schweigen zu verpflichten.

Der insgesamt sehr zu begrüßende Entwurf benötigt sicher noch die eine oder andere Anpassung: So ist der Einsatz von Unterauftragnehmern nicht in § 203 StGB, wohl aber in der geplanten Rechtsanwaltsordnung erwähnt. Auch die Beauftragung einer juristischen Person scheint bezüglich der zu verpflichtenden Personen noch nicht zu Ende gedacht. Wenig überzeugend ist es auch, die korrespondierenden Zeugnisverweigerungsrechte erst in einem gesonderten Gesetz regeln zu wollen. Schließlich könnte das Kriterium der Erforderlichkeit erneut für Rechtsunsicherheit sorgen.

Volatility 2.6

Das Forensik-Framework Volatility ist nach 14 Monaten kontinuierlicher Weiterentwicklung seit dem 27.12.2016 nun als Release 2.6 verfügbar. Das bewährte Werkzeug für die Speicherforensik der Betriebssysteme Windows, Linux, Android und iOS hat viele neue und sinnvolle Funktionen für den Praktiker erhalten. Dazu zählen insbesondere die Unterstützung der aktuellen Versionen von Windows 10, Windows Server 2016 und KASLR Linux, deren neue Kernelstrukturen es schon längere Zeit deutlich erschwerten, spezifische Informationen aus dem Hauptspeicher zu analysieren.

Der standardisierte Funktionsumfang ist ebenfalls stark angewachsen. Inzwischen umfasst er 111 Windows-, 77 Mac- und 71 Linux-Plugins. Gerade für Mac und Linux sind viele Plugins mit den Schwerpunkten Prozesse und Dateien hinzugekommen, mit denen in der Analyse deutlich mehr Einsichten verfügbar sind als zuvor. Für Windows wurde in zahlreichen *dump-Plugins eine "--memory"-Option ergänzt, die es ermöglicht, auch die umliegenden Adressbereiche ausgeführter Prozesse automatisiert zu extrahieren. Das vereinfacht die Lokalisierung aktiven Schadcodes, der sich häufig außerhalb des eigentlichen Prozess-Adressraums befindet.

Die Standardausstattung an Plugins wird durch das Community-Repository fast verdoppelt, und dank ausgiebiger Tests konnte die Robustheit des Werkzeugs erneut gesteigert werden.

Der letzte Vorhang

Bereits am 21.12.2016 hat der EuGH ein neues Urteil zur Vorratsdatenspeicherung gefällt. Nachdem die Richtlinie zur Vorratsdatenspeicherung am 08.04.2014 für nichtig erklärt worden war, wurden jetzt auch die Schranken für nationale Regelungen geklärt. Die Entscheidung misst die allgemeine und unterschiedslose Vorratsdatenspeicherung von Telekommunikationsdaten an Art. 15 der ePrivacy-Richtlinie und an den Artikeln 7 (Achtung des Privatlebens), 8 (Schutz personenbezogener Daten) und 11 (Meinungsfreiheit) der Europäischen Grundrechtecharta. Im Ergebnis wiegen nach Überzeugung des Gerichtshofs die Grundrechte schwerer als Überwachungs- und Ermittlungsinteressen.

Eine Vorratsdatenspeicherung soll wegen des damit erzeugten Eindrucks einer ständigen Überwachung nur bei einem konkreten Bezug zwischen gespeicherten Daten und dem Überwachungsziel möglich sein. Eine allgemeine und unterschiedslose Vorrats-

datenspeicherung sei hingegen nicht zu rechtfertigen. Der Zugriff auf Vorratsdaten darf nur auf Grundlage eines gerichtlichen Beschlusses ermöglicht werden, die Speicherung ist auf das absolut Notwendige zu beschränken. Mit diesem Urteil wird auch die deutsche Neuauflage vom Dezember 2015 hinfällig, denn inhaltliche Beschränkungen der Vorratsdaten sind darin nicht vorgesehen.

Noch eine Verordnung

Die EU-Kommission hat am 10.01.2017 einen weiteren, die Datenschutz-Grundverordnung ergänzenden Verordnungsentwurf „Regulation on Privacy and Electronic Communication“ veröffentlicht. Er soll u. a. die e-Privacy-Richtlinie (RL 2002/58/EG) ersetzen und Widerspruchsfreiheit mit der neuen Regelungslage herstellen und ist Teil der Digital Single Market Strategy.

Die Verordnung zielt auf elektronische Kommunikationsdienste, Verzeichnisdienste und auch auf Software-Provider, die elektronische Kommunikationsdienste bedienen, sowie auf das Direkt-Marketing mittels elektronischer Kommunikation und auf Dienstleister, die Daten von Endgeräten sammeln. Sie soll als spezielle Regulierung der Datenschutz-Grundverordnung vorgehen.

Darin wird die Verwendung von Verkehrs- und Nutzungsdaten (außerhalb von technischen und Abrechnungszwecken) weitgehend auf Einwilligungen gestützt. Enthalten sind weiter umfangreiche Informationspflichten, Regelungen für Verzeichnisdiensteanbieter sowie Einwilligungserfordernisse bei Verwendung personenbezogener Daten und Regelungen zum Direkt-Marketing, die den bisherigen § 7 UWG berühren. Die Sanktionen lehnen sich an die Datenschutz-Grundverordnung an.

Gelten soll die Verordnung ab dem 25.05.2018. Sie führt zu tiefgreifenden Änderungen des deutschen Telemedienrechts und enthält eine Reihe neuer Bestimmungen. Für einen sorgfältigen Gesetzgebungsprozess erscheint der Zeitplan ambitioniert.

Secorvo News

Enkeltrick für Fortgeschrittene

Seit einem guten Jahr gehören auch deutsche Unternehmen zu den Opfern der als „CFO Fraud“ oder „Fake President Fraud“ bekannt gewordenen Social-Engineering-Angriffe. Dabei erhalten gezielt ausgewählte Mitarbeiter mittelständischer oder großer Unternehmen E-Mails und Anrufe, die vermeintlich von der Unternehmensleitung stammen oder von ihr initiiert wurden. Unter der Vortäuschung streng vertraulicher Akquisitionen werden die Mitarbeiter dazu gebracht, große Zahlungen unter Umgehung interner Prozesse auszulösen.

Auf der Jahresauftaktveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) berichten Dr. Boris Hemkemeier und Ronny Wolf von der Commerzbank AG am **02.02.2017** über diese und andere aktuelle Cybercrimeangriffe gegen Unternehmen und zeigen, wie man sich dagegen schützen kann.

Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (zur Anmeldung).

Ihr Weg zum Zertifikat

In Kürze fällt die „magische Marke“ der 1.000 Informationssicherheitsexperten, die ihre Kenntnisse und Erfahrungen mit einem T.I.S.P.-Zertifikat gekrönt haben. Falls auch Sie diesem wachsenden Kreis von Experten angehören möchten, bieten wir Ihnen vom **06. bis 10.03.2017** die Gelegenheit, Ihre Kenntnisse und Erfahrungen zertifizieren zu lassen. Das einwöchige T.I.S.P.-Seminar und das von uns verfasste Begleitbuch bereiten Sie gründlich auf die Prüfung vor.

Auch Absolventen einer T.I.S.P.-Zertifizierung kommen im März auf ihre Kosten: Vom **14. bis 16.03.2017** bietet Ihnen das Seminar „IT-Sicherheit heute“ die Gelegenheit, Ihre für die Rezertifizierung erforderliche fachliche Weiterbildung nachzuweisen.

Entwickler und Systemdesigner bereitet das Seminar T.P.S.S.E. (vormals CPSSE) vom **27. bis 30.03. 2017** systematisch auf die Prüfung als zertifizierter Professional für sicheres Software-Engineering vor. Hier erlernen Sie die konkrete Umsetzung von Security by Design in der Praxis. Weitere Seminarangebote und die Möglichkeit zur Anmeldung finden Sie unter www.secorvo.de/seminare.

Save the Date

Informationssicherheit und Datenschutz erfreuen sich seit Jahren wachsender Aufmerksamkeit. Inzwischen fordern Compliance-Erwartungen und staatliche Regulierung wie das IT-Sicherheitsgesetz oder die Datenschutz-Grundverordnung immer umfassendere Nachweise und belegbare Dokumentation. Damit rücken IT-Sicherheitszertifizierungen in den Mittelpunkt des Interesses.

Was aber bedeutet eine ISO-27001-Zertifizierung in der Praxis? Welcher Aufwand ist damit verbunden – und lohnt sich der? Was lässt sich aus den Erfahrungen zertifizierter Unternehmen lernen?

Diesen Fragen widmet sich die diesjährige **Secorvention** am **30. und 31.05.2017**. Das Programm finden Sie in Kürze auf unseren Webseiten.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2017	
02.02.	Wenn der Vorstand zweimal klingelt ... (KA-IT-Si, Karlsruhe)
14.-15.02.	24. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
15.-16.02.	27. Smart Card Workshop (Fraunhofer SIT, Darmstadt)
März 2017	
06.-10.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.-16.03.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Überlingen)
27.-30.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
April 2017	
05.-06.04.	Security Forum 2016 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-28.04.	2nd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Paris/FRA)
30.04.-04.05.	Eurocrypt 2017 (IACR, Paris/FRA)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Michael Knopp, Jochen Schlichting.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Februar 2017



Die Awareness-Falle

Wie haben wir uns das doch vor 20 Jahren herbeigesehnt: Kaum ein Tag ohne Schlagzeile über einen Security-Vorfall und nur noch wenige Unternehmensleitungen, die dem Thema Informationssicherheit mit Ignoranz begegnen.

Allerdings drohen wir inzwischen diesem Awareness-Erfolg selbst zum Opfer zu fallen. Immer häufiger lotst er Sensibilisierte in eine Fatalismus-Sackgasse: Wenn jedes Kryptoverfahren früher oder später gebrochen und jede Webanwendung geknackt wird – was nützen da noch Schutzmaßnahmen? Warum nicht die Ausgaben sparen und das Beste hoffen?

Nachlässig recherchierte oder mit Halbwissen verfasste Meldungen geben dieser Haltung immer wieder neue Nahrung. Nicht genug damit: Die jüngste Salonfähigkeit von „Fake News" gibt uralten Verschwörungstheorien neuen Aufwind („Tolles Geschäftsmodell: erst Viren(warnungen) verbreiten und dann Virenschutz verkaufen").

Aber die Komplexität der Wirklichkeit ist bekanntlich schwer zu vermitteln. Dabei gleicht die Arbeit eines Sicherheitsbeauftragten der eines Lotsen, der bekannte Untiefen umschifft und für alle unbekannten einen Notfallplan bereithält. Natürlich senkt er mit seiner Expertise Wahrscheinlichkeit und Schadensausmaß einer Havarie – wenn auch er sie nie gänzlich ausschließen kann.

Geht der Lotse seiner Arbeit still und sorgfältig nach, werden mangels Wertschätzung womöglich seine Einflussmöglichkeiten beschnitten oder sein Budget gekürzt. Buhlt er (oder die Öffentlichkeit) umgekehrt zu viel um Aufmerksamkeit für sein Thema, kann ihm dasselbe drohen: Denn wenn wenig passiert, kann das sein Verdienst sein – oder aber der Wirbel um das Thema erscheint übertrieben.

Das richtige Maß zu finden ist im Leben häufiger eine Herausforderung. Helfen kann die Orientierung an Standards und Best Practices: Ruhige Professionalität statt aufregungsgetriebener operativer Hektik wird auch hier auf mittlere Sicht den größeren Nutzen stiften.



Inhalt

Die Awareness-Falle

Security News

SHA-1-Kollision

DSAnpUG-EU

VPN-Apps im Playstore

DIY-Umkopierstation

Zulässige Videoüberwachung

Metasploit-Erweiterung

Secorvo News

Seminare

SECORVENTION 2017

Lass den Bauch entscheiden …

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

SHA-1-Kollision

Schon lange war das näher rückende Unwetter am Horizont zu sehen, nun hat der erste Blitz eingeschlagen: Am 23.02.2017 präsentierte eine Gruppe von Forschern des CWI Amsterdam und Google die erste SHA-1-Kollision – zwei PDF Dateien mit gleichem Hashwert. Mit 6.500 CPU-Jahren (oder 110 GPU-Jahren) ist der Aufwand zwar unrealistisch für Massenangriffe, aber immerhin um den Faktor 10^5 schneller als ein „Brute-Force"-Angriff.

Damit ist der SHA-1 nicht komplett gebrochen: Anwendungen, bei denen nur die Einweg-Eigenschaft gefordert ist, sind von dem Angriff nicht betroffen; auch Fingerprints und Signaturen, die nachweislich schon vor längerer Zeit erstellt wurden, sind nicht akut gefährdet. Die Autoren des Angriffs bieten sogar einen File-Tester an, der typische Muster ihres Angriffs erkennt.

Die Normung des SHA-2 und die ersten Angriffe auf den SHA-1 liegen 15 bzw. 12 Jahre zurück. Einen zügigen Wechsel hat behindert, dass der SHA-1 in Standards festgeschrieben war und Systeme in Umlauf gebracht wurden, deren Kryptofunktionen nicht per (Firmware-)Update ausgetauscht werden konnten. Vorausschauende Hersteller sollten gleich zusätzlich den SHA-3 implementieren, damit der nächste Wechsel weniger holperig verläuft.

DSAnpUG-EU

Das Bundeskabinett hat am 01.02.2017 nach einem neuen Anlauf des Bundesministeriums des Inneren ein Datenschutz-Anpassungs- und Umsetzungsgesetz EU beschlossen. Kernstück ist ein an die DS-GVO angepasstes Bundesdatenschutzgesetz (BDSG-E). Nachdem der vorausgegangene Gesetzentwurf sehr unübersichtlich und wiederholungslastig war (SSN 12/2016) hat sich nun Einiges getan: Er wurde unterteilt in die Umsetzung der Datenschutz-Grundverordnung und der Datenschutzrichtlinie für Polizei und Justiz. Ein wichtiger Regelungsgegenstand ist die künftige Aufsichtsstruktur: Die Vertretung im Europäischen Ausschuss übernimmt die Bundesdatenschutzbeauftragte mit einem gewählten Vertreter aus den Bundesländern.

Die §§ 32 ff. BDSG-E enthalten Einschränkungen der Informationspflichten und Betroffenenrechte. Dabei bleibt fraglich, ob diese ausreichend durch Öffnungsklauseln der DS-GVO gedeckt sind. Der Beschäftigtendatenschutz wurde um eine Freiwilligkeitsdefinition zur Einwilligung ergänzt, ansonsten entspricht er im Wesentlichen dem (ursprünglich provisorischen) bisherigen § 32 BDSG. Die Zulässigkeit der Videoüberwachung wird in § 4 BDSG-E massiv ausgedehnt. Daran haben die Aufsichtsbehörden bereits deutliche Kritik geübt.

Immerhin handelt es sich um einen Stand, an dem sich Unternehmen bei der Umsetzung der DS-GVO bereits vorsichtig orientieren können. Als Stärkung des Datenschutzes kann der Gesetzentwurf allerdings kaum gewertet werden.

VPN-Apps im Playstore

Seit Edward Snowdens Veröffentlichungen haben zahlreiche Apps mit VPN-Funktionalität den Weg in Googles Playstore gefunden. Ernüchternd allerdings die Ergebnisse einer Untersuchung von 238 VPN-Apps, die am 15.11.2016 auf der ACM-Konferenz IMC vorgestellt wurde: Danach weisen die meisten der von den Forschern analysierten Apps schwere Mängel auf. So verschlüsseln ganze 18 % den Datenverkehr gar nicht, nur 16 % verschlüsseln IPv6-Pakete und 66 % tunneln keine DNS-Anfragen. Einige verwenden Proxys, um den HTTP-Verkehr zu manipulieren und JavaScript-Code für Werbung oder Tracking in HTTP-Antworten unterzubringen. Andere haben keinen definierten Tunnelendpunkt, sondern leiten die Daten über andere Nutzer in Peer-to-Peer-Netzwerken weiter. Vier der untersuchten Apps brechen sogar den TLS-Verkehr auf.

Beim Einsatz von VPN-Apps muss man sich darüber im Klaren sein, dass das virtuelle Netzwerkinterface vollständig in der Hand des App-Herstellers liegt. Der Betrieb einer VPN-Infrastruktur ist nicht gratis, und dies kompensieren die Betreiber kostenfreier VPNs auch durch den Handel mit Nutzerdaten. Wem es mit dem Schutz der Privatsphäre ernst ist, der sollte nur Apps von Herstellern verwenden, die eine gute Reputation genießen – auch wenn dies mit Kosten verbunden sein sollte.

DIY-Umkopierstation

Am 02.02.2017 veröffentlichte das Computer Incident Response Center Luxembourg Version 2.1 des Projekts CIRCLean, einer Open Source-Lösung zum sicheren Umkopieren von Dokumenten von einem potentiell mit Malware infizierten auf einen vertrauenswürdigen USB-Stick. Die auf einem Raspberry Pi zu installierende Software unterstützt zahlreiche Datei- und Dateisystemformate, die auf der Projektseite aufgelistet sind.

Zur Installation der Umkopierstation genügt es, das Image auf eine SD-Karte zu schreiben, die SD-Karte und den zu kopierenden USB-Stick in den Raspberry Pi einzustecken und die Stromversorgung herzustellen. Auf dem Zielsystem werden die Dateien nach Datenarten (Text, Video, Audio etc.) sortiert abgelegt. Gefährliche Formate erhalten im Dateinamen

die Ergänzung "Dangerous"; dabei werden u. a. komprimierte Dateien auf Zip-Bomben überprüft. Der Abschluss des Kopiervorgangs wird akustisch signalisiert – solange der Raspberry Pi beschäftigt ist, spielt er einen Song aus der mitgelieferten Musiksammlung. Zumindest für das gelegentliche Kopieren von Dateien ist das ein praktikabler Ansatz – sicherlich verträglicher als das generelle Aussperren von USB-Speichermedien und womöglich wirksamer als ein Virenscanner.

Zulässige Videoüberwachung

Der Bayerische Landesbeauftragte für den Datenschutz, Prof. Dr. Petri, hat sich in seinem jüngsten, am 31.01.2017 veröffentlichten 27. Tätigkeitsbericht mit der Videoüberwachung vor allem in problematischen Umgebungen auseinandergesetzt. So fordert er z. B. für den Krankenhausbereich u. a. die Umsetzung einer maximalen Speicherfrist von zehn Tagen; im medizinischen Bereich habe die Aufzeichnung gänzlich zu unterbleiben.

Die umstrittene Frage, ob auf Kameraattrappen auch die datenschutzrechtlichen Bestimmungen anzuwenden sind, befürwortet der Landesbeauftragte unter Verweis auf das Bundesverfassungsgericht. Zudem fordert er als Nachweis für bestehende Gefahren als Überwachungsgrund eine längerfristige Vorfallsdokumentation.

Kameras, die sich selbst nur bei bestimmten Aktionen wie bspw. dem Betätigen eines Öffnungsschalters aktivieren, werden dagegen als regelmäßig unbedenklich eingeschätzt. Allerdings seien Kameras nach Wegfall der Gefährdungslage (z. B. dem Ausbleiben abzuwehrender Schadensfälle) auch wieder abzubauen. Insgesamt belegt der Bericht zahlreiche Fehler bei der Einrichtung von Videoüberwachungen, stellt allerdings – unter Verweis auf die bereit gestellten Schemata und Hilfestellungen des Landesbeauftragten – hohe Anforderungen an die Ausgestaltung.

Metasploit-Erweiterung

Mit der Veröffentlichung der Metasploit Hardware Bridge wurde das bekannte Exploitation Framework am 02.02.2017 um Schnittstellen erweitert, mit denen auch Systeme angegriffen werden können, die nicht über TCP/IP erreichbar sind. Ursprünglich lag der Fokus darauf, eine Schnittstelle zum CAN-Bus zu schaffen, um darüber beispielsweise Abläufe beim Car-Hacking denen „klassischer" Exploits anzunähern. Entstanden ist daraus jedoch eine generische Schnittstelle, die es zukünftig sehr erleichtert, Metasploit um neue Schnittstellen zu erweitern. ZigBee und JTAG werden bereits getestet. Da heute kaum mehr ein Gerät ohne eingebauten Computer und komplexe Software auskommt, ergeben sich so zahlreiche neue Angriffsszenarien, zumal Schnittstellen abseits von TCP/IP vielfach als Angriffsvektor vernachlässigt werden. Aus der Sammlung von Exploits ist mittlerweile ein für Pentester unverzichtbarer Werkzeugkasten mit mächtigen Tools zur Entwicklung von Exploits und Ausnutzung von Schwachstellen geworden.

Secorvo News

Seminare

Für Kurzentschlossene: Vom **14. bis 16.03.2017** geben wir Ihnen auf dem Seminar „IT-Sicherheit heute" einen Überblick über aktuelle Themen der IT-Sicherheit. Ein besonderes Highlight: der „Live Hacking Day" mit der Vorführung verschiedener Angriffsmethoden (Programm und Anmeldung).

Wie sichere Software-Entwicklung professionell funktioniert, zeigt das Seminar „T.P.S.S.E." am **27.-30.03.2017** mit der anschließenden Möglichkeit zur Zertifizierung (Agenda und Anmeldung).

SECORVENTION 2017

Compliance-Erwartungen und staatliche Regulierung wie das IT-Sicherheitsgesetz oder die Datenschutz-Grundverordnung fordern immer umfassendere Nachweise und belegbare Dokumentation. Damit rücken IT-Sicherheitszertifizierungen verstärkt in den Mittelpunkt des Interesses. Was aber bedeutet beispielsweise eine ISO-27001-Zertifizierung in der Praxis? Welcher Aufwand ist damit verbunden – und lohnt sich das? Was lässt sich aus den Erfahrungen zertifizierter Unternehmen lernen? Diesen Fragen geht die diesjährige SECORVENTION am **30. und 31.05.2017** auf den Grund. Sie findet statt in den stilvollen Räumlichkeiten der Buhlschen Mühle in Ettlingen. Das vollständige Programm und die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.secorvention.de.

Lass den Bauch entscheiden ...

... oder warum klassische Risikoanalysen in der Informationssicherheit nicht funktionieren: Bei unserem kommenden KA-IT-Si-Event am **23.03.2017** wirft Kai Jendrian (Secorvo) in seinem Vortrag einen tieferen Blick auf die Herausforderungen bei der praktischen Durchführung von Risikoanalysen in der Informationssicherheit. Dabei wird er verbreitete Ansätze gegenüberstellen und Anregungen für eine praxisorientierte Umsetzung gegeben.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2017	
14.-16.03.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Überlingen)
23.03.	No risk, no fun. (KA-IT-Si, Karlsruhe)
27.-30.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
April 2017	
05.-06.04.	Security Forum 2016 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-25.04.	a-i3/BSI-Symposium 2017 (Arbeitsgruppe Identitätsschutz im Internet, Bochum)
25.-26.04.	Datenschutztage 2017 (Forum für Datenschutz, Mainz)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-28.04.	2nd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Paris/FRA)
30.04.-04.05.	Eurocrypt 2017 (IACR, Paris/FRA)

Fundsache

Ein Team von Sicherheitsforschern (u. a. von Mozilla und Google) hat die HTTPS-Verbindungen von Security-Software und -Appliances untersucht. Dabei stellten sie fest, dass bei einigen Lösungen Angriffe auf die gesicherten Verbindungen möglich sind.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Dr. Safuat Hamdy, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2017



Sündenfall

In der Genesis beendet der Biss in die verbotene Frucht vom Baum der Erkenntnis, zu dem sich Adam und Eva verführen lassen, ihr Leben im Paradies. Wie auch immer man diese Szene interpretieren mag – die Strafe folgt dem Verstoß gegen das Verbot auf dem Fuße.

Selbst aus dieser existentiellen Erfahrung hat der Mensch offenbar nichts gelernt, und wird bis heute selten aus Erfahrung klüger. Denn auch die Informatik hat ihren Sündenfall, den sie bis heute nicht korrigiert hat. Die von *John von Neumann* (1903-1957) im Jahr 1945 veröffentlichte Referenzarchitektur für Computer, die auf Ideen *Konrad Zuses* (1910-1995) basierte, gehorchte ebenso wie die konkurrierende Harward-Architektur einem zentralen Grundprinzip: der strikten Trennung von Daten und Programm. Bis heute folgen Prozessorarchitekturen diesem Grundsatz: Befehle stehen in Befehls-, Daten in Datenregistern.

Bei den Betriebssystemen und Anwendungen nahmen es die Entwickler mit dem Prinzip schon bald nicht mehr so genau. Schließlich bereicherte die Makro-Programmiersprache Visual Basic for Applications Microsofts Office-Programme – der Biss in den Apfel: Wer seitdem ein Word-Dokument oder ein Excel-Sheet öffnet, startet zugleich etwaige darin enthaltene Programme oder Skripte.

Anfang der 90er Jahre folge die Strafe: Eine Welle von Makro-Viren verseuchte großflächig ganze PC-Netze. Gelernt haben wir fast nichts daraus: Seit fast 30 Jahren versuchen (nicht nur) Microsoft-Programmierer eifrig, jedes nur denkbare Skript in einem Office-Dokument auszuführen. Damit später niemand mit dem Finger auf sie zeigt, schalten sie Makros standardmäßig ab; klickt der Benutzer auf die Warnung („Inhalt aktivieren“ – klar, will ich doch das Dokument lesen), liegt die Verantwortung bei ihm, wenn anschließend unerwünschte Dinge passieren. Fallen die besonders hässlich aus, runzelt Microsofts Security Officer darob überrascht die Stirn.



Inhalt

Sündenfall

Security News

oldClouds

Nicht gehackt = sicher?

Datenschutz an der Grenze

Zertifikatsdesaster

Google Analytics

Secorvo News

Seminare

ISMS – Ready2Go

Software ist sicher.
Und die Erde eine Scheibe.

Veranstaltungshinweise

secorvo
security consulting

Security News

oldClouds

Am 16.03.2017 warnte das BSI, dass über 20.000 der in Deutschland betriebenen ownCloud- (bzw. Nextcloud-) Instanzen verwundbare Softwareversionen einsetzen, die kritische Sicherheitslücken enthalten. ownCloud wird oft als Alternative zu Dropbox oder ähnlichen Diensten für den vertraulichen Austausch großer Dateien empfohlen. Der Eigenbetrieb birgt allerdings die Herausforderung, die eigene Instanz sicher zu betreiben.

Auch andere Web-Anwendungen (wie Online-Shops oder CMS) werden oft nicht ausreichend gewartet und auf dem aktuellen Stand gehalten. Eine Hilfe dabei sind kostenfreie Dienste zur Prüfung von ownCloud (bzw. Nextcloud) auf bekannte Schwachstellen. Die automatische Installation von Sicherheitsupdates steht jedoch oft im Konflikt mit Schutzmaßnahmen wie dem Entzug von Schreibrechten auf den Verzeichnissen des Webservers. Daher sollte man einen zuverlässigen Dienstleister, der die Anwendung professionell wartet, einem halbherzigen Eigenbetrieb immer vorziehen.

Nicht gehackt = sicher?

Am 26.01.2017 spendierte Mozilla seinem Browser Firefox in Version 51 ein neues Feature: Der Browser warnt nun vor Passwortfeldern, die über eine unsichere HTTP-Verbindung übertragen werden. Der Betreiber einer Nachrichtenseite über die Öl- und Gasindustrie nahm diese Neuerung zum Anlass, am 20.03.2017 einen Fehlerbericht bei Mozilla einzureichen, da die Warnung die Nutzer seiner Seite verunsichere. Er betreibe ein selbstentwickeltes Sicherheitssystem, das in 15 Betriebsjahren kein einziges Mal geknackt worden sei. Diese Aussage nahmen einige Internet-Nutzer zum Anlass, die Seite einmal auf Herz und Nieren zu prüfen. Kurze Zeit später war ein Login nicht mehr möglich – die Benutzerdatenbank war gelöscht worden. Mittlerweile ist die Webseite nicht mehr erreichbar.

Leider ist der Glaube an die eigene Unfehlbarkeit bei der Entwicklung „unknackbarer" Sicherheitssysteme noch immer verbreitet. Oder, um es mit Bruce Schneier zu sagen: Jeder kann ein Sicherheitsystem erfinden, dass so sicher ist, dass er es selbst nicht knacken kann. Unknackbar ist es deshalb noch lange nicht...

Datenschutz an der Grenze

Die Electronic Frontier Foundation veröffentlichte am 07.03.2017 ein Whitepaper zum Datenschutz bei der Einreise in die USA. Laut Regierungsinformationen hat sich die Zahl der Durchsuchungen von Smartphones oder Notebooks 2016 auf knapp 24.000 verfünffacht. Für Berufsgeheimnisträger, aber auch für Reisende mit umfangreichen privaten oder geschäftlichen Daten auf ihren Geräten können solche Kontrollbefugnisse zum Problem werden. Das Papier empfiehlt daher vor Reiseantritt eine Risikoabschätzung, zu der zu beachtende Kriterien vorgeschlagen werden.

Der Rechtsteil erläutert u. a. die zugrunde liegende Ausnahme für Grenzkontrollen von dem vierten Verfassungszusatz, der gegen unverhältnismäßige Durchsuchungen oder Beschlagnahmen schützt. Durch die Ausnahme werden Durchsuchungen ohne richterlichen Beschluss an der Grenze möglich. Das Herausverlangen von Passwörtern wird am fünften Verfassungszusatz gemessen, nach dem niemand gezwungen werden darf sich selbst zu beschuldigen, und die unterschiedlich interpretierte Befugnislage thematisiert. Gewarnt wird vor einer unbeabsichtigten oder voreiligen Einwilligung in die Durchsuchung, da diese die Betroffenen weitgehend schutzlos stellt.

Die Maßnahmenvorschläge beginnen mit dem Löschen vor Reiseantritt und der Warnung vor der Wiederherstellbarkeit. Umfangreich diskutiert wird die verschlüsselte Speicherung über Cloud-Dienste. Eine empfehlenswerte Lektüre für USA-Reisende.

Zertifikatsdesaster

Am 23.03.2017 publizierte der Chrome-Entwickler Ryan Sleevi die Entscheidung des Chrome-Teams, von Symantec ausgestellten Zertifikaten das Vertrauen zu entziehen. In mehreren Fällen hätten die Entwickler seit Mitte Januar insgesamt über 30.000 Zertifikate identifiziert, bei denen Symantec sich bei der Ausstellung nicht an die Grundprinzipien eines seriösen Zertifikatsausstellungsprozesses gehalten habe. Sleevi kündigte an, in Chrome – gestuft nach Browser-Versionen – Symantecs Root-Zertifikate auf „ungültig" zusetzen und damit geschützte Webseiten als „unsicher" zu qualifizieren, beginnend mit Version 64 in neun Monaten.

Die relativ lange Übergangszeit für offensichtlich nicht vertrauenswürdige Zertifikate ist der Tatsache geschuldet, dass (Statistiken von Mozilla zu Folge) etwa 42 % aller Zertifikatsprüfungen Symantec-Zertifikaten zuzuordnen sind, da Symantec inzwischen zahlreiche CAs der ersten Stunde übernommen hat. Derzeit „verhandelt" Symantec noch mit Google. Bleibt es bei der Entscheidung und ziehen die anderen Browseranbieter nach, könnte das erhebliche Erschütterungen auslösen – beim Vertrauen der Nutzer in HTTPS ebenso wie bei den Unternehmen, die dann kurzfristig ihre Zertifikate ersetzen müssen.

Google Analytics

Der Hamburgische Datenschutzbeauftragte hat seine Handreichung zum Einsatz von Google Analytics am 21.02.2017 aktualisiert. Anlass war zum einen die EU-US-Privacy Shield Zertifizierung von Google, zum anderen das Schrems-Urteil des EuGH zur Safe Harbor Entscheidung. Die Handreichung hält nach wie vor einen datenschutzkonformen Betrieb von Google Analytics für möglich, nun gestützt auf die Angemessenheitsentscheidung über den Privacy Shield.

Als Voraussetzungen werden weiterhin die Beschränkung auf pseudonyme Profile, der Hinweis auf das Widerspruchsrecht und dessen technische Umsetzung sowie der Abschluss des von Google zur Verfügung gestellten Auftragsdatenverarbeitungsvertrages genannt. Bei letzterem ist die Nichtigkeit des Verweises auf Safe Harbor zu beachten. Weiter sind die Nutzer durch Verlinkung auf den von Google formulierten Datenschutzhinweis aufzuklären. Besondere Pflichten ergeben sich, wenn Webangebote durch Browser genutzt werden, die den Widerspruch nicht unterstützen. Auch hierfür wird von Google eine Lösung bereitgestellt. Außerdem ist weiter der Programmcode zur Kürzung der IP-Adressen durch Google zu verwenden. Bis Mai 2018 ist damit die Nutzung von Google Analytics rechtssicher möglich. Welche Konsequenzen sich aus der Datenschutzgrundverordnung ergeben lässt die Handreichung leider offen.

Secorvo News

Seminare

Wer beim PKI-Aufbau und –Betrieb nicht in dieselben oder ähnliche Fallen tappen will wie Symantec (siehe oben), dem sei das Seminar „PKI – Grundlagen, Vertiefung, Realisierung“ vom **25. bis 28.04. 2017** ans Herz gelegt. 20 Jahre Erfahrung mit der Konzeption und dem Aufbau von PKIs verstecken sich hinter der ständig aktualisierten Konzeption. Sie werden in Theorie und praktische Umsetzung eingeführt und dürfen selbst „Hand anlegen“. Es gibt nur noch wenige freie Plätze.

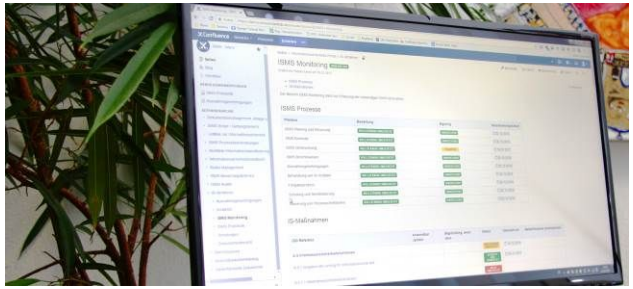
Im Juni bietet sich Ihnen vom **19.–23.06.2017** die nächste Möglichkeit, Ihre Kenntnisse und Erfahrungen in der Informationssicherheit mit dem T.I.S.P.-Zertifikat zu krönen. Ihre Referenten sind die Autoren des Begleitbuchs zum T.I.S.P., das sie vorab zur Vorbereitung erhalten.

Programm und Online-Anmeldung unter
https://www.secorvo.de/seminare

ISMS – Ready2Go

Aufbau und Betrieb eines Informationssicherheits-Managementsystems (ISMS) gemäß DIN ISO/IEC 27001:2015 erfordern in der Regel erhebliche Aufwände: ISMS-Prozesse müssen gestaltet und gelebt, die erforderliche Dokumentation erstellt und gepflegt, die Umsetzung von Vorgaben muss überwacht und kontrolliert werden. Nicht zuletzt müssen belastbare Umsetzungsnachweise erbracht werden. Die Erfüllung all dieser Anforderungen stellt insbesondere kleinere und mittlere Unternehmen vor besondere Herausforderungen.

Mit ISMS ready2go bietet Secorvo nun eine Lösung: Anstatt das Rad ständig wieder neu zu erfinden, hat Secorvo Best-Practice-Vorgaben aus über 15 Jahren Erfahrung mit Aufbau und Zertifizierung von ISMS in ein Produkt einfließen lassen, das es Unternehmen erlaubt, mit überschaubarem Aufwand und geringen Anpassungen in sehr kurzer Zeit die Anforderungen und Vorgaben der DIN ISO/IEC 27001 zu erfüllen und eine Zertifizierung effizient vorzubereiten. In Kürze steht die Zertifizierung der beiden ersten Kunden bevor.



Sollten Sie ebenfalls den Aufbau eines ISMS planen, setzen Sie sich gerne mit uns in Verbindung. Und melden Sie sich für die diesjährige SECORVENTION 2017 am **30.+31.05.2017** an.

Software ist sicher.
Und die Erde eine Scheibe.

Das nächste KA-IT-Si-Event am **18.05.2017** nimmt das Thema „Sichere Softwareentwicklung“ in den Fokus: Matthias Honka (asknet AG) wird die wichtigsten Prinzipien für die Softwareentwicklung und das technische Design sicherer Software-Systeme vorstellen.

Wenige einfache Regeln reichen dafür aus – und erschließen sich dem gesunden Menschenverstand. Oft genug jedoch werden sie missachtet, und Produktmanager, Entwickler und Administratoren reißen dadurch Sicherheitslücken.

Im Anschluss an den Vortrag haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2017	
24.-25.04.	a-i3/BSI-Symposium 2017 (Arbeitsgruppe Identitätsschutz im Internet, Bochum)
25.-26.04.	Datenschutztage 2017 (Forum für Datenschutz, Mainz)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-28.04.	2nd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Paris/FRA)
30.04.-04.05.	Eurocrypt 2017 (IACR, Paris/FRA)
Mai 2017	
03.-04.05.	OWASP Middle East Cyber Security Conference 2017 (OWASP Foundation, Dubai/AE)
08.-12.05.	OWASP AppSec EU 2017 (OWASP Foundation, Belfast/NIR)
09.-12.05.	European Identity & Cloud Conference 2017 (KuppingerCole Ltd., München)
16.-18.05.	15. Deutscher IT-Sicherheitskongress (BSI, Bonn)
17.-18.05.	18. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)
22.-24.05.	Entwicklertag 2017 (VKSI, GI, ObjektForum, Karlsruhe)
30.-31.05.	SECORVENTION (Secorvo, Ettlingen)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Kai Jendrian, Michael Knopp.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

April 2017



Moving Targets

Es ist die Königsdisziplin des Jägers: das Erlegen bewegten Wildes, „Bewegungsschießen“ genannt. Kein Auflegen der Waffe, kein ruhiges Zielen auf ein stehendes Tier – sondern Zielen und Schießen direkt aus der Bewegung.

Dabei dürfte sich der Jäger fühlen wie ein CISO: ständig neue, plötzlich auftauchende Ziele (≈ Bedrohungen) und wechselnde Bewegungsmuster (≈ Angriffstechniken) bei durch Bäume verstellter Sicht (≈ unvollständigen Spuren).

Dennoch hat der Jäger dem CISO etwas voraus: Er kann die Bewegungsabläufe am Schießstand üben. Der CISO hingegen ist dem Haken schlagenden Angreifer ausgeliefert: Während dieser seinen Angriff planen und strukturieren kann, ist jener zum Reagieren verdammt. Kein Wunder, dass sich da häufig das Bild eines „Katz‘ und Maus“-Spiels aufdrängt – bei dem der CISO nicht die Katze ist.

Aber stimmt das Bild tatsächlich? Die zahlreichen Berichte über erfolgreiche Angriffe täuschen leicht darüber hinweg, dass die weit überwiegende Mehrzahl der Angriffsversuche gerade nicht erfolgreich ist. Denn oft ist auch für einen Angreifer das Ziel ein *Moving Target*: Ständige Software-Patches und Betriebssystem-Upgrades, Änderungen an der Infrastruktur oder Wechsel des Schutzmechanismus‘ lassen wochenlange Recherchen und Vorbereitungen schnell Makulatur werden. Und auch der Angreifer hat keinen Schießstand – viele IT-Infrastrukturen sind so individuell, dass kein „Standardvorgehen“ zum gewünschten Ziel führt.

Warum machen wir daraus nicht eine Tugend? „Hase und Igel“ statt „Katz‘ und Maus“? Updates und Patches sollten ohnehin selbstverständlich sein – warum also das Ziel nicht auch durch Weiterentwicklungen der Schutzmechanismen „in Bewegung“ halten? Wer genug schnelle Haken schlägt, wird auch den Jäger ermüden. Bis dieser sich auf seinen Hochsitz zurückzieht und sich wieder dem äsenden Schwarzwild zuwendet.



Inhalt

Moving Targets

Security News

Versteckte Open-Source-Software

Anti-Virus Assisted Attacks

DSAnpUG-EU

Volatility automatisiert

Vorbeigefahren

Secorvo News

Secorvo Seminare

SECORVENTION 2017

9. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Versteckte Open-Source-Software

Am 19.04.2017 veröffentlichte die Firma Black Duck die Open Source Security and Risk Analysis (SSRA) 2017. Der Bericht basiert auf der Analyse von über 1.000 kommerziellen Anwendungen auf die Verwendung quelloffener Software. Bei 96% der untersuchten Anwendungen wurden die Autoren fündig. Dabei interpretiert ein Großteil der Hersteller die Lizenzbedingungen der quelloffenen Komponenten offenbar recht freizügig.

Aus Sicherheitssicht bedenklich ist allerdings, dass in 67% der Anwendungen verwundbare quelloffene Komponenten enthalten sind. Typische Kandidaten sind OpenSSL, jQuery oder Apache Tomcat. Ähnliches gilt für die am 20.04.2017 veröffentlichte Schwachstelle im NVIDIA-Grafikkartentreiber: Die proprietäre Software enthält einen NodeJS-Server, den Angreifer zum Umgehen von Sicherheitsmechanismen nutzen könnten. Das eigentliche Sicherheitsrisiko ist dabei nicht die Open-Source-Software an sich, sondern das unzureichende Schwachstellenmanagement der Softwarehersteller.

Um den Überblick zu behalten, sollten Abhängigkeiten wie Frameworks und Bibliotheken inklusive eingesetzter Versionsstände inventarisiert werden. Da sind die Entwickler in der Pflicht: Unter Rückgriff auf Schwachstellen-Datenbanken könnten sie so rechtzeitig Software-Updates bereitstellen.

Anti-Virus Assisted Attacks

Auf der diesjährigen ASIACCS am 05.04.2017 stellten Forscher der TU Braunschweig und der Universität Göttingen „Anti-Virus Assisted Attacks“ vor. Dabei werden keine Implementierungsfehler in der Antivirensoftware ausgenutzt, sondern die prinzipielle Funktionsweise signaturbasierter Erkennungsverfahren als Angriffsmittel missbraucht. Auf raffinierte Weise gelang es Wressnegger, Freeman, Yamaguchi und Rieck Bytefolgen herauszufinden, auf welche die untersuchten Virenscanner anschlagen. Diese Bytefolgen sind ein Erkennungsmerkmal („Marker“) infizierter Dateien.

Gelingt es nun, diese Bytefolgen in Dateien einzuschleusen, können erhebliche Störungen ausgelöst werden. Werden die Marker beispielsweise als Teil eines Textes oder Headers per E-Mail übermittelt, schlägt ein Virenscanner in der Regel nicht an, da er nur Anhänge prüft. Wird diese E-Mail von einem E-Mail-Client wie Thunderbird in einer Inbox-Datei gespeichert, kann ein lokaler Virenscanner die Inbox-Datei als „infiziert“ klassifizieren und entweder löschen oder in Quarantäne nehmen.

Kennt man den verwendeten Virenscanner, kann die Marker-Wahl auf ein bestimmtes Zielsystem abgestimmt werden. Zwar sind solche gezielten Angriffe mit einem gewissen Aufwand verbunden; auch hilft es, die „Inbox“ des E-Mail-Systems vom Virenscan auszunehmen. Dennoch ist dies ein weiterer überraschender Ansatz, um eine Schutzsoftware für Angriffe zu missbrauchen. Der erwartete Nutzen von Sicherheitslösungen sollte daher immer möglichen neuen Gefährdungen durch die Lösung selbst gegenübergestellt werden.

DSAnpUG-EU

Das Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG-EU) wurde am 27.04.2017 vom Bundestag verabschiedet, knapp drei Monate nach Beschluss des Kabinettentwurfs und ein halbes Jahr nach Bekanntwerden des stark kritisierten ersten Entwurfs.

Von den Änderungsvorschlägen des Bundesrats und der Kritik aus der Sachverständigenanhörung aus dem Innenausschuss wurde nur wenig berücksichtigt. Den Bedenken gegenüber den zusätzlichen Ausnahmeregelungen zu den Transparenzpflichten und Betroffenenrechten wurde lediglich durch kleinere Korrekturen Rechnung getragen. Die Einschränkung des Rechts auf Löschung beispielsweise wurde zwar auf analoge Daten beschränkt, ergeht aber immer noch ohne Öffnungsklausel in Art. 17 der DS-GVO.

Immerhin ist das One-Stop-Prinzip der Aufsicht von der europäischen Ebene auf die nationale übertragen worden: auch bei den Landesaufsichtsbehörden bestimmt jetzt die Hauptniederlassung des für die Verarbeitung Verantwortlichen die Zuständigkeit (§ 40 Abs. 2). Ansonsten behält das Gesetz die bisherigen Regelungen zum Beschäftigtendatenschutz, zum Datenschutzbeauftragten oder zum Scoring mit geringen Abweichungen bei.

In einigen für die Praxis und die Umsetzung der DS-GVO wichtigen Punkten herrscht nun Klarheit, etwa bei der Aufsichtsstruktur oder den Datenschutzbeauftragten. Das „neue BDSG“ ist allerdings erkennbar von dem Gedanken getragen, die DS-GVO entgegen den Betroffeneninteressen zu entschärfen. Letztere könnten der rekordverdächtigen Verabschiedungsgeschwindigkeit zum Opfer gefallen sein.

Volatility automatisiert

Volatility, das bewährte Werkzeug der Speicherforensik, lässt nur sehr wenige Wünsche offen. Einer davon ist mit dem am 06.04.2017 veröffent-

lichten robusten Volatize-Script in Erfüllung gegangen. Die kommandozeilenbasierte Ergänzung erlaubt es, mit automatischer Windows-Profilerkennung die wichtigen Aspekte der Bereiche Dump, Plugins, Strings, Timeline, VAD und Yarascan ohne weitere Interaktion für ein Hauptspeicherabbild abzuarbeiten.

Sehr hilfreich ist die automatische Erstellung der zentralen .volatilityrc-Konfigurationsdatei, die zeitsparende Umgebungsvariablen z. B. bei den Plugin-Aufrufen bereitstellt, und die dann von Volatility via Volatize für Performancesteigerungen von 30%-40% genutzt werden kann. Erzeugt man z. B. für eine große Zahl an Hauptspeicherabbildern vorab alle .volatilityrc-Konfigurationsdateien und skriptet den Volatize-Aufruf, kann man über den Playbook-Modus spezifische Datendumps direkt an die Virustotal-API übergeben.

Da Volatize quellcodeoffen ist, lassen sich damit auch Playbooks für spezifische Incident-Szenarien erstellen. In Kombination mit der yarascan-Option kann über eine große Anzahl von konvertierten hiberfil.sys-Hauptspeicherauslagerungsdateien mit der Signaturregel zur Equation Group vom 20.04. 2017 die Historie analysiert werden. Welches Unternehmen wüsste nicht gerne, ob es schon einmal Opfer eines erfolgreichen Angriffs war?

Vorbeigefahren

Bereits am 30.03.2017 hat der Bundestag das Gesetz zur Änderung des Straßenverkehrsgesetzes beschlossen. Ziel des Gesetzes ist es, einen gesetzlichen Rahmen für den Einsatz automatisierter Systeme in Fahrzeugen zu schaffen. Das Gesetz konzentriert sich zunächst auf die Regelung der Verantwortung, Sanktionen und Pflichten der Fahrzeugführer.

Bereits der Bundesrat hatte darauf hingewiesen, dass Verbraucherinteressen nicht ausreichend berücksichtigt, die Zulassungsvoraussetzungen für die Systeme nicht konkretisiert und dass vor allem Sicherheitsanforderungen bezüglich möglicher Angriffe von außen nicht geregelt würden.

Geregelt wurden dagegen Datenschutzfragen der Aufzeichnungen im Fahrzeug. Zwar wurde die Löschfrist von drei Jahren auf ein halbes Jahr verkürzt; dennoch blieben umfangreiche Zugriffsbefugnisse der Verkehrsbehörden bestehen. Der Schutz der Daten vor unbefugtem Zugriff, die diesbezügliche Verantwortung, eine ausreichende grundsätzliche Zweckbeschränkung und der erlaubte Umfang der Datenerhebung wurden dagegen nicht geregelt.

Insgesamt verfehlt das Gesetz das Ziel, einen verlässlichen Rahmen zu schaffen, da es letztlich nur einen Teil des Regelungsbedarfs aufgreift. Daher würde es nicht überraschen, wenn der Bundesrat nun den Vermittlungsausschuss anriefe.

Secorvo News

Secorvo Seminare

Vom **19. bis 23.06.2017** bieten wir Ihnen die nächste Möglichkeit, Ihre Kenntnisse und Erfahrungen in der Informations- und IT-Sicherheit mit einem T.I.S.P.-Zertifikat zu krönen. Zur Vorbereitung auf das einwöchige Intensivseminar mit anschließender Zertifizierung erhalten Sie vorab das Begleitbuch „Zentrale Bausteine der Informationssicherheit“. Sollte Ihnen eine Teilnahme an diesem Termin nicht möglich sein, bieten sich Ihnen am **25.** bis **29.09.2017** und am **27.11.** bis **01.12.2017** zwei weitere Gelegenheiten.

Programm und Online-Anmeldung unter https://www.secorvo.de/seminare

SECORVENTION 2017

Was bedeutet eine ISO-27001-Zertifizierung in der Praxis? Welcher Aufwand ist damit verbunden - und lohnt sich dieser? Was lässt sich aus den Erfahrungen zertifizierter Unternehmen lernen?

Antworten auf diese und ähnliche Fragen gibt es auf der SECORVENTION am **30.** und **31.05.2017** in der Buhlschen Mühle in Ettlingen. Das vollständige Programm finden Sie auf unserer Webseite www.secorvention.de.

9. Tag der IT-Sicherheit

Der „Karlsruher Tag der IT-Sicherheit“, eine Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative mit der IHK Karlsruhe und dem Cyber-Forum e.V., beschäftigt sich in diesem Jahr zum neunten Mal mit aktuellen Herausforderungen der IT-Sicherheit für Unternehmen. Als Keynote-Speaker konnten wir Herrn Dr. Stefan Brink, den frisch gekürten Landesbeauftragten für den Datenschutz in Baden-Württemberg gewinnen. Fachvorträge behandeln die Themen Risikomanagement, Aufbau eines DIN ISO 27001 orientierten ISMS und Social Engineering. Schließlich zeichnet das BSI ein aktuelles Lagebild der Cybersicherheit.

Gelegenheit zum fachlichen Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern gibt es am Buffet. Die Veranstaltung findet statt am **28.06.2017** im Saal Baden der IHK Karlsruhe. Das Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2017	
03.-04.05.	OWASP Middle East Cyber Security Conference 2017 (OWASP, Dubai/AE)
04.05.	BvD Verbandstag 2017 (BvD, Berlin)
08.-12.05.	OWASP AppSec EU 2017 (OWASP, Belfast/NIR)
09.-12.05.	European Identity & Cloud Conference 2017 (KuppingerCole Ltd., München)
16.-18.05.	15. Deutscher IT-Sicherheitskongress (BSI, Bonn)
17.-18.05.	18. Datenschutzkongress (EUROFORUM, Berlin)
22.-24.05.	Entwicklertag 2017 (VKSI, GI, ObjektForum, Karlsruhe)
30.-31.05.	SECORVENTION (Secorvo, Ettlingen)
Juni 2017	
07.-08.06.	Annual Privacy Forum 2017 (ENISA, EC DG Connect, Universität Wien, Wien/AT)
19.-23.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
28.06.	9. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)

Fundsache

Am 26.04.2017 veröffentlichte das SEI CERT (Software Engineering Institute der Carnegie Mellon University) eine sehr umfassende Liste von C++ Secure Coding Standards.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Mai 2017



Fragile IT-Sicherheit

Am 13.05.2017 wirbelte der Kryptotrojaner ‚WannaCry' die IT weltweit durcheinander. Von oft reißerischen Presseberichten getrieben beschäftigte der Vorfall Security-Verantwortliche auf der ganzen Welt. Mit etwas Abstand können wir heute den Fall genauer unter die Lupe nehmen: Was können wir daraus lernen?

WannaCry war weder ein besonders neuartiger noch ein besonders gut gemachter Angriff – im Gegenteil: Die Autoren machten Fehler, die frühere Kryptotrojaner schon nicht mehr enthielten. Eine Neuerung war die Verwendung eines der von der NSA gesammelten Exploits, die im April von Hackern veröffentlicht worden waren. So verbreitete sich der Trojaner sowohl via E-Mail (und die Schwachstelle Mensch) als auch über eine Wurmkomponente, die alle erreichbaren Rechner attackierte, die die vom Exploit ausgenutzte Windows-Schwachstelle aufwiesen. Wie andere Kryptotrojaner verschlüsselte er alle Dateien, auf die der betroffene Nutzer oder Rechner Zugriff hatte.

Vor derartiger Schadsoftware schützen nur aufeinander abgestimmte präventive und Schaden begrenzende Maßnahmen wirkungsvoll. Der Virenschutz hilft, bekannte Schädlinge aus dem Netz und vom Rechner fernhalten – gegen neue Schadsoftware hilft er selten. Daher gilt es, Benutzer zu sensibilisieren – und für den Fall der Fälle den Schaden einzudämmen und die Verbreitung zu begrenzen. Eine restriktive Berechtigungsvergabe und systematische Netzwerksegmentierung tragen ebenso dazu bei wie ein funktionierendes Backup- und Recovery-Konzept, ein sorgfältiges Patch-Management und der professionelle Umgang mit Vorfällen.

Das Zauberwort zur sinnvollen Abstimmung von Schutzmaßnahmen heißt übrigens Informationssicherheitsmanagement. Kombinierte Angriffe wie WannaCry werden zukünftig der Standard sein. Daher sollte man WannaCry als Weckruf verstehen, das eigene ISMS einmal auf den Prüfstand zu stellen.



Inhalt

Fragile IT-Sicherheit

Security News

Virus per Virenscanner

Sichere Passwörter revisited

Anfängerfehler

Interessenkollision

Phishing mit Unicode-Domains

Secorvo News

PKI-Policy-Rahmenwerk

Zertifizieren Sie Ihr Know-how

9. Tag der IT-Sicherheit

ISMS für alle

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Virus per Virenscanner

Im Schatten der allgemeinen Aufregung über die Schadsoftware WannaCry wurde im Mai eine kritische Schwachstelle in Microsofts Defender entdeckt: Am 05.05.2017 publizierte Travis Ormandy via Tweet die Entdeckung der gefährlichsten Windows-Schwachstelle seit langem. Sie steckte in der NScript-Komponente des Windows Defender, die mit erhöhten Rechten und ohne Sandbox-Mechanismen dynamische Analysen von JavaScript-Code durchführt, und lässt sich mit wenigen Zeilen JavaScript-Code beispielsweise in einer Website, E-Mail oder Datei platzieren. Der Angreifer kann darüber das komplette System übernehmen. Betroffen sind die meisten Windows-Versionen, allerdings ist die Ausnutzung bei neueren Versionen (Windows 10 und 8.1) durch zusätzliche Schutzmechanismen erschwert. Microsoft reagierte schnell und lieferte am 08.05.2017 ein Update aus, das die Schwachstelle behebt. Keine acht Tage später fanden Google-Forscher am 16.05.2017 via Fuzzing die nächste kritische Schwachstelle im Defender – für die Microsoft am 25.05.2017 einen Bugfix außerhalb des Update-Zyklus' lieferte.

Da signaturbasierte Ansätze heute praktisch wirkungslos sind, setzen Virenscanner verstärkt auf die dynamische Analyse von Inhalten. Dabei werden die Daten interpretiert oder ausgeführt. Solche Analysen sind riskant, denn wie bei jeder anderen Software muss man auch hier mit Schwachstellen rechnen – dank erhöhter Rechte und fehlendem Sandboxing eine heikle Angelegenheit. Daher ist die Frage berechtigt, ob Virenscanner inzwischen nicht mehr schaden als nützen.

Sichere Passwörter revisited

Am 02.05.2017 beendete das National Institute of Standards and Technology (NIST) die Diskussion des Entwurfs der Richtlinie für Digitale Identitäten. (NIST Special Publication 800-63B). Bemerkenswert sind der Wegfall der Empfehlung von Komplexitätsvorgaben und die Verankerung der Sicherheit von Passwörtern vor allem an deren Länge.

Die Begründung des Standards deckt sich mit unseren Erfahrungen – schon seit 2009 weisen wir auf Fehlsteuerungen durch die gängigen Hinweise zur Gestaltung von Passwörtern hin.

Anfängerfehler

Intels Active Management Technology ist ein Fernwartungsverfahren mit Webinterface. Mitte Februar 2017 wurde darin eine Sicherheitslücke entdeckt, die es einem Angreifer ermöglicht, damit ausgestattete Geräte fernzusteuern. Die besondere Brisanz dieser Schwachstelle liegt in der Möglichkeit, die Authentifizierung als Administrator zu umgehen.

Am 05.05.2017 wurden weitere Details öffentlich. Ursache war ein Fehler, dem ein Ehrenplatz in Lehrbüchern für Softwaresicherheit gebührt: Für den Vergleich zweier MD5-Hashwerte verwendeten die Programmierer die C-Funktion `strncmp()` – und übergaben als String-Länge die Angabe des Clients. Behauptete dieser, die Länge sei null, lieferte der Vergleich – Sie ahnen es – als Ergebnis „ok". Dabei ist der Fehler spätestens seit der Entdeckung des OpenSSL-Bugs Heartbleed im April 2014 (SSN 4/2014) ein Klassiker: Ein Server darf sich nie ungeprüft auf (nicht authentisierte) Längenangaben des Clients verlassen.

Interessenkollision

Am 05.05.2017 ist das Videoüberwachungsverbesserungsgesetz in Kraft getreten, das § 6b BDSG für die Überwachung öffentlich zugänglicher großflächiger Anlagen oder von Fahrzeugen und Einrichtungen des öffentlichen Personenverkehrs um eine Vorgabe für die Abwägung zwischen Betroffenen- und Überwachungsinteressen ergänzt: Der Schutz von Leben, Gesundheit oder Freiheit von Personen im Überwachungsbereich gilt danach als besonders wichtiges Interesse.

Der so entstandene § 6b BDSG ist auch bereits in dem (nun ebenfalls verabschiedeten) Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG) enthalten. Ausdrückliches Ziel ist es, die Sicherheit der Bevölkerung präventiv zu erhöhen, auch durch private Videoüberwachung.

Dass es sich hierbei um eine geeignete Maßnahme handelt wird von Aufsichtsbehörden und Datenschützern bezweifelt. Auf die Einordnung in das System der Datenschutz-Grundverordnung, etwa das Verhältnis zur hierfür verlangten Datenschutz-Folgenabschätzung oder die herangezogene Öffnungsklausel, wird im DSAnpUG nicht eingegangen.

Für Unternehmen, die ihr Gelände oder ihr Hausrecht durch eine Videoüberwachung schützen möchten, ändert sich durch das Gesetz wenig. Die Abwägungsvorgabe ist jedoch eine weitere Abwertung der Betroffeneninteressen. Ungeachtet der Intention ist die Bezugnahme auf Leben, Gesundheit und Freiheit jedoch paradox, denn auch die informationelle Selbstbestimmung ist ein Freiheitsgrundrecht. Daher wäre der Formulierung nach auch dem Betroffeneninteresse, unbeobachtet zu bleiben, besonderes Gewicht beizumessen.

secorvo
security consulting

Phishing mit Unicode-Domains

Namen von Unicode-Domains können so gewählt werden, dass eine gefälschte URL visuell praktisch nicht vom Original unterschieden werden kann – eine Steilvorlage für Phisher. Neu ist das nicht, aber durchaus unterhaltsam – siehe den Blogeintrag von Xudong Xheng vom 14.04.2017. Danach zeigt der Firefox-Browser mit Standardeinstellungen die URL apple.com (bitte mit Firefox öffnen) mit grünem Schloss-Symbol an. Nur wer sich das Zertifikat genauer ansieht (wofür eigentlich kein Anlass besteht) wird erkennen, dass die Website eigentlich www.xn--80ak6aa92e.com heißt.

Gegen solche Angriffe hilft, URLs „vertrauter" Domains manuell oder via Symbolleiste auszuwählen und nicht auf angebotene Links zu klicken. Alternativ setze man in den erweiterten Einstellungen (`about:config`) von Firefox den Parameter `network.IDN_show_punycode` auf `true`: Die URL wird dann als „echte" Adresse angezeigt. Die aktuelle Version 58 des Chrome-Browsers ist für solche Unicode-Angriffe nicht (mehr) anfällig.

Secorvo News

PKI-Policy-Rahmenwerk

Im Mai 2017 wurde das – in einer ersten Fassung bereits 2007 veröffentlichte – Secorvo White Paper zum Policy Rahmenwerk einer PKI überarbeitet und auf einen aktuellen Stand gebracht. Es enthält praxiserprobte und konkrete Hinweise zur Gestaltung von *Certificate Policies* (CP), *Certification Practice Statements* (CPS) und *PKI Disclosure Statements* (PDS). Im Anhang ist zusätzlich die deutsche Übersetzung des Gliederungsrahmens für eine PKI-Policy nach RFC 3647 enthalten.

Zertifizieren Sie Ihr Know-how

Kurzentschlossene können sich noch einen Platz auf dem nächsten T.I.S.P.-Seminar vom **19. bis 23.06.2017** sichern. Im Anschluss können Sie Ihre Fachkenntnisse und Erfahrungen in der Informationssicherheit zertifizieren lassen. Zur Vorbereitung erhalten Sie gleich nach Ihrer Anmeldung das Begleitbuch „Zentrale Bausteine der Informationssicherheit" zugesandt. Programm, Online-Anmeldung und weitere Termine: secorvo.de/seminare.

9. Tag der IT-Sicherheit

Auf dem neunten Karlsruher „Tag der IT-Sicherheit", einer Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe und dem CyberForum e.V., werden aktuelle Herausforderungen der IT-Sicherheit für Unternehmen aufgezeigt und Präventionsmöglichkeiten vorgestellt. Diesjähriger Keynote-Speaker ist Dr. Stefan Brink, Landesbeauftragter für den Datenschutz in Baden-Württemberg. Anschließend behandeln Fachvorträge die Themen Risikomanagement, Aufbau eines an der DIN ISO/IEC 27001 orientierten ISMS und Social Engineering.

Die Veranstaltung findet am **28.06.2017** im Saal Baden der IHK Karlsruhe statt. Das Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

ISMS für alle

Wie viel kostet ein DIN ISO/IEC 27001-konformes Sicherheitsmanagement-System? Die (realistische) Antwort auf diese Frage hat schon die eine oder andere Geschäftsleitung erblassen lassen. Die Etablierung eines wirksamen Risiko-Managements und die Definition der für die systematische Organisation der Informationssicherheit erforderlichen Rollen, Regelwerke, Prozesse, Berichte und Dokumentationen – auch als Nachweise für eine Zertifizierung – sind unvermeidlich mit Aufwand verbunden.

Dabei unterscheiden sich ISM-Systeme in der Praxis meist nur geringfügig – Prozesse, Dokumentationen und oft sogar Regelwerke gleichen sich sogar über Branchengrenzen hinweg. Warum also das Rad jedes Mal neu erfinden?

Aus unseren über 15 Jahren Erfahrung mit dem Aufbau und der Zertifizierung von ISM-Systemen haben wir ISMS ready2go entwickelt – eine Lösung, die die Einführung eines ISMS mit sehr überschaubarem Aufwand und geringen Anpassungen in sehr kurzer Zeit ermöglicht und den Anforderungen und Vorgaben der DIN ISO/IEC 27001 genügt. Die ersten Kunden äußern sich begeistert. Zwei Beispiele:

„ISMS ready2go folgt dem Need-2-Have-Prinzip: Mehr braucht es nicht, weniger auch nicht. Ein übersichtliches, individuell anpassbares und schlankes CMS, der ideale Begleiter für Ihr ISMS-Projekt."
(Detlef Pouw, Stiftung Kirchliches Rechenzentrum Südwestdeutschland)

„Automatische Auswertungen auf Knopfdruck, ein hierarchischer Workflow, so haben wir unser Risikomanagement sicher im Griff!"
(Markus Hotz, 3iMedia GmbH).

Sollten Sie ebenfalls am Aufbau eines ISMS arbeiten, setzen Sie sich gerne mit uns in Verbindung.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2017	
07.-08.06.	Annual Privacy Forum 2017 (ENISA, EC DG Connect, Universität Wien, Wien/AT)
19.-23.06.	Audit Challenge 2017 (ARC Institute, Frankfurt)
19.-23.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
28.06.	9. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
Juli 2017	
03.-05.07.	EssoS 2017 – International Symposium on Engineering Secure Software and Systems (EssoS, Bonn)
12.-14.07.	SOAPS 2017 – 13th Symposium on Usable Privacy and Security (USENIX, Santa Clara/US)
18.-21.07.	PETS 2017 – 17th Privacy Enhancing Technologies Symposium (Univ. of Minnesota, Minneapolis/US)
19.-20.07.	DuD 2017 (COMPUTAS, Berlin)
26.-27.07.	Blackhat USA 2017 (Blackhat, Las Vegas/US)
27.-30.07.	DEF CON 25 (DEFCON, Las Vegas/US)

Fundsache

Ein Forscherteam der Universität Braunschweig um Konrad Rieck fand in mehr als 200 Android-Apps Ultraschall-Seitenkanäle zum „Cross Device Tracking“ (SSN 01/2016). Eine (nicht nur) für Datenschützer beunruhigende Entwicklung – auch wenn sich die Zahl der betroffenen Apps mit 0,015% (noch) deutlich unterhalb der Relevanzschwelle bewegt.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick, Fabian Ebner, Stefan Gora, Kai Jendrian (Editorial), Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2017



In der Matrix

Der Wirtschaftsnobelpreisträger Daniel Kahnemann („Schnelles Denken – Langsames Denken") hat nicht nur dem Bild des rationalen „homo oeconomicus" den Todesstoß versetzt, sondern deutlich gemacht, dass unsere vermeintlich vernünftigen Entscheidungen allzu oft das Ergebnis „kognitiver Verzerrungen" sind: Wir schätzen Risiken falsch ein, werden von irrelevanten Relationen abgelenkt und lassen uns durch „Anker" z. B. bei Käufen auf Preise festlegen.

Zwar sind uns solche Wirkungen grundsätzlich vertraut: Wir kennen den Trick der Lebensmittelläden, neben der Kasse Schokolade in Kinderaugenhöhe zu platzieren. Wir wissen aus Blindtests, dass Marken unser Geschmacksempfinden beeinflussen. Und uns ist klar, dass die „Wird-oft-zusammen-gekauft"-Vorschläge des Online-Shops nicht philanthrop gemeint sind, sondern der Umsatzmaximierung dienen. Dennoch bilden wir uns ein, auf diese Einflüsse souverän zu reagieren – schließlich können wir auch anders entscheiden.

Unter der Oberfläche ist die Technik dank Big Data aber schon viel weiter. Shops lernen, ab welchem prozentualen Preisnachlass wir zugreifen, sie können aus unserem Einkaufsverhalten prognostizieren, wann wir in Spendierlaune sind, und passen ihre Angebote an unsere IT-Umgebung an: Für Mac-Nutzer ist das Leben meist teurer. Google-Remarketing sorgt für individualisierte Online-Anzeigen, die sich aus früheren Seitenbesuchen ableiten – da kann auch mal ein Shop dabei sein, der uns an einen abgebrochenen Kaufvorgang erinnert. Die virtuelle Welt wird bereits für uns zurechtgebastelt.

Und jetzt kommt die Wirklichkeit an die Reihe: Plakatwände, die uns wiedererkennen und die Werbung anpassen oder Läden, die unser Surfverhalten am WLAN-Hotspot auswerten und Preisvergleiche unterbinden, sind nicht mehr fern. Alles anonym, natürlich, und somit kein Datenschutzproblem.

Heimlich, still und unbemerkt sind wir auf dem Weg in die Matrix.



Inhalt

In der Matrix

Security News

Blackout real

Spyware as a Service

Kritische Infrastrukturen, Teil 2

Anonymes Internet 3.0

OpenVPN erwischt

Grenzwertiges Marketing

Diskrete Anpassung

Secorvo News

Secorvo Seminare

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Blackout real

Pünktlich zum fünfjährigen Jubiläum des Bestsellers Blackout haben Sicherheitsexperten von ESET am 12.06.2017 die detaillierte Analyse einer Schadsoftware veröffentlicht, die sie „Industroyer" getauft haben. Die Autoren spekulieren, dass die Software für den weitreichenden Stromausfall in Kiew am 17.12.2016 verantwortlich war – die technischen Fähigkeiten dafür besitzt sie offenbar. Die auf 17 Seiten dokumentierten technischen Details machen deutlich, dass es Angreifer gibt, die sich mit viel Know-how und Ressourcen industriellen Zielen widmen. Die dort verbreiteten Protokolle IEC 101 und IEC 104 sind zwei der Angriffspunkte, die über dynamisch aktivierbare Module attackiert werden.

Die erschreckende Vision von Marc Elsberg ist leider wohl (noch immer) näher an der Realität als Mancher es wahrhaben möchte. Für Betreiber von KRITIS-Infrastrukturen ist eine Absicherung nach dem Stand der Technik im Sinne des IT-SiG spätestens jetzt überfällig.

Spyware as a Service

Am 09.06.2017 erschienen erste Berichte zu einer neuen Spyware, die es auf Macs abgesehen hat. Das Besondere daran: Sie wird über das Darknet als Service verkauft. Gegen eine Gebühr von 30 Bitcoins (derzeit etwa 75.000 €) kann man den Service als Franchisenehmer weiterverkaufen. Die Spyware ermöglicht einem Angreifer, Bildschirmfotos, Umgebungsgeräusche und Tastaturanschläge aufzuzeichnen, Browserdaten auszulesen, iCloud-Fotos zu kopieren und die Zwischenablage zu sichern. Seit dem 15.06.2017 erkennen die gängigen Antivirenprogramme die Schadsoftware. Etwa zum gleichen Zeitpunkt erschien mit MacRansom ein Kryptotrojaner „as a Service" für MacOS.

Aufgrund seiner wachsenden Verbreitung zieht MacOS immer mehr Aufmerksamkeit von Hackern und Kriminellen auf sich. „Macs sind sicher" – so einfach ist die Welt mittlerweile nicht mehr.

Kritische Infrastrukturen, Teil 2

Das Bundeskabinett hat am 31.05.2017 den Referentenentwurf für den zweiten Korb der Verordnung zur Bestimmung Kritischer Infrastrukturen verabschiedet. Damit wird in Kürze auch für die Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr feststehen, welche Betreiber den Regelungen für Kritische Infrastrukturen unterfallen.

Die Änderungsverordnung bedarf keiner Zustimmung des Bundesrats, so dass noch im Juni mit einer Veröffentlichung im Bundesgesetzblatt gerechnet werden kann. Die nun erfassten Betreiber haben anschließend ein halbes Jahr Zeit, ihre Kontaktstelle für Meldungen (§ 8b Abs. 3 BSIG) einzurichten und zwei Jahre, um die nach § 8a BSIG geforderten Sicherheitsmaßnahmen umzusetzen.

Die Änderungsverordnung ergänzt zudem die bereits erlassenen Anhänge und Kataloge um Definitionen der Anlagen und passt einige Schwellenwerte an. Auch bei den neuen Sektoren wird die Kritikalität nach Versorgungs- oder Kapazitätsschwellenwerten festgestellt.

Während das Finanz- und Versicherungswesen bereits heute einer vergleichsweise strengen Regulierung in Sachen IT-Sicherheit unterliegt, kommen auf die Gesundheitsbranche und die Transport- und Verkehrsbetriebe vielfach neue Anforderungen zu, die bei den betroffenen Unternehmen und Einrichtungen für erheblichen Beratungs- und Dokumentationsbedarf sorgen werden.

Anonymes Internet 3.0

Wie werden Surfer im Internet identifiziert? Früher (und manchmal noch heute) geschah dies mit Hilfe von Cookies oder der IP-Adresse. Aber auch wer Cookies vermeidet und über mobile Netze surft, kann über weitere Merkmale identifiziert werden. Durch eine Korrelation der über den Browser zugänglichen Informationen wie Browserversion, Betriebssystem oder die installierten Plugins kann ein Benutzer „wiedergefunden" werden.

Wer dies vermeiden möchte, verwendet dedizierte Browser für einen anonymeren Zugang wie den am 07.06.2017 in Version 7.0 veröffentlichten Tor-Browser. Darin wird eine Identifikation des Nutzers durch Härtung des Browsers hinsichtlich der preisgegebenen Informationen erschwert und die Analyse der Internetnutzung durch Verwendung des Tor-Netzwerks verhindert. Wem dieses Maß an Privatheit noch nicht reicht, dem sei nahegelegt, sich die Mitte Juni angekündigte runderneute Version von Tails anzusehen. Tails 3.0 bietet eine - in der Regel von einem USB-Stick gestartete – Plattform an, welche ebenfalls das Tor-Netzwerk und den Tor-Browser nutzt. Durch die Nutzung dieser allgemeinen Plattform und Vermeidung individueller Informationen wird eine persönliche Zuordnung des Nutzers weiter erschwert.

OpenVPN erwischt

Wieder hat es ein Open-Source-Produkt erwischt: Am 21.06.2017 gab Guido Vranken in seinem Blog die Entdeckung von vier schwerwiegenden Sicherheitsschwächen bekannt – die zuvor von zwei un-

abhängigen Sicherheitsaudits nicht entdeckt und durch ein Code-Hardening nicht beseitigt worden waren. Aufdecken konnte er die Fehler durch Fuzzing, eine bereits 1989 entwickelte Analysemethode, der wir inzwischen die Entdeckung zahlreicher Bugs in unterschiedlichsten Anwendungen verdanken. OpenVPN-Nutzer sollten umgehend auf die Versionen 2.3.17 bzw. 2.4.3 wechseln.

Der Fall macht deutlich, dass eine Standardisierung der Methoden zur Code-Auditierung überfällig sind: zu häufig blieben kritische Schwachstellen unentdeckt, obwohl Verfahren zu deren Aufspürung existieren.

Grenzwertiges Marketing

Bereits am 30.05.2017 wurde Amazon ein Patent für ein von Miles J. Ward entwickeltes Verfahren erteilt, mit dem der Einzelhandel einen Internet-Preisvergleich der Kunden über das Laden-WLAN registrieren und unterbinden kann. Zwar muss man in Europa vorläufig nicht mit dem Einsatz dieser Lösung rechnen: Eine Sperrung des Zugriffs auf Vergleichsportale und andere Anbieter über das WLAN-Angebot ist rechtlich zulässig, nicht aber eine Auswertung der WLAN-Nutzung – das wäre ein rechtswidriger Eingriff in das Telekommunikationsgeheimnis.

Derzeit testen die Deutsche Post in rund 100 und Real in 40 Filialen im Rahmen eines Feldversuchs eine vom Fraunhofer-Institut in Erlangen entwickelte Analysesoftware, mit der sich die Inhalte von Werbetafeln über eine Auswertung von Videoaufzeichnungen der Betrachter steuern lassen. Dabei bestimmt die integrierte Gesichtserkennung Alter, Geschlecht und Verweildauer des Kunden.

Die Rechtmäßigkeit dieser Videoanalysen wurde vom Bayerischen Landesamt für Datenschutzaufsicht bestätigt. Auf die Videoüberwachung werde hingewiesen, und die Analyse erhebe keine personenbezogenen Daten.

Die beiden Beispiele zeigen, dass die Grenzen des datenschutzrechtlich Erlaubten nicht nur in der Online-Werbung sondern auch bei Ladenbesuchen zunehmend ausgereizt werden. Bei den Videoanalysen mit Gesichtserkennung treffen dabei durchaus plausible Anonymisierungskonzepte auf das Problem mangelnder Transparenz und Vertrauenswürdigkeit. Dabei wird zweifellos bei den Betroffenen ein Überwachungsdruck erzeugt, dessen datenschutzrechtliche Berücksichtigung allerdings umstritten ist.

Diskrete Anpassung

Weitgehend unbeachtet von der Öffentlichkeit treibt der Gesetzgeber die Anpassung des Datenschutzrechts an die Europäische Datenschutz-Grundverordnung voran. Die jüngsten Änderungen von immerhin 12 Gesetzen verstecken sich in einem am 01.06.2017 verabschiedeten Artikelgesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften.

Darin behandelt werden vor allem Betroffenenrechte in Bezug auf öffentliche Register, bspw. das Handelsregister, das Patent- und Markenregister oder das Register vergriffener Werke, sowie die Verarbeitung von Daten durch die Finanzbehörden (Änderungen der AO). Hier ist besonders die Regelung zur Auftragsdatenverarbeitung von Steuerdaten hervorzuheben: Die hier vorgenommenen strengen Einschränkungen bilden einen Gegensatz zu den Planungen bzgl. der Dienstleister anderer Berufsgeheimnisträger. Beschränkt werden das Auskunftsrecht, Mitteilungspflichten gegenüber dem Betroffenen und Berichtigungsansprüche.

Bei den vorgenommenen Beschränkungen kann sich der Gesetzgeber auf Art. 23 DSGVO stützen. Dieser lässt allerdings Einschränkungen der Betroffenenrechte nur zu spezifischen Zielen im öffentlichen Interesse zu, nicht zur Aufwandsbegrenzung der Behörden. Zudem gibt Abs. 2 Kompensationen vor. Hier hat der Gesetzgeber den Gestaltungsspielraum der DSGVO womöglich überschritten.

Secorvo News

Secorvo Seminare

Nach dem T.I.S.P. ist vor dem T.I.S.P. – gerade erst haben sich zwölf Teilnehmer unseres T.I.S.P.-Seminars erfolgreich auf die Zertifizierung vorbereitet, und schon läuft die Vorbereitung des nächsten T.I.S.P.-Seminars vom **25. bis 29.09.2017**. Die Sommerpause ist die beste Zeit zur Vorbereitung: Nach Ihrer Anmeldung erhalten Sie das Begleitbuch „Zentrale Bausteine der Informationssicherheit“ zugesandt. Die letzte Gelegenheit zur T.I.S.P.-Zertifizierung im Jahr 2017 bieten wir Ihnen vom **27.11. bis 01.12.2017**.

Für unser PKI-Seminar vom **06. bis 09.10.2017** gibt es bereits zahlreiche Anmeldungen, daher empfehlen wir allen Interessenten an einem vertieften Einblick in Public Key Infrastrukturen eine baldige Buchung.

Programme, Online-Anmeldung und weitere Termine: secorvo.de/seminare.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2017	
03.-05.07.	EssoS 2017 – International Symposium on Engineering Secure Software and Systems (EssoS, Bonn)
12.-14.07.	SOAPS 2017 – 13th Symposium on Usable Privacy and Security (USENIX, Santa Clara/US)
18.-21.07.	PETS 2017 – 17th Privacy Enhancing Technologies Symposium (Univ. of Minnesota, Minneapolis/US)
26.-27.07.	Blackhat USA 2017 (Blackhat, Las Vegas/US)
27.-30.07.	DEF CON 25 (DEFCON, Las Vegas/US)
August 2017	
06.-09.08.	DFRWS USA 2017 - Digital Forensic Research Workshop (DFRWS, Austin/US)
16.-18.08.	26th USENIX Security Symposium (Usenix, Vancouver/BC)
20.-24.08.	Crypto 2017 (IACR, Santa Barbara/US)

Fundsache

Bereits am 18.11.2016 hat die Group Privacy der Deutschen Telekom eine erste Fassung von konzernweit gültigen „Binding Interpretations" der DSGVO verfasst. Das hilfreiche, gut 100 Seiten starke Dokument ist online zugänglich.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Fabian Ebner, Stefan Gora, Kai Jendrian, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Juli 2017



EDA-Daten

Ein beliebter Fehler in Kostenrechnungen sind die übersehenen EDA- (oder „Eh-da“-) Kosten: Fixkosten für Personal, Infrastruktur oder bereits verfügbare IT-Systeme. Sie erzeugen keine unmittelbaren Kosten – sind (oder waren) aber natürlich irgendwann einmal fällig. Würde man sie konsequent berücksichtigen, wären zahlreiche Projekte und Maßnahmen erheblich teurer als kalkuliert, und viele davon unwirtschaftlich. Genau deshalb sind sie bei Projektleitern so beliebt wie bei Controllern verhasst: Wer EDA-Kosten geschickt zu verstecken weiß, kann die Durchsetzung eines Lieblingsprojekts mit Wirtschaftlichkeitsargumenten forcieren.

Was dem Controller die EDA-Kosten sind dem Datenschützer die EDA-Daten: Mit jeder neuen Anwendung fallen sie an. Meist sind es Log-Daten, die ursprünglich zur Fehlersuche dienten. Für viele dieser Daten lassen sich zahlreiche andere Nutzungen finden: Verknüpft man Login- und Logout-Zeiten eines Administrators mit seinen Urlaubszeiten, lassen sich Unregelmäßigkeiten entdecken; leitet man aus den E-Mail-Logfiles die Intensität von Kommunikationsbeziehungen ab, kommt man womöglich Insidergeschäften auf die Spur.

Aber die Begehrlichkeiten machen bei Compliance- und Sicherheitsanwendungen nicht halt. Gewöhnt haben wir uns an die Auswertung unseres Online-Verhaltens, auch wenn uns vielleicht nicht klar ist, was diese Spuren alles enthüllen: Schon wenige hundert Likes erlauben Kaufprognosen, die so zuverlässig sind wie die Einschätzung unseres Lebenspartners. Auch Microsoft hat die Möglichkeiten der EDA-Daten entdeckt und bietet in Office 365 einen Dienst zur Analyse des Mitarbeiterverhaltens. Und der Hersteller des Mäh- und Staubsaugerroboters iRobot, Roomba, deutete kürzlich an, er wolle die über Wohnungen und Grundstücke erhobenen Daten verwerten.

Dabei gibt es – anders als bei EDA-Kosten – ein sehr einfaches und probates Mittel gegen EDA-Daten: Löschen.



Inhalt

EDA-Daten

Security News

WhatsApp illegal

Trau, schau, wem!

Schöne neue Arbeitswelt

Berufsgeheimnisträger

Ende der Störerhaftung

Secorvo News

SSN-Jubiläum

Frisches aus der Hackerküche

Secorvo-Publikationen

Secorvo-Seminare

Veranstaltungshinweise

secorvo
security consulting

Security News

WhatsApp illegal

Das Amtsgericht Bad Hersfeld hat sich in einem unterhaltsamen Sorgerechtsbeschluss vom 20.03. 2017 detailliert zur Legalität der Nutzung von WhatsApp geäußert und die Eltern zum Einholen von Einwilligungen aller im Adressbuch des Sohnes geführten Personen oder zur Deinstallation verpflichtet. Daneben stellte es eine Pflicht der Eltern zur Aneignung digitaler Kompetenz fest.

Der 12-jährige Sohn hatte vorgetragen, sein Vater habe ihn „auf WhatsApp blockiert". Das Gericht sah sich daraufhin veranlasst, Anordnungen zur Abwehr von Gefahren für das Kind zu treffen. Durch den Upload des Adressbuchs zur – nach den Geschäftsbedingungen – undefinierten weiteren Nutzung durch WhatsApp werde das Recht auf informationelle Selbstbestimmung (!) der geführten Personen verletzt, wodurch der Sohn möglichen Abmahnungen und Unterlassungsbegehren nach § 823 BGB ausgesetzt sein könne. Eine genauere Betrachtung der Rechtsgrundlagen des BDSG und der Verantwortlichkeiten erfolgte allerdings nicht.

Dass der Upload des Adressbuchs unter Vorbehalt undefinierter Nutzungszwecke rechtlich problematisch ist, ist zutreffend und führt zu Recht auch zu entsprechenden Warnungen bzgl. der WhatsApp-Nutzung im Unternehmensumfeld. Die hier verlangte Einwilligung kann dies allerdings mangels Bestimmtheit nicht heilen. Für das private Umfeld ist die Begründung des Amtsgerichts schlicht unzureichend. Als Beleg für die (durchaus vertretbare) Rechtswidrigkeit der WhatsApp-Nutzung ist das Urteil trotz seines klaren Tenors deshalb leider gänzlich ungeeignet.

Trau, schau, wem!

Die NSA hat Ende Juni die Liste ihrer Tools, die im Rahmen des NSA Technology Transfer Program (TTP) der Open Source Community zugänglich gemacht wurden, aktualisiert. Die Liste umfasst mehr als 30 Einträge, darunter WELM, GRASSMARLIN, SHB und LOCKLEVEL.

WELM extrahiert die in Windows Binaries eingebetteten Definitionen für Windows Event-Log-Einträge und konvertiert diese in besser auswertbare Formate wie JSON oder CSV. Um die Topologien von ICS- (*Industrial Control System*) bzw. SCADA- (*Supervisory Control and Data Acquisition*) Netzwerken zu analysieren, kann auf GRASSMARLIN zurückgegriffen werden. SHB (*Secure Host Baseline*) oder LOCKLEVEL beschäftigen sich mit der Härtung von Windows-Betriebssystemen.

Die Tools erfüllen den vorgesehenen Zweck – dennoch ist ein gesundes Misstrauen gegenüber den NSA-Tools zweifellos angebracht.

Schöne neue Arbeitswelt

Microsoft plant Analysetools anzubieten, die es ermöglichen sollen, das Zeitmanagement der Mitarbeiter bspw. bei der E-Mail-Nutzung oder Terminplanung sowie die Ressourcennutzung und Zusammenarbeit zu analysieren und auszuwerten. Workplace Analytics soll als Teil von Office 365 angeboten werden.

Workplace Analytics ist seit dem 05.07.2017 bereits als Add-On für Kunden der O365-Suite verfügbar. Der Deutsche Gewerkschaftsbund hat bereits reagiert und die spätestens durch dieses Angebot eingetretene betriebliche Mitbestimmungspflichtigkeit der O365-Einführung postuliert.

Dass es sich bei diesem Angebot um einen gut überlegten Schritt von Microsoft handelt, darf bezweifelt werden. Mit dem neuen Angebotsbestandteil werden die dem bisherigen Einsatz zugrunde liegenden datenschutzrechtlichen und betriebsverfassungsrechtlichen Erwägungen hinfällig. Unternehmen, die bereits O365 einsetzen, werden ihre Entscheidung nachbessern müssen – mit Blick auf die Mitbestimmung mit ungewissem Ausgang. Aus Datenschutzsicht ist der neue Dienst hinsichtlich der Rechtsgrundlagen und Datenschutzanforderungen kritisch zu prüfen; danach sind mindestens neue Prozesse und Regelungen zum Umgang mit diesem Dienst zu schaffen.

Berufsgeheimnisträger

Am 29.06.2017 hat der Deutsche Bundestag das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen verabschiedet. Das Gesetz beendet die Strafbarkeit der Auslagerung von IT-Dienstleistungen durch Berufsgeheimnisträger, die eintritt, sobald der Dienstleister Einblick in geschützte Daten erhält (§ 203 StGB). Im Ausgleich regelt es Voraussetzungen der Dienstleistereinbindung und das Zeugnisverweigerungsrecht des Dienstleisters (§ 53 StPO-neu).

Die Pflichten des Auftraggebers regelt das Gesetz in Änderungen der einschlägigen Berufsordnungen. Daher profitieren vor allem Ärzte zunächst noch nicht, da hier Landesregelungen angepasst werden müssen. Berufsgeheimnisträger müssen die Möglichkeit des Dienstleisters, auf vertrauliche Daten zuzugreifen, auf das Erforderliche beschränken, den Dienstleister sorgfältig auswählen und in einem schriftlichen Vertrag auf Verschwiegenheit verpflichten.

Die Strafbarkeit der Geheimnisoffenbarung wird auf die mitwirkenden Personen erstreckt; das Versäumen der Verpflichtung wird ebenfalls unter Strafe gestellt. Das Erfordernis von Auftragsdatenverarbeitungen bleibt unberührt.

Das Gesetz schafft eine überfällige Rechtsgrundlage vor allem für die zahlreichen IT-Dienstleistungen, deren Berufsgeheimnisträger bedürfen; diesbezüglich kann es nur begrüßt werden (SSN 1/2017). Der Schutz der Geheimnisse wird jedoch unweigerlich erheblich geschwächt.

Ende der Störerhaftung

Mit dem Dritten Gesetz zur Änderung des Telemediengesetzes hat der Bundestag nach der zaghaften Einschränkung vom 21.07.2016 nun in § 8 Abs. 1 TMG-neu die Haftung auf Schadensersatz oder auf Unterlassung von WLAN-Anbietern für rechtswidriges Nutzerverhalten ausgeschlossen. Das Gesetz wurde am 30.06.2017 verabschiedet, der Bundesrat muss nicht mehr zustimmen.

Mit der Abschaffung reagiert der Gesetzgeber auf das EuGH-Urteil zur WLAN-Haftung vom 15.09.2016. Für WLAN-Anbieter wird durch den Ausschluss der Störerhaftung ein wesentliches Rechtshindernis beseitigt, sodass Internetanschlüsse nun ohne Identifizierungserfordernisse oder Belehrungen der Nutzer Dritten zur Verfügung gestellt werden können. § 7 TMG-neu ermöglicht den Rechteinhabern allerdings, von den Anbietern Sperrungen von Inhalten zu verlangen. Die Kosten einer solchen Anordnung können jedoch nicht mehr dem Anbieter auferlegt werden.

Der Abmahnindustrie wird durch die Neuregelung weiter Boden entzogen. Für Anbieter und Internetnutzer handelt es sich trotz der verbliebenen Sperrthematik um eine lange erwartete gute Nachricht.

Secorvo News

SSN-Jubiläum

Am 04.07.2002 erschien die erste Ausgabe der Secorvo Security News. Seit nunmehr 15 Jahren versorgen wir Sie monatlich mit Hintergrundinformationen und Einschätzungen zu den (nach unserer Bewertung) wichtigsten Security-Ereignissen des jeweiligen Monats. 180 Ausgaben mit insgesamt 720 Seiten – trotz der von uns angestrebten inhaltlichen „Verdichtung“ ein kolossales Werk.

Wir danken Ihnen für Ihre Lese-Treue, mit der Sie dazu beigetragen haben, dass die SSN heute zu den wichtigsten Informationsquellen zur IT- und Informationssicherheit in Deutschland zählen.

Frisches aus der Hackerküche

Nach der Sommerpause werden Benjamin Lipp und Timon Hackenjos (Fraunhofer IOSB) beim KA-IT-Si-Event am **21.09.2017** zeigen, wie ein im September 2016 veröffentlichter Angriff auf Windows-Anmeldeinformationen in abgewandelter Form auch heute noch funktioniert. Anschließend stellen Benny Görzig und Florian Loch (ebenfalls Fraunhofer IOSB) Angriffe auf das Netzwerkauthentifizierungsprotokoll WPA2-PSK vor, das die meisten von uns in ihren privaten WLAN-Netzen benutzen. Wird die Authentifikation von einem Angreifer mitgeschnitten, liefert sie einen Hashwert, den der Angreifer für einen Angriff auf das WLAN-Passwort verwenden kann.

Im Anschluss an die Vorträge haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (zur Anmeldung).

Secorvo-Publikationen

Webanwendungen sind eines der beliebtesten Einfallstore von Angreifern. Systematische Analysen und Penetrationstests können oft das Schlimmste verhüten. Wie man dabei vorgehen sollte, stellt Dr. Safuat Hamdy in Ausgabe 04/2017 der iX vor.

Und wer bloggen möchte, aber die Sicherheitsrisiken dynamischer Content-Management-Systeme (CMS) scheut, findet in Ausgabe 08/2017 der iX hilfreiche Hinweise von Kai Jendrian auf Alternativen.

Secorvo-Seminare

Die Sommerpause ist eine perfekte Gelegenheit zur Vorbereitung auf Ihre T.I.S.P.-Zertifizierung: Nach Ihrer Anmeldung für das T.I.S.P.-Seminar vom **27.11. bis 01.12.2017** erhalten Sie das Begleitbuch „Zentrale Bausteine der Informationssicherheit“ von uns.

Für unser PKI-Seminar vom **06. bis 09.10.2017** gibt es bereits zahlreiche Anmeldungen, daher empfehlen wir allen Interessenten an einem vertieften Einblick in Public Key Infrastrukturen eine baldige Buchung.

Und vom **16. bis 19.10.2017** bieten wir Software Engineers das T.P.S.S.E.-Seminar mit der Möglichkeit zur anschließenden Zertifizierung als *TeleTrusT Professional for Secure Software Engineering*.

Programme, Online-Anmeldung und weitere Termine: secorvo.de/seminare.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2017	
06.-09.08.	DFRWS USA 2017 - Digital Forensic Research Workshop (DFRWS, Austin/US)
16.-18.08.	26th USENIX Security Symposium (Usenix, Vancouver/BC)
20.-24.08.	Crypto 2017 (IACR, Santa Barbara/US)
September 2017	
05.-06.09.	D • A • CH Security (GI, OCG, TeleTrusT, München)
18.09.	Sommerakademie 2017 (Unabhängiges Landes-zentrum für Datenschutz Schleswig-Holstein, Kiel)
19.-22.09.	OWASP AppSec USA 2017 (OWASP Foundation, Orlando/US)
26.09.	Anwendertag IT-Forensik (Fraunhofer-Institut SIT, Darmstadt)
26.-28.09.	Future Security 2017 (Fraunhofer VVS, Nürnberg)
Oktober 2017	
10.-12.10.	it-sa 2017 (Nürnberg Messe, Nürnberg)
16.-19.10.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-19.10.	IDACON 2017 (WEKA-Akademie, München)
24.-26.10.	heise devSec 2017 (dpunkt.verlag, Heidelberg)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2017



Neuland

Am 19.06.2013 äußerte Bundeskanzlerin Angela Merkel in einer Pressekonferenz mit Barack Obama, dass das Internet „für uns alle Neuland“ sei – und musste für diese Formulierung viel Hohn und Spott einstecken. Dabei ging ihr Satz weiter: Das Internet „ermöglicht auch Feinden und Gegnern unserer demokratischen Grundordnung mit völlig neuen Möglichkeiten und völlig neuen Herangehensweisen unsere Art zu leben in Gefahr zu bringen.“

Die Äußerung fiel zwar im Kontext der NSA-Überwachung, doch brachte Frau Merkel damit (wenn auch womöglich unwillentlich) eine empfindliche Wahrheit auf den Punkt: Nach wie vor treiben Hersteller mit einer erschütternden Naivität die Digitalisierung ihrer Produkte voran und schaffen mit unausgereiften und offenbar unzureichend getesteten Lösungen gefährliche neue Angriffspunkte.

Solange es sich dabei um via Internet zugängliche Überwachungskameras handelt, mag das noch als handwerkliche Ungeschicklichkeit mit Spaßfaktor durchgehen. Inzwischen erfasst die von Sicherheitsaspekten unbelastete Digitalisierung allerdings immer mehr Produkte, bei denen Angriffe eine unmittelbare Gefahr für Leib und Leben darstellen. Blieb der Angriff auf ein motorisiertes Skateboard noch eher unbeachtet, sorgte die von einem Journalisten im Selbstversuch dokumentierte Attacke auf einen Chrysler Cherokee im Juli 2015 immerhin für etwas Wirbel. Gelernt haben daraus allerdings noch lange nicht alle, wie der am 18.07.2017 bekannt gewordene Angriff auf einen Segway MiniPro zeigt.

Jeder Sicherheitsgurt, jeder Reifen und jede Stoßstange muss einen Sicherheitstest absolvieren. Aber IT-Schnittstellen, bei denen Fehler zu wesentlich dramatischeren Eingriffen in die Fahrzeugsicherheit führen können, dürfen ohne vertiefte Prüfung verbaut werden. Es fehlen sogar anerkannte, standardisierte Testverfahren, mit denen wir solche Systeme verlässlich prüfen könnten. Neuland eben.



Inhalt

Neuland

Security News

Wie gut ist mein Passwort?

Einheitlicher Beschäftigtendatenschutz

Meinungswandel

Suricata extended

Alexas lokale Überwachung

Rekall's Agent

Secorvo News

BSIG-Prüfverfahrens-Kompetenz

Frisches aus der Hackerküche

Secorvo-Seminare

Veranstaltungshinweise

secorvo
security consulting

Security News

Wie gut ist mein Passwort?

In den SSN 05/2017 haben wir über die geänderten Empfehlungen des NIST zur Wahl geeigneter Passwörter berichtet. Unter anderem wird empfohlen, Passwörter mit Listen kompromittierter Passwörter abzugleichen. Der Sicherheitsforscher Troy Hunt, bekannt durch die Bereitstellung von Listen gehackter Accounts, bietet seit dem 03.08.2017 die Online-Prüfung von Passwörtern gegen ca. 320 Millionen bekanntermaßen kompromittierter Passwörter an. Sie kann per Formular oder via API erfolgen.

Hunt warnt selbst davor, solche Webdienste mit Passwörtern zu nutzen, die in Gebrauch sind – was den Nutzwert des Angebots deutlich reduziert. Immerhin bietet er die Passwörter auch als SHA1-Hashes zum Download an. Mit etwas Programmierung (Stichwort: binäre Suche) lässt sich damit schnell ein Werkzeug erstellen, mit dem man seine Passwörter lokal überprüfen kann.

Einheitlicher Beschäftigtendatenschutz

Bereits am 08.06.2017 hat die Art. 29 Gruppe unter anderem eine Stellungnahme zum Beschäftigtendatenschutz (WP 249 – Opinion 2/2017 on data processing at work) verabschiedet. Diese aktualisiert die Stellungnahmen WP 48 und 55 aus den Jahren 2001 und 2002, ausgehend noch von der Datenschutzrichtlinie, aber mit Bezug auf die künftige Datenschutz-Grundverordnung und den aktuellen Entwurf der ePrivacy-Verordnung.

Der Beschäftigtendatenschutz wird durch die Öffnungsklausel in Art. 88 DS-GVO den Mitgliedsstaaten zur eigenständigen Regelung überlassen. Die Stellungnahme fasst Verhältnismäßigkeitserwägungen zu typischen Verarbeitungskontexten zusammen. Allgemein werden Anforderungen an die Ausfüllung von Art. 88 DS-GVO formuliert, die deutlich über den deutschen § 26 BDSG-neu (vorher § 32 BDSG) hinausgehen.

Es wird klargestellt, dass Arbeitgeber Arbeitnehmer nicht ausschließlich auf vorgegebene Social-Media-Profile verpflichten können, auch nicht, wenn diese öffentlich das Unternehmen vertreten. Es wird die Erforderlichkeit von Transparenz und dokumentierten Datenschutzrichtlinien bei IT-Nutzungsüberwachungen betont. Bezüglich Mobile Device Management Lösungen wird generell eine Datenschutz-Folgenabschätzung für erforderlich gehalten.

Gesichtserkennungstechnologien im Beschäftigungskontext werden abgelehnt. Für Einwilligungen und berechtigte Interessen des Arbeitgebers als Rechtsgrundlage wird nur ein sehr eingeschränktes Anwendungsfeld gesehen. Die Stellungnahme stellt eine hilfreiche Zusammenfassung und Orientierungshilfe dar, zumal viele aktuelle und praktische Problemstelllungen angesprochen und mit Szenarien erläutert werden.

Meinungswandel

Ob eine juristische Person (bspw. eine Firma) als externer Datenschutzbeauftragter bestellt werden kann, ist eine in der Praxis durchaus relevante, aber bislang umstrittene und nicht entschiedene Frage. Der Hessische Datenschutzbeauftrage empfiehlt nun in einem Informationspapier zum betrieblichen Datenschutzbeauftragten nach der Datenschutz-Grundverordnung vom 29.06.2017, die Bestellung einer juristischen Person bis zu einer endgültigen Klärung durch den Europäischen Datenschutzausschuss mit der zuständigen Aufsichtsbehörde lediglich abzusprechen.

Die sich abzeichnende Kehrtwende der Aufsichtsbehörden zu dieser durch den Gesetzeswortlaut weiter offenen Frage geht auf ein bereits im Dezember 2016 veröffentlichtes Arbeitspapier (WP 243) der Art. 29 Datenschutzgruppe zurück. Die Europäischen Aufsichtsbehörden halten darin die Bestellung einer juristischen Person ausdrücklich für möglich. Voraussetzung ist, dass die für die juristische Person handelnden Mitarbeiter die Qualifikationsvoraussetzungen erfüllen. Dabei wird ausdrücklich anerkannt, dass die Kombination der Qualifikationen mehrerer Einzelpersonen einer Firma die Wirksamkeit der Tätigkeit in der Praxis steigern kann.

Auch wenn eine endgültige Anerkennung des Modells noch abzuwarten bleibt, öffnet sich damit der Weg für eine praxistauglichere Bestellpraxis, die die bisherigen mühsamen Konstrukte zur persönlichen Bestellung externer Datenschutzbeauftragte überflüssig macht. Bisherige Appelle in diese Richtung waren bislang bei den Aufsichtsbehörden eher auf Ablehnung gestoßen.

Suricata extended

Bereits am 27.07.2017 erschien das robuste Network Intrusion Detection/Prevention/Security Monitoring System Suricata nach ca. 18 Monaten in der Version 4.0.0-stable. Eine wesentliche Neuerung ist die Integration der Programmiersprache RUST, dank der neben deutlich gesteigerter Geschwindigkeit auch eine sicherere Speicherverwaltung und Threats ohne Race Conditions möglich wurden.

Technisch neu sind bei TLS die Dekodierung und das Logging von STARTTLS für SMTP und FTP sowie von

TLS Session Resumptions. Hinzugekommen ist die Unterstützung für das NFS-Protokoll, welches im kommerziellen Umfeld nach wie vor eine wichtige Rolle spielt. Hinzugekommen ist mit der Implementierung des Extensible Event Format (EVE) die Möglichkeit, bei gekapseltem Netzwerkverkehr (encapsulated traffic) auch die innere und äußere IP-Adresse inklusive der zugehörigen Ports auszuwerten.

Alexas lokale Überwachung

Am 01.08.2017 stellte Mark Barnes einen Angriff auf Amazons Echo vor, der das Gerät in eine Abhörstation verwandelt. Auf der Unterseite des Geräts kann über die dortige Kontaktleiste eine SD-Karte angeschlossen werden, mit der das Gerät gebootet werden kann. Anschließend lassen sich über geeignete Skripte das interne Laufwerk ansprechen und die Firmware modifizieren. Auf diesem Weg ist es beispielsweise möglich, Mikrofon-Aufzeichnungen von Echo unbemerkt an einen Dritten zu übermitteln.

Auch wenn Barnes' Angriff nur für bis 2016 verkaufte Geräte nachweislich funktioniert und in neueren Geräten ab 2017 unterbunden wurde, sollte man die Gefahr durch Abhör-Angriffe über manipulierte Geräte mit Mikrofon nicht gering schätzen: Zwar benötigt der Angreifer Zugang zum Gerät, aber die Kosten sind vernachlässigbar.

Selbst führende Hersteller sind sich dieser Gefahr offenbar wenig bewusst, wenn sie von außen zugängliche Daten-Schnittstellen am Gerät vorsehen. Aber auch ein hermetisch verschlossenes Gerät birgt ein Restrisiko: Dass der Hersteller die mitgeschnittenen Worte nicht selbst zu anderen als den im Prospekt versprochenen Zwecken nutzt, darauf müssen Sie in jedem Fall vertrauen.

Rekall's Agent

Pünktlich zum jährlichen Rekall-Workshop auf der DFRWS 2017 ist seit dem 07.08.2017 die Version 1.7 für Windows, Linux und OSX verfügbar. Neben vielen Weiterentwicklungen bei den Plugins (z. B. iexport für NTFS-Dateiextraktion via $MFT) und der Ausweitung auf ca. 2.000 vordefinierte, spezifische Kernelprofile steht die Agenten-Komponente im Mittelpunkt, die sich nun als dauerhafter Service (Daemon) auf Endsystemen installieren lässt.

Mit diesem Release wandelt sich Rekall von einer Stand-Alone-Installation zu einem eigenständigen forensischen Client-Server Incident Response Framework und bietet Unterstützung für Echtzeitforensik auf Client-Systemen. Praktisch ist u. a. die Ausführung von WMI-Queries in Live-Systemen, um Erkenntnisse jenseits eines reinen Hauptspeicherabzugs zu erhalten.

Der Agent stößt außerdem eine spannende Entwicklung an: Client-side Plugins. Dies wird bereits durch das neue vfs_ls-Plugin ermöglicht, mit dessen Hilfe nun „Remote Timelines" auf Clients erstellt werden können – fast in Echtzeit und mit hoher Aussagekraft.

Secorvo News

BSIG-Prüfverfahrens-Kompetenz

Vier Berater und Auditoren von Secorvo haben inzwischen erfolgreich die Prüfverfahrens-Kompetenz nach § 8a (3) BSIG erworben. Sie ist Eignungsvoraussetzung für die Prüfung Kritischer Infrastrukturen und weiterer vom IT-Sicherheitsgesetz betroffener Unternehmen und Institutionen – und hilfreich beim Aufbau geeigneter Informationssicherheits-Management-Systeme.

Frisches aus der Hackerküche

Am **21.09.2017** startet die KA-IT-Si in die zweite Jahreshälfte. Benjamin Lipp und Timon Hackenjos (Fraunhofer IOSB) zeigen, wie ein im September 2016 veröffentlichter Angriff auf Windows-Anmeldeinformationen in abgewandelter Form auch heute noch funktioniert. Benny Görzig und Florian Loch (ebenfalls Fraunhofer IOSB) stellen Angriffe auf das Netzwerkauthentifizierungsprotokoll WPA2-PSK vor, das die meisten von uns in ihren privaten WLAN-Netzen benutzen. Wird die Authentifikation von einem Angreifer mitgeschnitten, liefert sie einen Hashwert, den der Angreifer für einen Angriff auf das WLAN-Passwort verwenden kann.

Im Anschluss an die Vorträge haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Secorvo-Seminare

Interessenten an unserem PKI-Seminar vom **06. bis 09.10.2017** mit einem vertieften Einblick in Public Key Infrastrukturen empfehlen wir eine baldige Buchung. Und vom **16. bis 19.10.2017** bieten wir Software Engineers das T.P.S.S.E.-Seminar mit der Möglichkeit zur anschließenden Zertifizierung als *TeleTrusT Professional for Secure Software Engineering*.

Die nächste Möglichkeit zur T.I.S.P.-Zertifizierung bieten wir Ihnen mit dem T.I.S.P.-Seminar vom **27.11. bis 01.12.2017**; das Begleitbuch „Zentrale Bausteine der Informationssicherheit" erhalten Sie vorab zur Vorbereitung.

Programme, Online-Anmeldung und weitere Termine: secorvo.de/seminare.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2017	
05.-06.09.	D • A • CH Security (GI, OCG, TeleTrusT, München)
18.09.	Sommerakademie 2017 (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel)
19.-22.09.	OWASP AppSec USA 2017 (OWASP Foundation, Orlando/US)
21.09.	Frisches aus der Hackerküche (KA-IT-Si, Karlsruhe)
26.09.	Anwendertag IT-Forensik (Fraunhofer-Institut SIT, Darmstadt)
Oktober 2017	
10.-12.10.	it-sa 2017 (Nürnberg Messe, Nürnberg)
16.-19.10.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-19.10.	IDACON 2017 (WEKA-Akademie, München)
24.-26.10.	heise devSec 2017 (dpunkt.verlag, Heidelberg)
November 2017	
06.-09.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
14.-15.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
21.-23.11.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
27.11.-01.12.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

September 2017



Sie haben die Wahl...

Am 07.09.2017 sorgte der Chaos Computer Club (CCC) kurz vor der Bundestagswahl für Aufregung: Er hatte zahlreiche Schwachstellen in der Software ‚PC-Wahl' identifiziert. Diese Software dient zwar nur zur Ermittlung des vorläufigen Endergebnisses, dennoch könnte dessen Manipulation zu einem Chaos und einer Verunsicherung der Bevölkerung führen. Ein derartiger Vorfall dürfte auch das Vertrauen in den Wahlvorgang nachhaltig erschüttern.

Das Thema Wahlcomputer und Online-Wahlen hielten viele nach dem Urteil des Bundesverfassungsgerichts (BVerfG) im Jahr 2009 für abgeschlossen. Dennoch brachte BSI Präsident Arne Schönbohm in einem Interview vom 11.09.2017 das Thema Online-Wahlen für die nächste Legislaturperiode ins Gespräch. Mit seiner Kritik an der Briefwahl schlägt Prof. Dr. Müller-Quade – Gewinner des deutschen IT-Sicherheitspreises für das Bingo-Voting-Verfahren – in eine ähnliche Kerbe.

Alle denkbaren kryptografischen Wahlverfahren basieren jedoch auf der Grundannahme, dass die Sicherheit des unterliegenden Wahl-Clients gewährleistet sein muss. Das ist gerade bei Online-Wahlen eine wohl kaum umsetzbare Voraussetzung, zumal viele Wahlberechtigte erreicht werden müssen. Dies ist ein bekanntes Problem der IT-Sicherheit: Immer neue Angriffe auf das Online-Banking zeigen, dass es den Banken trotz Jahrzehnten Erfahrung bisher nicht gelungen ist, eine für den Anwender benutzbare und von der Sicherheit des Client unabhängige Online-Banking-Anwendung zu entwickeln. Das lässt sich auf Online-Wahlen übertragen. Komplexe technische Lösungen behindern zudem die vom BVerfG geforderte Überprüfbarkeit der Wahl durch den Bürger – ohne besondere Sachkenntnis – und lösen daher das grundlegende Problem nicht.



Inhalt

Sie haben die Wahl...

Security News

Vertrauen entzogen

BlueBorne

Malware mit Brief und Siegel

Neues vom Privacy Shield

Weitere IT-Sicherheitspflichten

Secorvo News

Secorvo Seminare

CyberWehr-Gipfel in Karlsruhe

Watching. You.

Veranstaltungshinweise

secorvo
security consulting

Security News

Vertrauen entzogen

In der März-Ausgabe (SSN 3/2017) berichteten wir von dem Zertifikatsdesaster von Symantec. Bereits damals waren die Google-Chrome-Entwickler entschlossen, den von Symantec ausgestellten SSL/TLS-Zertifikaten das Vertrauen zu entziehen. Nach längeren Diskussionen und Verhandlungen verkündete Google nun am 11.09.2017 in seinem Security Blog den genauen Zeitplan für diesen in der PKI-Geschichte einmaligen Vorgang. Ausgelöst von Googles Vorstoß hatte Symantec bereits am 02.08.2017 den Verkauf seiner Trustcenter-Sparte an den Mitbewerber DigiCert bekanntgegeben.

Spätestens zum 01.12.2017 sollen Zertifikate für Kunden der (Ex-)Symantec-Marken über DigiCerts Trustcenter-Infrastruktur erstellt werden. Sollten nach diesem Stichtag noch Zertifikate von Symantecs jetziger Infrastruktur ausgestellt werden, wird Chrome diesen nicht mehr vertrauen. Vorhandene Zertifikate, die von Symantecs Trustcenter-Marken (u. a. VeriSign, Thawte und GeoTrust) vor dem 01.06.2016 ausgestellt wurden, verlieren mit dem Erscheinen der Chrome-Version 66 ihre Gültigkeit (geplant für den 15.03.2018). Symantec-Zertifikaten, die zwischen dem 01.06.2016 und dem 01.12.2017 erstellt wurden, soll spätestens mit Erscheinen der Chrome-Version 70 das Vertrauen entzogen werden (geplant für den 13.09.2018).

Mozilla hat bereits angekündigt, sich diesem Zeitplan (bis auf wenige Tage Abweichung aufgrund der Release-Zyklen des Firefox-Browsers) anzuschließen. Betroffene Serverbetreiber sollten sich daher frühzeitig um neue Zertifikate von Symantec/DigiCert oder anderen Anbietern kümmern.

BlueBorne

Insgesamt acht kritische Lücken in den Bluetooth-Stacks entdeckten Sicherheitsforscher von Armis Labs und publizierten diese am 12.09.2017 in ihrem Blog. Vier dieser Schwachstellen erlauben einem Angreifer, Schadcode auf allen gängigen Android-, Linux-, Windows- und iOS-Geräten (mit iOS Versionen bis einschließlich 9.3.5) auszuführen: Zwei ermöglichen das Extrahieren sensibler Informationen unter Linux und Android, die beiden anderen Man-in-the-middle-Angriffe unter Windows und Android.

Das Fatale an den gefundenen Schwachstellen ist die Möglichkeit, ein Gerät anzugreifen, ohne es zuvor mit dem Gerät des Angreifers zu koppeln. Es genügt, eine eingeschaltete Bluetooth-Schnittstelle beim Opfer. Unsichtbare Bluetooth-Geräte sind ebenfalls nicht wirksam geschützt. Zwar konnten Microsoft, Google und die Linux-Foundation im September passende Patches für alle betroffenen Geräte bereitstellen; ob diese jedoch von den Herstellern zügig verbreitet werden, ist vor allem bei Android unsicher. Die Bluetooth-Schnittstelle sollte daher deaktiviert werden, bis eine entsprechende Aktualisierung erfolgt ist.

Malware mit Brief und Siegel

Am 18.09.2017 wurde bekannt, dass das beliebte Festplatten-Bereinigungstool CCleaner etwa vier Wochen lang mitsamt einem Trojaner ausgeliefert wurde. Besonders pikant daran ist zum einen, dass kurz zuvor CCleaner-Hersteller Piriform vom Antiviren-Unternehmen Avast übernommen worden war. Zum anderen trugen die befallenen Softwarepakete gültige Code-Signaturen von Piriform. Dennoch braucht der Hersteller wohl keine Welle an Schadenersatz-Klagen aufgrund einer irgendwie gearteten Produkthaftung zu befürchten, was auch die am 19.09.2017 abgewiesene Klage FTC gegen D-Link unterstreicht.

Entdeckt wurde die Schadsoftware unabhängig voneinander in Kunden-Installationen zweier Unternehmen, die aufwändige neuere Ansätze beim Malwareschutz verfolgen. Der klassische, signaturbasierte Virenschutz dagegen gelangte wieder einmal an seine Grenzen: Selbst nach dem Bekanntwerden vergingen noch ca. drei Tage, bevor ein Großteil der unter VirusTotal versammelten Virenscanner den befallenen Installer nicht mehr als „Clean“ meldete. Die Aufarbeitung des Vorfalls folgt eher dem herkömmlichen Muster: Nach ersten Beschwichtigungen, eine Sekundärinfektion wäre unwahrscheinlich, ergab die forensische Analyse des beschlagnahmten C&C-Servers doch knapp zwei Dutzend auf eben diese Weise angegriffene Unternehmen. Inzwischen ist von APT, bekannten Angriffsmustern und asiatischen Netzwerken die Rede – gäbe es die sprichwörtlichen ‚Chinesischen Hacker' nicht, man müsste sie als Synonym für „höhere Gewalt“ erfinden.

Angesichts der Zunahme von „Supply Chain Attacks“ ist jedoch der Blick nach vorn wichtiger als die Suche nach Entschuldigungen. Ein erster Schritt könnte sein, dass Softwarehersteller im Freigabeprozess ihre Softwarepakete zunächst eine Weile mit neueren, bspw. verhaltensbasierten Anti-Malware-Methoden prüfen, ehe sie per Code-Signatur die – wenn schon nicht justiziable, so doch moralische – Verantwortung für ihren so versiegelten Code übernehmen.

Neues vom Privacy Shield

Seit dem 01.08.2016 ist das Europäisch-US-amerikanische Privacy Shield eine Alternative zu den übri-

gen Wegen, die ein gleichwertiges Schutzniveau bei der Verarbeitung personenbezogener Daten sicherstellen sollen. Teil des Abkommens ist eine Beschwerdemöglichkeit, zu deren Unterstützung mehrere deutsche Datenschutzaufsichtsbehörden nun ein Beschwerdeformular publiziert haben.

Das Formular erfragt die erforderlichen Informationen zur Überprüfung der Datenübermittlung ab. Die Beschwerde kann dann von einer unabhängigen Stelle bearbeitet werden. Führt dies nicht zu Abhilfe bleibt dem Betroffenen die Beschwerde bei den eigenen lokalen Datenschutz-Aufsichtsbehörden.

Das Formular ist eine Erleichterung zur Wahrung der Betroffenenrechte. Ob das Instrument jedoch tatsächlich zu einem verbesserten Schutz der personenbezogenen Daten führt, ist zweifelhaft: Nur wenige Betroffene werden überhaupt von der Möglichkeit zur Nachforschung wissen, geschweige denn den dafür erforderlichen Aufwand treiben.

Weitere IT-Sicherheitspflichten

Am 30.06.2017 ist weitgehend unbemerkt das Umsetzungsgesetz zur Richtlinie EU 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (kurz: NIS-Richtlinie) in Kraft getreten. Die Neuregelungen für Anbieter digitaler Dienste gelten ab dem 10.05. 2018. Das Gesetz nimmt auch zahlreiche Änderungen an den durch das IT-Sicherheitsgesetz eingeführten Bestimmungen vor.

Kern ist die Erweiterung des BSI-Gesetzes um einen § 8c, der die Anbieter zum Ergreifen verhältnismäßiger technischer und organisatorischer Maßnahmen verpflichtet, eine Meldepflicht für erhebliche Vorfälle einführt und das BSI zur Prüfung sowie zum Erlass von Anordnungen ermächtigt. Mit ‚digitalen Diensten' sind Dienste der Informationsgesellschaft gemeint, einschließlich Online-Marktplätzen, Suchdiensten und Cloud-Diensten.

Die sonstigen Befugnisse des BSI werden um Regelungen zu Mobilen Incident Response Teams (MIRTs) ergänzt, die andere Stellen nach Sicherheitsereignissen bei der Wiederherstellung ihrer Systeme unterstützen sollen. Auch in Bezug auf die digitalen Dienste wird eine Mitwirkungspflicht von Anwendungsherstellern eingeführt. Die Erweiterungen bezüglich der Betreiber Kritischer Infrastrukturen beziehen sich hauptsächlich auf die Behandlung grenzüberschreitender Belange.

Mit dem Umsetzungsgesetz wird ab Mai 2018 ein weiterer Anbieterkreis gesetzlich zur IT-Sicherheit verpflichtet. Nach den bisherigen Erfahrungen mit dem IT-Sicherheitsgesetz wird sich die Begeisterung bei den betroffenen Unternehmen wohl in Grenzen halten.

Secorvo News

Secorvo Seminare

Noch vier Gelegenheiten zur Weiterqualifikation bieten wir Ihnen in diesem Herbst:

- das T.P.S.S.E.-Seminar zur sicheren Software-Entwicklung (**16.–19.10.2017**),
- unser PKI-Seminar (**06.–09.11.2017**),
- IT-Sicherheit heute (**21.–23.11.2017**) und
- das T.I.S.P.-Seminar (**27.11.–01.12.2017**)

Alle Seminare sind bereits gut gebucht – wir empfehlen daher eine schnelle Anmeldung und freuen uns auf Ihre Teilnahme. Programme und die Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

CyberWehr-Gipfel in Karlsruhe

Um den wachsenden Schäden durch Cyberangriffe zu begegnen, plant Innenminister Strobl den Aufbau einer CyberWehr Baden-Württemberg. Auf Einladung des Wirtschafsrats wird er das Konzept am **11.10.2017** in einer Keynote auf dem in Zusammenarbeit mit der KA-IT-Si veranstalteten CyberWehr-Gipfel im ZKM | Karlsruhe vorstellen und sich anschließend mit weiteren Experten der Diskussion stellen (Teilnahme frei; zur Anmeldung).

Watching. You.

Als einer der Partner der IT-Sicherheitsregion Karlsruhe lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem ZAK | Zentrum für Angewandte Kulturwissenschaft und Studium Generale am **19.10.2017** zum Filmevent in die Karlsruher Schauburg. Bei der Eröffnungsveranstaltung der Traumfabrik #14/2017-18 „BIG BROTHER – Surveillance Cinema" wird der Oscar-prämierte Film „Citizenfour" von Laura Poitras gezeigt, der einen persönlichen Blick auf das Leben von Edward Snowden gibt. Wolfgang Petroll wird eine Einführung in den Film geben; im Anschluss folgt eine Diskussion mit Dr. Oliver Raabe (Zentrum für Angewandte Rechtswissenschaft), Prof. Dr. Caroline Robertson-von Trotha (ZAK), Dr. Dirk Achenbach (Kompetenzzentrum IT-Sicherheit) und Jan Linders (Badisches Staatstheater Karlsruhe).

Danach bieten wir Ihnen wie gewohnt die Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2017	
10.-12.10.	it-sa 2017 (Nürnberg Messe, Nürnberg)
11.10.	Wehrhafte IT-Sicherheit: Cyberwehr-Gipfel in Karlsruhe (Wirtschaftsrat Deutschland/ Wirtschaftsjunioren Karlsruhe/KA-IT-Si, Karlsruhe)
16.-19.10.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
18.10.	Swiss Cyber Storm 2017 (Swiss Cyber Storm Association, Luzern/CH)
19.10.	Watching. You. (Partner der IT-Sicherheitsregion Karlsruhe/ZAK, Karlsruhe)
24.-26.10.	heise devSec 2017 (dpunkt.verlag, Heidelberg)
November 2017	
06.-09.11.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
14.-15.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
14.-17.11.	DeepSec In-Depth Security Conference Europe (DeepSec GmbH, Wien/AT)
15.-17.11.	41. DAFTA (GDD Gesellschaft für Datenschutz und Datensicherheit, Köln)
21.-23.11.	IT-Sicherheit heute - praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
27.11.-01.12.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick (Editorial), Fabian Ebner, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Oktober 2017



Die Schildkröte

Eine meiner Lieblingsparadoxien ist die von Achilles und der Schildkröte. Überliefert von Aristoteles und zugeschrieben Zenon von Elea lautet sie etwa wie folgt:

Achilles, Sohn des Peleus und der Nymphe Thetis, Held der Griechen beim Kampf gegen Troja und schneller Läufer, tritt im Wettlauf gegen eine Schildkröte an. Um das Rennen fairer zu gestalten, räumt er ihr einen Vorsprung ein – und verliert.

Denn während er die Strecke des der Schildkröte gewährten Vorsprungs durchläuft, ist diese bereits weiter gekrabbelt – und hat sich einen neuen, wenn auch kleineren Vorsprung erarbeitet. Holt er diesen auf, hat die Schildkröte wiederum etwas Strecke gut gemacht, und passiert er auch die, ist sie wieder ein Stück weiter – Achilles wird sie daher, so schnell er auch laufen und so unendlich nah er ihr auch kommen mag, niemals überholen.

Mathematiker werden jetzt einwenden, dass unendliche Reihen auch endliche Summen haben können. Aber das rettet uns nicht aus der Denkfalle – denn als Sicherheitsexperte erkennen wir uns in Achilles wieder: Fühlen wir uns nicht oft wie er, wenn wir durch präventive Maßnahmen, Patches oder Policies Angriffsfläche reduzieren – dabei aber feststellen müssen, dass wir Angreifern nachjagen, die sich derweil wieder mit neuen Angriffsmethoden oder unter Ausnutzung neu entdeckter Sicherheitslücken erneut einen kleinen Vorsprung erarbeitet haben.

Dabei widerspricht Zenons Paradoxon unserer Erfahrung. Und tatsächlich ist es die Perspektive, die uns täuscht: Wenn wir uns selbst als hinter Angreifern her hechelnden Achilles sehen, der ständig die von jenen aufgerissenen Löcher stopft, werden wir die Aufholjagd nicht gewinnen können.

Deshalb sollten wir die Perspektive wechseln und uns klarmachen: Für Resignation gibt es keinen Grund. Denn wenn wir schneller sind als die Schildkröte werden wir sie auch überholen.



Inhalt

Die Schildkröte

Security News

Deterministischer Zufall

WLAN-Ü-Ei

Versteckte Minenarbeiter

Nutzungsanalyse

Zielgruppenansprache à la Facebook

Kopieren oder nicht kopieren...

Secorvo News

Verstärkung

Secorvo-Seminare

Sicherheit auf Wolke sieben

Krypto im Advent – 24 Tage, 24 Rätsel

Veranstaltungshinweise

secorvo
security consulting

Security News

Deterministischer Zufall

Am 18.10.2017 wurde eine Schwachstelle in Infineons Firmware-Bibliothek für Smartcard- und TPM-Chips veröffentlicht – gleich mit GitHub-Archiv. Sie steckt in einem Beschleunigungsalgorithmus für die RSA-Schlüsselerstellung: Er testet nicht einfach Zufallszahlen, bis zwei Primzahlen gefunden sind, sondern konstruiert stattdessen zufallsabhängig Kandidaten, die nicht durch kleine Primzahlen teilbar und somit wahrscheinlicher prim sind.

Hier zeigt sich wieder die Schwierigkeit, Sicherheit als Qualitätsmerkmal nachzuweisen: Die inkriminierte Firmware-Bibliothek wurde u. a. vom BSI nach Common Criteria zertifiziert. Jahre später griffen nun tschechische Forscher auf eine Angriffsmethode zurück, die bei heutiger Schlüssellänge eigentlich nicht mehr relevant ist. Von Infineon-Chips konstruierte 2048 bit lange RSA-Schlüssel aber kann man damit in der Amazon-Cloud für ca. $ 40.000 binnen Tagen brechen. Ob der eigene RSA-Schlüssel betroffen ist, lässt sich übrigens mit Hilfe verschiedener Testtools prüfen.

Als etwas hilflose Panik-Reaktion muss man wohl die Beschränkung des Zugriffs auf die öffentlichen RSA-Schlüssel 750.000 estnischer Ausweiskarten bewerten: das Nicht-Veröffentlichen öffentlicher Schlüssel ist nicht nur eine Contradictio in Adiecto, sondern zudem wirkungslos, denn schon zwei digitale Signaturen können ausreichen, um daraus den öffentlichen Schlüssel zu ermitteln – zumindest wenn dafür wie üblich das traditionelle RSA-Padding-Verfahren (PKCS#1 v1.5) anstelle des seit gut 15 Jahren empfohlenen PSS-Verfahrens verwendet wird.

WLAN-Ü-Ei

In postfaktischen Zeiten benötigt eine Schwachstelle einen griffigen Namen, ein Logo und eine eigene Webseite. Daneben vereint die am 16.10.2017 veröffentlichte KRACK-Attacke drei Dinge auf einmal: Angriff, Ansatzpunkt und Theorie.

Zunächst deckt sie einen in Linux und Android weit verbreiteten Bug auf, der es Angreifern ermöglicht, Nutzer betroffener Geräte unbemerkt und ohne Social Engineering in ein Evil-Twin-Netz umzuleiten. Dahinter steckt eine im WLAN-Standard begründete Schwäche, über die die unterste Ebene der Schlüsselableitung angegriffen werden kann: der pseudozufällige Schlüsselstrom einzelner Datenpakete. In Kombination mit geratenen oder bekannten Inhalten lassen sich so einzelne Pakete in einem per AES-CCMP gesicherten WPA2-Netz entschlüsseln oder wiedereinspielen. Dies ist meist noch nicht schwerwiegend, jedoch ein potenter Ansatzpunkt für weitere Angriffsschritte. Und schließlich erhellt KRACK unser Verständnis vom Wert theoretischer Sicherheitsbeweise: Der Angriff auf das Kryptoprotokoll widerlegt nicht die formalen Beweise, sondern bewegt sich haarscharf außerhalb deren Gültigkeitsbereichs.

Eilige Warnungen, deswegen auf Online-Banking per WLAN zu verzichten, sind jedoch unangemessen: Dass anstelle von leicht aus der Ferne zu dirigierender Man-in-the-Browser-Malware jetzt Flotten von Kleintransportern mit WLAN-Man-in-the-Middle-Ausrüstung in deutsche Wohnviertel ausschwärmen, ist wohl eher unwahrscheinlich. Handlungsbedarf ergibt sich dagegen aus dem Schlaglicht, das KRACK auf das zu erwartende Schwachstellenmanagement im Internet-of-Things wirft: Man beachte, welche Hersteller und Geräte *nicht* in den Listen verfügbarer Patches auftauchen.

Versteckte Minenarbeiter

Seit Mitte September erfreuen sich JavaScript-Miner immer größerer Beliebtheit. Ursprünglicher Zweck solcher Bitcoin-Miner war es, Webseitenbetreibern eine – im Vergleich zu Werbung – beständigere und effizientere Möglichkeit der Finanzierung zur Verfügung zu stellen. Dabei sollte der Nutzer den eingebetteten Miner selbst starten und während des Webseitenbesuchs laufen lassen. Seiten wie „The Pirate Bay“ erweiterten dieses Konzept jedoch und lieferten einen Miner aus, der sofort mit seiner Arbeit beginnt – auch ohne Einverständnis des Nutzers und meist sogar ohne dessen Wissen. Nun haben die Entwickler des JavaScript-Miner reagiert und erzwingen ein Opt-In.

Wer sicher gehen will, dass sein Endgerät nicht für Fremde Bitcoins schürft, sollte JavaScript im Browser blockieren – z. B. mittels Erweiterungen wie NoScript. Alternativ kann man einzelne Seiten auch über den Dienst „Who runs Coinhive?“ prüfen.

Nutzungsanalyse

Das am 13.10.2017 von Harlan Carvey veröffentlichte PlugIn recentapps für das forensische RegRipper Toolset erlaubt die Gewinnung zusätzlicher Informationen über Benutzeraktivitäten unter Windows 10 (und ergänzt damit den UserAssist-Registry-Key). Dazu zählen zum Beispiel die ‚Last-Write Time‘ des Application GUID Subkeys, die unabhängig von der ‚LastAccess Time‘ im NTFS-Dateisystem gespeichert wird. Diese Zeitinformation stellt eine wertvolle Möglichkeit zur Validierung von Programmaufrufen eines Benutzers dar, sogar wenn die Zeitangaben im Dateisystem selbst und in der Master-Dateitabelle manuell verändert wurde.

Praktischerweise liefert das Plugin seine Ergebnisse im Timeliner-Format *.TLN, womit es die forensische Timeline eines Benutzerkontos ergänzt und z. B. Informationen darüber liefert, welche Programme eine Schadsoftware in diesem Benutzerkontext aufgerufen hat.

Zielgruppenansprache à la Facebook

Das Bayerische Landesamt für Datenschutzaufsicht führt in einem Bericht vom 04.10.2017 aus, ob und unter welchen Voraussetzungen der Facebook-Dienst „Custom Audience" den Datenschutzanforderungen des BDSG und der DS-GVO entspricht.

Gemeinsam ist den nach Anwendungsfällen unterschiedenen Varianten des Werbedienstes die zielgenaue Ansprache von Facebook-Nutzern. Dazu erhält Facebook von seinem Auftraggeber entweder eine Adressatenliste oder es wird ein Facebook-Pixel auf der Auftraggeber-Website eingebunden.

Beim Pixel-Verfahren seien die Auftraggeber verpflichtet, Betroffene über die Datenerhebung zu informieren und ein Opt-Out-Verfahren anzubieten. Die Verantwortung für den rechtmäßigen Einsatz der „Facebook Custom Audience" obliege dabei dem jeweiligen Unternehmen. Die Übermittlung der Listendaten erfordere eine gesonderte Rechtsgrundlage, in der Regel die Einwilligung der betroffenen Personen.

Sowohl das Einwilligungserfordernis als auch die Informationspflicht über die Verarbeitung durch Facebook machen eine rechtskonforme Umsetzung faktisch unmöglich. Mit Blick auf die empfindlichen Ordnungsgelder der DS-GVO sollte daher von einer Nutzung der Dienste Abstand genommen werden.

Kopieren oder nicht kopieren...

Mit einer Änderung von § 20 Personalausweisgesetz (PAuswG) vom 07.07.2017 wurde das Kopieren von Personalausweisen unter bestimmten Voraussetzungen ermöglicht. So muss die Kopie als solche dauerhaft erkennbar sein (z. B. schwarz-weiß) und die Einwilligung des Inhabers vorliegen. Dient die Ablichtung zur weiteren Verwendung der Personalausweisdaten, so bedarf dies einer gesonderten Einwilligung; selbstverständlich sind zudem alle einschlägigen Datenschutzvorschriften einzuhalten.

Bislang war die vielfach auch in Privatunternehmen bestehende Praxis, zur Dokumentation des Identitätsnachweises den Ausweis zu scannen oder zu kopieren, durch § 14 PAuswG untersagt. Das Verbot hat sich in der Praxis nie wirklich durchgesetzt, die der neue § 20 nun legitimiert. Ein wenig wirkt dieser Interessensausgleich daher wie eine Kapitulation.

Secorvo News

Verstärkung

Im Sommer ist es uns gelungen, unser Beratungsteam zu erweitern: Seit dem 01.10.2017 verstärkt Sarah Niederer den Bereich Datenschutz. Sie bringt vieljährige Berufserfahrung aus den Bereichen Compliance, Business-Impact-Analysen, Risikomanagement und insbesondere vertieftes Datenschutz-Know-How mit.

Secorvo-Seminare

Für Schnellentscheider bieten wir in diesem Jahr noch drei Seminare an: PKI (06.-09.11.2017), IT-Sicherheit heute (21.-23.11.2017) und das T.I.S.P.-Seminar (27.11.-01.12.2017) mit anschließender Zertifizierung.

Programme, die Möglichkeit zur Anmeldung und die Seminartermine 2018 finden Sie unter www.secorvo.de/seminare.

Sicherheit auf Wolke sieben

Die Verarbeitung von Daten in der ‚Cloud' stößt immer wieder (und oft berechtigt) auf Sicherheitsbedenken. Dabei ginge es auch anders: Mit ‚Privacy & Security by Design' lassen sich Cloud-Lösungen mit hohem Sicherheits- und Datenschutzniveau realisieren. Wie das geht, zeigen wir bei unserem kommenden KA-IT-Si-Event am **23.11.2017** an Beispielen aus anwendungsnahen Forschungs- und Entwicklungsprojekten. Gastgeber ist das Karlsruher „House of Living Labs" des Forschungszentrums Informatik (FZI). Für Interessierte bieten wir vorab eine Führung durch dieses Innovationslabor an.

Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Krypto im Advent – 24 Tage, 24 Rätsel

Verschlüsseln und entschlüsseln, grübeln und Spaß haben, lösen und gewinnen: Das ist Krypto im Advent. Mehr als 2.400 begeisterte Rätselknacker begaben sich im vergangenen Advent täglich in die Welt der Kryptologie. Am 01.12.2017 geht es nun wieder los. An diesem Adventsrätsel, das in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe entwickelt wurde, können alle Schülerinnen und Schüler der **Klassen 3 bis 9** teilnehmen. Dank unseren Sponsoren gibt es wieder zahlreiche Preise zu gewinnen. Auch ältere, an Ver- und Entschlüsselungsverfahren Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2017	
30.10.-03.11.	ACM CCS 2017 (ACM/SIGSAC, Dallas/US)
November 2017	
06.-09.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
14.-15.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
14.-15.11.	ISSE 2017 (EEMA, Brüssel/BEL)
14.-17.11.	DeepSec In-Depth Security Conference Europe (DeepSec GmbH, Wien/AT)
15.-17.11.	41. DAFTA (GDD Gesellschaft für Datenschutz und Datensicherheit, Köln)
21.-23.11.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
27.-28.11.	7. Handelsblatt Jahrestagung - Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
27.11.-01.12.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
Dezember 2017	
04.-07.12.	Black Hat Europe 2017 (Blackhat, London/UK)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Fabian Ebner, Hans-Joachim Knobloch, Michael Knopp, Sarah Niederer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

November 2017



Panoptikum

Jeremy Bentham (1748-1832), einer der großen Vordenker des Liberalismus und unseres heutigen Rechtsstaatsverständnisses, huldigte einem heute nur schwer nachzuvollziehenden Freiheitsbegriff: Er war überzeugt, dass nur ein mächtiger Staat mit strengen Sanktionen die allein auf ihren Vorteil bedachten Bürger an der rücksichtslosen Durchsetzung ihrer eigenen Interessen hindern könne. Und dass dieser Staat dafür einen umfassenden Überwachungsapparat benötige, damit aus der Erzwingung rechtskonformen Verhaltens echte Freiheit erwachse. Seine Vorstellungen kulminierten in dem Konstruktionsentwurf eines Gefängnisses, bestehend aus einem zentralen Bewachungsturm, um den die Zellen kreisförmig angeordnet und vom Turm aus durch Glaswände einsehbar sind.

Diese von ihm als Panoptikum bezeichnete Konstruktion erlaubte eine Überwachung ohne Wächter: Da der Turm von den Zellen aus nicht einsehbar war, mussten die Gefangenen ständig davon ausgehen, beobachtet zu werden. Mit dem Resultat, dass sie ihr Verhalten automatisch an die vermeintlichen Erwartungen der Überwacher anpassten. So beschreibt es auch Winston Smith in Orwells „1984“: *“You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.”*

Benthams Gefängnisse konnten sich nicht durchsetzen. Dafür mutiert unsere Welt gerade zum Panoptikum: Hunderttausende Videokameras auf Straßen, in öffentlichen Gebäuden, Bussen und Bahnen, Kuscheltiere und Kinderuhren mit Mikrofon, HD-Kamera und SIM- oder SD-Karte, Spy-Tools für Smartphones und trackende Navigations-Apps – und natürlich die Kommunikationsfilter der Nachrichtendienste. Orwells Dystopie funktioniert offenbar auch gänzlich ohne „Großen Bruder“. Welchen Preis wir dafür bezahlen, werden wir vor lauter Gewöhnung womöglich nicht einmal bemerken.



Inhalt

Panoptikum

Security News

Übermorgen ist morgen gestern

TeleTrusT Innovationspreis 2017

OWASP Top 10 – 2017

Happy Birthday Privacy Shield

Forensik inside

Secorvo News

Vom Rack zum RZ

24 Verschlüsselungsrätsel

Who watches the watchmen?

Secorvo Seminare

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Übermorgen ist morgen gestern

In den vergangenen Jahren haben sich die öffentlichen Trustcenter, die SSL-Serverzertifikate verkaufen, nicht gerade mit Ruhm bekleckert (u. a. SSN 03/2011, 09/2011 und 09/2017).

Da wäre es doch eine gute Idee, wenn der Browser reagieren könnte, falls ein HTTPS-Server plötzlich ein ganz anderes Zertifikat vorweist als erwartet, dachte man bei Google und entwarf 2011 bis 2015 den HPKP-Standard zum *Public Key Pinning*. Mit dieser HTTP-Header-Erweiterung kann ein Webserver dem Browser mitteilen, wie die Zertifikate aussehen werden, die er in den nächsten Monaten erwarten darf. Bei anderen Zertifikaten blockiert der Browser dann künftig den Zugriff auf die Seite.

Die Krux dabei ist, dass sich im schnelllebigen Internet „erwartet" und „unerwartet" nicht ganz so einfach unterscheiden lassen. Was ist, wenn bspw. der langjährige Zertifikatslieferant plötzlich vom Markt verschwindet? Ein weiteres schlagendes Argument der HPKP-Kritiker ist, dass sich dadurch ein neues Geschäftsfeld für Internet-Erpresser auftut: Wer den Besuchern eines kompromittierten Webservers manipulierte Public Key Pinning Header unterschiebt, könnte einen stolzen Preis für den passenden Private Key verlangen – selbst dann, wenn der Server HPKP eigentlich gar nicht nutzt.

Am 27.10.2017 verkündete Google nun, HPKP in Chrome zum Mai 2018 wieder abschaffen zu wollen – noch bevor Public Key Pinning eine breite Akzeptanz gefunden hat.

TeleTrusT Innovationspreis 2017

Auf dem mit rund 200 Teilnehmern sehr gut besuchten (und sehr empfehlenswerten) T.I.S.P. Community Meeting wurde am 14.11.2017 der TeleTrusT Innovationspreis 2017 an die PointBlank Security/Steen Harbach AG für eine smarte und einfallsreiche IoT-Lösung verliehen.

Man könnte meinen, der Begriff IoT-Security sei ein Widerspruch in sich, da es doch das Ziel der Hersteller (und oft auch der Nutzer) ist, Steuerungen für Alltagsgegenstände möglichst günstig zu realisieren und an das Internet anzubinden. Sicherheitsaspekte müssen dabei in der Regel zurückstehen – sie kosten Ressourcen und erfordern Know-how. Genau in diese Bresche springt die prämierte Lösung: Ein winziger Hardware-Chip ertüchtigt IoT-Geräte mit aktuellen Kryptofunktionen, der Authentisierung von Kommunikationspartnern und einer TLS-Absicherung der Kommunikationsverbindungen.

Der Chip wird in die Kommunikation eingeschleift und ermöglicht trotz der geringen Rechenleistung Kyptofunktionen auf Augenhöhe mit aktuellen PC-Systemen. Laut Herstellerangaben konnte z. B. der TLS-Handshake durch den sehr schlanken Code von ursprünglich mehreren Minuten auf 300 Millisekunden reduziert werden. Ein vielversprechender Ansatz, um einfache IoT-Geräte mit State-of-the-Art-Security-Mechanismen auszustatten. Security Made in Germany eben.

OWASP Top 10 – 2017

Seit inzwischen 13 Jahren veröffentlicht das OWASP regelmäßig die 10 wichtigsten Risiken bei Webanwendungen. Die am 20.11.2017 veröffentlichte finale Version der OWASP Top 10 2017 basiert zum ersten Mal auf Daten der Community. Erschreckend ist die große inhaltliche Übereinstimmung mit der ersten Version der OWASP TOP 10 aus dem Jahr 2004. Offensichtlich ist das Thema Sicherheit trotz vieler Bemühungen noch immer nur in Teilbereichen der Softwareentwicklung angekommen.

Sehr häufig werden die OWASP Top 10 als Standard missverstanden. Tatsächlich sind die Top 10 ein Awareness-Dokument. Für andere Zwecke bieten OWASP und auch andere Organisationen geeignetere Hilfestellungen, wie die Sicherheitsspickzettel für Entwickler, die Top 10 für Entwickler, den Application Security Verification Standard, den Testing Guide und vieles mehr.

Happy Birthday Privacy Shield

Das EU-U.S. Privacy Shield regelt seit 2016 den transatlantischen Datenverkehr personenbezogener Daten in die USA. Es ersetzte das vom Europäischen Gerichtshof für nichtig erklärte Safe-Harbor-Abkommen. Die Effizienz und Effektivität des Privacy Shield muss jährlich von der Europäischen Kommission überprüft werden. In dem am 18.10.2017 publizierten ersten Jahresbericht wurde dessen Wirksamkeit grundsätzlich bestätigt. Jedoch wurden konkrete Maßnahmen zur Verbesserung identifiziert, z. B. hinsichtlich der Kontrolle zertifizierter U.S.-Unternehmen oder der ausstehenden Ernennung eines Privacy-Shield-Ombudsmanns.

Die geforderte Umsetzung der Privacy-Shield-Vorgaben wird genau überwacht und teilweise kontrovers diskutiert. So wird beispielsweise moniert, dass EU-Datenschutzbeauftragte durch die Europäische Kommission ungenügend zur jährlichen Überprüfung einbezogen wurden, weshalb diese nun an einem eigenen Bericht arbeiten.

Inwieweit sich die Resultate mit denjenigen der Europäischen Kommission decken, bleibt abzuwarten. Falls die datenschutzrechtlichen Bedenken nicht ausgeräumt werden können, wird es zu einem wichtigen Indikator für die künftige Datenschutzausrichtung der Europäischen Kommission, wie diesem Umstand Rechnung getragen wird. Denn europäische Datenschutzbeauftragte zeigten und zeigen sich noch immer unzufrieden mit dem vom Privacy Shield vorgegebenen Datenschutzniveau.

Forensik inside

Seit dem 21.11.2017 liegen die Ergebnisse des diesjährigen Volatility Plugin Contest der Volatility Foundation vor, bei dem einige interessante und hilfreiche Erweiterungen prämiert wurden.

Besonders hervorzuheben ist darunter das Plugin SqliteFind, mit dem nun der Hauptspeicher nach jeglichen vorhandenen Table-Definitionen des „sqlite_master table" logisch und automatisiert durchsucht werden kann. In einem zweiten Schritt können dann spezifische Tables zeilenweise als Row ausgelesen werden.

Da SQLite inzwischen von sehr vielen Programmen genutzt wird und es immer seltener bei einer forensischen Analyse zu Beginn bekannt ist, wo ggf. wichtige Datenspuren vorhanden sind, schließt dieses Plugin einen wirklich blinden Fleck bei der forensischen Datenaufbereitung.

Secorvo News

Vom Rack zum RZ

In vielen Unternehmen ist die IT-Infrastruktur über die Jahre gewachsen – und manchmal sieht man ihr das auch an: Der Serverraum war eigentlich nie als Serverraum gedacht, und es sind eher die Erfordernisse des Tagesgeschäfts, die den Ausbau prägen, als eine systematische Planung. Der Sicherheit und Wartbarkeit der Infrastruktur kommt das selten zugute.

Wie aus dem gewachsenen Serverraum ein kleines Rechenzentrum werden kann, das heutigen Sicherheits- und Verfügbarkeitserwartungen genügt, zeigt Marco Müller (DC-Datacenter-Group GmbH) bei unserem kommenden KA-IT-Si-Event am **07.12.2017**, diesmal in den Räumen des Cyber-Forum. Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „**Buffet-Networking**" (zur Anmeldung).



24 Verschlüsselungsrätsel

Am 01.12.2017 beginnt unser Adventsrätsel „Krypto im Advent" für Schülerinnen und Schüler der Klassen 3 bis 9. Der in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe entwickelte interaktive Adventskalender entführt in die Welt der Kryptologie. Diesmal gilt es, die drei Spione innerhalb von 24 Tagen davon abzuhalten, die Weihnachtsfeier der Agenten zu entlarven...

Wer alle Aufgaben richtig beantwortet, kann einen der zahlreichen, von unseren Sponsoren beigesteuerten Preise gewinnen. Auch ältere, an der Kryptologie Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

www.krypto-im-advent.de

Who watches the watchmen?

Merken Sie sich schon einmal die Abschlussveranstaltung der Traumfabrik-Filmreihe „BIG BROTHER: Surveillance Cinema" am **27.02.2018** (18-21 Uhr) im Karlsruher Filmtheater Schauburg vor – einer Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit dem Zentrum für Angewandte Kulturwissenschaft (ZAK) am KIT. Wir zeigen den Film „The Circle" (OmU) und diskutieren anschließend mit **Dr. Stefan Brink** (Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg), **Beate Bube** (Präsidentin des Landesamtes für Verfassungsschutz Baden-Württemberg) und **Thomas Rüttler** (Leiter der Kriminalpolizeidirektion des Polizeipräsidiums Karlsruhe) – eine Anmeldung ist nicht erforderlich.

Secorvo Seminare

Im kommenden Jahr bieten wir Ihnen wieder zahlreiche Gelegenheiten, Ihre Kenntnisse in der IT- und Informationssicherheit aufzufrischen, zu vertiefen und zu zertifizieren. Das nächste T.I.S.P.-Seminar findet **vom 16. bis 20.04.2018** statt – nach Ihrer Anmeldung erhalten Sie zur Vorbereitung ein Exemplar des T.I.S.P.-Begleitbuchs.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2017	
04.-07.12.	Black Hat Europe 2017 (Blackhat, London/UK)
Januar 2018	
19.-21.01.	ShmooCon 2018 (The Shmoo Group, Washington/US)
22.-24.01.	Omnisecure 2018 (in TIME berlin, Berlin)
28.-29.01.	AppSec California 2018 (OWASP Foundation, L.A./US)
Februar 2018	
21.-22.02.	28. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
27.-28.02.	25. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)

Fundsache

Mozilla wartet in diesem Jahr mit einem besonderen Weihnachtsgeschenk auf: Auf einer ansprechend gestalteten Webseite bewertet es die (US-amerikanischen) technischen „Must-Haves“ dieser Geschenkesaison nach einer einfachen Privacy-Taxonomie: Kann es mich ausspionieren? Was weiß es über mich? Und: Was kann passieren, wenn etwas schiefgeht?



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Sarah Niederer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Dezember 2017



Bärendienst

Noch fünf Monate bis zum Inkrafttreten der Datenschutz-Grundverordnung. Kaum ein Magazin, das nicht mahnt und erinnert – und an prominenter Stelle mit den Sanktionen droht: bis zu 20 Mio. € oder 4 % des weltweiten Vorjahresumsatzes.

Das sind Zahlen, die jede Geschäftsleitung erblassen lassen. Stand der Datenschutz bisher abgeschlagen auf der „Da-sollte-ich-mich-vielleicht-auch-mal-drum-kümmern"-Liste, hat er es nun unter die Top 10 der „Wichtig-und-dringend"-Liste geschafft. Datenschützer frohlocken, Aufsichtsbehörden schwitzen unter den signifikant gestiegenen Beratungsanfragen und Datenschutzexperten schießen allerorts wie Pilze aus dem Boden.

Dabei gibt es für Torschlusspanik nicht den geringsten Grund, ist die DS-GVO doch wenig mehr als eine Kopie des BDSG: Kaum eine Bestimmung, die (zumindest in Deutschland) nicht bereits heute gilt. Neu sind die erweiterten Dokumentationspflichten – aber das kann auch als Ruf nach einem höheren „Reifegrad" des Datenschutz-Managements verstanden werden: Wie die Informationssicherheit wird sich zukünftig auch der Datenschutz mit Prozessen und deren Nachweisbarkeit beschäftigen müssen.

Aber diese Anpassungen rechtfertigen kaum den Handlungsdruck, der mit Blick auf den 25. Mai 2018 aufgebaut wird. Denn wie viele Besuche von Aufsichtsbehörden gab es 2017 tatsächlich? Und woher soll das Personal kommen, das diese Anzahl erhöhen könnte? Wenn aber der letzte Vorstand verstanden hat, dass die DS-GVO doch nicht so heiß gegessen wird, wie sie gekocht wurde, kann der Datenschutz schnell wieder in der Asche landen, aus der er gerade aufsteigt. Und dann könnte es sich als Fehler erweisen, dass es Ordnungsgelder waren, die ihn wichtig gemacht haben – und nicht die Einsicht, dass es beim Datenschutz gar nicht um den Schutz von Daten, sondern von Persönlichkeitsrechten geht. Vermutlich ist es nie eine gute Idee, Grundrechte einem Ablasshandel zu überlassen.



Inhalt

Bärendienst

Security News

Geschenktipp 1

Geschenktipp 2

Geschenktipp 3

Geschenktipp 4

Geschenktipp 5

Geschenktipp 6

Geschenktipp 7

Secorvo News

Wie ich lernte, die Blockchain zu lieben.

Who watches the watchmen?

Veranstaltungshinweise

secorvo
security consulting

Security News

Geschenktipp 1

Nachdem am 16.12.2017 bekannt wurde, dass Firefox unerwünscht ein Plug-In installiert, das Daten über die Firefox-Nutzung erhebt, empfehlen wir, Chrome mit den folgenden Plug-Ins zu bescheren, die unerwünschte Werbung und Skripte abschalten.

Das wohl interessanteste ist Privacy Badger der Electronic Frontier Foundation, das über einen lernenden Algorithmus unerwünschte Tracker, Werbung und Cookies zu blockieren versucht. Eine ähnliche Funktionalität bietet das von Firefox bekannte Ghostery. Das Besondere: es kann Tracker verschiedener Kategorien selektiv deaktivieren. Ein klassischer Werbeblocker ist uBlock Origin, der die gängigen Listen unterstützt und nutzt. Erfahrene Anwender können zu uMatrix greifen, das ähnliche Funktionen wie NoScript für Firefox mitbringt.

Am sinnvollsten ist eine Kombination der genannten Plug-Ins: Privacy Badger oder Ghostery als Grundgerüst und als Ergänzung einen Werbeblocker wie uBlock oder uMatrix. Von allen oben genannten Plug-Ins gibt es übrigens auch eine Firefox-Version.

Geschenktipp 2

Sich selbst beschenkt haben die beiden Autodiebe, die in dem am 26.11.2017 von der West Midlands Police veröffentlichten Video die Funkstrecke zwischen dem Autoschlüssel hinter der verschlossenen Eingangstür und dem in der Einfahrt geparkten Wagen mit passender Gerätschaft verlängern.

Uns bescheren sie damit zweierlei: Einerseits eine schöne bildliche Illustration des Man-in-the-Midde Prinzips. Und andererseits die Bestätigung, dass Videoüberwachungen oft nur von beschränktem Nutzen sind – von den Dieben und dem Wagen fehlt bis heute offenbar jede Spur.

Geschenktipp 3

Am 23.11.2017 veröffentlichte Matt Edmondson in seinem Blog, wie sich ein exemplarischer Hidden Service im Tor-Netzwerk durch das Tool Burp Collaborator deanonymisieren lässt: Hidden Services erlauben es, über das Tor-Netzwerk Dienste wie Webserver anzubieten, ohne die IP-Adresse des Servers preiszugeben.

Der Burp Collaborator ist eine 2015 erschienene Erweiterung für das verbreitete Pentesting-Tool Burp Suite, das hilft, Schwachstellen durch die zeitlich versetzte Verarbeitung von Daten zu erkennen – sogenannte Out-of-Band-Angriffe. Dafür werden Hostnamen und URLs mit eindeutigen Merkmalen für jede Anfrage injiziert und danach überwacht, ob diese durch den Server oder nachgelagerte Systeme per DNS aufgelöst bzw. per HTTP angefragt werden. Mit der Erweiterung Collaborator Everywhere lassen sich solche Payloads noch flexibler und großflächiger injizieren.

Der verwundbare Hidden Service löste den HTTP-Header X-Forwarded-For auf und verriet dabei seine tatsächliche IP-Adresse. Der Angriff stellt zwar keine grundsätzliche Verwundbarkeit der Hidden Services dar, illustriert jedoch sehr gut, wie sich der Collaborator einsetzen lässt. Deshalb ist er unser diesjähriger Geschenktipp für Pentester.

Geschenktipp 4

Das Ergebnis des dreijährigen, gemeinsamen Normungsprojekts von Deutscher Bahn, Blancco, DATEV, Secorvo und Toll Collect, die Ende 2016 verabschiedete DIN 66398 („Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“) ist nun, immerhin noch vor Inkrafttreten der Datenschutz-Grundverordnung, in englischer Sprache erschienen und kann beim Beuth Verlag bezogen werden.

Für international tätige Unternehmen – insbesondere mit europäischen Tochter- oder Muttergesellschaften – gehört sie zwingend unter den Weihnachtsbaum.

Geschenktipp 5

Das Bundesarbeitsgericht hat in einem bereits am 25.04.2017 verkündeten und nun schriftlich begründeten Urteil sehr deutlich Grenzen für die Leistungs- und Verhaltenskontrolle gesetzt. Es führt beispielhaft den Abwägungsprozess zwischen Persönlichkeitsrechten und dem Interesse der Arbeitgeber anhand eines Tools zur Erstellung einer „Belastungsstatistik“ vor.

Gegenstand war ein Einigungsstellenspruch über die Auswertung der Schadensfallabwicklung in verschiedenen Außenstellen einer Versicherung. Während der Betriebsrat wegen der – allerdings nicht ausreichend dargelegten – Gesundheitsgefährdung klagte, befand das Bundesarbeitsgericht die gesamte Auswertung für unzulässig. Nach dem aufgeführten Zweck sollten Auslastungsunterschiede der Außenstellen analysiert werden. Hierzu sollte anhand von wöchentlichen bis halbjährlichen, auf den einzelnen Mitarbeiter bezogenen Kennzahlen die quantitativ gemessene Leistung erfasst und bei Abweichung von Schwellenwerten individuell untersucht werden. Das BAG sieht hierin eine unverhältnismäßige ständige Überwachung. Zuvor äußerte es bereits Zweifel an der Eignung und

Erforderlichkeit zum behaupteten, grundsätzlich anzuerkennenden Zweck.

Ausgedruckt ein perfektes Last-Minute-Geschenk für Betriebsräte – Datenschützer müssen hingegen die Kröte schlucken, dass das Bundesarbeitsgericht strikt mit dem Persönlichkeitsrecht argumentiert und weder die informationelle Selbstbestimmung noch § 32 BDSG heranzieht.

Geschenktipp 6

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) informierte am 24.11.2017 über ein interessantes Angebot: Über einen spielerischen Onlinetest können Unternehmen kostenfrei ihre DS-GVO Konformität überprüfen. Hintergrund der Sensibilisierungsaktion ist u. a., dass das BayLDA mit Anfragen zur DS-GVO überhäuft wird. Auf Basis der Online-Selbsteinschätzung wird Unternehmen die Möglichkeit gegeben, ihren aktuellen Datenschutzreifegrad bewerten zu lassen. Die Test-Ergebnisse inklusive Erläuterungen werden in Berichtsform zum Download bereitgestellt. Das perfekte Geschenk für die Geschäftsleitung, falls das Datenschutzbudget 2018 noch umstritten sein sollte...

Geschenktipp 7

Die CNIL (Commission Nationale de l'Informatique et des Libertés) hat neben den bereits veröffentlichten Leitfäden zur Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 DS-GVO nun ein Open-Source-Software-Tool bereitgestellt.

Das Tool führt anhand von Fragen mit Erläuterungen zu den erwarteten Antworten durch die Datenschutz-Folgenabschätzung eines Verfahrens und unterstützt deren Dokumentation. Die Erfassung ist gegliedert in die Verfahrenserfassung (Beschreibung der Verarbeitung), die Abfrage der Rechtsgrundlage und der Verhältnismäßigkeit, die ergriffenen Schutzmaßnahmen und die Bewertung der Risiken nach Eintrittswahrscheinlichkeit und Folgen für die Betroffenen. Als Risiken sind pauschal unbefugter Zugriff, unbefugte Veränderung und Datenverlust vorgegeben. Umfangreicher sind die vorgegebenen und anhand der Hinweise zu beschreibenden Schutzmaßnahmen.

Für Datenschutzbeauftragte, die nur vereinzelt Datenschutz-Folgenabschätzungen durchzuführen haben, kann diese mit dem Tool dokumentiert werden. Es bietet zudem eine gute Orientierung, wenn es auch nur wenige Anpassungen zulässt.

Secorvo News

Wie ich lernte, die Blockchain zu lieben.

Blockchain, die Technologie hinter der Kryptowährung Bitcoin, hat einen regelrechten Hype ausgelöst. Mit ihr können Transaktionen unveränderlich und für jedermann nachvollziehbar erfasst werden, und das ohne eine zentrale Vertrauensinstanz. Viele reagieren auf dieses Versprechen mit Begeisterung: So habe die Blockchain-Technologie noch ganz andere Anwendungen über elektronische Währungen hinaus: In der Musikindustrie ebenso wie zur Absicherung von Militärsystemen. Andere begegnen der Blockchain mit zurückhaltender Skepsis.

Dirk Achenbach erklärt auf dem Jahresstartevent der KA-IT-Si am **01.02.2018** die Blockchain aus kryptographischer Sicht – und stellt in seinem Vortrag dar, wie seine Skepsis der Begeisterung wich. Blockchain ist nämlich keine Universallösung, sondern eine Technologie, die spannende Fragen aufwirft. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Wegen der großen Nachfrage empfehlen wir eine baldige Anmeldung.

Who watches the watchmen?

Wie weit sind wir tatsächlich noch von einem Überwachungsstaat entfernt? Vorratsdatenspeicherung, Sammlung von Nutzungs- und Bewegungsprofilen durch Internet-Dienstleister, Massenüberwachung durch Nachrichtendienste – die Informationstechnik ist dabei, aus Verbrauchern „gläserne Bürger" zu machen. Doch was, wenn die Kontrolleure unkontrollierbar werden?

Als einer der Partner der IT-Sicherheitsregion Karlsruhe lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem ZAK | Zentrum für Angewandte Kulturwissenschaft und Studium Generale am **27.02.2018** wieder zum Filmevent in die Karlsruher Schauburg.

Bei der Abschlussveranstaltung der Traumfabrik #14/2017-18 „BIG BROTHER – Surveillance Cinema" wird der Film „THE CIRCLE" von James Ponsoldt gezeigt. Wolfgang Petroll wird in den Film einführen; im Anschluss folgt eine Diskussion mit Dr. Stefan Brink (Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg), Beate Bube (Präsidentin des Landesamtes für Verfassungsschutz Baden-Württemberg) und Thomas Rüttler (Leiter der Kriminalpolizeidirektion des Polizeipräsidiums Karlsruhe). Danach bieten wir Ihnen wie gewohnt die Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Januar 2018	
19.-21.01.	ShmooCon 2018 (The Shmoo Group, Washington/US)
22.-24.01.	Omnisecure 2018 (in TIME berlin, Berlin)
28.-29.01.	AppSec California 2018 (OWASP Foundation, L.A./US)
Februar 2018	
01.02.	Wie ich lernte, die Blockchain zu lieben. (KA-IT-Si)
21.-22.02.	28. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
27.02.	Who watches the Watchmen? (IT-Sicherheitsregion Karlsruhe)
27.-28.02.	25. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2018	
12.-15.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
20.-22.03.	IT-Sicherheit heute - praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Florenz/IT)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Dr. Volker Hammer, Hans-Joachim Knobloch, Michael Knopp, Sarah Niederer

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2018



Über Mittel und Zwecke

Er ist nicht nur einer meiner Lieblingsfilme, sondern er zählt zweifellos zu den Meisterwerken der Filmgeschichte: Hitchcocks „Das Fenster zum Hof“. Kürzlich konnte ich ihn das erste Mal im Kino bewundern – und war erneut fasziniert von den zahlreichen Parallelgeschichten, die er aus der Perspektive des Fotografen Jefferies (meisterhaft gespielt von James Stewart) erzählt. Der langweilt sich mit einem gebrochenen Bein in seinem New Yorker Apartment – und beobachtet die Nachbarn im Hinterhof durch sein Teleobjektiv. Dabei meint er, einem Mord auf die Spur gekommen zu sein und bittet seinen Freund Doyle von der Kriminalpolizei um Unterstützung. Nach dieser Szene sah ich den Film diesmal aus einer neuen Perspektive. Denn Doyle stellt seinem Freund zuliebe tatsächlich Ermittlungen an – allein auf der Grundlage vager Vermutungen. Erst als Jefferies ihn bittet, eine heimliche Wohnungsdurchsuchung vorzunehmen, erinnert sich Doyle an die rechtsstaatlichen Grenzen der Polizeiarbeit und verweigert seine Unterstützung – für Datenschützer eine Schlüsselszene. Wie vermutlich bei vielen Zuschauern stößt diese Haltung bei Jefferies auf Unverständnis: Schließlich ist für ihn die Sache klar, steht des von ihm Verdächtigten Schuld außer Frage.

Dabei geht es um eine große Errungenschaft des Rechtsstaats: die Unschuldsvermutung, die Beschränkung der Mittel der Strafverfolgung und eine Strafprozessordnung, die nicht der besseren Ahndung von Verbrechen dient, sondern nach Möglichkeit ausschließen soll, dass es zur Verurteilung von Unschuldigen kommt – und sei es um den Preis, einen Schuldigen davonkommen zu lassen. Diese Beschränkung in der Wahl der Mittel gilt es immer wieder aufs Neue zu verteidigen, damit sie nicht im Eifer der Verbrechensbekämpfung der Aufklärungsrate geopfert wird. Und da gibt eine kürzlich veröffentlichte Zahl zu denken: 310.000 stille SMS setzte der Verfassungsschutz 2017 zur Ortung von Mobilfunkteilnehmern ab. 44% mehr als 2016, 214% mehr als 2015. Sind wir da noch auf Kurs?



Inhalt

Über Mittel und Zwecke

Security News

Bürgerrating

HSMs jenseits der Donnerkuppel

WPA ... zum Dritten

Komplexitätsklippen

Big brother is watching

Secorvo News

Weiterbildung 2018

DSMSready2go

Who watches the watchmen?

Veranstaltungshinweise

secorvo
security consulting

Security News

Bürgerrating

Bereits Ende 2017 berichteten verschiedene Online-medien über Chinas Pläne für ein *Social Credit System*. Das bereits im Aufbau befindliche System für einen Score-Wert aller Bürger kann als Beweis für die Berechtigung der Kernaussagen des vor über 30 Jahren ergangenen Volkszählungsurteils des Bundesverfassungsgerichts dienen. Das wegweisende Urteil, das viele Kernelemente des Datenschutzrechts auf den Punkt gebracht hat, warnt davor, dass ein Bürger, der die Erfassung und Auswertung seines Verhaltens nicht einschätzen kann, in seiner persönlichen Freiheit eingeschränkt wird, und dies auch die Wahrnehmung seiner demokratischen Rechte beschränkt. Chinas Pläne, anhand des Verhaltens auf Shopping-Plattformen, Social-Media-Plattformen und der Nutzung von Finanzdienstleistungen, aber auch anhand des Verhaltens vernetzter Freunde, für jeden seiner Bürger einen Score-Wert zu bilden, stellen die Umsetzung der schlimmsten Befürchtungen der damals urteilenden Richter dar.

Aus europäischer Sicht sollte hieraus ein starkes Argument für die bestehenden Datenschutzprinzipien, für Datensparsamkeit und Transparenz erwachsen. Doch das System zeigt auch, was sich bei vielen Nutzern sozialer Medien bereits abzeichnet: Mit dem Angebot zu erlangender Privilegien, Boni oder vereinfachten Zugängen bei „geeignetem" Score-Wert ist offenbar die Versuchung groß, trotz der offensichtlichen Verhaltenssanktionierung sogar freiwillig an der Bestimmung des Score-Werts teilzunehmen. Vor allem Kritiker des Datenschutzes wären gut beraten, die sich nun entwickelnden Szenarien genau zu beobachten.

HSMs jenseits der Donnerkuppel

„Zwei gehen rein, einer kommt raus" heißt es des Öfteren bei Firmenübernahmen wie derjenigen von Gemalto durch Thales, die am 17.12.2017 angekündigt wurde. Betroffen davon sind auch die beiden auf dem überschaubaren Markt für Hardware Security Module (HSMs) weit verbreiteten Produktreihen nShield/nCipher und Safenet/Luna, die ihrerseits durch vorherige Übernahmen im Portfolio der beiden Anbieter gelandet waren. Falls nicht noch die Kartellbehörden zur Auflage machen, eine der beiden Marken an einen Mitbewerber abzutreten, ist zu erwarten, dass Thales über kurz oder lang nur noch eine HSM-Produktreihe weiterführen wird.

Wer HSMs von Thales oder Gemalto z. B. für den Schutz von langlebigen CA-Schlüsseln einsetzt, sollte sich daher bald Gedanken über den langfristigen Support machen. Es wäre nicht das erste Mal, dass Sicherheitsforscher Nutzern helfen müssen, Schlüssel aus ihrem eigenen HSM zu hacken, um den Lieferanten (in diesem Fall: die Produktlinie) wechseln zu können.

WPA ... zum Dritten

Am 08.01.2018 kündigte die Wi-Fi Alliance an, im Laufe dieses Jahres einen neuen WLAN-Sicherheitsstandard WPA3 zu etablieren, der WPA und WPA2 ablösen soll. WPA3 soll in mindestens den folgenden vier Punkten Verbesserungen bringen:

- Eine nicht-authentifizierte Mindestverschlüsselung für bislang völlig offene WLAN-Netze wie öffentliche Hotspots
- Ein Verfahren für die WLAN-Security-Konfiguration von IoT-Geräten ohne eigenes Display (wohl ähnlich WPS, aber hoffentlich sicherer)
- Die bekannte Anfälligkeit von WPA2 Personal gegen Offline-Attacken auf schwache WLAN-Passwörter in einmal mitgeschnittenen Handshakes
- Zum Suite-B-Nachfolger CNSA kompatible Kryptoverfahren für „National Security Systems" in den USA

Genaue technische Details sind noch nicht bekannt, aber es darf vermutet werden, dass die Wi-Fi Alliance dieses Mal nicht direkt auf den IEEE 802.11 Standard zurückgreift, sondern u. a. auf RFC 7664 und RFC 8110.

Es lohnt wohl, evtl. geplante Investitionen in eine neue WLAN-Infrastruktur noch etwas zurück zu stellen, bis WPA3-fähige Geräte verfügbar sind – oder zumindest jetzt schon auf entsprechende Upgrade-Fähigkeit zu achten. Die Vorgänger WPA und WPA2 verbreiteten sich jeweils relativ zügig, wenn auch vor dem Hintergrund der Angriffe auf das bereits konzeptionell missratene WEP.

Komplexitätsklippen

Am 06.01.2018 veröffentlichten Paul Rösler, Christian Mainka und Jörg Schwenk von der Ruhr-Universität in Bochum eine vergleichende Untersuchung über die Sicherheit der Gruppen-Chats der verbreiteten Messenger-Dienste WhatsApp, Signal und Threema. Im Rahmen ihrer Analysen entdeckten die Autoren Schwachstellen in der Ende-zu-Ende-Verschlüsselung von Gruppen-Chats in WhatsApp und Signal, die einem Angreifer erlauben, unautorisiert beliebige Benutzer zu einer bestehenden Gruppe hinzuzufügen. Hierbei nutzen sie das Fehlen einer Authentisierung von *group management messages* aus. Diese Nachrichten werden an alle Gruppenmitglieder gesendet,

woraufhin diese einen Schlüsselaustausch mit dem neuen Mitglied durchführen.

Im Detail unterscheiden sich die Schwachstellen der beiden Messenger jedoch, sodass die Schwachstelle von WhatsApp als schwer wiegender einzustufen ist. Bei WhatsApp gibt es nur einzelne Administratoren, die berechtigt sind, neue Benutzer zu einer Gruppe hinzuzufügen. Hierfür laufen die Nachrichten über die zentralen Server von WhatsApp, um die Berechtigung der Benutzer zu prüfen. Eine Ende-zu-Ende-Verschlüsselung findet dabei nicht statt. Um die Schwachstelle auszunutzen, muss ein Angreifer einen WhatsApp-Server unter seiner Kontrolle haben und zusätzlich die komplexe ID des Chats kennen.

Beide Schwachstellen sind insgesamt diffizil und lassen sich in der Praxis wohl eher nicht ausnutzen, zumal die Nachricht, dass ein neuer Benutzer hinzugefügt wurde, weiterhin angezeigt wird. Dennoch zeigt die Analyse, wie komplex Ende-zu-Ende-Kommunikation in Gruppen sein kann. Gerade die Schnittstellen zwischen kryptografischen Protokollen und Management sind hierbei kritisch.

Big brother is watching

Der am 15.01.2018 in der Frankfurter Allgemeine erschienene Beitrag zu WeChat sollte aus Datenschutzsicht zu Vorsicht mahnen. Hinter der Entwicklung des Kurznachrichtendienst WeChat, der mittlerweile sehr viel mehr kann als Nachrichten auszutauschen und z. B. das Buchen von Reisen und Tickets, das Begleichen von Rechnungen, Arztterminvereinbarungen oder Geldtransfers ermöglicht, steht die chinesische Firma Tencent. Mittlerweile wird die App (überwiegend in China) von knapp einer Milliarde Menschen genutzt.

Durch die geografische Angebotserweiterung soll nun der Vorstoß in neue Weltmärkte gelingen. Seit 2017 ist die App auch aus Deutschland offiziell im App Store downloadbar. Obwohl die Messaging App von TrustArc (ehemals TRUSTe) zertifiziert ist und ein „Höchstmaß an Kontrolle über die Privatsphäre“ verspricht, raten wir – zumindest aus Datenschutzsicht – dringend vor einer Installation ab. Es sei denn, man möchte, dass alle Daten an den chinesischen Staat geliefert werden und diesem zur Datenauswertung zur Verfügung stehen.

Secorvo News

Weiterbildung 2018

Die Secorvo-Seminare starten in diesem Jahr mit einem Vorbereitungsseminar für sichere Softwareentwicklung und der Zertifizierung als T.P.S.S.E. (**12.–15.03.2018**), gefolgt von IT-Sicherheit heute (**20.–22.03.2018**). Im April bieten wir Ihnen die nächste Gelegenheit, sich als T.I.S.P. zu zertifizieren (**16.–20.04.2018**).

Die aktuellen Seminarprogramme und eine Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

DSMSready2go

Eine der wichtigen Änderungen, die die europäische Datenschutz-Grundverordnung mit sich bringt, sind die erweiterten Dokumentationspflichten. Damit wird, davon sind wir überzeugt, der Datenschutz zukünftig den Aufbau von Managementsystemen erfordern, wie wir sie bereits aus der Informationssicherheit, insbesondere der ISO/IEC-Standard-Familie 2700x kennen.

Um diesen Prozess zu unterstützen hat Secorvo ein Datenschutz-Management-System auf der Grundlage eines Confluence CMS entwickelt, das Vorlagen, Prozesse, Richtlinien, Verfahrensverzeichnis und eine Methode zur Datenschutzfolgenabschätzung für die DSGVO-konforme Umsetzung des Datenschutzes in KMU bereitstellt – angelehnt an das erfolgreiche ISMSready2go. Nehmen Sie bei Interesse gerne Kontakt mit uns auf.

Who watches the watchmen?

Wie weit sind wir tatsächlich noch von einem Überwachungsstaat entfernt? Die Informationstechnik ist dabei, aus Verbrauchern „gläserne Bürger“ zu machen. Doch was, wenn die Kontrolleure sich der Kontrolle entziehen – oder gar unkontrollierbar werden?

Zusammen mit dem ZAK (Zentrum für Angewandte Kulturwissenschaft und Studium Generale des KIT) lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **27.02.2018** wieder zum Filmevent in die Karlsruher Schauburg. Bei dieser Abschlussveranstaltung der Traumfabrik „BIG BROTHER – Surveillance Cinema“ wird der Film „THE CIRCLE“ von James Ponsoldt gezeigt. Die Einführung in den Film übernimmt Wolfgang Petroll, der bereits durch die gesamte Filmreihe führte. Im Anschluss an den Film findet eine Diskussion mit **Dr. Stefan Brink** (Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg), **Beate Bube** (Präsidentin des Landesamtes für Verfassungsschutz Baden-Württemberg) und **Thomas Rüttler** (Leiter der Kriminalpolizeidirektion des Polizeipräsidiums Karlsruhe) statt. Anschließend können Sie den Abend im persönlichen Austausch beim „Buffet-Networking“ ausklingen lassen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2018	
01.02.	Wie ich lernte, die Blockchain zu lieben (KA-IT-Si, Karlsruhe)
21.-22.02.	28. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
27.02.	Who watches the watchmen? (KA-IT-Si, Karlsruhe)
27.-28.02.	25. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2018	
12.-15.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
20.-22.03.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Florenz/IT)
April 2018	
10.-11.04.	Datenschutztage 2018 (FFD Forum für Datenschutz, Wiesbaden)
16.-20.04.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
24.-26.04.	3rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, London/UK)
29.04.-03.05.	Eurocrypt 2018 (IACR, Tel Aviv/ISR)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Hans-Joachim Knobloch, Michael Knopp. Sarah Niederer.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2018



Des Kaisers neue Kleider

Keine Gazette, die etwas auf sich hält, konnte sich in den vergangenen 24 Monaten eines Beitrags zum Thema „Blockchain“ enthalten. „Disruptiv“, ja „revolutionär“ sei diese Technologie, kann man da lesen. Sie stelle ganze Wirtschaftszweige in Frage und ermögliche neue Geschäftsmodelle. Ein solches Wunderding mag man nicht unbeachtet vorbeiziehen lassen – und so stürzen sich allerorten große und größere Unternehmen darauf: Wer lässt sich schon gerne abschaffen? Also werden Kooperationen ausgerufen und Konzeptideen in die Welt gesetzt – und die Blockchain mutiert zum „Must have“: Wer jetzt noch nicht dabei ist, hat die Zukunft verspielt.

Unglücklicherweise ist das Blockchain-Konzept nicht so einfach zu verstehen; selbst Kryptologen ringen mit den Sicherheitsannahmen, die dem Verfahren zu Grunde liegen. Und so darf nicht verwundern, dass viele Beiträge nebulös bleiben – daher hat wohl auch der eine oder andere, der gerade neue Blockchain-Geschäftsideen herbeiträumt, nicht genau verstanden, wie das alles funktioniert. Details werden schließlich ohnehin meist überbewertet. Darum stieg das Vertrauen in die „Kryptowährung“ Bitcoin ins Unglaubliche – und machte das Konzept zur *self fulfilling prophecy*: Wenn alle vertrauen, dann ist das Verfahren sicherlich vertrauenswürdig…

So faszinierend die Ideen hinter der Blockchain, so schwer lassen sich Anwendungen jenseits von Bitcoin vorstellen, für die eine dezentrale, komplett transparente und aufwändig zu verifizierende Blockchain die richtige technische Umsetzung ist. Selbst für ein Zahlungssystem ist Bitcoin nur eingeschränkt geeignet: Transaktionen dauern lange, die Verifikation ist aufwändig und die dezentral zu speichernde Transaktionskette wird immer größer. Schließlich darf man seinen geheimen Schlüssel nicht verlieren, sonst ist das Vermögen futsch.

Für die Bitcoin- und Blockchain-Investoren bleibt daher zu hoffen, dass so schnell niemand „Der König ist ja nackt!“ ruft.



Inhalt

Des Kaisers neue Kleider

Security News

Hack & Mine

Hidden Champions & Risks

Tot & lebendig

Zertifikate & Kleingedrucktes

Hilfe & Selbsthilfe

Secorvo News

Das Netz, die Kaffeemaschine & unsere Fehler

Wissensaktualisierung

Veranstaltungshinweise

Security News

Hack & Mine

Der sinkende Tauschwert der Krypto-Währung Bitcoin motiviert derzeit neue Geschäftsideen: Wenn die Kosten für Strom und Rechnerinfrastruktur bei der rechenintensiven Prüfung der Transaktionen der Bitcoin-Blockchain (derzeit jährlich ca. 52,48 TWh, etwa 800 kWh pro Transaktion) den Wert der dabei „geschürften" Bitcoin übersteigen, liegt es nahe, die Kosten zu „externalisieren" – sprich: sich den Zugang zu leistungsfähigen Rechnernetzen zu verschaffen und diese im Auftrag schürfen zu lassen. Bereits in den SSN 10/2017 haben wir vor Drive-By-Minern gewarnt. Inzwischen kommt es vermehrt zu gezielten Angriffen auf Rechenzentren, um deren Rechenleistung in Bitcoins zu transferieren. So wurde am 08.01.2018 öffentlich, dass das Landesamt für Besoldung und Versorgung Baden-Württemberg Opfer von „Cryptojacking" geworden war, am 12.02.2018 wurde vom Missbrauch eines europäischen Wasserwerks berichtet und offenbar erwischte es auch Tesla, wie am 21.02.2018 bekannt wurde.

Zwar entsteht durch die Kryptowährungen kein neuer Angriffsvektor – wohl aber eine neue Motivation, da sich beim Cryptojacking ein erfolgreicher Angriff unmittelbar in (un)bares Geld verwandeln lässt.

Hidden Champions & Risks

Als zu Beginn dieses Jahres die Meltdown-Sicherheitslücke bei Intel-x86-Prozessoren die Schlagzeilen beherrschte, war den meisten Anwendern weltweit klar, dass es dabei um die Sicherheit ihrer PCs ging. Schließlich hatte Intel über die Jahre mit etlichen Marketing-Millionen das „Intel Inside" Warenzeichen im Bewusstsein der Käufer verankert. Auch dass und wofür man sich den monatlichen Patch-Tuesdays des Windows Update Zyklus anschließen sollte, ist bei fast allen IT-Profis und vielen Durchschnittsbürgern längst angekommen.

Aber wer kennt – selbst unter IT-Fachleuten – beispielsweise Kalignite von der schottischen Softwarefirma KAL oder ForeSite von Orpak Systems Ltd. in Israel? Erstere ist eine Anwendungsplattform für Windows, die die Geldautomaten von 40 verschiedenen Herstellern in 80 Ländern antreibt. Letztere ist eine Software, die den Betrieb von 35.000 Tankstellen auf vier Kontinenten automatisiert. Und neben der weiten Verbreitung haben beide Systeme noch eines gemeinsam: Am 11.01. bzw. am 31.01.2018 wurde gemeldet, dass sie Schwachstellen enthalten, die in einem Fall bereits nachweisbar, in anderen potenziell von Kriminellen ausgenutzt werden und jeweils signifikante Teile einer ganzen Branche betreffen können.

Die Gefahr von „Monokulturen" bei Prozessoren und Betriebssystemen ist bekannt. Daneben bergen aber gerade die weniger augenfälligen „Hidden Champions" unter den Branchenanwendungen ein hohes Flächenrisiko, das dank der Goldgräberstimmung in den Buzzword-Themen Digitalisierung, IoT und Industrie 4.0 in nächster Zeit weiter zunehmen wird.

Da wäre es keine schlechte Idee für das im Koalitionsvertrag avisierte IT-Sicherheitsgesetz 2.0, die Prozesse für sichere Softwareentwicklung, Schwachstellensuche und -behebung bei marktbeherrschender Fachanwendungs-Software in kritischen Bereichen unter die Lupe zu nehmen – und zu regulieren.

Tot & lebendig

Der Entwickler der Bibliothek go-bindata hatte vor einiger Zeit seinen GitHub-Account gelöscht. Am 07.02.2018 tauchte der Account erneut mit dem gleichen Namen auf – denn der Benutzername eines gelöschten GitHub-Accounts kann unmittelbar danach wieder benutzt werden. Über diesen Mechanismus könnte ein Angreifer ein gefälschtes Repository einrichten und eine trojanisierte Version einer bekannten (Open Source) Software verbreiten. Darüber kann ein Angreifer beliebigen Code auf Systemen auszuführen, die eine Bibliothek aus dem (übernommenen) Repository beziehen.

Besondere Brisanz erlangt diese Schwachstelle dadurch, dass diverse Anwendungen und sogar Paketmanager mit namensbezogenen URLs auf GitHub-Repositories arbeiten. Für den Anwender sind solche Zusammenhänge jedoch bestenfalls erst mit einem zweiten, intensiveren Blick erkennbar.

GitHub prüft derzeit noch intern, ob ehemals verwendete Benutzernamen permanent oder temporär gesperrt werden sollen. Andere Anbieter wie Google setzen dies bereits seit langer Zeit um. Manchen wie beispielsweise Twitter wurden derartige Probleme in der Vergangenheit ebenfalls zum Verhängnis. Entwickler, die ihr kostenpflichtiges Konto nicht weiter benutzen möchten, sollten es nicht löschen sondern auf einen kostenlosen Account herunterstufen.

Die Prüfung auf Schwachstellen bei der Account-Löschung ist gängiger Bestandteil eines Penetrationstests einer Anwendung. Dies findet sich sogar in Prüfkatalogen wie dem OWASP Testing Guide. Neu ist diese Problematik also keinesfalls.

Zertifikate & Kleingedrucktes

Am 28.02.2018 erhielten ca. 23.000 Kunden des Zertifikats-Resellers Trustico eine E-Mail-Nachricht über die unmittelbar bevorstehende Sperrung ihres Webserver-Zertifikats aufgrund einer gemeldeten Kompromittierung des zugehörigen privaten Schlüssels. Hintergrund dieser Massen-Rückrufaktion war kein Cyberangriff, sondern ein bizarrer Vertragsstreit zweier Unternehmen, deren Geschäftsgrundlage eigentlich das Vertrauen in ihre sorgfältige und regelkonforme Arbeitsweise darstellt.

Trustico wollte nach der nicht ganz freiwilligen Übergabe des Trustcenter-Geschäfts von Symantec an DigiCert (vgl. SSN 09/2017) die Bezugsquelle wechseln, kündigte den bestehenden Reseller-Vertrag und schloss einen neuen mit Mitbewerber Comodo ab. Soweit noch ganz normale unternehmerische Handlungsweise. Offenbar wollte man aber kurzfristig auch die Zertifikate des Kundenbestands gegen solche des neuen Partners wechseln und dazu die vorhandenen Zertifikate der DigiCert-Marken sperren lassen. Da nach den Baseline Requirements (BR) des CA/Browser-Forums (Abschnitt 4.9.1.1) ein Vertragswechsel jedoch kein zulässiger Sperrgrund ist, verweigerte DigiCert dies solange, bis Trustico seiner Bitte offenbar 23.000 geheime Kundenschlüssel beifügte: Damit war ein Sperrgrund nach Abschnitt 4.9.1.1 Nr. 3 gegeben – Anzeichen für eine Kompromittierung privater Schlüssel.

Offenbar hat Trustico nicht nur – nach BR zulässig (!) – private Keys stellvertretend für Kunden erzeugt, sondern diese auch archiviert. Auch dies wäre zulässig, jedoch nur mit Einwilligung des Kunden (BR Abschnitt 6.1.2), die eventuell beim (Über-)Lesen der AGB erteilt wurde. Spätestens jedoch mit der Weitergabe hat Trustico wohl gegen die BR verstoßen – besonders pikant, da das Unternehmen auch selbst als CA auftritt. Die Lehre für Zertifikatskäufer: Das Vertrauen in einen Anbieter sollte man nicht nur am Preis festmachen, sondern u a. auch daran, wie klar und verständlich das „Kleingedruckte" präsentiert wird.

Hilfe & Selbsthilfe

Die Datenschutz-Grundverordnung (DSGVO) nimmt die Datenschutz-Aufsichtsbehörden in die Pflicht, insbesondere für kleine und mittelständige Unternehmen Praxishilfen für die Umsetzung der DSGVO zu entwickeln und zu veröffentlichen.

Dem ist die Bundesdatenschutzbeauftragte am 11.01.2018 mit der Veröffentlichung von Kurzpapieren nachgekommen, die von der Datenschutzkonferenz (dem ehemaligen „Düsseldorfer Kreis" der Aufsichtsbehörden des Bundes und der Länder) entwickelt und verabschiedet wurden. Darunter finden sich Erläuterungen beispielsweise zum Verzeichnis der Verarbeitungstätigkeiten, der Nutzung personenbezogener Daten für Werbezwecke, der Datenschutz-Folgenabschätzung oder dem Recht auf Löschung.

Die Nutzung dieser Kurzpapiere ist auch schon deshalb anzuraten, weil die Aufsichtsbehörden darin zugleich ihre Erwartungen an die Umsetzung der DSGVO konkretisieren.

Secorvo News

Das Netz, die Kaffeemaschine & unsere Fehler

Bei der Vernetzung der Produkte und Produktionsmaschinen tappen die Hersteller derzeit in die gleichen Fallen wie bei der Vernetzung der Computer „damals". Ob in Großindustrieanlagen, im Auto, im Stromzähler oder im trauten Heim: Überall sind inzwischen Computer eingebaut. Damit kaufen wir uns ein, dass diese Systeme nun dieselben Schwachstellen besitzen wie unsere PCs. Laptops, Smartphones und Tablets. Das Ergebnis: Industrieanlagen können via Internet herunter gefahren werden, unsere Autos lassen sich von Fremden öffnen, Stromzähler plaudern unsere Verbrauchswerte aus und der Staubsauger streamt Live-Videos aus unserem Wohnzimmer.

Dabei sind diese Schwachstellen alle vermeidbar: Angriffspunkte und auch die Schutzmaßnahmen sind meist bekannt – nur nicht an der richtigen Stelle.

Am Beispiel einer App-gesteuerten Kaffeemaschine wird Klaus J. Müller (Leitwerk AG) beim kommenden Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **15.03.2018** zeigen, was schief laufen kann und wie Sie die typischen Fallstricke vermeiden können. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (zur Anmeldung).

Wissensaktualisierung

Im März startet die Secorvo-Seminar-Saison mit einem Vorbereitungsseminar für sichere Softwareentwicklung und der Zertifizierung als T.P.S.S.E. (**12.–15.03.2018**). Und im April bieten wir Ihnen die nächste Möglichkeit, sich als T.I.S.P. zu zertifizieren (**16.–20.04.2018**), danach erneut im Juni (**11.–15.06.2018**).

Die aktuellen Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2018	
12.-15.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
15.03.	Das Netz, die Kaffeemaschine und unsere Fehler (KA-IT-Si, Karlsruhe)
20.-21.03.	a-i3/BSI-Symposium 2018 (Arbeitsgruppe Identitätsschutz im Internet, Bochum)
21.-23.03.	DFRWS EU Conference (DFRWS, Florenz/I)
April 2018	
10.-11.04.	Datenschutztage 2018 (FFD Forum für Datenschutz, Wiesbaden)
12.-13.04.	11. GDD-Fachtagung Datenschutz international (Gesellschaft für Datenschutz und Datensicherung, Berlin)
19.-20.04.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
24.-26.04.	3rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, London/UK)
25.-26.04.	BvD Verbandstag 2018 (BvD e.V., Berlin)
25.-27.04.	Sicherheit 2018 (Gesellschaft für Informatik e.V., Fachbereich Sicherheit, Konstanz)
29.04.-03.05.	Eurocrypt 2018 (IACR, Tel Aviv/ISR)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Hans-Joachim Knobloch.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

März 2018



Der Kern des Problems

Werbung hat Streuverluste. Niemand hat das so treffend auf den Punkt gebracht wie *Henry Ford* (1863-1947) in dem ihm zugeschriebenen Bonmot: „Ich weiß, die Hälfte meiner Werbung ist hinausgeworfenes Geld. Ich weiß nur nicht, welche."

Folgerichtig ist eines der zentralen Ziele im Marketing, diese Verluste zu reduzieren. Das gelingt allerdings nur, wenn der Werber möglichst präzise weiß, *wen* er erreichen muss und *wie* er diese Zielgruppe wirksam anspricht.

In beiderlei Hinsicht ist das Internet der Heilige Gral. Denn anders als bei einer Zeitschriftenanzeige, einer Plakatwerbung oder einem TV-Spot weiß jede Webseite, wer sie gerade besucht – und kann die zum Besucher passende Werbung einblenden.

Und zugleich, noch wertvoller, ist „im Netz" weit mehr über den Besucher bekannt, als anonyme Zuschauer- oder Leserbefragungen verraten – obendrein personalisiert. Dabei sind es sind nicht die „klassischen" personenbezogenen Daten wie Name, Geburtsdatum oder E-Mail-Adresse, die den eigentlichen Wert darstellen, sondern von vielen Betroffenen als wenig relevant eingestufte „Meta-Informationen": Zu welchen Zeiten wurden welche Seiten besucht? Welche Personen werden wie oft kontaktiert? Wie oft wurde wann nach was gesucht? Diese vermeintlich harmlosen Daten entblößen jedoch mit zunehmender Internet-Nutzung nahezu alles: die tatsächlichen Interessen (Suchziele), typische Verhaltensmuster (Nutzungszeiten, Verweildauern und Standortverläufe), Neigungen (Kontaktintensität) bis hin zur sexuellen Orientierung – und bei automatischer Auswertung von Nachrichteninhalten auch die persönlichsten Überzeugungen. Und mit jeder neuen App werden es mehr.

Ihre Analyse zielt dabei nicht auf Überwachung. Sondern darauf, die Unterschiede zu finden – bis zur Vorhersage des Verhaltens. Anders formuliert: Sie will die Persönlichkeit. Und genau deshalb ist nicht der Datenmissbrauch das Problem. Sondern diese Daten selbst.



Inhalt

Der Kern des Problems

Security News

Illegalisierte Blockchain

Man in the ISP

Darf's ein bisschen mehr sein?

Schwachstellensuche bei LTE

Orientierungspunkte

Secorvo News

Für Kurzentschlossene

Sesam, öffne Dich – nicht.

Veranstaltungshinweise

secorvo
security consulting

Security News

Illegalisierte Blockchain

Wie in den SSN 2/2018 thematisiert, hat wohl nicht jeder, der die Blockchain als Lösung verschiedenster Probleme propagiert, das Konzept und seine Eigenschaften komplett durchdrungen. Einige „Nutzer" scheinen aber zumindest ein wesentliches Feature erfasst zu haben: Etwas, das einmal gültig in der Blockchain verzeichnet ist, kann nie wieder daraus verschwinden, allenfalls mit einem späteren Eintrag wieder rückabgewickelt werden.

Am 12.03.2018 veröffentlichten Forscher aus Frankfurt und Aachen eine Untersuchung von Dateninhalten, die bei vergangenen Transaktionen unauslöschlich in die Bitcoin-Blockchain aufgenommen wurden. Unter knapp 150 auffindbaren Bild-Dateien ist auch eine, die mutmaßlich den Tatbestand der Kinderpornographie erfüllt; dazu kommen mehrere Dutzend Links zu entsprechendem Material im sogenannten Darknet.

Damit sind die Beschaffung und der Besitz einer Kopie der kompletten Bitcoin-Blockchain, wie sie für das Bitcoin-Mining grundsätzlich erforderlich ist, in Deutschland und vielen anderen Ländern vermutlich illegal – ganz unabhängig vom rechtlichen Status der Bitcoin als Zahlungsmittel.

Man in the ISP

Citizen Lab beschreibt in einer Veröffentlichung vom 09.03.2018, wie die Internet Service Provider (ISP) Türk Telekom und Telecom Egypt Deep-Packet-Inspection-Technologien (DPI) nutzen, um ihren Kunden Schadsoftware oder Krypto-Miner unterzuschieben. DPI erlaubt es, nicht nur Metadaten von Datenpaketen zu durchsuchen, sondern auch deren Inhalte. Diese Möglichkeit wurde vor allem zur Erkennung und Filterung von Schadsoftware und Spam im Netzwerkverkehr entwickelt, lässt sich jedoch auch für Zensur und Einschränkung der Netzneutralität nutzen.

Offenbar werden von Türk Telekom unverschlüsselte Programmdownloads bekannter Programme wie VLC, Skype oder Opera mit einer Schadsoftware infiziert, die es erlaubt, die Computer der Benutzer auszuspähen. In Ägypten werden Teile des Verkehrs auf Affiliate-Programme und Krypto-Miner geleitet, um zusätzliche Einnahmen zu generieren.

Auch der Download von Programmen sollte wie jede andere sensible Kommunikation über einen TLS geschützten Kanal stattfinden. Mechanismen wie HSTS verhindern dabei ungewollte Downgrades auf HTTP. Manipulationsangriffe muss man dabei offenbar nicht mehr nur bei offenen WLANs unbekannter Anbieter befürchten, sondern sollte auch besser Providern keinen Vertrauensvorschuss mehr gewähren. Leider gibt es noch immer zahlreiche Softwareanbieter und andere Hersteller, die ihre Downloads unverschlüsselt bereitstellen.

Darf's ein bisschen mehr sein?

Weltweit gültige TLS-Serverzertifikate bekommt man nach den Richtlinien des CA/Browser-Forums in den Geschmacksrichtungen DV, OV und EV. Die EV (Extended Validation) Zertifikate enthalten über den oder die Servernamen hinaus weitere Angaben zum dahinter stehenden Unternehmen. In einem für Antragsteller und Trustcenter gleichermaßen aufwändigen Validierungsprozess wird sichergestellt, dass alle enthaltenen Angaben korrekt sind, das Unternehmen die fragliche Internet-Domain besitzt und die Erstellung des Zertifikats auch tatsächlich veranlasst hat. EV-Zertifikate werden eingesetzt, wo dies regulatorisch verlangt ist, bspw. beim Online-Banking, oder wo immer der Serverbetreiber Wert auf den „grünen Balken" legt, mit dem Browser besondere Vertrauenswürdigkeit anzeigen.

OV (Organization Validation) Zertifikate vereinen die Nachteile der beiden anderen Typen: Bei der Ausstellung werden zwar ähnlich wie bei EV Angaben zum Unternehmen geprüft, vom Browser wird jedoch kein Unterschied zu DV-Zertifikaten angezeigt.

Bei der einfachsten Kategorie, den DV (Domain Validation) Zertifikaten, wird vor der Ausstellung lediglich geprüft, ob der Antragsteller Kontrolle über die Internet-Domain hat, in der der zu zertifizierende Servername liegt. Dieser Check ist gut automatisierbar. Genau das macht sich die gemeinnützige CA Let's Encrypt zunutze, die kostenfrei DV-Zertifikate ausstellt.

Am 13.0.3.2018 aktivierte Let's Encrypt ACMEv2, die neue Version ihres Protokolls zum automatischen Zertifikatsbezug. Damit sind nun auch Wildcard-DV-Zertifikate für alle Server einer bestimmten Subdomain kostenfrei erhältlich.

Seither gibt es kaum noch Gründe, bei einem kommerziellen Trustcenter zu kaufen, wenn es kein EV-Zertifikat sein soll. Interne Serverzertifikate der eigenen PKI kann jedoch auch Let's Encrypt nicht komplett ersetzen – rein intern genutzte Server- bzw. Domain-Namen oder IP-Adressen sind für öffentliche DV-Zertifikate tabu.

Schwachstellensuche bei LTE

Am 06.03.2018 veröffentlichten Forscher der Universitäten Purdue und Iowa Details zu dem von ihnen entwickelten Tool LTEInspector. Ähnlich wie der bekannte IMSI-Catcher zu GSM-Zeiten setzt sich

dieses Tool als Emulation eines Access Points und eines Endgeräts zwischen LTE-Endgerät und Providernetz und erlaubt es, Analysemethoden für Kryptoprotokolle automatisiert auf reale LTE-Netze anzuwenden. Damit wurden auch gleich zehn neue und neun bereits bekannte Angriffe gegen den LTE-Verbindungsaufbau (wieder-)entdeckt und in echten LTE-Netzen durchgespielt.

So hoch der Wert des Tools für Analyse und Validierung von Sicherheitsprotokollen einzuschätzen ist, muss man doch die Tragweite der Schwachstellen relativieren. Ein Angreifer muss sich in Funkreichweite des Opfers befinden: Dadurch sind bspw. eine grobe Lokalisation des Opfers und die Möglichkeit, dessen Funknetz-Aktivitäten zeitlich zu erfassen, auch ohne elaborierten Protokollangriff gegeben. Auch ein Denial-of-Service wäre protokollunabhängig durch einen Störsender möglich.

Einer der Angriffe erlaubt, unautorisiert für Erdbeben oder Tsunamis gedachte Warnmeldungen abzusetzen. Dies scheint im Sinne einer Risikoabwägung plausibel – dass Sicherheitshürden im Katastrophenfall fatal sein könnten, hat sich u. a. bei der verzögerten Entwarnung nach dem Raketen-Fehlalarm auf Hawaii im Januar bestätigt.

Verblüffend ist, dass bei einem großen US-Provider unverschlüsselte LTE-Verbindungen möglich waren. Warum Handys nicht – wie jeder WWW-Browser – dem Anwender den Verschlüsselungsstatus seiner Verbindung anzeigen, bleibt nach wie vor ein Rätsel.

Orientierungspunkte

Die Art. 29 Gruppe beschloss am 06.02.2018 eine Reihe neuer Orientierungshilfen zur DSGVO. Mehrere beziehen sich auf den Datenverkehr mit Drittstaaten, u. a. mit Bezug die einschlägige EuGH-Rechtsprechung und Art. 44 ff DSGVO. Sie beschäftigen sich mit der Feststellung eines angemessenen Datenschutzniveaus (WP 254 rv.01), den Ausnahmeregelungen des Art. 49 (WP261/262) und mit den notwendigen Elementen von *Corporate Binding Rules* (BCR, WP 257 rev.01). Zur Feststellung des angemessenen Datenschutzniveaus sei nur die Umsetzung der Kerninhalte der Europäischen Gesetzgebung zu prüfen; dabei wird jedoch sehr weitgehend auf die bestehenden Instrumente wie Zweckbindung, Betroffenenrechte und Transparenz zurückgegriffen. Daneben werden eine unabhängige Aufsicht und eine wirkungsvolle Beschränkung staatlicher Eingriffsbefugnisse gefordert. Die Ausführungen zu BCR umfassen eine Tabelle mit kommentierten Inhaltsanforderungen, darunter direkte Ansprüche des Betroffenen als Drittbegünstigtem. Der Art. 49 schließlich sei als Ausnahmeregelung zu verstehen und sehr eng auszulegen.

Weiter passte die Art. 29 Gruppe die Richtlinien zur Meldung von Datenschutzvorfällen (WP250rev.01), zu automatisierten Einzelentscheidungen (WP251-rev.01) und zur Bußgeldbemessung (WP253) an.

WP250 setzt sich umfangreich mit dem Zusammenspiel von Auftragsverarbeiter und Verantwortlichem, dem Meldeinhalt und dem Ablauf zur Vorfallsklärung auseinander. Am Ende steht eine Liste mit Beispielvorfällen. Eine Meldung wird regelmäßig innerhalb von drei Tagen erwartet; Prozesse zur technischen Vorfallserkennung und –untersuchung werden nach Art. 32 DSGVO vorausgesetzt.

WP251 zu automatisierten Einzelfallentscheidungen fasst in einer Liste am Ende konkrete Umsetzungsanforderungen als *best practice* zusammen. Das Papier zur Bußgeldfestsetzung (bereits vom Oktober 2017) enthält zahlreiche Bemessungskriterien, eine sehr weite, Art. 4 Nr. 19 DSGVO ignorierende Unternehmensdefinition zur Erfassung ganzer Konzerne, allerdings keine konkreten beispielhaften Bemessungen. Intensiv diskutiert werden jedoch alternative Maßnahmen wie Verwarnungen.

Insgesamt tragen die Orientierungshilfen dazu bei, das künftige Vorgehen der Aufsichtsbehörden besser einschätzen zu können. Teilweise tendieren die Papiere allerdings zu einer eher restriktiven Auslegung der einzelnen Bestimmungen.

Secorvo News

Für Kurzentschlossene

Noch wenige freie Plätze können wir für unser nächstes T.I.S.P.- (**16.–20.04.2018**) und das PKI-Seminar (**23.–26.04.2018**) anbieten. Programme, weitere Termine und Online-Anmeldung unter https://www.secorvo.de/seminare

Sesam, öffne Dich – nicht.

Dass der Betreiber der hausinternen IT gerne eigenständig kontrolliert, was in seinem Rechenzentrum vorgeht und wie die dortigen Betriebsbedingungen sind, ist bekannt. Doch um das Ziel einer möglichst hohen Verfügbarkeit zu erreichen, muss auch immer der Gefahrenfaktor Mensch betrachtet werden. Bei unserem kommenden KA-IT-Si-Event am **12.04.2018** werden Ihnen von Fabian Schäfer (Rittal) an Anwendungsbeispielen die technischen Einsatzmöglichkeiten automatisierter Zutrittskontrollsysteme im IT-Umfeld vorgestellt.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2018	
10.-11.04.	Datenschutztage 2018 (FFD Forum für Datenschutz, Wiesbaden)
19.-20.04.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
24.-26.04.	3rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, London/UK)
25.-27.04.	GI SICHERHEIT 2018 (Gesellschaft für Informatik e.V., Konstanz)
25.-26.04.	BvD Verbandstage 2018 (BvD e.V., Berlin)
29.04.-03.05.	Eurocrypt 2018 (IACR, Tel Aviv/ISR)
Mai 2018	
02.-03.05.	Security Forum 2018 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
07.-09.05.	11th International Conference on IT Security Incident Management & IT Forensics (GI, SIDAR, DFN-Cert, Hamburg)
15.-18.05.	European Identity & Cloud Conference 2018 (KuppingerCole Ltd., München)
16.-18.05.	19. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

April/Mai 2018



Der Spion, den ich liebe

Tim Berners-Lees Vision des World Wide Web war die eines freien Informationszugangs und der virtuellen Zusammenarbeit. Aber schon Mitte der 90er Jahre änderte sich der Charakter des WWW: Zwischen die Informationsquellen mischten sich die ersten Shops, die neben Besuchsdaten (IP-Adresse, Herkunft, Verweildauer) auch Kontaktdaten (Adresse, Kreditkartendaten oder die Bankverbindung) erfragten und Käuferprofile erstellten. Seither fordern immer mehr Dienste Daten, wie Sport-Coaches, Tourenplaner oder Gesundheitsberater. Dank Social Networks werden sie immer persönlicher: Fotos, Lebensläufe und Chatinhalte landen nun auch im Netz. Mit Smartphones wurden die Dienste mobil und werten jetzt auch Ortsinformationen aus, und inzwischen liefert das Internet of Things (IoT) Daten unserer smarten Fahrzeuge (Geschwindigkeit, Fahrverhalten) und smarten Homes (Kameraaufzeichnungen, Stromverbrauch, Steuerbefehle).

Was noch fehlte, war die Sprache. Nur auf den ersten Blick sind Alexa, Siri und Cortana lediglich eine Sprachsteuerung. Denn die Internet- und KI-basierten Sprachdienste funktionieren nur, wenn sie viel über uns wissen – unseren Geschmack, unsere Gewohnheiten und unseren Haushalt kennen. Und hemmungsbefreit beginnen wir, ihnen bereitwillig so viel wie möglich mitzuteilen: welche Musik wir präferieren, über welche Steckdose die Kaffeemaschine angeschaltet werden kann und wann wir das Haus verlassen oder betreten. Wir machen unsere Stimme, unsere Wünsche, unseren Tagesablauf, unsere Vorlieben, unseren Geschmack und sogar die Stimmen unserer Gäste zugänglich – weil wir möchten, dass Alexa & Co. verstehen, was wir wollen: Dass der Morgenkaffee fertig ist, wenn Alexa uns weckt und die Wohnung beleuchtet ist, wenn wir nach Hause kommen.

Und wenn sie das erste Mal das Badezimmer vorheizt, bevor wir selbst wissen, dass wir gleich ein Bad nehmen wollen, werden wir sie wirklich lieben.



Inhalt

Der Spion, den ich liebe

Security News

Netflix schnorren mit Gmail

Efail – HTMLfail?

Facebook-Nachlese

Hoteltüren-Crack

APT-Simulation

Simple DSGVO-Compliance

Secorvo News

ISO-zertifiziertes ISMS

Secorvo Seminare

10. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Netflix schnorren mit Gmail

Ein schönes Beispiel, wie durch die Kombination zweier unabhängiger Internet-Dienste eine neue Angriffsmöglichkeit entsteht, beschreibt James Fischer in seinem Blogeintrag vom 07.04.2018: Warum Punkte in E-Mail-Adressen wichtig sind ("dots do matter"). Hintergrund ist, dass Googles Gmail-Dienst die Punkte in E-Mail-Adressen nicht auswertet – james.hfisher@gmail.com wird also genauso behandelt wie jameshfisher@gmail.com. Eine Ergonomiefunktion.

Dies kann bei der Netflix-Registrierung ausgenutzt werden. Durch einen Rateangriff lässt sich feststellen, ob für eine Gmail-Adresse bereits ein Konto existiert. Da Netflix die Punkte in der E-Mail-Adresse auswertet, kann ein zweiter Netflix-Account zu einem existierenden angelegt werden, indem bei der E-Mail-Adresse die Punkte verwendet respektive weggelassen werden. Die E-Mail-Adresse wird nicht überprüft, eine weitere Ergonomiefunktion: Warum auch, schließlich ist die Nutzung für vier Wochen kostenfrei. Die E-Mail-Adresse wird nur zur Benachrichtigung z. B. über neue Serien verwendet.

Was passiert aber, wenn man für das künstlich geschaffene Zweitkonto eine Kreditkarte mit sehr kurzer Laufzeit hinterlegt? Dann wird jameshfisher@gmail.com benachrichtigt, seine Kreditkartendaten zu aktualisieren. Die Nachricht geht, Google-intern, an james.hfisher@gmail.com. Kommt von Netflix, ist original Netflix. Wenn James Fisher dann die Daten aktualisiert, bestehen auf einmal zwei Netflix-Konten – dass doppelt abgebucht wird, fällt frühestens bei der nächsten Abrechnung auf.

Stutzig wurde James Fischer nur, weil die zu aktualisierenden Kreditkartendaten überhaupt nicht zu seiner echten Kartennummer passten. Unser Tipp, wie im Straßenverkehr: Augen auf – und mit dem Fehlverhalten anderer rechnen. Auch wenn im konkreten Fall keine der Parteien wirklich etwas falsch gemacht hat, gehen Sie einfach nicht davon aus, dass sich ein Internet-Dienst so verhält, wie Sie das erwarten.

Efail – HTMLfail?

Als am 13.05.2018 die Entdecker der Efail-Angriffe und die EFF die ersten Hinweise und Warnungen veröffentlichten, war die Rede von Schwachstellen in der PGP- und S/MIME-Verschlüsselung. Wenn man jedoch auf die Website schaut, die ein Forschungsergebnis – ebenso wie ein mehr oder weniger eingängiges Logo – in der heutigen Aufmerksamkeitsökonomie offenbar braucht, dann sieht man schnell den eigentlichen Schuldigen an der Misere: HTML.

Was anfänglich eine Möglichkeit war, die ursprünglich spartanischen reinen Text-E-Mails ansprechender zu formatieren, zieht einen Rattenschwanz an Missbrauchsmöglichkeiten nach sich. Angefangen mit Aufrufen externer URLs, die Efail nutzt, um entschlüsselte E-Mail-Inhalte zu exfiltrieren, könnte das bis zur Echtzeit-Übertragung von Bildschirm-Inhalten oder Kamera-Bildern gehen, falls denn die HTML-„formatierten" Inhalte über einen WebRTC-fähigen Browser gerendert werden.

Mit PDF/A wurde eine Teilmenge von PDF standardisiert, die keine externen Referenzen oder aktiven Inhalte erlaubt und zur Darstellung der meisten üblichen Dokumente völlig ausreicht. Es wird Zeit, über ein vergleichbares statisches HTML/A-Format nachzudenken, das es ermöglicht, bspw. E-Mails wesentlich gefahrloser aufzuhübschen, als über unbeschränktes HTML mit allen zwischenzeitlich definierten Erweiterungen inklusive JavaScript. Auch oder gerade, wenn damit ein Tracking von Mail-Empfängern über Web-Bugs o. ä. ebenfalls nicht mehr möglich wäre.

Facebook-Nachlese

In seiner Anhörung vor dem US-Repräsentantenhaus hat Mark Zuckerberg, CEO von Facebook, am 11.04.2018 die weltweite Anwendung der im neuen europäischen Datenschutzrecht vorgesehenen Kontrollen angekündigt. Falls das kein Lippenbekenntnis bleibt, könnte dies ein wichtiger Schritt zu einer amerikanisch-europäischen Annäherung beim Datenschutzverständnis sein. Immerhin: Anders, als sein Statement aus dem Jahr 2010 vermuten lässt, Privatheit sei nicht länger eine „social norm", ist Zuckerberg zumindest um seine eigene Privatsphäre sehr besorgt: Im Jahr 2013 kaufte er die vier an sein Haus angrenzenden Grundstücke in Palo Alto – für 30 Mio. US$.

Während sich die Facebook-Aktie nach dem 18% Einbruch vom 17.03.2018 inzwischen wieder erholt hat, hat die Aufregung um die Nutzung der Daten von 87 Mio. Facebook-Nutzern für den britischen Datenanalysedienstleister Cambridge Analytica nun handfeste Konsequenzen: Am 02.05.2018 musste das Unternehmen Insolvenz anmelden. Offensichtlich gibt es eine große Diskrepanz zwischen den Erwartungen der Nutzer an den Umgang mit ihren Daten – und der tatsächlichen Rechtslage in Teilen der Welt.

Hoteltüren-Crack

Am 25.04.2018 veröffentlichten Tomi Tuominen und Timo Hirvonen, Mitarbeiter des finnischen Sicherheitsunternehmens F-Secure, dass es ihnen bereits 2017 gelungen ist, durch die Kombination mehrerer kleiner Schwachstellen den Master-Key für das Türschließsystem von Assa Abloy aus einer einzigen Schlüsselkarte abzuleiten. Inzwischen hat der schwedische Hersteller ein Update für das in mehr als 42.000 Hotels weltweit eingesetzte Schließsystem bereitgestellt – das allerdings manuell in jedes einzelne Schloss eingespielt werden muss.

Der Angriff ist ein Beispiel für die latente Gefahr, die in allen digitalen Zutrittssystemen lauert: Jede entdeckte Schwachstelle, die den Zutrittsschutz aushebelt, skaliert sofort, da sie alle bereits installierten Einheiten betrifft. Und da die Installation von Updates – anders als bei PCs oder Smartphones – weder üblich ist noch automatisiert erfolgt, ist eine erfolgreiche Ausnutzung einer solchen Lücke sogar sehr wahrscheinlich.

APT-Simulation

Am 30.04.2018 erweiterte MITRE sein vor ziemlich genau einem Jahr veröffentlichtes ATT&CK-Framework über auftretende Angriffsklassen, -typen und -techniken von 188 auf 219 Angriffstypen, verständlich gruppiert in einer technischen Angriffs-Matrix. Nicht erst seitdem fragen sich viele CISOs, ob ihr Netzwerk nicht bereits Opfer eines Advanced Persistent Threat-Angriffs geworden ist.

Mit dem APT Simulator von Florian Roth, der seit dem 09.04.2018 in einer stabilen Version 0.80 verfügbar ist, kann das eigene Red Team die Erkennung von APT-Angriffen trainieren: Damit lassen sich Windows-Enterprise-Clients per *.bat-Script mit derzeit bis zu 25 Testfällen aus den Bereichen Antivirus, Network Intrusion Detection, Endpoint Detection, Security Monitoring und Compromise konfrontieren – und jede zweite Kalenderwoche einen vermeintlichen Incident simulieren. Noch vielversprechender ist die Möglichkeit, auch eigene Testfälle zu ergänzen.

Simple DSGVO-Compliance

Für alle, bei denen Weihnachten jedes Jahr ganz überraschend kommt und der Datenschutz erst seit der DSGVO (General Data Protection Regulation, GDPR) ein Thema ist, gibt es eigenwillige Angebote wie https://gdpr-shield.io.

Falls die Seite wegen Überlastung nicht erreichbar sein sollte, kann man dem Suchmaschinen-Cache die Zielsetzung entnehmen: „Making your website GDPR compliant can take thousands in legal fees ...“. Die Idee des Angebotes: Man sperre EU-Besucher von den eigenen Webseiten aus – was wäre auch einfacher? Geo-IP-Filterung als Compliance-Maßnahme...

Secorvo News

ISO-zertifiziertes ISMS

Anfang 2017 hat das Kirchliche Rechenzentrum Südwestdeutschland (KRZ-SWD), einer der führenden IT-Dienstleister für Kirche, Diakonie und Caritas begonnen, sich mit dem Information Security Management System ISMS ready2go von Secorvo auf eine ISO 27001-Zertifizierung vorzubereiten.

Mit dem Auditbericht vom 02.05.2018 wurde dem Rechenzentrum nun nach wenig mehr als einem Jahr Vorbereitung die Erfüllung der Anforderungen der ISO 27001 bestätigt – ohne eine einzige Abweichung: der „Proof of Concept“, dass ein ISMS „out of the box“ den Weg zum Zertifikat erheblich beschleunigen kann. Wir gratulieren herzlich und bedanken uns für die hervorragende Zusammenarbeit!

Secorvo Seminare

Vor der Sommerpause bieten wir Ihnen noch einmal die Möglichkeit, sich Ihre Kenntnisse und Erfahrungen in der IT-Sicherheit mit einem T.I.S.P.-Zertifikat bestätigen zu lassen: Das T.I.S.P.-Seminar findet statt vom **11. bis 15.06.2018**. Wir freuen uns auf Ihre Anmeldung.

10. Tag der IT-Sicherheit

Auf dem diesjährigen zehnten Karlsruher „Tag der IT-Sicherheit“, einer Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe und dem CyberForum e. V., werden aktuelle Herausforderungen der IT-Sicherheit für Unternehmen diskutiert und Präventionsmöglichkeiten vorgestellt. Als Keynote-Speaker konnten wir in diesem Jahr Stefan Krebs gewinnen, den CIO Baden-Württemberg, Beauftragter der Landesregierung für Informationstechnologie. Er verfügt über vieljährige Erfahrung im IT-Sicherheitsbereich, im Bankensektor und der Verwaltung.

Die Veranstaltung findet am **07.06.2018** im Saal Baden der IHK Karlsruhe statt. Das Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2018	
07.06.	10. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
11.-12.06.	DuD 2018 (COMPUTAS, Berlin)
11.-15.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
13.-14.06.	Annual Privacy Forum 2018 (ENISA, EC DG Connecct, Universität Wien, Barcelona/ES)
15.-16.06.	AREA41 Security Conference (DC4131 DEFCON Switzerland, Zürich/CH)
17.-21.06.	OWASP AppSec EU 2018 (OWASP Foundation, Tel Aviv/ISR)
20.-22.06.	Entwicklertag 2018 (VKSI, GI, ObjektForum, Karlsruhe)
26.-27.06.	EssoS 2018 (EssoS Organization, Paris/FR)
Juli 2018	
24.-27.07.	PETS 2018 (University of Minnesota, Barcelona/ES)

Fundsache

Unter dem Titel „Human Rights under Surveillance“ veröffentlichte Amnesty International einen spannenden und betroffen machenden Bericht über IT-Angriffe auf Menschenrechts-Aktivisten in Pakistan. Langfristig geplante Attacken, unter anderem über Spearfishing-E-Mails und gefakte Social-Media Seiten sowie gefakte Personen, werden im Detail beschrieben. Lesenswert.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2018



Panik 4.0

Unter Panik verstehen wir eine durch eine plötzliche, echte oder vermeintliche Gefahr hervorgerufene, übermächtige Angst, die zu unüberlegten Reaktionen führt. Sie kann sich zur kollektiven oder Massenpanik entwickeln, wenn in „eng stehenden Gruppen“ Menschen ihre Handlungen gegenseitig beobachten und darauf reagieren – und dabei ihre Selbstkontrolle verlieren.

In Zeiten allgegenwärtiger Digitalisierung kann auch Panik digital werden: Verursacht im digitalen Kontext und verstärkt durch die Verbreitung über verzugsfreie digitale Kommunikationsmedien wie Instant Messaging oder Social Networks entsteht so schnell eine Massenpanik 4.0. Dabei zeigen sich die fatalen Folgen des zunehmenden Fast-Food-Gebarens bei der Erzeugung und Verbreitung von Informationen: Publizierte Nachrichten sind immer nachlässiger recherchiert und werden allerorten ungeprüft kopiert – die Empfänger haben sich bereits so daran gewöhnt, dass sie den Wahrheitsgehalt nicht mehr aus der Seriosität einer Quelle (gibt es das noch?) sondern aus der Anzahl der Nachrichten ähnlichen Inhalts ableiten.

Erleben konnte man das in den vergangenen Wochen im Zusammenhang mit dem Inkrafttreten der DS-GVO. Bestenfalls halbrichtige Darstellungen der Anforderungen in den Medien ließen den Verdacht aufkeimen, es kämen völlig neue Herausforderungen auf Unternehmen, Vereine und Verbände zu – und es sei mit Ordnungsgeldern in Höhe von 4% des Jahresumsatzes zu rechnen.

Zu den Panik-Reaktionen auf dieses Halbwissen zählen E-Mails von Vereinen, die eine Einwilligung der Mitglieder für die erforderliche Verarbeitung personenbezogener Mitgliederdaten erbitten, Kühlschränke mit Datenschutzerklärung oder Tageszeitungen, die den Webauftritt abschalten. Blenden wir den volkswirtschaftlichen Schaden aus, so bleibt ein sehr bitterer Nachgeschmack: Dem Schutz unserer Persönlichkeitsrechte hat das mehr geschadet als genutzt.



Inhalt

Panik 4.0

Security News

Alte Zöpfe

Stand der Technik

Unter der Gürtellinie

Gezahnter Papiertiger

Bulk-Forensik

Secorvo News

Teamverstärkung

Secorvo@itsa

Secorvo Seminare

Freiwild im Cyberspace

Veranstaltungshinweise

secorvo
security consulting

Security News

Alte Zöpfe

Nachdem sich seit März 2018 Version 1.3 des Protokolls Transport Layer Security (TLS) in den letzten Zügen der Standardisierung befindet, gibt es zunehmend Bestrebungen, alte Zöpfe abzuschneiden. Gemeint sind insbesondere die Protokollversionen TLS 1.0 (1999) und 1.1 (2006). Die alten Protokollversionen weisen kryptografische Schwächen auf und sind im Vergleich mit TLS 1.2 und 1.3 nicht mehr zeitgemäß. Diese Erkenntnis ist auch im Standard PCI DSS angekommen: Ab dem 01.07.2018 sind TLS 1.0 und 1.1 nicht mehr erlaubt.

In den meisten Fällen sollte eine Deaktivierung der alten Versionen keine merkbaren Folgen nach sich ziehen: TLS 1.2 ist bereits seit 10 Jahren standardisiert und wird dementsprechend auch von allen gängigen Browsern und Bibliotheken unterstützt. Diverse aktuelle Browser unterstützen übrigens bereits TLS 1.3. – sind Sie schon dabei?

Stand der Technik

Am 14.06.2018 veröffentlichte TeleTrusT die deutlich überarbeitete Fassung der „TeleTrusT-Handreichung zum Stand der Technik“ nach IT-Sicherheitsgesetz und DSGVO. Die Erstfassung von 2016 wurde um Erklärungen zur Bestimmung des Technologiestandes und um eine Methode zur Bewertung der Maßnahmen ergänzt. Die Beiträge wurden gründlich überprüft und ggf. gestrichen oder überarbeitet. Eine Bewertung soll transparent machen, warum Maßnahmen aufgrund von „Grad der Anerkennung“ und „Grad der Bewährung in der Praxis“ als Stand der Technik aufgeführt sind. Zusätzlich wurden die Struktur verbessert und neue Maßnahmen und Prozesse ergänzt.

Ein weiterer schöner Meilenstein für die Pioniere der IT-Sicherheit und eine hilfreiche Grundlage zur Positionsbestimmung, wenn es um die Konzeption von Maßnahmen und Prozessen geht.

Unter der Gürtellinie

Traditionell setzten viele Bedrohungsanalysen und Sicherheitskonzepte auf der Ebene des Betriebssystems an. Durch zunehmende Virtualisierung kommt u. U. noch ein unterliegendes Hypervisor-System mit ins Bild. Seit ein paar Monaten gerät nun die Sicherheit unterhalb der Betriebssystem-Ebene zusehends ins Blickfeld: Seit der Entdeckung der Spectre- und Meltdown-Schwachstellen finden Forscher immer neue Varianten, um Informationen über Prozessgrenzen hinweg auszuspähen. So veröffentlichte OpenBSD am 05.06.2018 einen Patch gegen eine Prozessor-Schwachstelle – das zugehörige Advisory wurde von Intel erst am 13.06.2018 veröffentlicht.

Und auch auf der proaktiven Seite gibt es Aktivitäten: Microsoft hat – experimentell und unabhängig von Schwachstellen durch spekulative Ausführung von Befehlen – bereits Windows 10 auf eine Prozessor-Architektur portiert, bei der der Compiler die optimierte Abarbeitungsfolge vorgibt. Und am 18.06.2018 veröffentlichten Forscher einen Vorschlag für eine „Leak“-freie spekulative Ausführung.

Derweil holen uns wieder totgehoffte Altlasten ein: So wurde am 19.06.2018 gemeldet, dass sich die Anmeldung an HPs iLO4 Management-System mittels eines simplen Pufferüberlaufs übertölpeln lässt.

Wer heute neue Sicherheitskonzepte erstellt, tut gut daher daran, in die Bedrohungsanalyse auch die relevanten Ebenen unterhalb des Betriebssystems einzubeziehen.

Gezahnter Papiertiger

„Lieber offline als abgemahnt“, „Was Ihr Chef jetzt verbieten kann“ oder „Selbst Anwälte sind ratlos über die neuen Datenschutzregeln“ sind nur einige der Headlines, welche dieser Tage in den Medien zum Thema Datenschutz gestreut werden. Nach Ablauf der zweijährigen Übergangsfrist gelten seit dem 25.05.2018 die Vorgaben der Datenschutz-Grundverordnung (DS-GVO). Den Aufsichtsbehörden wird nun eine wesentlich höhere Bedeutung zugemessen als bisher. Wer sich nicht datenschutzkonform verhält, riskiert Bußgelder bis zu 20 Mio. € oder 4% des weltweit erzielten Jahresumsatzes. Zahlen, die mittlerweile durch die Medien Omnipräsenz erlangt haben und einen Großteil der Angst und Unsicherheit verantworten, die sich in den letzten Monaten ausgebreitet haben.

Seit Inkrafttreten des Gesetzes ist nun ein Monat vergangen. Haben die Unternehmen nun überreagiert, oder wurden sie gerechtfertigt dazu gedrängt, in hektische Tätigkeit zu verfallen, um DS-GVO-konform zu werden? Sicher ist: Vieles, was bereits im nun von der DS-GVO verdrängten Bundesdatenschutzgesetz (BDSG) gefordert wurde, behält seine Gültigkeit. Und angesichts der Übergangsfrist von zwei Jahren hatten Unternehmen ausreichend Zeit, sich auf die neuen Anforderungen vorzubereiten.

Die Verantwortung sollte jedoch nicht allein den betroffenen Unternehmen zugeschoben werden. Denn es bestehen gerechtfertigt Unsicherheiten, die aufgrund dehnbarer DS-GVO-Bestimmungen

noch ausgelegt und geklärt werden müssen. Nicht zuletzt auch aufgrund der noch im Entwurfsstadium befindlichen E-Privacy-Verordnung für den Bereich der elektronischen Kommunikation, deren „go live" nicht vor 2019 zu erwarten ist, und von welcher erwartet wird, dass sie konkretisierende und ergänzende Anforderungen zu den Vorgaben der DS-GVO formuliert.

Doch was bedeutet diese aktuelle Rechtslage für Unternehmen konkret: Soll man sich von dem aktuellen Hype mitreißen lassen? Ist mit einem Abflachen des Datenschutz-Aktivismus zu rechnen, sobald sich die Unruhe etwas gelegt hat?

Tatsächlich wäre es ratsam, sich auf die (Weiter-) Entwicklung des Grundgerüsts der Datenschutz-Organisation und deren Implementierung zu konzentrieren. Denn mit entsprechender Dokumentation der Prozesse und kontinuierlicher Verbesserung ist nicht nur ein nachhaltigerer Datenschutz-Reifegrad zu erreichen – es ist auch der beste Schutz vor behördlichen Maßnahmen.

Bulk-Forensik

Lange Zeit war es recht still um die Weiterentwicklung des forensischen Carving-Werkzeuges bulk_extractor. Dies hat sich aber am 30.12.2017 geändert: Die hilfreiche Scanner-Komponente „scan_ntfsusn" wurde integriert, mit der USN-Journal-Metainformationen (Zeitstempel und Schreibtransaktionen für Dateien und Verzeichnisse) in einem NTFS-Dateisystem von Windows parallel ausgewertet werden können.

Da bulk_extractor tatsächlich jeden CPU-Core und Thread nutzt, kann mit Nutzung von scan_ntfsusn ein erheblicher Zeitgewinn bei der vollautomatischen Datenaufbereitung erzielt werden. Dazu kommt seit 28.01.2018 eine Weiterentwicklung namens bulk_extractor-rec, die nicht der offiziellen Entwicklung folgt, aber dafür aus den verschiedenen internen NTFS-Logdaten noch die Record-Typen INDX, RSTR/RCRD und FILE durch zusätzliche Scanner-Komponenten extrahiert. Wer also schnell Informationen braucht und nicht auf Plaso warten möchte, den werden diese Funktionen freuen.

Secorvo News

Teamverstärkung

Dank der zunehmenden Nachfrage nach Unterstützung benötigt auch Secorvo personelle Verstärkung. Und wir freuen uns, in den vergangenen Wochen mit Michael Knöppler und Thomas Maus zwei sehr kompetente IT-Sicherheitsexperten für unser Team gewonnen zu haben.

Secorvo@itsa

In diesem Jahr werden wir vom 09. bis 11.10.2018 auf der IT-Security-Messe it-sa in Nürnberg vertreten sein und dort am Stand 10.1-628 unsere Datenschutz- (DSMSready2go) und Informationssicherheits-Management-Lösungen (ISMSready2go) zeigen. Sie sind herzlich eingeladen, bei Interesse vorab einen Termin mit uns zu vereinbaren.

Secorvo Seminare

Nach der Sommerpause startet die Herbst-Seminarserie von Secorvo im Oktober mit den beiden Zertifizierungsseminaren T.I.S.P. (15.-19.10.2018) und T.P.S.S.E. (12.-15.11.2018). Wir freuen uns auf Ihre Teilnahme – und empfehlen für das T.I.S.P.-Seminar eine frühzeitige Anmeldung.

Programm und Online-Anmeldung unter https://www.secorvo.de/seminare

Freiwild im Cyberspace

Die Anforderungen an die Mobilität von Arbeitnehmern steigen beständig - unterstützt von immer kleineren und leistungsfähigeren Endgeräten. Wie aber lässt sich diese Flexibilität mit Sicherheitsanforderungen vereinbaren? Bei unserem kommenden KA-IT-Si-Event am **12.07.2018** stellt Dirk Fox (Secorvo) in seinem Vortrag wichtige Anforderungen und technische Möglichkeiten für sicheres mobiles Arbeiten vor. Anschließend geht Holger Bajak (ophelis) in seinem Vortrag "Mobil und vernetzt" auf das Arbeiten in neuen Strukturen ein. Arbeiten ist im digitalen Zeitalter überall und jederzeit möglich. Das Büro gewinnt dadurch eine neue Bedeutung: Es ist weit mehr als ein Arbeitsraum. Das Büro wird zum Treffpunkt, dient dem Austausch und der Zusammenarbeit. Es erzeugt Zugehörigkeit und bietet den Mitarbeitern Heimat.

Die Veranstaltung findet in Kooperation mit feco-feederle und ophelis statt. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2018	
12.07.	Freiwild im Cyberspace (KA-IT-Si Karlsruhe)
24.-27.07.	PETS 2018 (University of Minnesota, Barcelona/ES)
August 2018	
04.-09.08.	Blackhat USA 2018 (Blackhat, Las Vegas/US)
09.-12.08.	DEF CON 26 (DEFCON, Las Vegas/US)
14.08.	SOUPS 2018 (usenix, Baltimore/US)
15.-17.08.	27th USENIX Security Symposium (usenix, Baltimore/US)
15.-18.08.	DFRWS USA 2018 (DFRWS, Providence/US)
19.-23.08.	Crypto 2018 (IACR, Santa Barbara/US)
September 2018	
04.-05.09.	D • A • CH Security (GI, OCG, TeleTrusT, Gelsenkirchen)
10.09.	Sommerakademie 2018: Beschäftigtendatenschutz im digitalen Zeitalter (ULD, Kiel)
24.09.	Datenschutztag 2018 (COMPUTAS Gisela Geuhs GmbH, Köln)
28.-30.09.	FIfFKon 2018 (FIfF e.V., Berlin)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Hans-Joachim Knobloch, Sarah Niederer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2018



Falsche Baustelle

Seit Jahren geistert das Bild der E-Mail als „Postkarte“ unausrottbar durch Gazetten und Datenschutzempfehlungen: Wer E-Mails unverschlüsselt versende, der müsse damit rechnen, dass sie mitgelesen werden. Tatsächlich übermitteln Mailserver die ihnen anvertrauten Nachrichten heute meist wirksam verschlüsselt: Als Reaktion auf Edward Snowdens Veröffentlichungen stellten 2014 im Projekt „E-Mail made in Germany“ mehrere Provider und immer mehr Unternehmen ihre Mailserver auf eine TLS-Verbindungsverschlüsselung um, und Zugriffe auf das Postfach werden sowohl von Web-Clients als auch unternehmensintern schon längst verschlüsselt. Ein Mitlesen von E-Mails erfordert daher heute einen erfolgreichen DNS-Angriff – oder den direkten Zugriff auf die Postfächer.

Genau dort lauert in Wirklichkeit die reale Bedrohung: Amerikanische Anbieter kostenloser E-Mail-Dienste wie insbesondere GMail geben Drittfirmen, die Apps mit E-Mail-Anbindung realisieren, großzügig den Zugriff auf Kundenpostfächer frei, sofern diese dafür eine Zustimmung der Benutzer einholen. Und dann wird, automatisiert oder manuell, die persönliche Nachrichtenablage durchwühlt – z. B. um Spam-Diensten die Optimierung der Empfängeransprache zu ermöglichen (wie Return Path), passende Werbung zu generieren oder Testdaten für die Verbesserung der eigenen App zu gewinnen. Immerhin: Wer wissen will, welchen Apps er bereits Zugriff auf sein GMail-Konto eingeräumt hat, kann dies in den Privacy-Einstellungen seines Google-Accounts nachprüfen.

Dass es so etwas wie ein Fernmeldegeheimnis gibt und persönliche Kommunikationsinhalte nicht in Testumgebungen gehören hat sich offenbar noch nicht bei allen Anbietern herumgesprochen. Und für Anwender ist es noch immer nicht selbstverständlich, dass man Datenschutzerklärungen von Apps sehr genau lesen sollte, bevor man ihnen zustimmt – allen Datenschutzskandalen zum Trotz.



Inhalt

Falsche Baustelle

Security News

WPA ... zum Dritten

1:0 für 802.11 vs. Bluetooth SIG

Framing 4.0

1000 x T.I.S.P.

Löschkonzept goes ISO

Informationspflicht

Facebook unter Druck

Secorvo News

Weiterbildung

Digitale Mülltrennung

Secorvo@itsa

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

WPA ... zum Dritten

Nicht nur das TLS-Protokoll (SSN 06/2018), sondern auch das als WPA2 bekannte und ebenfalls in die Jahre gekommene Sicherheitsverfahren hat ein Facelifting erhalten: Die WiFi Alliance veröffentlichte am 09.04.2018 eine Zusammenfassung der neueren Sicherheitsmechanismen, die in 802.11s, 11w bzw. 11ac standardisiert wurden, unter der Bezeichnung WPA3:

- das Passwort-basierte Schlüsselaustauschverfahren SAE, das Sicherheit gegen Offline-Wörterbuchattacken auf das WLAN-Passwort verspricht,
- die Absicherung von Management-Frames, wie bspw. Deauthentication, die Angreifer zum Abmelden einer angegriffenen Station missbrauchen konnten und
- die durchgängige Nutzung von Kryptoalgorithmen, die einer 192-bit-Stärke nach aktuellen US-Behördenstandards entsprechen.

Dass dabei recht sorgfältig gearbeitet wurde, zeigt sich u. a. daran, dass nicht nur die Stärke der WLAN-Verschlüsselung selbst, sondern auch die TLS Cipher Suites festgelegt wurden, die bei einer vorangegangenen EAP-Authentifikation zum Einsatz kommen dürfen.

1:0 für 802.11 vs. Bluetooth SIG

Ordentlich implementierte WPA3-Produkte sollten auch gegen die Schwachstelle vieler Bluetooth-Implementierungen gefeit sein, die am 24.07.2018 publiziert wurde – die Bluetooth SIG hingegen muss ihre Spezifikation um einen Schritt zur Prüfung der übergebenen Elliptische-Kurven-Punkte nachbessern, um von Angreifern konstruierte Punkte zuverlässig zu verwerfen. Für SAE ist eine solche Prüfung bereits in Abschnitt 12.4.5.4 von IEEE 802.11-2016 beschrieben – siehe Seite 1942.

Framing 4.0

Bisher waren für einen kritischen, mit den Möglichkeiten der Bildmanipulation und Bildsynthese vertrauten Beobachter Fälschungen durch Video-Rewriting meist mit bloßem Auge erkennbar. Diese Zeiten sind nun allerdings vorbei: Am 29.05.2018 wurde von einer Forschergruppe um das Max-Planck-Institut für Informatik ein Verfahren veröffentlicht, welches dreidimensionale Kopfmodelle erstellt und die Qualität der Fälschung durch einen KI-Gegenspieler prüfen lässt.

Ob die von den Autoren der Studie in den Vordergrund gestellte Lippenkorrektur bei synchronisierten Filmen zukünftig der bevorzugte Anwendungsfall sein wird, darf bezweifelt werden – Fake News und Fake Porn erscheinen da viel wahrscheinlicher. Auch der Aufwand wird eine breite Anwendung kaum verhindern: Diese Hoffnung war schon vor 35 Jahren trügerisch, als erste Warnungen vor digitaler Foto-Fälschung ausgesprochen wurden. Hardware für rund 2.000 € und eine Rechenzeit von einigen Stunden bis wenigen Tagen sind bereits heute kein unüberwindliches Hindernis.

1000 x T.I.S.P.

Das deutsche Schwergewicht der Personenzertifizierung für Informationssicherheit T.I.S.P. (TeleTrusT Information Security Professional) wurde am 10.04.2018 zum 1.000sten Mal verliehen – an Herrn Kai Riecke, CTO der Hubert Burda Media Holding.

Prof. Dr. Norbert Pohlmann, Vorstand von TeleTrusT, äußert sich stolz: „Der T.I.S.P. hat eine Anerkennung erreicht, die den Vergleich mit ähnlichen Personen-Zertifikaten im deutschsprachigen Raum nicht scheuen muss."

Mit der erfolgreich abgelegten Prüfung zum T.I.S.P. belegt ein IT-Sicherheits-Spezialist seine umfassenden Kenntnisse im IT-Sicherheitsumfeld auf technischem, rechtlichem und strategischem Gebiet. Das Zertifizierungsprogramm umfasst eine fünftägige Schulung, an die sich eine intensive Prüfung anschließt. Die Schulungsanbieter Secorvo, isits und Fraunhofer SIT freuen sich bereits auf die Ausstellung von Zertifikat Nr. 2.500...

Löschkonzept goes ISO

Die englische Fassung der von den Unternehmen Deutsche Bahn, Blancco, DATEV, Secorvo und Toll Collect geförderten „Leitlinie Löschkonzept", die am 08.04.2016 als DIN 66398 verabschiedet worden ist (siehe SSN 4/2016), wurde jetzt bei der ISO als Grundlage eines internationalen Standards eingereicht.

Nach den bisherigen Rückmeldungen wird sich an der darin beschriebenen Vorgehensweise nichts ändern. Anpassungen sind notwendig, weil die Beispiele in der Norm noch auf das alte BDSG und nicht auf die DSGVO oder andere internationale Vorschriften abstellen und einige Begriffe an die ISO-Terminologie angepasst werden sollen.

Das Standardisierungsprojekt soll in den kommenden Wochen vom zuständigen Gremium beschlossen werden. Ein ISO-Standard könnte dann Ende 2021 verabschiedet werden und die in Deutschland bereits genormte Vorgehensweise für Löschkonzepte sich auch international durchsetzen.

Informationspflicht

Nach der Datenschutz-Grundverordnung (DSGVO) entsteht zum Zeitpunkt der Erhebung personenbezogener Daten eine Informationspflicht des verantwortlichen Datenverarbeiters gegenüber dem Betroffenen (Art. 13 DSGVO). Dabei können sich in der praktischen Umsetzung zahlreiche Problemfälle ergeben:

- das Unternehmen erhält spontan zugesandte Informationen (z. B. eine Initiativbewerbung),
- es laufen Hintergrundprozesse ab (wie eine automatisierte Erhebung z. B. bei Bonitätsprüfungen),
- es sind gar keine Interaktionen vorgesehen oder
- ein Dienstleister erhebt die Informationen.

Meist liegt die Hauptschwierigkeit darin, einen geeigneten Kommunikationskanal zu finden, der den Betroffenen erreicht und die Anforderungen der DSGVO erfüllt – auch in Bezug auf den Inhalt der Information: So lassen sich komplexe Verarbeitungen oft nicht ohne weiteres in zugleich präziser, transparenter, verständlicher und leicht zugänglicher Form darstellen.

Bleibt zu hoffen, dass die Aufsichtsbehörden eine pragmatische Auslegung dieser Anforderungen vornehmen, die noch etwas einfacher ausfällt als die derzeitigen Vorschläge zur Ausweisung der Videoüberwachung. Denn es wird immer wieder Fälle geben, in denen die Daten verarbeitende Stelle ihren Informationspflichten entweder nicht unmittelbar oder nicht zugleich präzise und verständlich nachkommen kann.

Facebook unter Druck

Nachdem der Europäische Gerichtshof in seinem Urteil vom 05.06.2018 die grundsätzlich gemeinsame Verantwortlichkeit für die Verarbeitung der Nutzerdaten von Unternehmensauftritten bei Facebook („Fanpages“) geklärt hat, haben auch die deutschen Datenschutzaufsichtsbehörden erste Stellungnahmen abgegeben.

Die Pflichten gemeinsam Verantwortlicher regelt die DSGVO in Art. 26. Danach müssen die Zuständigkeiten insbesondere bezüglich der Betroffenenrechte und Informationspflichten in einer transparenten Vereinbarung festgelegt werden. Dementsprechend fordern die Aufsichtsbehörden, dass dem Fanpage-Besucher diese Informationen beim Besuch zugänglich gemacht werden müssen. Für das Tracking soll Facebook grundsätzlich eine Einwilligung einholen; die Seitenbetreiber müssen sich vergewissern, dass Facebook die Pflichten erfüllt.

Bislang hat Facebook den Seitenbetreibern keine entsprechende Vereinbarung zur Verfügung gestellt. Für Seitenbetreiber ist damit auch nach dem Urteil unklar, womit sie zu rechnen haben und in wieweit sie derzeit ihre Pflichten bezüglich der Informationspflichten auf der Fanpage erfüllen.

Secorvo News

Weiterbildung

Schon im Sommer an den Herbst denken: Im Oktober starten wir unsere Seminarserie mit den beiden Zertifizierungsseminaren T.I.S.P. (**15.–19.10.2018**) und T.P.S.S.E. (**12.–15.11.2018**). Wir freuen uns, sie in unserem frisch renovierten Seminarbereich begrüßen zu dürfen – und empfehlen für das T.I.S.P.-Seminar eine baldige Anmeldung, da uns schon zahlreiche Anmeldungen vorliegen.

Programm und Online-Anmeldung unter https://www.secorvo.de/seminare

Digitale Mülltrennung

Die DSGVO fordert das Löschen personenbezogener Daten. Wie aber organisiert man diese Aufgabe für eine Organisation effizient und systematisch? Die DIN 66398 „Leitlinie Löschkonzept“, an deren Entwicklung Secorvo maßgeblich beteiligt war, gibt zahlreiche Hilfestellungen dafür.

Dr. Volker Hammer (Secorvo) war Editor der Norm und gibt beim kommenden **KA-IT-Si-Event** am **13.09.2018** im Panoramasaal der IHK Karlsruhe einen Überblick über die Inhalte aus erster Hand (Beginn: 18 Uhr). Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (zur Anmeldung).

Secorvo@itsa

In diesem Jahr werden wir vom 09. bis 11.10.2018 auf der IT-Security-Messe it-sa in Nürnberg vertreten sein und dort am Stand 10.1-628 unsere Datenschutz- (DSMSready2go) und Informationssicherheits-Management-Lösungen (ISMSready2go) zeigen. Sie sind herzlich eingeladen, bei Interesse vorab einen Termin mit uns zu vereinbaren.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2018	
04.-09.08.	Blackhat USA 2018 (Blackhat, Las Vegas/US)
09.-12.08.	DEF CON 26 (DEFCON, Las Vegas/US)
14.08.	SOUPS 2018 (usenix, Baltimore/US)
15.-17.08.	27th USENIX Security Symposium (usenix, Baltimore/US)
15.-18.08.	DFRWS USA 2018 (DFRWS, Providence/US)
19.-23.08.	Crypto 2018 (IACR, Santa Barbara/US)
September 2018	
04.-05.09.	D • A • CH Security (GI, OCG, TeleTrusT, Gelsenkirchen)
10.09.	Sommerakademie 2018: Beschäftigtendatenschutz im digitalen Zeitalter (ULD, Kiel)
13.09.	Digitale Mülltrennung (KA-IT-Si, Karlsruhe)
Oktober 2018	
01.-03.10.	ISSE 2018 (EEMA, Rom/IT)
08.-12.10.	OWASP AppSec USA 2018 (OWASP Foundation, San Jose/US)

Fundsache

Studien zur IT-Sicherheit gibt es viele – aber nur wenige liefern statistisch belastbare Aussagen und sind deutlich mehr als eine willkürliche Befragung zufällig ausgewählter Unternehmen. Daher hebt sich die wik-Studie „Aktuelle Lage der IT-Sicherheit in KMU“ vom 18.05.2018 erfreulich vom sonstigen Einerlei der Kaffeesatzerkenntnisse ab.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Dr. Volker Hammer, Hans-Joachim Knobloch, Michael Knopp, Thomas Maus, Sarah Niederer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, 76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

August 2018



Früher war die Realität besser

Realität kommt aus der Mode. War sie in der Aufklärung der Prüfstein und das Bindeglied der gemeinsamen Welterkenntnis – ein objektiv von jedermann beobachtbarer und per reproduzierbarem Experiment befragbarer Bezugsrahmen – so genügt sie heute nicht mehr: „Augmented Reality", „Virtual Reality" und „Fake-News" erheben – in unterschiedlichen Graden der Transparenz – die Illusion über die Realität.

Die technisch vermittelte Realitätswahrnehmung steht jedoch an vielen Fronten unter Beschuss: Fotofälschungen sind ein alter Hut, signifikante Fortschritte in der Videofälschung (SSN 7/2018) erschweren deren Erkennung, gefälschte Stimmen und andere biometrische Merkmale täuschen erfolgreich biometrische Sensoren.

Der Glaube an die unbewiesenen Versprechungen der Technik ist regelmäßig weit verbreitet, das Vertrauen in fundierte Warnungen (selbst der Techniker) hingegen oft gering - bis an die Grenzen der Realitätsverweigerung, siehe schon Joseph Weizenbaums Eliza.

Technik bändigt die Komplexität der Welt in vereinfachenden, aber selbst immer komplexeren Modellen. Das kann dazu führen, dass die Technik der Realität nicht mehr glaubt – zum Beispiel wenn selbstfahrende Autos immer anhalten, solange ein Stoppschild in der Karte verzeichnet ist. Selbst wenn jemand das Schild abmontiert. Wie kalkulierbar das für andere Verkehrsteilnehmer ist und wie rücksichtsvoll das autonome Fahrzeug auf dieses fehlende Verkehrsschild reagiert, ist eine offene Frage, ebenso wie die Aktualität und Akkuratesse der Karte, die Reaktion auf rechtmäßig entfernte Vorfahrtsschilder, Aufhebungszeichen und viele, viele weitere Szenarien.

Über eines aber sollten wir uns im Klaren sein: Die Realität kann Illusionen länger ignorieren als umgekehrt. Wenn sich der helle Himmel des Modells als die weiße Plane eines LKWs entpuppt, hat die Realität das letzte Wort. Hybris.



Inhalt

Früher war die Realität besser

Security News

WPA2-Schwachstelle

Sennheisers Root-Zertifikat

Grundschutz runderneuert

Fax-Angriff

Biometriekritik

Staatstrojaner

Secorvo News

Teamverstärkung

Secorvo@it-sa

Seminare

Geburtstag

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

WPA2-Schwachstelle

Am 04.08.2018 wurde im hashcat-Forum unter dem Pseudonym atom ein neuartiger Angriff auf WLAN-Netzwerke vorgestellt, die mit WPA-PSK und WPA2-PSK gesichert sind. Bisher mussten Angreifer einen Vier-Wege-Handshake eines Clients abwarten, diesen aufzeichnen und im Anschluss eine Wörterbuchattacke über den gesamten Handshake ausführen.

Einige Router-Hersteller integrieren jedoch gleich im ersten Paket einen SHA1-Hash über Informationen, die auch einem Angreifer bekannt sind. Der Schlüssel, der zur Bildung des Hash verwendet wird, ist in diesem Fall der Pre-Shared-Key. Da der zu brechende Hash deutlich kürzer ist als ein Vier-Wege-Handshake benötigt die Wörterbuchattacke deutlich weniger Zeit.

Der vor kurzem verabschiedete WLAN-Standard WPA3 (SSN 07/2018) ist nicht von diesem Angriff betroffen und sollte daher möglichst bald eingesetzt werden – auch unter dem Gesichtspunkt, dass alte WLAN-Standards auch weiterhin von Sicherheitsforschern unter die Lupe genommen werden und daher das Bekanntwerden weiterer Schwächen nicht auszuschließen ist.

Sennheisers Root-Zertifikat

Sennheiser Communications sorgte in diesem August bei manchen Anwendern der Software HeadSetup, die die Schnittstelle zwischen einem Sennheiser-Headset und dem Softphone bildet, für Unbehagen: Wird die Software installiert, so bringt diese huckepack ein vom Hersteller selbstsigniertes Root-Zertifikat mit, welches unbemerkt im Windows-Zertifikatspeicher als vertrauenswürdige Stammzertifizierungsstelle installiert wird. Damit nicht genug: Das Zertifikat trägt den „vertrauenswürdigen" Common Name 127.0.0.1. Der Aussteller des Zertifikats (oder ein Angreifer, der den zugehörigen Private Key erbeutet) kann damit Man-in-the-Middle-Angriffe auf mit TLS gesicherte Verbindungen beteiligter Systeme durchführen.

Dabei ist der Zweck des CA-Zertifikats unklar: Wir konnten keine negativen Folgen nach dem Löschen des ungebeten installierten Zertifikats feststellen. Bis Redaktionsschluss erhielten wir auch keine Antwort vom Hersteller auf die Frage nach dem Zweck dieser Maßnahme.

Dieser fahrlässige Umgang eines Herstellers mit der Sicherheit der IT-Infrastruktur der Kunden erinnert an Vorfälle wie Superfish auf Lenovo-PCs und -Laptops. Betroffenen empfehlen wir, Kontakt mit Sennheiser aufzunehmen und das Zertifikat aus dem Windows-Zertifikatspeicher zu entfernen.

Grundschutz runderneuert

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 08.08.2018 einen neuen Online-Kurs veröffentlicht, der allen Anwendern einen Einstieg in und einen Überblick über den in den vergangenen Jahren modernisierten IT-Grundschutz bietet.

Im Rahmen der Modernisierung wurden Überarbeitungen der BSI-Standards veröffentlicht: Managementsysteme für Informationssicherheit (200-1), IT-Grundschutz-Methodik (200-2) und Risikomanagement (200-3). Die IT-Grundschutz-Kataloge löste das IT-Grundschutz-Kompendium ab. Es besteht weiterhin aus Bausteinen, allerdings trennt der IT-Grundschutz jetzt zwischen Bausteinen mit Anforderungen und solchen mit Umsetzungshinweisen. Deren Vermischung war eine große Schwäche der alten Bausteine.

Eine Zertifizierung nach dem modernisierten IT-Grundschutz ist seit Ende 2017 möglich. Die Übergangsfrist für eine Zertifizierung nach dem bisherigen IT-Grundschutz endet am 30.09.2018.

Insgesamt ist dem BSI damit eine deutliche Qualitätsverbesserung gelungen. Die größte verbleibende Schwäche in der Praxis ist, dass leider nicht alle existierenden Bausteine in das neue Format übertragen wurden.

Fax-Angriff

Die von Checkpoint Research entdeckte und am 15.08.2018 veröffentlichte Schwachstelle „Faxploit" ermöglicht einem Angreifer, HP-Multifunktionsdrucker zu übernehmen. Sie nutzt eine Buffer-Overflow-Verwundbarkeit in dem Codeteil, der JPEG-Dateien interpretiert. Da Farb-Faxe als JPEG-Dateien übertragen werden, kann der Angriff über die Telefonleitung erfolgen – vorbei an Firewalls, Intrusion-Detection-Systemen und Content-Scannern. Betroffen sind möglicherweise nicht nur andere Fax-Empfangsgeräte, sondern auch Fax-Konvertierungssoftware, die den betroffenen Code verwendet.

Der Fall erinnert daran, dass alle Peripheriegeräte, die von außen erreicht werden können, Schwachstellen enthalten und daher ein Einfallstor für Angriffe sein können. Solche Geräte sollten daher geeignet abgeschottet werden, um im Falle eines erfolgreichen Angriffs ein Eindringen in das interne Netzwerk wirksam zu verhindern.

Biometriekritik

Die Kritik an der Nutzung biometrischer Merkmale für die Authentifikation ist nicht neu: Biometrische Merkmale können nicht abgelegt oder ausgetauscht werden, viele der heute eingesetzten Systeme lassen sich täuschen und können sogar deren Nutzer zum (physischen) Angriffsziel machen.

Am 06.08.2018 berichteten Deutschlandfunk und Bayerischer Rundfunk, dass schon heute der Handel mit gefälschten biometrischen Pässen und biometrischen Daten blüht. Selbst Prof. Dr. Udo Helmbrecht, Präsident der ENISA, warnt, der Überwindungssicherheit biometrischer Systeme nicht blind zu vertrauen. Dabei sind noch immer Anwendungen im Einsatz, die biometrische Daten im Klartext übermitteln – während die Verbreitung biometrischer Authentifikationsverfahren rasant wächst.

Wer seine eigenen einmaligen biometrischen Merkmale vor unerwünschter Verbreitung schützen will, sollte bei der Nutzung solcher Verfahren Zurückhaltung üben – und bei sicherheitskritischen Anwendungen lieber auf Zwei-Faktor-Authentifikationsverfahren mit „Besitz und Wissen" zurückgreifen.

Staatstrojaner

Im Jahr 2007 hat das Bundesverfassungsgericht hohe Hürden für die technische Ausspionierung von IT-Systemen Verdächtiger formuliert (SSN 10/2007). Nun hat der Bundestag am 22.06.2017, wenig beachtet, über einen Änderungsantrag der Bundesregierung eine Ausweitung von Quellen-Telekommunikationsüberwachung und Online-Durchsuchung beschlossen. Dass neben unverschlüsselten Kommunikationsdaten bspw. von Messenger-Diensten wie WhatsApp weitere Inhalte eines mit einem „Staatstrojaner" infiltrierten informationstechnischen Systems abgezogen werden ist nach § 100b StPO nur bei besonders schweren Straftaten zulässig – und „wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre": eine sehr weit auslegbare Ermächtigung. Dank einer Anpassung des § 100e StPO dürfen bei einer Online-Durchsuchung gewonnene Daten nun auch „zu Zwecken der Gefahrenabwehr" genutzt werden.

Gegen diese Ausweitung der Online-Durchsuchung hat nach dem Verein Digitalcourage am 20.08.2018 auch die FDP Verfassungsbeschwerde eingelegt. Hoffentlich bleibt das Bundesverfassungsgericht seinen 2008 formulierten Grundsätzen treu.

Secorvo News

Teamverstärkung

Am 01.09.2018 stößt Friederike Schellhas-Mende, Juristin und Datenschützerin, zu unserem Consulting-Team dazu. Und ebenfalls am 01.09.2018 übernimmt Joanna Klotz den Seminarbereich bei Secorvo. Willkommen im Team!

Secorvo@it-sa

Vom 09. bis 11.10.2018 sind wir mit einem Stand auf der IT-Security-Messe it-sa in Nürnberg vertreten und werden dort unsere Managementsysteme für Datenschutz und Informationssicherheit DSMS ready2go und ISMS ready2go zeigen. Sie finden uns in Halle 10 (Standnummer: 10.1-628). Gerne lassen wir Ihnen einen Registrierungscode zukommen, mit dem Sie Ihr kostenfreies E-Ticket (Tageskarte) ausdrucken können. Schicken Sie uns bei Interesse bitte eine kurze E-Mail.

Seminare

Bald ist es so weit: Im Oktober startet unsere Herbst-Seminarserie mit den beiden Zertifizierungsseminaren T.I.S.P. (**15.–19.10.2018**) und T.P.S.S.E. (**22.–25.10.2018**). Im November folgen das PKI-Seminar (**12.–15.11.2018**) und das Seminar IT-Sicherheit heute (**20.–22.11.2018**).

Wir freuen uns, sie in unserem renovierten Seminarbereich begrüßen zu dürfen – und empfehlen insbesondere für das T.I.S.P.-Seminar eine baldige Anmeldung, da uns schon zahlreiche Anmeldungen vorliegen. Programm und Online-Anmeldung unter https://www.secorvo.de/seminare.

Geburtstag

Vor genau 20 Jahren, am 01.09.1998, wurde Secorvo als Beratungsunternehmen für IT-Sicherheit und Datenschutz gegründet – in einer Zeit, in der die Informationstechnik zwar aus vielen Bereichen des (vor allem Wirtschafts-) Lebens schon nicht mehr wegzudenken war, die Beschäftigung mit IT- oder Informationssicherheit aber doch eher bestimmten Branchen wie dem Bankenbereich oder leicht pathologisch veranlagten Menschen vorbehalten schien. Seitdem hat sich die Welt verändert – kaum jemand, den die Themen Informationssicherheit oder Datenschutz heute nicht beträfen.

Diese Entwicklung haben wir über 20 Jahre aktiv begleitet. Fast 200 Ausgaben der Security News sind in dieser Zeit erschienen, unterstützt von rund 98.000 Tassen Kaffee und einem Team von mittlerweile 25 Mitarbeitern. Und wir sind ein wenig stolz auf das uns von unseren Kunden in mehr als 2.000 erfolgreichen Projekten entgegengebrachte Vertrauen. Vielen Dank dafür – und auf hoffentlich viele weitere Jahre so guter Zusammenarbeit.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2018	
04.-05.09.	D•A•CH Security (GI, OCG, TeleTrusT, Gelsenkirchen)
10.09.	Sommerakademie 2018 (ULD, Kiel)
13.09.	Digitale Mülltrennung (KA-IT-Si, Karlsruhe)
24.09.	Datenschutztag 2018 (COMPUTAS, Köln)
28.-30.09.	FIfFKon 2018 (FIfF, Berlin)
Oktober 2018	
01.-03.10.	ISSE 2018 (EEMA, Rom/IT)
08.-12.10.	OWASP AppSec USA 2018 (OWASP, San Jose/US)
09.-11.10.	it-sa 2018 (NürnbergMesse, Nürnberg)
15.-19.10.	T.I.S.P. (Secorvo, Karlsruhe)
15.-19.10.	ACM CCS 2018 (ACM/SIGSAC, Toronto/CA)
16.-18.10.	heise devSec 2018 (dpunkt.verlag, Heidelberg)
22.-25.10.	T.P.S.S.E. (Secorvo, Karlsruhe)
23.10.	Anwendertag IT-Forensik (Fraunhofer, Darmstadt)
30.10.	Swiss Cyber Storm 2018 (Swiss Cyber Storm Association, Bern/CH)

Fundsache

Der Zentralverband des Deutschen Handwerks bietet mit 10 Tipps eine gute Antwort auf die Frage, was Handwerker für die IT-Sicherheit unternehmen sollten. Darin werden wichtige Schritte beschrieben und gute Hinweise und Empfehlungen in Form von Broschüren oder verlinkten Webseiten gegeben.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick, Fabian Ebner, Stefan Gora, Kai Jendrian, Thomas Maus (Editorial).

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2018



Ein bisschen besser

Ende des vergangenen Jahrtausends, genauer am 01.09.1998, wurde Secorvo gegründet. Vier Tage vor Google. Und das fühlt sich ein wenig an wie ein Beleg für das schöne Bonmot von Herbert Hainer (von 2001 bis 2016 CEO bei Adidas) aus einem Interview im Jahr 2003: „Wenn Größe allein entscheidend wäre, würden die Dinosaurier heute noch leben und die Ameisen wären alle tot."

Wie lang uns ein solcher Zeitraum von zwanzig Jahren erscheint, hängt ganz von der Perspektive ab. Vor der (vermutlichen) Unendlichkeit des Universums ist er ein Nichts, für uns Menschen rund ein Viertel der Lebenszeit – und im IT-Bereich eine gefühlte Ewigkeit.

In den vergangenen 20 Jahren haben vor allem Kommunikationstechniken unseren Alltag grundlegend verändert. Die Welt ist dadurch kleiner und schneller geworden. Und dies hat zugleich schleichend – und zumeist unbemerkt – neue Rahmenbedingungen gesetzt. So entwickelt sich insbesondere Vertrauen, das „Schmiermittel" menschlicher Zivilisation, in einer zunehmend virtualisierten Welt aus anderen Zutaten als in zwischenmenschlicher Interaktion. Deutlicher ausgedrückt: Ohne wirksame Sicherheit und verlässlichen Datenschutz ist Vertrauen in technisch vermittelter Kommunikation schlicht unmöglich. Die Ableitung vertrauenswürdiger Sicherheit aus persönlichen Schlüsseln oder Passwörtern und die Umsetzung von Datenschutzanforderungen wie z. B. Löschfristen sind jedoch technisch komplex und organisatorisch anspruchsvoll. Vor allem aber höchst sensibel: Denn Nutzer müssen sich blind darauf verlassen können, dass Software, Hardware und Organisation dies sicherstellen. Davon sind wir leider noch immer ein ganzes Stück entfernt.

Wir hatten das Glück, in den vergangenen 20 Jahren in über 2.500 kleineren und größeren Projekten gemeinsam mit unseren Kunden an der Gestaltung solcher vertrauenswürdiger Prozesse und Datenschutz konformer Lösungen mitzuwirken. Und so, Tag für Tag, die Welt ein kleines bisschen besser zu machen. Vielen Dank dafür.



Inhalt

Ein bisschen besser

Security News

Umfrage ist E-Mail-Werbung

Last Call für Zertifikate

Fortschritte bei Facebook

Nicht nur Server soll man härten

Überwachungsvideo als Beweis

Beschränkt einsatzfähig

Secorvo News

Secorvo@it-sa

Secorvo-Seminare

Verordnete IT-Sicherheit

Veranstaltungshinweise

secorvo
security consulting

Security News

Umfrage ist E-Mail-Werbung

Am 10.07.2018 hat der sechste Zivilsenat des Bundesgerichtshofs entschieden, dass es unzulässig ist, Kunden per E-Mail zur Teilnahme an einer Kundenzufriedenheitsbewertung aufzufordern. Der Kläger hatte über „Amazon Marketplace" bei der Beklagten Waren bestellt. Per E-Mail übersandte die Beklagte die Rechnung, bedankte sich für den Kauf und bat den Kläger an einer Kundenzufriedenheitsumfrage teilzunehmen. Der Bundesgerichtshof teilte die Auffassung des Klägers, dass diese E-Mail eine unaufgeforderte unerlaubte Zusendung von Werbung war, die den Kläger in seinem allgemeinen Persönlichkeitsrecht verletzte.

Der BGH stellte fest, dass eine Zufriedenheitsnachfrage Werbung im Sinne des Art. 13 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) bzw. § 7 Abs. 2 Nr. 3 UWG ist. Dies sei auch dann der Fall, wenn sie zusammen mit einer Rechnung übersandt wird. Die Einwilligung des Nutzers ist folglich Voraussetzung für die Zulässigkeit der (Direkt-)Werbung.

Die Entscheidung des BGH ist richtig, da damit zu rechnen ist, dass sich derartige Fälle durch die Automatisierungsmöglichkeiten häufen werden. Daher überwiegt bei der in solchen Fällen durchzuführenden Interessenabwägung das Interesse des Nutzers, in Ruhe gelassen zu werden, das (wiewohl legitime) Werbeinteresse des Händlers.

Last Call für Zertifikate

Am 18.09.2018 erschien das Beta-Release von Chrome 70 – jener Version, die ihre Benutzer nun auch vor den letzten unter der Ägide von Symantec erstellten SSL-Zertifikaten der Marken VeriSign, Thawte, GeoTrust etc. warnt (vgl. SSN 09/2017). Wer noch ein solches „ranziges" Zertifikat einsetzt, sollte schleunigst ein frisches ordern, bevor Mitte Oktober das „stable" Release von Chrome 70 per Update die meisten Anwender erreicht.

Fortschritte bei Facebook

Am 05.06.2018 hat der Europäische Gerichtshof in seinem Urteil zu Facebook Fanpages die gemeinsame Verantwortung von Seitenbetreiber und Facebook für die Datenverarbeitung gegenüber den Nutzern festgestellt. Der Anforderung, eine Vereinbarung zur Verantwortungsabgrenzung nach Art. 26 Abs. 1 und 2 DSGVO vorzulegen, ist Facebook nun nachgekommen. Darin erkennt Facebook die Hauptverantwortung für die Verarbeitung der Nutzungsdaten bei den Seitenaufrufen an und bestimmt Facebook Ireland Ltd. als Verantwortlichen. Das schließt die Gewährleistung der Betroffenenrechte nach Art. 12 ff, 15 bis 22 DSGVO ein. Facebook erklärt sich auch für die Sicherheit der Verarbeitung zuständig (Art. 32 DSGVO). Die Vereinbarung knüpft an die Verwendung von Facebook Insight an. Seitenbetreiber, die im Anwendungsbereich der DSGVO agieren und denen Insight zur Verfügung steht, erkennen die Vereinbarung an. Für die Vereinbarung wird irisches Recht für anwendbar erklärt. Der Seitenbetreiber wird verpflichtet, Kontakte der Aufsichtsbehörden an Facebook zu melden. Für die Angabe einer Rechtsgrundlage seiner Datenverarbeitung, die Erfüllung der nicht näher bestimmten verbleibenden Datenschutzpflichten und die Benennung des Seitenverantwortlichen bleibt der Seitenbetreiber verantwortlich.

Mit der Vereinbarung geht Facebook einen großen Schritt Richtung Rechtssicherheit für Seitenbetreiber. Es ist jedoch noch zu klären, ob die Bestimmung irischen Rechts, die Beschränkung auf Insights-Daten ohne nähere Definition und die Herstellung von Transparenz rechtskonform sind und eine ausreichende Umsetzung darstellen. Für die Seitenbetreiber ist jedoch eine wesentliche Grundlage für die weitere Nutzung des Dienstes geschaffen.

Nicht nur Server soll man härten

Sicherheitsforscher von ESET stellten am 27.09.2018 in ihrem Blog Erkenntnisse über eine neue Art Rootkit vor. Konkret handelt es sich um eine Schadsoftware, die sich in der Firmware (*Unified Extensible Firmware Interface*, UEFI) ihrer Opfer einnistet und von dort ihr Unwesen treibt – unsichtbar für Virenscanner und Anwender.

Ein solch kleines und unscheinbares Rootkit führt uns vor, warum man bei der Härtung von Betriebssystemen nicht nur Server, sondern auch Client-Systeme im Blick haben sollte. Die einfache Aktivierung von *Secure Boot* verhindert zumindest bei diesem speziellen Rootkit eine Infektion. Und das Laden unsignierter Firmware-komponenten beim Systemstart sollte ohnehin generell auf Firmenrechnern verhindert werden.

Überwachungsvideo als Beweis

In einem von Bundesarbeitsgericht am 23.08.2018 entschiedenen Fall hatte ein Arbeitgeber seine Geschäftsräume (hier einem Tabak- und Zeitschriftenhandel mit angeschlossener Lottoannahmestelle) mit einer offenen Videoüberwachung

überwacht, um sein Eigentum vor Straftaten seiner Kunden und seiner Mitarbeiter zu schützen. Nachdem im 3. Quartal 2016 ein Fehlbestand an Tabakwaren festgestellt worden war, wertete der beklagte Arbeitgeber die Videoaufzeichnungen aus und stellte dabei fest, dass die klagende Arbeitnehmerin schon im Februar 2016 vereinnahmte Gelder nicht in die Registrierkasse gelegt hatte. Daraufhin kündigte der Arbeitgeber der Arbeitnehmerin fristlos. Gegen diese Kündigung erhob die Klägerin Kündigungsschutzklage.

Das BAG entschied (auch unter Berücksichtigung der DSGVO), dass, wenn eine offene, rechtmäßige Videoüberwachung stattfindet, die Videoaufzeichnungen als Beweis verwertet werden können. Arbeitgeber seien aufgrund des datenschutzrechtlichen Löschgebots nicht verpflichtet, Videoaufzeichnungen umgehend auszuwerten. Es sei rechtmäßig damit solange zu warten, bis es einen (berechtigten) Anlass zur Auswertung des Bildmaterials gab. Die Prüfung, ob eine rechtmäßige Videoüberwachung gegeben war, muss das Gericht treffen, an welches die Sache zurückverwiesen wurde.

Die Entscheidung des BAG ist vor allem deshalb Aufsehen erregend, weil daraus gefolgert werden kann, dass ein Verstoß gegen die datenschutzrechtlichen Löschregeln kein allgemeines Beweisverwertungsverbot nach sich zieht. Aus datenschutzrechtlicher Sicht bleibt es aber dabei, dass Daten aus einer Videoüberwachung nicht unbegrenzt lange gespeichert werden dürfen. Damit ist ein neues Spannungsfeld zwischen den Grundsätzen des Datenschutzes und den rechtlichen Konsequenzen in anderen Rechtsbereichen bei Datenschutz-Verstößen eröffnet.

Beschränkt einsatzfähig

Nachdem das *besondere elektronische Anwaltspostfach* (beA) Ende 2017 aus Sicherheitssicht eine Bruchlandung hinlegte, gelobten die Verantwortlichen Besserung. Nach der Erstellung eines Sicherheitsgutachtens und Behebung mehrerer festgestellter Schwachstellen ging die Anwendung am 03.09.2018 wieder in Betrieb. Nach wie vor begrenzen jedoch Designansätze die Sicherheit: Zwar erfolgt die Nachrichtenverschlüsselung auf dem Client, die eigentliche Anwendung wird jedoch als Web-Applikation von den Servern des Betreibers ausgeliefert und kommuniziert nur für die kryptografischen Operationen mit der Client-Security-Komponente des Anwenders. Ein Angreifer, der die Web-Anwendung kontrolliert, kann Betreff und Nachrichtentext einsehen sowie weitere Empfänger hinzufügen. Dies wurde im Gutachten als „betriebsverhindernd" eingestuft und sollte somit vor der Inbetriebnahme behoben werden.

Angesichts der nötigen umfangreichen Änderungen an der Anwendungsarchitektur wäre vermutlich eine planmäßige Inbetriebnahme nicht möglich gewesen. Die Bundesrechtsanwaltskammer entschied daher, die Priorität der Schwachstelle herabzustufen: Es sei keine Einsichtnahme in die Anhänge möglich und der Schutzbedarf der Nachrichten sei geringer einzuschätzen. Diese Einschätzung beruht allerdings auf der Annahme, dass Benutzer tatsächlich keine sensiblen Daten in Text oder Betreff integrieren. Besser wäre es gewesen, klarzustellen, dass die technische Lösung nur unter bestimmten Voraussetzungen sicher ist. Das Beispiel zeigt, warum Sicherheit in allen Phasen der Software-Entwicklung Beachtung finden sollte: Denn Fehler in der Anforderungs- oder Design-Phase lassen sich in der Implementierung kaum noch beheben.

Secorvo News

Secorvo@it-sa

Besuchen Sie uns vom 9. bis 11. Oktober auf der it-sa – Sie finden uns in Halle 10, Standnummer 10.1.-628. Am 09.10.2018 um 14:00 Uhr spricht Dirk Fox im Forum M10 – Management zum Thema DSMS – Datenschutz mit System.

Sie haben noch kein Ticket? Registrieren Sie sich mit unserem Gutscheincode **A398906** für ein kostenfreies Tagesticket.

Secorvo-Seminare

Ende Oktober findet bei Secorvo das Zertifizierungsseminar T.P.S.S.E. (**22.–25.10.2018**) statt, gefolgt im November von dem Seminar IT-Sicherheit heute (**20.–22.11.2018**) und der letzten Gelegenheit in diesem Jahr, sich als T.I.S.P. zu qualifizieren (**26.–30.11.2018**). Wir freuen uns, sie in unserem renovierten Seminarbereich begrüßen zu dürfen. Programme und Online-Anmeldung unter https://www.secorvo.de/seminare.

Verordnete IT-Sicherheit

Die MiRO – Mineralölraffinerie Oberrhein ist als Teil der kritischen Infrastruktur verpflichtet, die Anforderungen des § 8a IT-Sicherheitsgesetz zu erfüllen. Beim kommenden KA-IT-Si-Event am **08.11.2018** stellt Alessandro Wittig vor, wie die MiRO diese Herausforderung bewältigt hat, welche Vorteile sich daraus ergeben haben und wie der Nachweis gegenüber dem BSI erbracht wurde. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking". Wir freuen uns auf Ihre Teilnahme (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2018	
09.-11.10.	it-sa 2018 (NürnbergMesse GmbH, Nürnberg)
15.-19.10.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
15.-19.10.	ACM CCS 2018 (ACM/SIGSAC, Toronto/CA)
16.-18.10.	heise devSec 2018 (dpunkt.verlag, Heidelberg)
22.-25.10.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
23.10.	Anwendertag IT-Forensik (SIT, Darmstadt)
30.10.	Swiss Cyber Storm 2018 (Swiss Cyber Storm Association, Bern/CH)
November 2018	
06.-07.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
14.-16.11.	42. DAFTA (GDD Gesellschaft für Datenschutz und Datensicherheit e.V., Köln)
20.-21.11.	7. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Hamburg)
20.-22.11.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
26.-30.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
27.-30.11.	DeepSec In-Depth Security Conference Europe (DeepSec GmbH, Wien/AT)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Hans-Joachim Knobloch, Michael Knopp, Friederike Schellhas-Mende.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2018



Rote Linien

Der Preikestolen ist ein Fels in der Nähe von Stavanger in Norwegen, der über 600 Meter senkrecht bis zum darunter liegenden Fjord abfällt. Hunderttausende besichtigen jährlich dieses Naturwunder. Aber keiner der Besucher, der noch bei Sinnen ist, käme auf die Idee, von dort im Wingsuit hinunter zu springen, ohne über ein gerüttelt Maß an Erfahrung als Fallschirmspringer zu verfügen.

Beim Software-Entwurf sind die roten Linien, die man tunlichst nicht überschreiten sollte, meist nicht ganz so leicht zu erkennen wie die Kante des Preikestolen. Und die möglichen Leidtragenden sind in der Regel die Anwender – und nicht die Entwickler, die die Linie überschreiten. Oft, oder besser: allzu oft verändern Designer einer Anwendung übergreifende Rechteeinstellungen des Systems, hantieren mit hoch privilegierten Benutzern und deren Credentials oder – so wie die in diesen Security News beschriebene Headset-Software – schieben dem System ein Root-Zertifikat unter, dessen Schlüssel sie gleich mit ausliefern. In solchen Fällen sollte man jedoch mindestens zweimal überlegen, ob man nicht auch ans Ziel kommt, ohne diese Linie zu überschreiten.



M M from Switzerland
(CC-BY-SA 2.0)

Wer sich dennoch in derart unsichere Gefilde begibt, der sollte beizeiten Experten für dieses Territorium hinzuziehen, die ein unabhängiges Design-Review durchführen. Zwar kann selbst dann noch etwas schief gehen – so wie leider nur zu oft auch bei Extremsportlern in Wingsuits – aber ohne eigene Erfahrung ist das Risiko unkalkulierbar und ein Scheitern wahrscheinlich.

Und noch etwas können Entwickler von Extremsportlern lernen: Hinter sich aufzuräumen und beim Gehen die Umgebung hinter der roten Linie so zurückzulassen, wie man sie vorgefunden hat.



Inhalt

Rote Linien

Security News

Sennheisers HeadSetup revisited

Gefährliche Abhängigkeiten

Gehackte Boxen

Abofalle „Datenschutzauskunft“

DSGVO-Abmahnungen

Secorvo News

Secorvo Seminare

Verordnete IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Sennheisers HeadSetup revisited

In den SSN 08/2018 warnten wir vor dem fahrlässigen Umgang der Software Sennheiser HeadSetup mit CA-Zertifikaten. Anschließend analysierten wir einige ältere Versionen der betroffenen Software genauer – und dabei zeigte sich, dass die Schwachstelle gravierender ist als ursprünglich angenommen. Denn mit Informationen aus der Anwendung konnte auch der geheime CA-Schlüssel ausgelesen und missbraucht werden. Als „Proof of Concept" realisierten wir mit der Root-CA einen Man-in-the-Middle-Angriff auf TLS-Verbindungen und hebelten so die HTTPS-Verschlüsselung aus: Die Schwachstelle untergräbt für betroffene Systeme die gesamte zertifikatsbasierte Vertrauensinfrastruktur.

Im Gespräch mit dem Hersteller stellte sich heraus, dass die CA lediglich genutzt wird, um vertrauenswürdige Serverzertifikate für den lokal betriebenen Websocket-Dienst bereitzustellen. Dieser Dienst soll Schnittstellen zwischen Headset und Web-basierten Softphones implementieren. Dafür hätte es jedoch keiner eigenen Root-CA bedurft.

Als sei das noch nicht genug, unterliefen dem Hersteller in seinem Deinstallations- bzw. Update-Programm weitere Fehler: So werden die nicht mehr benötigten CA-Zertifikate nicht aus dem Zertifikatsspeicher von Windows entfernt. Alle Systeme, auf denen irgendwann eine der von der Schwachstelle betroffenen Versionen von HeadSetup installiert war, sind daher weiterhin angreifbar – obwohl jüngere Versionen von HeadSetup mittlerweile eine nicht so einfach zu missbrauchende CA nutzen.

Auch wenn wir die Kopfhörer des Herstellers lieben - ein Beispiel, pars pro toto, für die drastischen Folgen eines unbesonnenen Umgangs mit Credentials und Zertifikaten. Details zur Schwachstelle und Empfehlungen zu Gegenmaßnahmen finden sich in unserem Vulnerability Report zur Schwachstelle CVE-2018-17612.

Gefährliche Abhängigkeiten

Bereits am 19.01.2017 wurde über den offiziellen Twitter-Account von PHP darauf hingewiesen, dass am 31.12.2018 die Versorgung mit Sicherheits-Updates für PHP 5.6 eingestellt wird. Knapp zwei Jahre später verwenden nach den Statistiken von W3Tecs jedoch immer noch 61% aller erfassten Webseiten diese bald nicht mehr unterstützte Version. Abhilfe schafft eine rechtzeitige Migration auf eine neuere PHP-Version – die kann allerdings (zeit-)aufwändig sein.

Derartige Abhängigkeiten von Komponenten stellen vor allem im Bereich von Web-Anwendungen ein steigendes Sicherheitsrisiko dar. In der jüngsten Ausgabe der OWASP Top 10, einer Auflistung der zehn größten Sicherheitsrisiken in Web-Anwendungen, ist die Nutzung verwundbarer Komponenten erstmals in den Risiko-Katalog aufgenommen worden.

Lösungsmöglichkeiten zeigen Projekte wie RetireJS oder OWASP Dependency Check auf, die bei der Erstellung von Anwendungen bei allen Abhängigkeiten (Komponenten, Bibliotheken) prüfen, ob Versionen mit bekannten Schwachstellen verwendet werden. Das Auslaufen des Supports lässt sich allerdings noch nicht automatisiert prüfen.

Gehackte Boxen

Wer sich für die Welt der Hacks und Exploits interessiert, findet in Hackthebox eine neue Herausforderung: ein Übfeld für Hacker-Trainings. Über einen kostenlosen VPN-Zugang können Zielsysteme auf Netzwerkebene untersucht und angegriffen werden. Auch die Pentesting-Experten von Secorvo zerlegen dort regelmäßig Maschinen, testen Tools und vertiefen dabei ihre Fertigkeiten.

Der Dienst steht allen offen, die – als kleine Fingerübung – die Registrierungsseite hacken. Eine klare Empfehlung!

Abofalle „Datenschutzauskunft"

Die Schreiben der selbsternannten „Datenschutzauskunft-Zentrale" schlagen derzeit hohe Wellen in der Presse, Verbraucherschutzzentralen und Datenschützer warnen. Was ist passiert? Die in Malta ansässige „Datenschutzauskunft-Zentrale" fordert Unternehmer per Schreiben auf, sich in das Datenschutzauskunft-Register eintragen zu lassen und bietet verschiedene Dienste an. Wie bereits früher bei den so genannten „Gewerbeauskünften" steckt eine „Abofalle" dahinter: Wer das Formular ausfüllt, unterschreibt und zurücksendet schließt einen Vertrag über einen Eintrag in das Datenschutzauskunft-Register – gegen Entgelt: Es folgt eine Rechnung über mehrere hundert Euro.

Zwar gibt es bereits einstweilige Verfügungen, die der Datenschutzauskunft-Zentrale untersagen, derartige Werbung per Fax zu übersenden. Dennoch: Was tun, wenn man auf die Masche hereingefallen ist und die Betreiber mit Mahnverfahren und gerichtlicher Vollstreckung der Forderung drohen?

Nach Auffassung des Bundesgerichtshofs sind Entgeltklauseln, die derart unauffällig im Gesamtbild

eines Schreibens eingefügt sind und Dienste betreffen, die für gewöhnlich unentgeltlich erbracht werden, überraschend und damit gem. § 305c Abs. 1 BGB nicht Vertragsbestandteil, da der Vertragspartner an dieser Stelle nicht damit rechnet. Daher entsteht mit der Unterschrift keine Zahlungsverpflichtung. Allerdings gibt es bisher im Internet keine derartigen Register (warum auch), deshalb ist offen, ob die Gerichte davon ausgehen werden, dass solche Dienste in einer Vielzahl von Fällen unentgeltlich erbracht werden. Das Tätigwerden externer Datenschutzbeauftragter ist schließlich in der Regel nicht kostenlos. Allein auf das Urteil des BGH sollte man sich daher nicht verlassen, sondern den Vertrag umgehend wegen arglistiger Täuschung anfechten und rechtliche Beratung in Anspruch nehmen.

DSGVO-Abmahnungen

Vor dem Inkrafttreten der DSGVO wurde häufig eine neue „Abmahnwelle" vorhergesagt. Nun ist zu dieser Frage am 13.09.2018 eine erste Entscheidung des LG Würzburg ergangen: Ein Wettbewerber hatte die Datenschutzerklärung einer Webseite, die nicht den Anforderungen der DSGVO genügte, als wettbewerbsrechtlichen Verstoß gegen § 3a UWG abgemahnt und eine einstweilige Verfügung beantragt, die das Landgericht auch erließ.

Von einer Abmahnwelle kann bislang aber noch nicht die Rede sein, auch wenn zu erwarten ist, dass noch viele solcher Entscheidungen folgen werden. Befürchtet werden ähnliche Fallzahlen wie bei fehlerhaften oder fehlenden Widerrufsbelehrungen. Anders als bei der Widerrufserklärung gibt es hier jedoch kein gesetzliches Muster, an dem sich der Anwender orientieren könnte. Daher ist die Gefahr von Fehlern bei Datenschutzerklärungen sogar größer, wenn man nicht die notwendige Sorgfalt walten oder sich diesbezüglich beraten lässt.

Das Bundesministerium für Justiz und Verbraucherschutz hat inzwischen einen Gesetzentwurf veröffentlicht, mit dem ein weiterer Versuch unternommen wird, missbräuchlichen, auf Gewinnerzielung ausgerichteten Abmahnungen einen Riegel vorzuschieben.

Dies soll über eine Beschränkung der Klagebefugnis auf Mitbewerber und Wettbewerbsverbände erfolgen; daneben ist eine Stärkung des Schutzes von Kleinstunternehmen vorgesehen, indem ein Gegenanspruch für den Abgemahnten geschaffen wird und unangemessen hohe Vertragsstrafen keinen Anlass zur Klage begründen – sie müssen in einem angemessenen Verhältnis zum abgemahnten Verstoß und seinen wettbewerbsrechtlichen Folgen stehen, und der Streitwert darf nicht missbräuchlich hoch angesetzt werden.

Die meisten Verbände befürchten, ihre Mitglieder bzw. Verbraucherinnen und Verbraucher würden in ihrem Schutz vor Wettbewerbsverstößen beschnitten und lehnen die Einschränkung der Klagebefugnis daher ab. Begrüßt wird jedoch die Abschaffung der datenschutzrechtlichen Klagebefugnis, da für kleinere und mittlere Unternehmen ein erhöhtes Abmahnungsrisiko bestehe.

Streicht man jedoch die Klagebefugnis wegen Verstößen gegen die DSGVO aus dem Gesetz gegen den unlauteren Wettbewerb (UWG), so dürfte das den Eindruck vermitteln, dass Unternehmen es zumindest aus wettbewerbsrechtlicher Sicht mit dem Datenschutz nicht so genau nehmen müssen. So verleiht man dem Datenschutz kein größeres Gewicht, daher sollte der Gesetzentwurf sich besser darauf beschränken, missbräuchliche Abmahnungen mit Gewinnerzielungsabsicht weiter zu erschweren.

Secorvo News

Secorvo Seminare

Aktuelle Fragen der IT-Sicherheit thematisieren wir im November auf unsrem Seminar IT-Sicherheit heute (**20.–22.11.2018**). Im neuen Jahr haben Sie dann im März die nächste Gelegenheit, sich als T.I.S.P. zu qualifizieren (**25.–29.03.2019**). Wir freuen uns, Sie auf einem unserer Seminare zu begrüßen. Programme und Online-Anmeldung unter https://www.secorvo.de/seminare.

Verordnete IT-Sicherheit

Die MiRO – Mineralölraffinerie Oberrhein ist als Teil der kritischen Infrastruktur verpflichtet, die Anforderungen des § 8a IT-Sicherheitsgesetz zu erfüllen. Beim kommenden KA-IT-Si-Event am **08.11.2018** stellt Alessandro Wittig vor, wie die MiRO diese Herausforderung bewältigt hat, welche Vorteile sich daraus ergeben haben und wie der Nachweis gegenüber dem BSI erbracht wurde. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking". Wir freuen uns auf Ihre Teilnahme (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2018	
06.-07.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
14.-16.11.	42. DAFTA (GDD Gesellschaft für Datenschutz und Datensicherheit e.V., Köln)
20.-21.11.	7. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Hamburg)
20.-22.11.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
27.-28.11.	8. Handelsblatt Jahrestagung – Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
27.-30.11.	DeepSec In-Depth Security Conference Europe (DeepSec GmbH, Wien/AT)
Dezember 2018	
03.-06.12.	Black Hat Europe 2018 (Blackhat, London/UK)
2019	
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-29.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)

Fundsache

Am 11.10.2018 veröffentlichte das BSI den Bericht zur "Lage der IT-Sicherheit in Deutschland 2018". Darin finden sich – gut dargestellt – zahlreiche Beispiele aufgedeckter Angriffe und konkrete Empfehlungen zum Schutz der eigenen Infrastruktur.



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick, Fabian Ebner, Stefan Gora, Hans-Joachim Knobloch (Editorial), Michael Knöppler, Friederike Schellhas-Mende

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

November 2018



Ende des Kuschelkurses

Jetzt sind sie da – die ersten DSGVO-Bußgelder. Und tatsächlich: Allen Unkenrufen und wilden Spekulationen zum Trotz, die höchste Bußgelder für Minimalverstöße bei kleinen und mittleren Unternehmen voraussagten, sind sie ein Zeichen von Augenmaß und klarer Kante zugleich.

Während Knuddels nach einem Daten-Leak von Millionen Kundendaten (inklusive Klartext-Passwörtern) als Anerkennung für die unverzügliche Vorfallsmeldung und die enge Kooperation mit der Aufsichtsbehörde bei der Beseitigung der Schwachstellen nur ein moderates Bußgeld in Höhe von 20.000 € auferlegt wurde (siehe den Beitrag in diesen SSN), haben die Aufsichtsbehörden von Großbritannien und den Niederlanden nun den amerikanischen Taxi-Konkurrenten Uber nach einem über ein Jahr geheim gehaltenen Datenschutzvorfall, von dem 57 Millionen Nutzer und Fahrer betroffen waren, mit einem Bußgeld von insgesamt mehr als einer Million Euro belegt.

Die Fälle zeigen dreierlei: So werden gerade aus den zahnlosen Tigern, die die Datenschutzaufsichtsbehörden mit ihren übersichtlichen maximalen Bußgeldern bislang waren, einflussreiche Mitspieler bei der Durchsetzung eines sicherheitssensiblen Umgangs mit personenbezogenen Daten. Dabei konzentrieren sich die Aufsichtsbehörden zweitens, wie von Experten erhofft, mit ihren Bußgeldbescheiden auf tatsächlich materiell relevante Vorfälle – und sanktionieren nicht bürokratische Nachlässigkeit, wie vielfach befürchtet wurde. Und sie senden drittens ein wichtiges Signal in alle Welt: Wer in einem der größten Binnenmärkte Geschäfte mit europäischen Bürgern macht, hat sich an europäisches Datenschutzrecht zu halten – und das gilt, wie der Europäische Gerichtshof schon 2014 deutlich gemacht hat, auch für amerikanische Anbieter. Google, Amazon, Facebook & Co. werden das in Bälde zu spüren bekommen. Womöglich bricht gerade ein neues Datenschutzzeitalter an – „Post Privacy" jedenfalls war gestern.



Inhalt

Ende des Kuschelkurses

Security News

Erstes DSGVO-Bußgeld

DSGVO-Services

Autopsy

HeadSetup – Nachlese

Datenschutz-Standardisierung

Secorvo News

Teamverstärkung

Seminare

Krypto im Advent

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Erstes DSGVO-Bußgeld

Bußgelder im Rahmen der DSGVO waren vor Inkrafttreten Zündstoff für hitzige Diskussionen. Es wurde erwartet, dass angesichts des Strafrahmens (maximal 10 bis 20 Mio. € bzw. 2-4% des weltweiten Gesamtumsatzes) hohe, wenn nicht sogar sehr hohe Strafen zur Abschreckung verhängt werden.

Im Fall des Daten-Leaks bei Knuddels, bei dem Millionen Nutzerdaten (inklusive Klartext-Passwörter) abgezogen wurden, wurde nun der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg tätig und verhängte das erste DSGVO-Bußgeld in Höhe von 20.000 € - eine entgegen den Erwartungen moderate Bußgeldhöhe. Doch der Landesdatenschutzbeauftragte begründet die Entscheidung klar und gut nachvollziehbar: Für ihn sei ausschlaggebend, wie sich ein Unternehmen im Falle eines Datenschutzvorfalls verhält. Die Reaktion von Knuddels – umgehende Information aller Betroffenen, zügige Meldung an die Aufsichtsbehörde und Kooperation mit den zuständigen Stellen – sei in dieser Hinsicht vorbildlich gewesen.

Die moderate Höhe des Bußgelds sollte daher nicht als Einladung zu einem nachlässigen Umgang mit Datenschutzbelangen missverstanden werden. Das gilt vor allem, wenn Passwörter und IDs von Nutzern betroffen sind – schließlich handelt es sich dabei um besonders schützenswerte Daten. Daraus folgt vor allem, dass diese sicher gespeichert werden müssen, beispielsweise als Hashwert – jedenfalls unter keinen Umständen im Klartext.

In jüngster Vergangenheit zeigte sich allerdings, dass auch einige andere Plattformbetreiber es mit der Passwortsicherheit nicht so genau nehmen. Mitte des Jahres blamierte sich T-Mobile Österreich auf Twitter, und dann schaffte es Instagram sogar, Passwörter durch ein DSGVO-Tool abfließen zu lassen. Kandidaten für höhere Bußgeldbescheide gibt es also bereits.

DSGVO-Services

Die Datenschutz-Grundverordnung hat die Benennung des Datenschutzbeauftragten gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) neu eingeführt und die Meldung von Datenschutz-Vorfällen (Art. 37 Abs. 7) deutlich aufgewertet, letztere durch eine enge Frist und erhöhte Sanktionen. Einige Aufsichtsbehörden haben die Sanktionierung bei unterbliebener Benennung bis Anfang 2019 ausgesetzt – vielleicht auch, weil für beide Meldeformen nach wie vor nicht alle Online-Meldeportale funktionsbereit sind.

Es fällt auf, dass gerade die großen Bundesländer hier Defizite aufweisen. Während die Online-Benennung außer in Thüringen überall möglich ist, ist eine Online-Vorfallsmeldung (neben Thüringen) auch in Brandenburg, Bremen, Nordrhein-Westfalen, Sachsen und Schleswig-Holstein nicht verfügbar.

Beinahe alle Bundesländer gehen zudem sehr unterschiedliche Wege bei dem Angebot; teilweise sind die Portale sehr versteckt und schlecht zu finden. Hessen bietet den Versand eines Upload-Links für ein ausgefülltes Vorfallsformular an. In Bayern und NRW ist für die Benennung des Datenschutzbeauftragten zudem eine vorherige Registrierung des Verantwortlichen erforderlich. Eine Benennung für mehrere Verantwortliche in einem Online-Formular ist durchweg nicht möglich, entgegen Art. 37 Abs. 2 DSGVO.

Bei der Meldung eines Vorfalls kann durchaus eine fallspezifische Vorlage sinnvoll sein, doch gerade wenn für Unternehmensgruppen die Benennungen vorzunehmen sind, sind die vorhandenen Erschwernisse durchaus ärgerlich – da hinkt die Praxis dem Vereinheitlichungsgedanken der DSGVO noch deutlich hinterher.

Autopsy

Seit dem 09.11.2018 ist die erheblich verbesserte Version 4.9.1 des kostenfreien forensischen Werkzeugs Autopsy verfügbar und läuft nun bei hoher Last mit vielen Falldaten noch einmal deutlich stabiler. Sehr hilfreich ist die neue Funktion einer zusammengeführten Datenbasis (Central Repository), die validierte und normalisierte Daten fallübergreifend vorhält. Wer bisher dachte, man kann mit Autopsy „nur" Datenträgerforensik durchführen, irrt, denn durch Aktivierung der „Experimental Plugin"-Funktion wird der Zugriff auf den weiterentwickelten Volatility Data Source Processor möglich, so dass Datenträger- und Hauptspeicherartefakte in einer Analyse zusammengeführt werden können.

Beide Funktionen zusammen erlauben eine mächtige Suche nach Gemeinsamkeiten, Querbeziehungen und Datenspuren sowohl für systembezogene als auch systemübergreifende Artefakte. Ein Tool, das in keinem Forensik-Labor fehlen sollte.

HeadSetup – Nachlese

In den SSN 10/2018 berichteten wir bereits über die Schwachstelle CVE-2018-17612 in Sennheisers HeadSetup. Mittlerweile beschäftigten sich auch

das Microsoft Security Advisory (ADV180029) und diverse weitere Medien mit der Schwachstelle.

Anschließend setzen wir uns mit den möglichen Ursachen dieser Schwachstelle auseinander, denn Katastrophen sind meist das Ergebnis einer Verkettung ungünstiger Ereignisse. So handelt es sich im vorliegenden Fall auch nicht um einen reinen Implementierungsfehler; auch bei Design und Architektur wurden gravierende Fehler begangen – die zur Lösung eines allerdings nicht von Sennheiser zu vertretenden Problems in Kauf genommen wurden.

Denn maßgeblich dafür, dass überhaupt eine CA zur Kommunikation mit dem lokalen Dienst zum Einsatz kam, ist der Umgang der Browser mit sogenanntem Mixed-Content – unverschlüsselten Inhalten, die in mittels HTTPS geschützte Seiten eingebunden werden. Mike West aus dem Chrome Security Team wies schon am 29.04.2016 darauf hin, dass unverschlüsselte Inhalte vom lokalen System als vertrauenswürdig angesehen werden sollten, da ansonsten die Anwender veranlasst werden könnten, neue Root-CAs nur zu diesem Zweck zu installieren. Dies führte Mitte 2016 zu einer Änderung des Standards. Trotzdem unterbindet derzeit ein Großteil der Browser (Firefox 63.0.1, Safari, Internet Explorer 11) genau diese Anfragen. Lediglich Google Chrome und in der aktuellen Version auch Microsoft Edge erlauben die unverschlüsselte Kommunikation mit den lokalen Diensten. Dies führt Entwickler, die lediglich die Kompatibilität ihrer Software mit verschiedenen Browsern gewährleisten wollen, auf dünnes Eis.

Ein „Zuviel" an Sicherheit kann auch Unsicherheit verursachen. Um ähnliche Schwachstellen zukünftig auszuschließen müssen die Browser-Hersteller schnellstens ihre Sicherheitsstrategie den Standards anpassen.

Datenschutz-Standardisierung

Am 10.09.2018 veröffentlichte das ULD Schleswig-Holstein neue Module des Standarddatenschutzmodells (SDM). Dabei handelt es sich noch um Entwürfe, zu denen nun Anwender ihre Erfahrungen mitteilen sollen. Die vorgestellten Bausteine betreffen die Themen Aufbewahrung, Planung und Spezifikation, Dokumentation, Protokollierung, Trennung, Löschen und Vernichten sowie Datenschutzmanagement. Das SDM soll eine Blaupause für die Prüfung von Verarbeitungstätigkeiten liefern, die gleichzeitig eine Prüfung der Gestaltungsentscheidungen ermöglicht. Die einzelnen Bausteine enthalten unverbindliche Maßnahmenkataloge, die sich am IT-Grundschutz des BSI und den Maßnahmen der früheren Anlage zu § 9 BDSG aF orientieren.

Ob das SDM in der Praxis die versprochene Erleichterung und den Nachvollziehbarkeitsgewinn liefert, hängt von der inhaltlichen Fortentwicklung der Module ab: Noch deckt das Vorgehen nur einen Teil der Verarbeitungstätigkeitsprüfung ab, die Prüfung der Rechtsgrundlage bleibt bspw. außen vor. Das Vorgehen und die Ausführungen zu den Gewährleistungszielen stellen sich recht kompliziert dar und erfordern erhebliche Datenschutzerfahrung zur Einordnung. Den betrieblichen Datenschutzbeauftragten in Nebentätigkeit dürfte dies überfordern.

Secorvo News

Teamverstärkung

Auch mit Blick auf die große Nachfrage nach unseren Penetrationstests freuen wir uns sehr, dass seit Mitte November Christian Titze unser Team verstärkt. Und Monika Contag hat das Rechnungswesen übernommen. Willkommen im Team!

Seminare

Wer seine Weiterbildung 2019 langfristig plant, findet das Seminarangebot, die Termine unserer PKI-, T.I.S.P.- und T.P.S.S.E.-Seminare (alle ab März 2019) sowie die Online-Anmeldung unter www.secorvo.de/seminare.

Krypto im Advent

Am 01.12.2018 startet unser viertes Adventsrätsel „Krypto im Advent" für Schülerinnen und Schüler der Klassen 3 bis 9. Der in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe entwickelte interaktive Adventskalender entführt in die Welt der Kryptologie. Diesmal gilt es, die entführte Geheimagentin Kryptina wiederzufinden.

Wer alle Rätsel richtig beantwortet, kann einen der zahlreichen von unseren Sponsoren beigesteuerten Preise gewinnen. Auch ältere, an der Kryptologie Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.



Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2018	
03.-06.12.	Black Hat Europe 2018 (Blackhat, London/UK)
27.-30.12.	35C3 – 35. Chaos Communication Congress 2018 (Messe Leipzig, Leipzig)
Januar 2019	
18.-20.01.	ShmooCon 2019 (The Shmoo Group, Washington/US)
21.-23.01.	Omnisecure 2019 (in TIME berlin, Berlin)
Februar 2019	
06.-07.02.	26. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
20.-21.02.	29. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
März 2019	
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-21.02.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Der Beuth Verlag hat das Taschenbuch 408 zum Informationssicherheitsmanagement herausgegeben. Es enthält acht Normen aus der ISO270xx-Familie sowie die DIN 66398 und ist mit € 180 sogar günstiger als je zwei der enthaltenen Normen zum Einzelpreis. Ein Weihnachts-Schnäppchen...

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Dr. Volker Hammer, Michael Knopp, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Dezember 2018



Es wird geschehen.

Seit Jahrzehnten verstehen wir Informationssicherheit in erster Linie als Prävention: Wir versuchen zu verhindern, dass etwas passiert, was nicht passieren soll.

Das ist nicht grundsätzlich falsch. Allerdings wachsen mit immer mehr Webanwendungen, IoT-Lösungen und Cloud-Angeboten die Zahl der angreifbaren Systeme, durch die zunehmende Abhängigkeit der Geschäftsprozesse das Schadenspotential und die Wahrscheinlichkeit, dass eine unentdeckte Schwachstelle eines Tages wirksam ausgenutzt wird.

Wir müssen daher davon ausgehen, dass Sicherheitsvorfälle passieren werden. Und uns darauf vorbereiten. Denn der Schaden entsteht nach dem Vorfall – und lässt sich in der Regel durch schnelles und richtiges Reagieren wenigstens begrenzen.

Genau darauf aber sind Unternehmen (Rechenzentren ausgenommen) meist schlecht vorbereitet. Wer verfügt denn über ein ernsthaft und regelmäßig erprobtes Notfallkonzept – nicht in der Schublade, sondern in den Köpfen der Mitarbeiter? Daher werden Sicherheitsvorfälle oft zum Desaster. Denn wo soll ein Unternehmen kurzfristig Hilfe suchen, wenn es keine Sicherheitsexperten im Haus hat? Wem kann es vertrauen – und wie wahrscheinlich ist es, dass sich kurzfristig ein geeigneter und verfügbarer Experte findet?

Diesem Problem rückt Baden-Württemberg nun mit einer Cyberwehr zu Leibe: Eine zentrale Telefonnummer mit Erstberatung und einem lokalen Netzwerk von qualifizierten (und zukünftig zertifizierten) Notfallexperten, aus dem kurzfristig ein Team zusammengestellt werden kann, das hilft, den Schaden vor Ort einzudämmen.

Wenn das vom Innenministerium des Landes finanzierte Pilotprojekt, das Anfang 2019 auf alle IHK-Unternehmen der Region Karlsruhe ausgedehnt wird, erfolgreich sein sollte, könnte dies eine Blaupause für Deutschland werden. Die Chancen stehen jedenfalls besser als beim Ansatz des BSI vom Oktober 2016...



Inhalt

Es wird geschehen.

Security News

Der Diesel und der Datenschutz

Zwei-Faktor-Trojaner

Der Schlüssel und die Fußmatte...

Facebook und der Datenschutz

Stille Kundenrückgewinnung

Secorvo News

Secorvo Seminare

Gut gehört und schon gehackt.

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Der Diesel und der Datenschutz

Die Wellen des Diesel-Skandals haben nun auch den Datenschutz erreicht. Der Bundesrat hat in seiner Stellungnahme vom 14.12.2018 zu einer Änderung des Straßenverkehrsgesetzes erhebliche Bedenken zur verfassungsrechtlichen Zulässigkeit der vorgesehenen Verarbeitung personenbezogener Daten geäußert und den Entwurf abgelehnt.

Der Entwurf sieht zur Durchsetzung von Fahrverboten eine Befugnis zum automatisierten Abgleich von KfZ-Kennzeichen sämtlicher Fahrzeuge in der Verbotszone mit dem Zentralen Fahrzeugregister vor. Weitere verarbeitete Daten sind Bilder von Fahrzeug und Fahrer, die relevanten Fahrzeugmerkmale und Ort sowie Zeit der Verkehrsteilnahme. Die Erhebung darf bei Zielgefährdung sogar verdeckt erfolgen. Die Daten von berechtigten Fahrzeugen werden unverzüglich gelöscht, positive Abgleiche aber erst ab Versand an die zuständige Ordnungsbehörde oder nach sechs Monaten. Die dreimonatige Verjährungsfrist aus § 26 Abs. 3 StVG wird damit um das Doppelte überschritten.

Der Bundesrat beruft sich in seiner Ablehnung auf das Urteil des Bundesverfassungsgerichts zum Kennzeichen-Scannen, das klare Grenzen für Abgleichprozesse formuliert. Durch die lange Aufbewahrungsfrist bis zur Durchführung des Abgleichs und durch die umfasste dauerhafte, nicht nur stichprobenweise Erfassung seien diese überschritten.

Da die Überschreitungen behebbar sind und die Ablehnung das Gesetzgebungsverfahren nicht beendet, werden automatisierte Kontrollen und Kennzeichenerfassungen in den Innenstädten damit nicht vom Tisch sein.

Der Vorgang zeigt jedoch erneut, wie weit datenschutzrechtliche Gestaltungsanforderungen reichen.

Zwei-Faktor-Trojaner

Am 13.12.2018 veröffentlichte ESET einen Bericht über einen neuen Android-Trojaner, der die PayPal-Bezahlapplikation angreift. Wie so oft wird die Trojaner-App – getarnt als vermeintlich nützliche Anwendung – über den Store eines Drittanbieters installiert (und nicht über Googles offiziellen App-Store). Besonders ist, dass der Trojaner sich in die Anmeldung an PayPal einklinkt und der Angriff sogar – da es die „echte" Anmeldung an der Bezahl-App ist – funktioniert, wenn eine 2-Faktor-Authentisierung genutzt wird.

Daraus lernen wir: Ein zweiter Faktor allein erhöht die Sicherheit nicht – schließlich können wir mit Alkohol im Blut auch nicht dadurch sicherer Auto fahren, dass wir uns anschnallen. In unserem Fall bestünde eine vorsichtige „Fahrweise" darin, nicht einfach beliebige, vermeintlich nützliche Apps und erst recht nicht aus irgendwelchen Dritt-Stores zu installieren – unabhängig davon, ob man einen zweiten Faktor nutzt oder nicht.

Wer es wirksam sicherer haben möchte, dem sei empfohlen, aus dem zweiten Faktor einen unabhängigen zweiten Faktor zu machen – indem dieser auf einem separaten Gerät und nicht auf dem empfangen wird, auf dem die PayPal App läuft.

Der Schlüssel und die Fußmatte...

...kommen einem in den Sinn, wenn man die von zwei Forschern der Radboud University am 05.11.2018 veröffentlichte Studie Self-encrypting deception: weaknesses in the encryption of solid state drives (SSDs) liest. Die Autoren stellen darin ihre Untersuchung handelsüblicher selbstverschlüsselnder Festplatten vor und kommen zu dem erschreckenden Ergebnis, dass sich bei allen Produkten die Daten leicht entschlüsseln lassen. Für jedes der untersuchten Festplattenmodelle wird im Detail beschrieben, wie die Datenverschlüsselung mit wenig Aufwand rückgängig gemacht werden kann.

Für Microsoft war die Studie Anlass genug, bereits einen Tag später den Sicherheitshinweis ADV180028 zu veröffentlichen – denn Bitlocker ersetzt per Default, sofern möglich, die Softwareverschlüsselung durch eine von der Festplatte angebotene Hardwareverschlüsselung. Diese Bitlocker-Option sollte umgehend deaktiviert werden.

Facebook und der Datenschutz

Bereits am 26.09.2018 bestätigte der bayrische Verwaltungsgerichtshof mit einem nun veröffentlichten Beschluss die Untersagung der Nutzung von *Facebook Custom Audience*, sofern dem Werbetreibenden keine Einwilligung der Betroffenen vorliegt.

Mit *Custom Audience* bietet Facebook Werbekunden an, zur Schaltung von gezielten Werbekampagnen eine Liste mit Hashwerten von Kunden-E-Mail-Adressen zu übermitteln und Selektionskriterien wie Alter, Interessen und weitere Eigenschaften festzulegen. Facebook gleicht die erhaltenen Daten mit seinem Mitgliederstamm ab und spielt die Werbung bei den Facebook-Nutzern aus, bei denen die Kriterien zutreffen.

Das Bayerische Landesamt für Datenschutzaufsicht hatte im Januar 2018 einem Shop-Betreiber die Nutzung untersagt und die Übermittlung der Liste als Übermittlung gewertet. Diese Einschätzung teilt

der bayerische VGH: Eine Auftragsverarbeitung sei dies nicht, da Facebook die beworbenen Mitglieder selbständig auswähle und dem Auftraggeber keine Kontrolle möglich sei. Zwar erging die Entscheidung noch auf Grundlage des BDSG aF, sie ist jedoch in den Wertungen vollständig auf die DSGVO übertragbar. Da in der Übermittlung selbst bei Daten, die zu Werbezwecken genutzt werden dürften, eine Zweckänderung läge, fordert der VGH eine Einwilligung der betroffenen Facebook-Nutzer.

Ungeachtet der hinsichtlich Facebook bestehenden Transparenzbedenken und der Einzelentscheidung ziehen die Ausführungen des Gerichts einen sehr engen Rahmen für die Auftragsverarbeitung, wenn der Auftragnehmer nicht vollständig offengelegte, aber durch Anweisungen bestimmte Verarbeitungen vornimmt. Der Entscheidung kommt daher eine über den konkreten Dienst hinaus gehende Bedeutung zu.

Stille Kundenrückgewinnung

Aufgrund der unüberschaubaren Fülle an Apps haben wir als Smartphone-Nutzer die Qual der Wahl: Wir installieren und deinstallieren, wie es uns gefällt. Mit erfolgter App-Löschung sind auch alle Daten auf unserem Smartphone weg. Aber sind sie es auch beim App-Anbieter?

Am 22.10.2018 informierte Bloomberg über eine neue Methode, mittels welcher App-Anbieter durch so genannte *Silent Push Notifications* verlorene Kunden wiedergewinnen können. Bei diesen Datenpaketen handelt es sich um Remote-Mitteilungen, die im Hintergrund und ohne weitere Hinweise (z. B. Ton oder Symbol) erfolgen und bspw. Inhaltsaktualisierungen ermöglichen.

Das Vorgehen kommt jedoch auch für Marketing Zwecke zum Einsatz. Die *Notifications* dienen dabei als Basis für ein Tracking des Nutzerverhaltens. Bleiben die erwarteten Antworten auf die *Notifications* aus, wird die entsprechende App als gelöscht eingestuft. Die Verknüpfung von sog. „Deinstallations-Trackern“ mit dem eigenen Smartphone ermöglicht dann die Schaltung gezielter Werbung zur Kundenrückgewinnung. Solche Deinstallations-Tracker werden bspw. von Adjust oder CleverTap angeboten.

Betroffene Enduser können das Schalten von Werbung beschränken, indem das Ad-Tracking entsprechend eingeschränkt wird. Noch ungeklärt ist allerdings die Frage, ob dieses Vorgehen gegen Nutzungsbestimmungen bspw. von Apple oder Google verstößt.

Secorvo News

Secorvo Seminare

Wem noch ein Weihnachtsgeschenk für sein Team fehlt: Wie wäre es mit einer Weiterbildung für das Jahr 2019? Das Seminarangebot und die Termine unserer PKI-, T.I.S.P.- und T.P.S.S.E.-Seminare (alle ab März 2019) sowie die Möglichkeit zur Online-Anmeldung finden Sie – noch rechtzeitig vor der Bescherung – unter www.secorvo.de/seminare. Wir freuen uns auf Ihre Teilnahme...

Gut gehört und schon gehackt.

Oder: Wie Sennheiser das TLS-Protokoll aushebelte. Leser der Security News kennen die Hintergründe (SSN 10/2018): Ein klitzekleiner „Workaround“ der Entwickler wuchs sich zu einem Sicherheits-Desaster für alle betroffenen Systeme aus: Eine Design-Schwachstelle im Zertifikatsmanagement der Software Sennheiser HeadSetup unterhöhlte ohne Wissen der Nutzer die Sicherheit aller TLS-Verbindungen – für die Beseitigung der Schwachstelle war die Mitwirkung von Microsoft erforderlich. Dass ein solches Desaster überhaupt möglich war, hatte allerdings mehrere Ursachen, für die nicht ausschließlich Sennheiser verantwortlich gemacht werden sollte.

Beim Jahresauftakt-Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 21.02.2019 zeigen die Secorvo-Experten André Domnick und Hans-Joachim Knobloch, wie durch die Schwachstelle ein Man-in-the-Middle-Angriff auf TLS gelingt, stellen dar, gegen welche lang bekannten Design-Prinzipien für sichere Software verstoßen wurde und wie eine sichere Lösung hätte aussehen können. Abschließend betrachten sie einige zentrale Grundprinzipien, gegen die Entwickler nie verstoßen sollten – erst recht nicht bei der Nutzung von Zertifikats-basierten Sicherheitslösungen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Januar 2019	
18.-20.01.	ShmooCon 2019 (The Shmoo Group, Washington/US)
21.-23.01.	Omnisecure 2019 (in TIME berlin, Berlin)
22.-25.01.	AppSec Cali 2019 (OWASP Foundation, California/USA)
Februar 2019	
06.-07.02.	26. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
20.-21.02.	29. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.02.	Gut gehört und schon gehackt. Oder: Wie Sennheiser das TLS-Protokoll killte. (KA-IT-Si, Karlsruhe)
März 2019	
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-29.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Im August 2018 veröffentlichte das US Government Accountability Office einen Untersuchungsbericht zum Angriff auf den Finanzdienstleister Equifax, bei dem 2017 Daten von ca. 143 Mio. US-Bürgern kompromittiert wurden. Der Bericht veranschaulicht sehr gut, welche katastrophalen Folgen auch einfache Schwachstellen haben können...



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2019



Protokoll

Ein Protokoll ist die Niederschrift einer Ereignisabfolge – oder die Beschreibung eines festgelegten Ablaufs. In der Kommunikationstechnik spielen Protokolle eine zentrale Rolle: Als standardisierte Ablaufbeschreibungen für den Austausch von Daten zwischen Endsystemen.

Eine der größten Herausforderungen der Kryptografie ist die Entwicklung „sicherer" Protokolle – Ablaufbeschreibungen für einen Datenaustausch, der bestimmte Sicherheitseigenschaften (authentisch, vertraulich, verbindlich etc.) besitzt und resistent gegen Angriffe ist. Dabei genügt es nicht, lediglich einzelne kryptografische Mechanismen zu kombinieren: Ohne eine enge Verzahnung der Mechanismen haben Angreifer leichtes Spiel. Ein Beispiel: So reicht eine (gar einseitige) Authentifikation der Endsysteme zu Beginn des Protokolls nicht aus, denn ein Angreifer kann sich später als „Man-in-the-Middle" in die Verbindung einklinken. Die Authentifikation muss gegenseitig erfolgen und mit weiteren Mechanismen über alle Datenpakete aufrechterhalten werden. Wie komplex und fehleranfällig das im Konkreten sein kann, haben viele erfolgreiche Angriffe auf kryptografische Protokolle gezeigt. Dafür verstehen Protokoll-Designer inzwischen einigermaßen, worauf es ankommt.

Ähnliches gilt für Abläufe im echten Leben. Zahlreiche Angriffe wie die Skimming-Attacken an Geldautomaten oder die automatische Überwindung von Captchas, die Angreifer auf Erotik-Seiten weiterleiten, um sie dort von Menschen lösen zu lassen, sind nichts anderes als „analoge" Man-in-the-Middle-Angriffe. Auch das 2018 erstmals aufgetretene „Job Scamming" gehört in diese Kategorie: Mit falschen Stellenangeboten werden Bewerber zur Versendung fotografierter Ausweispapiere oder zu einem Video-Ident-Verfahren verleitet – und diese vom Angreifer für die Eröffnung eines (Geldwäsche-) Kontos verwendet.

Dabei könnte man inzwischen von den Protokoll-Designern lernen.



Inhalt

Protokoll

Security News

Schwarzer Tag für die Biometrie

PKI in Entwicklungsumgebungen

Drum prüfe, wer sich ewig bindet

Patchen ist gut...

Eine für alle

Secorvo News

Secorvo Seminare

Teamzuwachs

Gut gehört und schon gehackt.

Veranstaltungshinweise

secorvo
security consulting

Security News

Schwarzer Tag für die Biometrie

Alle Jahre wieder beschert der Chaos Communication Congress zwischen Weihnachten und Neujahr einige interessante Angriffe. So kippten Julian und Starbug am 28.12.2018 auf dem 35c3 mit ihrem Vortrag „Venenerkennung hacken“ (Video) einen der letzten Hoffnungsträger biometrischer Systeme: die Venenerkennung.

Handvenen sind ein in Hochsicherheitsumgebungen (wie beispielsweise der Zentrale des BND in Berlin) beliebtes biometrisches Authentifikationsmerkmal, da ihre Analyse bisher als eines der sichersten Verfahren galt. Da die Systeme berührungslos arbeiten sind sie zudem für öffentliche Anwendungen wie Geldautomaten oder Hygienebereiche wie Krankenhäuser besonders gut geeignet. Die Sicherheitsforscher konnten jedoch zeigen, dass ein Foto einer Hand, aufgenommen mit einer Kamera ohne Infrarotfilter aus mehreren Metern Entfernung, und etwas Nachbearbeitung genügen, um mittels eines Laserdruckers und einfachem Bienenwachs eine Attrappe zu erstellen, die von Handvenenscannern akzeptiert wird. Getäuscht wurden auf diese Weise sowohl die Handflächen- als auch die Fingervenenerkennung. Trotz der (vom Hersteller behaupteten) Lebenderkennung der Zutrittskontrolllösung wurde die Attrappe nicht zurückgewiesen.

Die Forscher skizzierten weitere Angriffsszenarien wie einen in einem berührungslosen Handtrockner eingebauten Raspberry Pi mit Kameramodul, der ausreichend gute Bilder für einen erfolgreichen Angriff liefert. Damit werden sichere Biometrieverfahren langsam knapp.

PKI in Entwicklungsumgebungen

Wer PKI-Anwendungen nicht nur nutzt sondern auch selbst entwickelt oder in einer Testumgebung betreibt, steht gleich vor einem doppelten Dilemma: Einerseits sind Test- und Entwicklungssysteme oft nicht sicher genug – sie werden nicht auf dem gleichen Sicherheitsniveau betrieben wie Produktivsysteme. Schlüssel zu Zertifikaten sind dort weniger geschützt, Sperrprozesse oft nicht sorgfältig umgesetzt, und daher kann das Vertrauensniveau einer produktiven PKI leiden.

Andererseits sind produktive PKIs oft zu sicher – Zertifikate für Test und Entwicklung werden „auf Zuruf“ benötigt; sorgfältige manuelle Validierungsschritte bremsen die Entwicklungsarbeit aus. Hinzu kommt, dass fehlerträchtige Ereignisse wie die Sperrung oder der Ablauf eines Zertifikats in einem verglichen mit dem späteren Produktivbetrieb kurzen Entwicklungszeitplan meist nicht auftreten – Test-Zertifikate sollten daher eine deutlich kürzere Gültigkeit haben als in einer Produktivumgebung.

Eine schlechte Lösung für dieses Dilemma ist, bei Test- und Entwicklung mit selbstsignierten Zertifikaten und den üblichen, „wegzuklickenden“ Meldungen zu arbeiten. Eine aufwändige ist es, eine separate zweite PKI zu betreiben, deren Root-CA nur in der Entwicklung und für Tests vertraut wird.

Einen Mittelweg geht das von einem Google-Entwickler am 07.01.2019 veröffentlichte Paket mkcert. Es bietet einen einfachen Zugang zu einer ad-hoc erstellten OpenSSL-CA und platziert deren Zertifikat in alle gängigen lokalen Root-Stores. Eine künftige Version soll auch eine Zertifikatsbeantragung per ACMEv2 unterstützen. Für viele Test- und Entwicklungsumgebungen könnte dies die gesuchte Lösung sein.

Drum prüfe, wer sich ewig bindet

Aller europäischen Vereinheitlichung zum Trotz gibt es – nach wie vor – auch außerhalb der DSGVO und des neuen BDSG Datenschutzbestimmungen. Am 18.12.2018 hat das Bundessozialgericht (BSG) auf Grundlage des § 284 SGB V eine datenschutzrechtliche Entscheidung zu elektronischen Gesundheitskarten getroffen.

Die Versicherten (ausgenommen Kinder und Personen, die dazu außerstande sind) müssen den Krankenkassen Passbilder zur Ausstellung der elektronischen Gesundheitskarte zur Verfügung stellen. Wie dies zu geschehen hat ist gesetzlich nicht geregelt. Nach dem Urteil des BSG steht nun fest, dass die Krankenkassen die Bilder nach der Ausstellung der Karte unverzüglich zu löschen haben.

Dies entspricht dem Grundsatz der Zweckbindung und der Datensparsamkeit. Es ist zu begrüßen, dass die Bilder nicht dauerhaft, etwa zur Ausstellung von Ersatzkarten o. ä. gespeichert werden dürfen, auch wenn ganz offensichtlich ist, dass dies sowohl für die Kassen als auch für die Versicherten einen Mehraufwand bedeutet, wenn eine Karte abgelaufen, verloren gegangen oder auf andere Weise abhandengekommen ist.

Anderes gilt bei Ausweispapieren wie dem Reisepass, Personalausweis oder der Fahrerlaubnis. Hier liegen der Speicherung andere gesetzliche Ermächtigungen (PassG, PAuswG, StVG) zugrunde, die es den Behörden erlauben, die Bilder auch nach Erstellung der Ausweisdokumente weiter zu speichern.

Dabei dürfen die Daten im Fahrerlaubnisregister nach § 61 Absatz 4 StVG nur bis zur Vollendung des 110. Lebensjahres gespeichert werden dürfen. Was auch immer mit dieser Begrenzung bezweckt wurde – sie könnte sich eines Tages noch rächen...

secorvo
security consulting

Patchen ist gut...

...zum Schutz vor (bekannten) Sicherheitsschwachstellen. Das haben wir alle seit Jahren immer wieder gehört (und weitergesagt). Aber Patchen aus einer verlässlichen, integren Quelle ist besser. Das mussten all jene schmerzlich lernen, die im Zeitraum zwischen (vermutlich) Juli 2018 und Januar 2019 Software vom „PHP Extension and Application Repository“ (PEAR) auf ihrem Webserver installiert haben. Denn wie die Betreiber des Repositories am 19.01.2019 mitteilten, war mindestens eines der Installationspakete in diesem Zeitraum mit Schadsoftware bestückt.

Während immer mehr kommerzielle Softwarehersteller ein ISO 27001-Zertifikat für ihr Security Management vorweisen, scheinen manche Open-Source-Softwarequellen zwar mit viel Enthusiasmus zu arbeiten, aber dem sicheren Betrieb noch immer wenig Aufmerksamkeit zu widmen.

Angesichts geradezu inflationärer Security-Labels und -Zertifizierungen wäre ein Label für professionell sicher betriebene und regelmäßig auditierte Open Source Repositories ein deutlicher Fortschritt. So wie einige große OpenSSL-Anwender das am 21.01.2019 veröffentlichte Security Audit der TLS-1.3-Implementierung von OpenSSL mitfinanziert haben fänden sich bestimmt Sponsoren, denen die Integrität der von ihnen genutzten Softwarepakete am Herzen liegt.

Eine für alle

Die französischen Datenschutz-Aufsichtsbehörde CNIL hat am 21.01.2019 ein 50 Millionen Euro schweres Bußgeld gegen Google verhängt. Nach dem mit der DSGVO eingeführten „One-Stop-Shop“-Prinzip soll es bei grenzüberschreitenden Verarbeitungen für betroffene Unternehmen nur einen einzigen Ansprechpartner in Europa geben, die sogenannte „federführende Aufsichtsbehörde“, falls eigentlich mehrere verschiedene Aufsichtsbehörden zuständig wären. Dann müssen Unternehmen nur mit einer Behörde kommunizieren, es gibt nur ein Bußgeld – und damit zugleich mehr Rechtssicherheit. Die federführende Behörde muss sich mit den anderen zuständigen Datenschutzbehörden abstimmen.

Vor diesem Hintergrund stellt sich die Frage, was in Deutschland passiert, wenn es zwar keinen grenzüberschreitenden, wohl aber einen Verstoß gibt, der mehrere Bundesländer betrifft. Denn dann sind bis zu 18 Datenschutzbehörden zuständig. Zwar bezieht sich die Regelung in der DSGVO auf grenzüberschreitende Verstöße, aber die EU-weit geltenden Maßstäbe müssten auch innerhalb des Bundesgebietes angewendet werden, so dass sich die Landesdatenschutzbehörden untereinander und mit der federführenden Behörde abstimmen müssten, also derjenigen, in deren Bundesland das gegen die DSGVO verstoßende Unternehmen seinen Sitz hat.

Secorvo News

Secorvo Seminare

Im März 2019 starten wir mit einem PKI- (**18.–21.03.2019**), T.I.S.P.- (**25.–29.03.2019**) und „IT-Sicherheit heute“-Seminar (**02.–04.04.2019**) in die Weiterbildungs-Saison 2019. Die vollständigen Programme und eine Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/seminare. Wir freuen uns auf Ihre Teilnahme!

Teamzuwachs

Ab dem 01.02.2019 verstärkt Jannis Pinter das Secorvo-Team. Als Informatiker mit mehreren Jahren Erfahrung in der IT-Sicherheit bringt er insbesondere vertiefte technische Kenntnisse über Public Key-Infrastrukturen mit.

Gut gehört und schon gehackt.

Oder: Wie Sennheiser das TLS-Protokoll aushebelte. Leser der Security News kennen die Hintergründe (SSN 10/2018): Ein klitzekleiner „Workaround“ der Entwickler wuchs sich im vergangenen Herbst zu einem Sicherheits-Desaster für alle betroffenen Systeme aus. Eine Design-Schwachstelle im Zertifikatsmanagement der Software Sennheiser Head-Setup unterhöhlte ohne Wissen der Nutzer die Sicherheit aller TLS-Verbindungen – für die Beseitigung der Schwachstelle war die Mitwirkung von Microsoft erforderlich. Dass ein solches Desaster überhaupt möglich war, hatte allerdings mehrere Ursachen, für die nicht ausschließlich Sennheiser verantwortlich gemacht werden sollte.

Beim Jahresauftakt-Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 21.02.2019 zeigen die Secorvo-Experten André Domnick und Hans-Joachim Knobloch, wie durch die Schwachstelle ein Man-in-the-Middle-Angriff auf TLS gelingt, stellen dar, gegen welche lang bekannten Design-Prinzipien für sichere Software verstoßen wurde und wie eine sichere Lösung hätte aussehen können.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2019	
06.-07.02.	26. DFN-Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
20.-21.02.	29. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.02.	Gut gehört und schon gehackt. (KA-IT-Si, Karlsruhe)
März 2019	
13.-14.03.	secIT 2019 (Heise Medien GmbH&Co.KG, Hannover)
14.-15.03.	Future Security 2019 (Fraunhofer VVS, Nürnberg)
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-29.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
29.03.	SECMGT-Workshop: IoT – ein Thema für den CISO? (GI-Fachgruppe SECMGT, Frankfurt/Main)
April 2019	
02.-04.04.	IT-Sicherheit heute – praxisnah, aktuell, kompakt (Secorvo, Karlsruhe)
09.-10.04.	Datenschutztage 2019 (FFD Forum für Datenschutz, Wiesbaden)
11.-12.04.	Security Forum 2019 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-26.04.	DFRWS EU Conference (DFRWS, Oslo/NOR)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Hans-Joachim Knobloch, Friederike Schellhas-Mende

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Februar 2019



Datenschützer auf der Erbse

Es war einmal ein Unternehmer, der wollte einen Datenschützer bestellen. Aber das sollte ein wirklicher Datenschützer sein. Da reiste er in der ganzen Welt herum, um einen solchen zu finden, aber überall fehlte etwas. Datenschützer gab es genug, aber ob es wirkliche Datenschützer waren, konnte er nie herausfinden. Immer war da etwas, was nicht ganz in Ordnung war. Da kam er wieder nach Hause und war ganz traurig.

Eines Tages brach plötzlich der Umsatz des Unternehmens ein, es war ganz entsetzlich. Da klopfte es am Haupteingang, und der Unternehmer ging hin, um aufzumachen. Es war ein Datenschützer, der draußen vor dem Tor stand. Wie hatte ihn der Konjunktureinbruch gebeutelt! Das Wasser lief ihm in die Schuhe hinein und zu Löchern wieder hinaus. Aber er sagte, dass er ein wirklicher Datenschützer sei. ‚Ja, das werden wir schon erfahren!' dachte der CIO, aber er sagte nichts, ging in das Rechenzentrum, löschte alle personenbezogenen Daten und versteckte in einem Verzeichnis eine Geburtstagsliste. Dann nahm er hundert beliebige Dateien, legte sie in demselben Verzeichnis ab und verschob das Verzeichnis in eines von hundert Unterverzeichnissen.

Den ganzen nächsten Tag ließ er den Datenschützer nach Datenschutzverstößen suchen. Am Abend fragte er ihn, wie er das Datenschutzniveau bewerte. „Oh, entsetzlich schlecht!" sagte der Datenschützer. „Ich habe etwas Grässliches entdeckt! Eine Geburtstagsliste ohne Einwilligung. Es ist ganz entsetzlich!" Daran konnte man sehen, dass er ein wirklicher Datenschützer war, da er in einem von hundert Verzeichnissen mit hundert Dateien die Geburtstagsliste entdeckt hatte. So feinfühlig konnte niemand sein außer einem echten Datenschützer. Da bestellte ihn der Unternehmer, denn nun wusste er, dass er einen wirklichen Datenschützer gefunden hatte. Und die Geburtstagsliste kam zur Warnung in einen Schaukasten, wo sie heute noch zu sehen ist, wenn sie niemand gestohlen hat.



Inhalt

Datenschützer auf der Erbse

Security News

Encryption – Back to the Roots

TLS 1.3 auf dem iPhone

Grundschutz-Kompendium 2019

Datenkrake mit App-Zertifikaten

Kartellamt macht Datenschutzaufsicht

Steinige Anpassung

Secorvo News

Weiterer Black Belt

Nächste Seminare

Kaltblütig.

Veranstaltungshinweise

secorvo
security consulting

Security News

Encryption – Back to the Roots

Schon bevor 1977 die öffentliche Standardisierung von Verschlüsselungsverfahren mit dem DES Fahrt aufnahm suchten neben den Geheimdiensten auch kommerzielle Unternehmen nach effizienten und zugleich sicheren Algorithmen. So basierte der DES auf der einige Jahre zuvor bei IBM von Horst Feistel entwickelten Chiffre Lucifer, und bei der Wahl des DES-Nachfolgers AES wurde ausdrücklich auch auf eine gute Performance auf einfachsten CPUs geachtet.

Dennoch wäre die Verschlüsselung des kompletten Speichers eines TV-Sticks oder Billig-Handys per AES auch heute noch recht langsam. Daher werden bspw. unter Android Geräte mit einer AES-Leistung unter 50 MB/s nicht verschlüsselt – trotz der seit Version 6 obligatorischen Data Storage Encryption.

Am 07.02.2019 präsentierten Google-Forscher nun unter dem Namen Adiantum einen Algorithmus, mit dem der Datenspeicher eines Geräts ohne AES-Beschleuniger-Hardware etwa fünf Mal schneller verschlüsselt werden kann als per AES. Dazu kombinierten sie die von Daniel Bernstein und anderen unabhängigen Forschern entwickelten Algorithmen ChaCha12, Poly1305 und NH mit AES – zu einem Feistel-Netzwerk. Damit gibt es immer weniger Argumente für Gerätehersteller, den Speicher nicht zu verschlüsseln.

TLS 1.3 auf dem iPhone

Die jüngste Version des TLS-Protokolls – TLS 1.3 – wurde im August 2018 standardisiert. Während die meisten Browserhersteller das neue Protokoll bereits in ihren Produkten nachgerüstet haben, sieht es bei den Betriebssystemplattformen hingegen dürftig aus.

Apple kündigte am 29.01.2019 als erster Mobilplattformbetreiber an, dass die kommende Version 12.2 des Mobilbetriebssystems iOS TLS 1.3 unterstützen wird. Apps, Browser und E-Mail-Clients können dann ohne weiteres Zutun Verbindungen mit dem neuen Protokoll aufbauen, sofern die Gegenstelle dieses ebenfalls anbietet. Von Google und Microsoft fehlt bisher die Ankündigung, wann mit einer Unterstützung von TLS 1.3 durch das Betriebssystem gerechnet werden kann.

Im Februar 2019 hatte TLS 1.3 auf den Servern der populärsten 150.000 Webseiten bereits eine Verbreitung von über 11,6% – beachtlich für ein Protokoll, das seit gerade einmal sechs Monaten standardisiert ist. Derweil mehren sich die Stimmen, ältere Protokollversionen abzuschalten. So wollen Mozilla, Google, Apple und Microsoft die Unterstützung für TLS 1.0 und TLS 1.1 in ihren Browsern ab März 2020 einstellen. Webseitenbetreiber sollten bis dahin sicherstellen, dass ihre Webserver mindestens TLS 1.2 beherrschen.

Grundschutz-Kompendium 2019

Am 18.02.2019 veröffentlichte das BSI eine überarbeitete Version des IT-Grundschutz-Kompendiums. Anders als die Ergänzungslieferungen zu den IT-Grundschutz-Katalogen wird die Version nun als „Edition" mit der jeweiligen Jahreszahl bezeichnet. Einige Bausteine wurden ergänzt und zum Teil Überarbeitungen der Inhalte der „Edition 2018" vorgenommen. Gut gefallen hat uns, dass auch geringfügige Änderungen explizit ausgewiesen sind, so dass man mit wenig Aufwand Änderungsbedarf an ggf. bereits durchgeführten IT-Grundschutz-Checks erkennen kann. Die klare Unterscheidung nach Bausteinen (= Soll-Anforderungen) und Umsetzungshinweisen (= Möglichkeiten zur Erfüllung der Anforderungen) wurde beibehalten. Auch mit der zweiten Ausgabe des Kompendiums ist damit aus unserer Sicht die 2017 begonnene Modernisierung des IT-Grundschutzes gelungen.

Datenkrake mit App-Zertifikaten

Zwar ist es unter Apples iOS, anders als in Googles offenem Android-Ökosystem, nicht ohne weiteres möglich, Apps aus anderen Quellen als dem offiziellen App Store zu installieren. Eine Ausnahme macht Apple jedoch: Unternehmen, die am Apple Developer Enterprise Program teilnehmen, können mit Hilfe eines speziell für sie ausgestellten Unternehmenszertifikats eigene In-House-Apps signieren und auf den iOS-Geräten ihrer Mitarbeiter installieren. Genau solch ein Unternehmenszertifikat hat Facebook nun missbraucht, um eine datenschutzrechtlich höchst bedenkliche Marktforschungs-App unter dem Titel „Facebook Research" am App Store vorbei an iOS-Nutzer zu verteilen. Damit nicht genug: Die App erfordert die Installation eines Root-Zertifikats im Trust Store des Geräts, so dass Facebook sogar verschlüsselte Kommunikation mitlesen konnte.

„Wir bessern uns" war wenige Tage vor Bekanntwerden dieses neuerlichen Skandals die Kernaussage des öffentlichen Auftritts von Facebook-Vizechefin Sheryl Sandberg Ende Januar in München. Schon kurz darauf musste jedoch Apple einschreiten und widerrief unverzüglich das Unternehmens-Zertifikat von Facebook. Damit waren nicht nur Facebooks „Research App" sondern auch sämtliche Facebook-internen Apps nicht mehr lauffähig. Inzwischen darf Facebook seine eigenen Apps

wieder signieren, die zukünftig hoffentlich innerhalb des Unternehmens bleiben und nicht erneut dazu genutzt werden, Nutzer im Namen der „Marktforschung“ auszuspionieren.

Kartellamt macht Datenschutzaufsicht

Das Bundeskartellamt schützt als unabhängige Bundesbehörde den Wettbewerb in Deutschland. In dieser Funktion hat es sich nun in die Verarbeitung von Nutzerdaten bei Facebook eingeschaltet, da Facebook eine marktbeherrschende Stellung unter sozialen Netzwerken in Deutschland innehabe. Es unterliege daher auch dem Verbot der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung nach § 19 Abs. 1 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB), insbesondere, da der Umgang mit personenbezogenen Daten für die Stellung des Unternehmens im Wettbewerb maßgeblich ist.

Bislang war die Nutzung von Facebook nur möglich, wenn einer weitreichenden Sammlung von Daten auch außerhalb der Facebook-Seite mit Zuordnung zum Nutzeraccount zugestimmt wurde. Diese Drittquellen umfassen sowohl zum Facebook-Konzern zugehörige Gesellschaften (z. B. WhatsApp, Instagram) als auch bei der Nutzung von Apps und Drittwebseiten anfallende Daten, z. B. Facebook Business Tools wie der „Like“-Button.

Ein Zusammenführen dieser Daten ist nach der Entscheidung des Kartellamts nur zulässig, wenn der Nutzer darin (freiwillig) einwilligt – was außerdem bereits aus Art. 7 Abs. 4 DSGVO folgt.

Dieser Entscheid muss als Präzedenzfall für Online-Medien angesehen werden: Der Datenverarbeitung sind sowohl datenschutzrechtliche als auch kartellrechtliche Grenzen gesetzt.

Steinige Anpassung

Nach der Stellungnahme des Bundesrats vom 19.10.2018 hat der Bundestag das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz (2. DSAnpUG EU) am 08./09.11.2018 an verschiedene Ausschüsse überwiesen. Eine endgültige Fassung gibt es daher weiterhin nicht. Der gegenwärtige Entwurf der Bundesregierung ändert in 155 Artikeln auf 553 Seiten 154 Gesetze. Dementsprechend unübersichtlich ist das Anpassungsvorhaben, zumal nun weitere Änderungsvorschläge der Ausschüsse zu berücksichtigen sind. Darunter auch – vom Bundesrat abgelehnte – Vorschläge zu einer Lockerung der Bestellpflicht von Datenschutzbeauftragten.

Angepasst werden Datenschutzregelungen in den Sozialgesetzbüchern und in Gesetzen über Dateien und Register, zahlreiche medizinrechtliche Bestimmungen, zahlreiche Gesetze des besonderen Verwaltungsrechts, das BSI-Gesetz und das Strafgesetzbuch. Vielfach werden dabei die Betroffenenrechte aus Art. 12-22 DSGVO nach Art. 23 DSGVO eingeschränkt. Nicht berücksichtigt werden bisher das Telekommunikations- und das Telemediengesetz, deren Status damit bis zur Verabschiedung der europäischen ePrivacy-Verordnung weiter unklar bleibt.

Eine öffentliche Diskussion zu den Vorschlägen blieb bislang weitgehend aus. Die zahlreichen Anpassungen werden die Rechtslage jedenfalls nicht einfacher machen, zumal die speziellen Einschränkungen der DSGVO-Pflichten Zweifel an der Reichweite der Öffnungsklauseln nach sich ziehen werden.

Secorvo News

Weiterer Black Belt

Unser Penetrationstester Michael Knöppler ist jetzt ebenfalls Träger eines „Black Belt“: Anfang Januar bestand er die OSCP-„Gürtelprüfung“ – eine weitere fachliche Verstärkung unseres Pentest-Teams.

Nächste Seminare

Wir freuen uns auf Ihre Teilnahme am kommenden PKI- (**18.–21.03.2019**) oder T.I.S.P.-Seminar (**25.–29.03.2019**) – die vollständigen Programme und eine Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

Kaltblütig.

Zum Schutz von Daten vor unberechtigtem Zugriff ermöglichen Microsofts BitLocker und Apples FileVault deren Verschlüsselung – für mobile Geräte im geschäftlichen Umfeld oft eine Compliance-Anforderung. Nur wer das Passwort kennt, kommt an die Daten heran. Dass dies ein Irrglaube ist, haben Sicherheitsforscher bereits 2008 gezeigt: Hatten sie physischen Zugriff auf einen angeschalteten oder „schlafenden“ (Bereitschaftsmodus) Computer, konnten sie das Passwort aus dem Arbeitsspeicher auslesen. Zehn Jahre nach dieser Entdeckung sind die sogenannten Cold-Boot-Angriffe noch immer möglich. Beim nächsten KA-IT-Si-Event am **11.04.2019** werden Andreas Sperber und Daniel Matesic (aramido) live einen solchen Angriff auf einen Computer mit Festplattenverschlüsselung zeigen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2019	
13.-14.03.	secIT 2019 (Heise Medien GmbH&Co.KG, Hannover)
14.-15.03.	Future Security 2019 (Fraunhofer VVS, Nürnberg)
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-29.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
29.03.	SECMGT-Workshop: IoT – ein Thema für den CISO? (GI-Fachgruppe SECMGT, Frankfurt/Main)
April 2019	
09.-10.04.	Datenschutztage 2019 (FFD Forum für Datenschutz, Wiesbaden)
11.-12.04.	Security Forum 2019 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-26.04.	DFRWS EU Conference (DFRWS, Oslo/NOR)
Mai 2019	
06.-09.05.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
13.-17.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.-23.05.	Eurocrypt 2019 (IACR, Darmstadt)
21.-23.05.	16. Deutscher IT-Sicherheitskongress (BSI, Bonn)
22.-23.05.	20. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, Michael Knopp, Sarah Niederer, Jannis Pinter, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2019



Die Heuristikfalle

Computer lösen Aufgaben deterministisch: vorhersehbar und wiederholbar. Dafür füttern wir sie mit Lösungsalgorithmen. Für viele Probleme des echten Lebens (man könnte sagen: für alle, die diesen Titel verdienen) gibt es jedoch keine Lösungsalgorithmen. Da helfen uns bestenfalls *Heuristiken*: Dicker-Daumen-Regeln, die meist zum Ziel führen, aber nicht immer. So hindert uns die Heuristik "meide Unbekanntes", giftige Früchte zu verzehren, lässt uns aber auch vor Menschen mit fremdländischem Äußeren zurückweichen.

Nicht anders funktioniert künstliche Intelligenz, die uns jetzt allerorten begegnet. In vielen Fällen genügen da heuristische Ergebnisse - eine überwiegend richtige Übersetzung ist besser als keine, und auch für eine zu 80% zutreffende Rechtschreibkorrektur sind wir dankbar.

Aber es gibt auch Probleme, die heuristische Erfolgsquoten nicht gut vertragen. So veröffentlichte die Bundespolizei am 11.10.2018 eine Studie über die sechsmonatige Erprobung biometrischer Gesichtserkennung von Straftätern durch Videoanalyse am Bahnhof Berlin-Südkreuz. Drei Gesichtserkennungssysteme, die mit Fahndungsfotos trainiert worden waren, erreichten dabei eine durchschnittliche Trefferquote von bis zu 91,2%; die Falschakzeptanzrate (Anteil der fehlerhaft als "Gesuchter" erkannten Personen) lag bei 0,34%.

Würde das System für ein Jahr an allen Bahnhöfen eingesetzt und mit Fahndungsfotos der 175.000 per Haftbefehl gesuchten Personen gefüttert, dann könnte es - sofern die Gesuchten an wenigstens einer dieser Kamera vorbeieilen – fast 160.000 davon entdecken.

Eine beeindruckende Zahl. Allerdings würden auch 0,34% der Bahnreisenden fälschlich als Täter identifiziert: Bei jährlich 4,669 Milliarden Reisenden wären das etwa 15.875.000 Fehlidentifikationen. Die Erkennungsrate läge damit unter 1% aller Identifizierten – keine grandiose Systemleistung. Und in einer freiheitlichen Ordnung eine wohl kaum erträgliche „Unschärfe“.



Inhalt

Die Heuristikfalle

Security News

Office 365 und der Cloud Act

Reverse Engineering – powered by NSA

Löchrige Container

ACME wird Standard

DSFA leicht gemacht?

OWASP ASVS 4.0

Secorvo News

T.I.S.P. und T.P.S.S.E.

Kaltblütig.

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Office 365 und der Cloud Act

Microsoft bietet mit Office 365 Dienste wie Sharepoint, OneDrive, Teams und Exchange sowie Anwendungen wie Outlook, Word oder Excel für Privatanwender und Unternehmen an. Zur Sicherstellung von Datensicherheit und Datenschutz verpflichtete sich Microsoft zur Umsetzung wirksamer Maßnahmen. Ab Ende 2019 wird Microsoft seine Cloud-Dienste aus Deutschland in neuen Cloud-Regionen bereitstellen, die als „deutsche Region" Teil der globalen Cloud-Umgebung von Microsoft Office 365 sein werden. Damit wird das bisherige Modell von Microsoft Office 365 Deutschland abgekündigt. In den neuen Regionen mit Rechenzentren in Berlin und Frankfurt soll die Speicherung in Deutschland erfolgen, während die Cloud-Dienste aber auch an Microsofts weltweites Cloud-Netzwerk angebunden sind. Für Dienste aus seinen neuen Rechenzentrums-Regionen verspricht Microsoft die Einhaltung der DSGVO und will sich dazu vertraglich verpflichten. Wahrscheinlich wird Microsoft durch dieses Vorgehen unter den am 23.03.2018 in Kraft getretenen Cloud Act fallen (Clarifying Lawful Overseas Use of Data Act), der US-amerikanischen Ermittlungsbehörden Zugriff auf Daten einräumt, die US-Unternehmen auf europäischen Servern speichern. Es erscheint zweifelhaft, dass sich damit die Anforderungen der DSGVO erfüllen lassen.

Reverse Engineering – powered by NSA

Am 05.03.2019 stellte Robert Joyce (NSA) auf der RSA Conference („Come Get Your Free NSA Reverse Engineering Tool!") das Reverse-Engineering-Werkzeug Ghidra vor. Das Tool, dessen Existenz 2017 mit den Wikileaks-Enthüllungen Vault 7 bekannt geworden war, steht nun unter der Apache License 2.0 zur Verfügung. Es konkurriert mit seinem Funktionsumfang und der grafischen Benutzeroberfläche mit dem kommerziellen Werkzeug IDA des Herstellers Hex-Rays, dessen Lizenzkosten jenseits der tausend Euro liegen. Natürlich drängt sich bei einer Anwendung, die die NSA entwickelt hat, sofort die Frage nach Hintertüren auf. Innerhalb weniger Stunden nach Veröffentlichung wurden auch erste gravierende Schwachstellen in Ghidra entdeckt – keine Ausnahme bei „jungen" Open-Source-Projekten –, aber bisher keine Hintertüren. Die Bugs betreffen den Umgang mit dem Debug-Server und das Laden nicht vertrauenswürdiger Extensionen. US-Regierungsstellen haben bereits 32 Projekte im Quellcode im Rahmen ihrer Initiative zum Technologietransfer publiziert; sie erhoffen sich davon eine Beteiligung der Community an der Weiterentwicklung. Zwar sollte man mit dem Einsatz von Ghidra in sensiblen Bereichen noch vorsichtig sein – dennoch ist die Veröffentlichung eine Bereicherung, denn bisher stand kein freies Werkzeug mit ähnlichem Funktionsumfang zur Verfügung.

Löchrige Container

Software ohne Abhängigkeiten ist in der heutigen Zeit kaum noch vorstellbar. Wie problematisch das aus Sicherheitssicht ist, belegt das Unternehmen Snyk in seinem diesjährigen „The State of Open Source Security Report" mit konkreten Zahlen: Die Überprüfung von mehr als einer Million Open-Source-Projekten ergab, dass 78 % der dabei erkannten Schwachstellen auf indirekte Abhängigkeiten zurückzuführen sind. Indirekte Abhängigkeiten sind solche, die von explizit eingebundenen Komponenten benötigt und automatisch mitinstalliert werden. Ein Großteil der Abhängigkeiten in Paketverzeichnissen wie npm, Maven Central oder Ruby Gems sind solche indirekten Abhängigkeiten. Deshalb ist ein klarer Blick auf die Abhängigkeiten eigener Software von großer Bedeutung. Erkennen kann man bekannte Schwachstellen in den Abhängigkeiten z. B. mit dem Scanner von Snyk.

Wenn es – wie bei Containerlösungen – darum geht, die Bibliotheken und Programme eines gesamten Betriebssystems als Abhängigkeiten für den Container zu nutzen, zeichnet sich eine ähnliche Problematik ab: Laut Snyk besitzt jedes der Top 10 Docker Images mindestens 30 bekannte Schwachstellen. Sie gehen meist auf veraltete Bibliotheken im verwendeten Docker Base Image zurück. Als Gegenmaßnahme hilft in der Regel ein Upgrade, in vielen Fällen reicht sogar ein einfacher Rebuild. Auch der Einsatz von minimalen Base Images wie z. B. Alpine Linux trägt zu einer grundlegenden Sicherheits-„Hygiene" bei.

ACME wird Standard

Automatic Certificate Management Environment (ACME) ist ein von der Internet Security Research Group (ISRG) entwickeltes Protokoll zum automatisierten Bezug von TLS-Serverzertifikaten. Es wurde am 11.03.2019 in RFC 8555 als IETF-Standard veröffentlicht. Die ISRG ist die Dachorganisation hinter dem gemeinnützigen Trustcenter Let's Encrypt, das seit 2015 über das ACME-Protokoll kostenfreie, öffentlich gültige TLS-Serverzertifikate ausstellt.

ACME-Clients mit Internet-Zugang beantragen, installieren und erneuern ihre TLS-Serverzertifikate selbsttätig und reduzieren so den Administrationsaufwand erheblich. Auch der Nachweis, dass der Antragsteller berechtigt ist, ein öffentlich gültiges

DV-Zertifikat für den gewünschten Host-Namen zu erhalten, ist im ACME-Protokoll bereits vorgesehen.

Die nun verabschiedete Protokollversion (ACMEv2) schafft Planungssicherheit für die Entwickler alternativer Client- und Server-Implementierungen sowie für andere Trustcenter, die es ihren Nutzern ermöglichen wollen, ohne Änderung der bereits etablierten Prozesse und der Client-Software die Zertifizierungsstelle zu wechseln. Proof of Concept: Let's Encrypt selbst hat über ACMEv2 bereits mehr als 70 Millionen TLS-Serverzertifikate ausgestellt.

DSFA leicht gemacht?

Zum 01.03.2019 hat der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) einen Hinweis auf das PIA-Tool (Privacy Impact Assessment) der französischen Datenschutzbehörde CNIL veröffentlicht. Das Tool ist nicht neu, aber inzwischen auch in deutscher Sprache verfügbar und soll Verantwortlichen die Durchführung von Datenschutz-Folgenabschätzungen (DSFA) erleichtern. Die Oberfläche ist recht benutzerfreundlich und man kann die Folgenabschätzung Schritt für Schritt vornehmen. Die CNIL bietet weitere Hinweise zum Tool samt Youtube-Erklärvideo in englischer Sprache. Allerdings gibt es auch andere, teils komplexere Ansätze als die Methodik der CNIL zur Durchführung von DSFAs.

Eine Herausforderung wird durch die Software jedoch nicht gelöst: die Schwellwertanalyse, mit der vor der Durchführung einer DFSA geprüft wird, ob es sich bei dem abzuschätzenden Prozess tatsächlich um eine „Hochrisikoverarbeitung" handelt. Häufig werden DSFA daher vorsorglich durchgeführt. Um diesen Prozess zu erleichtern, hat der BayLfD eine überarbeitete Orientierungshilfe für Datenschutz-Folgenabschätzungen inklusive Prüfschema veröffentlicht. In der Theorie ist eine DSFA samt Vorprüfung also gar nicht so schwierig – ob sich dies auch so einfach in die Praxis umsetzen lässt, muss sich erst noch erweisen.

OWASP ASVS 4.0

Am 01.03.2019 hat das Open Web Application Security Project (OWASP) Version 4 des Application Security Verification Standard herausgegeben. Im Vergleich zur Vorversion haben sich viele Änderungen ergeben; die inhaltlich bedeutendste ist der Bezug auf NIST 800-63-3 Digital Identity Guidelines für die Abschnitte zu Authentisierung und Session Management, sowie PCI DSS – ein Audit nach ASVS Level 1 deckt die Anforderungen in Abschnitt 6.5 aus PCI-DSS 3.2.1 Abschnitt 6.5 ab. Neu ist auch der Bezug aller Prüfpunkte auf die Common Weakness Enumeration Identifier (CWE) – sehr nützlich für Tester, denn die einzelnen Prüfpunkte werden (wie in den vorangegangenen Versionen) nicht näher erläutert, obwohl einige dieser Punkte durchaus erklärungsbedürftig sind. Darüber hinaus wurde der Abschnitt zu Mobile Security gestrichen, da mittlerweile ein eigener Mobile Application Security Verification Standard (MASVS) existiert. Ebenfalls gestrichen wurde Level 0 ("Cursory"). Mit dem ASVS 4 wurden alle Punkte neu durchnummeriert; zusätzlich wurde eine neue Gliederungsebene eingeführt, da einige Abschnitte im Laufe der Zeit stark angewachsen und unübersichtlich geworden sind. Leider wurde auch die farbliche Unterscheidung der Punkte nach zugehörigem Level abgeschafft; für die Zuordnung eines Prüfpunkts zum Level muss man jetzt genauer hinsehen. Dennoch haben diese Überarbeitungen, vor allem die Anbindung an andere bekannte Werke, dem ASVS sehr gut getan und dürften die Akzeptanz bei Auftraggebern und Testern weiter erhöhen.

Secorvo News

T.I.S.P. und T.P.S.S.E.

Mit deutlich über 1.000 Absolventen ist der T.I.S.P. inzwischen eine nicht nur anerkannte, sondern auch weit verbreitete Berufsqualifikation für IT-Sicherheitsexperten. Das nächste T.I.S.P.-Seminar mit anschließender Zertifikatsprüfung bieten wir Ihnen am **13.–17.05.2019**. In der Woche davor (**06.–09.05.2019**) haben Sie die Gelegenheit, sich als T.P.S.S.E. (TeleTrusT Professional for Secure Software Engineering) zu qualifizieren.

Die detaillierten Seminarprogramme und eine Möglichkeit zur Online-Anmeldung finden Sie hier.

Kaltblütig.

Zum Schutz vor unberechtigtem Datenzugriff bieten Microsofts BitLocker und Apples FileVault deren Verschlüsselung – für mobile Geräte im geschäftlichen Umfeld oft eine Compliance-Anforderung. Nur wer das Passwort kennt, kommt an die Daten heran. Dass dies ein Irrglaube ist, haben Sicherheitsforscher bereits 2008 gezeigt: Hatten sie physischen Zugriff auf einen lediglich gesperrten oder „schlafenden" (Bereitschaftsmodus) Computer, konnten sie das Passwort aus dem Arbeitsspeicher auslesen. Zehn Jahre nach dieser Entdeckung sind die sogenannten Cold-Boot-Angriffe noch immer möglich. Beim nächsten KA-IT-Si-Event am **11.04.2019** werden Andreas Sperber und Daniel Matesic (aramido) live einen solchen Angriff auf einen Computer mit Festplattenverschlüsselung vorführen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2019	
11.-12.04.	Security Forum 2019 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-26.04.	DFRWS EU Conference (DFRWS, Oslo/NOR)
Mai 2019	
06.-09.05.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
13.-17.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.-23.05.	Eurocrypt 2019 (IACR, Darmstadt)
21.-23.05.	16. Deutscher IT-Sicherheitskongress (BSI, Bonn)
22.-23.05.	20. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)
26.-30.05.	OWASP AppSec Tel Aviv 2019 (OWASP Foundation, Tel Aviv/ISR)
Juni 2019	
03.-05.06.	Entwicklertag 2019 (VKSI, GI, ObjektForum, Karlsruhe)
03.-04.06.	DuD 2019 (COMPUTAS Gisela Geuhs GmbH, Berlin)

Fundsache

Über 140 Mal taucht „ji32k7au4a83“ in Datenbanken kompromittierter Passwörter auf. Was auf den ersten Blick verwundert, hat eine simple Erklärung: Im taiwanesischen Zeichenschema lautet der vermeintliche Zufallsstring übersetzt „Mein Passwort“.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Dr. Safuat Hamdy (Gastautor), Hans-Joachim Knobloch, Sarah Niederer, Jannis Pinter, Friederike Schellhas-Mende, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Telefon +49 721 255171-0

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

April 2019



High Noon

Zweifellos eine Sternstunde der Filmgeschichte: das Duell zwischen Recht und Verbrechen, vertreten durch Marshal Will Kane (Gary Cooper) und den Banditen Frank Miller. Fred Zinnemanns Film erzählt auch eine Geschichte von Feigheit und Pflichtbewusstsein, Treue und Mut – aber darum geht es hier nicht. Es ist die Unausweichlichkeit, mit der sich die Handlung von der ersten Filmminute an auf das große Finale hinbewegt, die an amerikanische Cloud-Anbieter denken lässt. Denn ganz ähnlich spitzt sich seit Jahren die Spannung zwischen ihnen und dem europäischen Datenschutzrecht zu.

Es begann mit kleinen Scharmützeln wie der Auseinandersetzung um Google Analytics (wenig überzeugend gelöst durch den AV-Kompromiss des Hamburgischen Datenschutzbeauftragten) oder den gerade vor dem EuGH verhandelten Social Media Plug-ins. Dann kamen 2013 die Enthüllungen Edward Snowdens, die das EU-Parlament zur Verabschiedung der Datenschutz-Grundverordnung (DSGVO) motivierten und dazu beitrugen, das Safe Harbor-Abkommen zu kippen – mit einem EuGH-Urteil, dessen Begründung auch den Standardvertragsklauseln den Boden entzog.

Nun drohen die Cloud-Geschäftsmodelle von Microsoft und Amazon am europäischen Datenschutzrecht zu zerschellen. Zwar reagierte Microsoft schnell: mit einem irischen Rechenzentrum, ausgereiften Verträgen und der Weigerung, einer richterlichen Anordnung Folge zu leisten, die Zugriff auf in Irland gespeicherte Daten verlangte. Da fiel ihnen am 23.03.2018 der US CLOUD Act in den Rücken, der amerikanische Unternehmen verpflichtet, im Ausland gespeicherte Daten auch ohne Rechtshilfeabkommen an US-Behörden herauszugeben – ein Verstoß gegen Artikel 48 der DSGVO. Am 07.11.2018 stellte daher die Datenschutzfolgenabschätzung der niederländischen Aufsichtsbehörde die DSGVO-Konformität von Office 365 in Frage. Fehlt noch, dass der US-EU Privacy Shield (erwartungsgemäß) vor dem EuGH scheitert. Dann ist High Noon. Mit offenem Ausgang.



Inhalt

High Noon

Security News

Firmenprofile in Social Networks

Altlasten und Seitenkanäle I

Zweifel an Office 365

Altlasten und Seitenkanäle II

Europäische Hilfestellung

Hambacher Manifest

Secorvo News

200 Security News

T.I.S.P.-Zertifizierung

Wie souverän ist der Souverän?

11. Tag der IT-Sicherheit

Veranstaltungshinweise

secorvo
security consulting

Security News

Firmenprofile in Social Networks

Die für den 11.04.2019 angekündigte Entscheidung des Bundesgerichtshofes (BGH) in der Sache I ZR 186/17 („Facebook“) mutierte zu einem Aussetzungsbeschluss: Der BGH will zunächst das in Kürze fällige Urteil des EuGH über Social Media Plug-ins (namentlich: Facebook Like Buttons) abwarten. Die bereits am 19.12.2018 veröffentlichten Schlussanträge des Generalanwalts Bobek lassen erwarten, dass der EuGH von einer gemeinsamen Verantwortung ausgehen wird – was dann analog auch für Firmenprofile in Social Networks zutrifft. Solche Profile müssen daher wie Webseiten mit einem Impressum und einer Datenschutzerklärung versehen sein – mindestens als Verlinkung der entsprechenden Erklärungen der Unternehmenswebseite.

Altlasten und Seitenkanäle I

Seit 2005 kann TLS nicht nur mit Zertifikaten, sondern auch mit einem vorab vereinbarten symmetrischen Pre-Shared-Key (PSK) genutzt werden. Israelische Sicherheitsforscher haben am 05.04.2019 einen *Selfie Attack* getauften Angriff auf TLS-PSK (1.3) veröffentlicht, bei dem ein Client durch einen aktiven MITM-Angriff zum „Selbstgespräch“ veranlasst wird – was zu erheblichen Problemen auf höheren Anwendungsschichten führen kann. Entwickler (und Nutzer) betroffener Anwendungen sollten die empfohlenen Schutzmaßnahmen ergreifen oder, besser noch, TLS ausschließlich mit Zertifikaten einsetzen.

Bereits am 06.02.2019 hat eine Forschergruppe um Adi Shamir einen Angriff auf den RSA-Schlüsselaustausch in TLS beschrieben, der Seitenkanäle wie das Cache-Timing nutzt, um trotz diverser Gegenmaßnahmen in neueren Browsern und TLS-Versionen das 1998 von Daniel Bleichenbacher publizierte adaptive Angriffsschema gegen das RSA-Padding nach dem veralteten PKCS#1 v1.5 umzusetzen. Zwar ist ein solcher RSA-Schlüsselaustausch in TLS 1.3 nicht mehr zulässig. Unterstützt ein Server aber auch ältere Protokollversionen mit RSA-Schlüsselaustausch, ist ein Downgrade-Angriff auch gegen TLS 1.3 möglich. Schutz bieten eine komplette Umstellung auf TLS 1.3 oder die Nutzung von Zertifikaten auf Basis von ECC-Verfahren.

Zweifel an Office 365

Bereits am 07.11.2018 hat die niederländische Datenschutzaufsichtsbehörde eine umfangreiche Datenschutz-Folgenabschätzung zu Microsoft Office 365 veröffentlicht. Darin wurden zahlreiche Punkte beanstandet und Microsoft aufgefordert, diese bis April 2019 zu beheben. Die Probleme umfassen nicht nur technische Aspekte wie z. B. die Beobachtung, dass umfangreiche Telemetriedaten „nach Hause gefunkt“ werden, ohne dass die Nutzer dies wissen. Problematisch ist auch, dass Unternehmen mit Sitz in den USA den US-Behörden im Falle von Ermittlungsverfahren aufgrund des CLOUD Act Zugriff auch auf (Cloud-) Server in Europa gewähren müssen, selbst wenn die Voraussetzungen des Art. 48 DSGVO nicht vorliegen.

Nach einer Pressemitteilung des europäischen Datenschutzbeauftragten werden nun auch die vertraglichen Beziehungen zwischen Microsoft und den EU-Behörden überprüft. Ziel ist es herauszufinden, ob hier – wie in den Niederlanden – Datenschutzverstöße festzustellen sind und ob die Datenübermittlungen im Einklang mit Art. 48 DSGVO stehen.

Unternehmen aus Drittstaaten, die Cloud-Dienste in Europa DSGVO-konform anbieten wollen, könnten diese von einem europäischen Anbieter als Treuhänder erbringen lassen, ohne selbst Zugriff auf die Daten zu haben. Aber auch hier steckt der Teufel im Detail: Betreibt der europäische Partner eine Niederlassung in den USA, könnten die US-Behörden durch diese Hintertür zugreifen.

Altlasten und Seitenkanäle II

Auch im neuen WLAN-Sicherheitsstandard WPA3-Personal (SSN 01/2018) haben Sicherheitsforscher mehrere Mängel entdeckt und am 10.04.2019 unter dem Namen *Dragonblood* veröffentlicht, die eine Rekonstruktion des WLAN-Pre-Shared-Key ermöglichen.

WPA3-Personal ersetzt den gegen Offline-Wörterbuchangriffe anfälligen Vier-Wege-Handshake von WPA2-Personal durch SAE – auch als Dragonfly bekannt –, das derartige Angriffe verhindern soll. Um den Übergang zum neuen Protokoll zu erleichtern, definiert WPA3 einen „Transition Mode“, in dem sowohl WPA3- als auch WPA2-Clients unterstützt werden. In diesem Mischbetrieb lässt sich jedoch ein Downgrade auf WPA2 provozieren, wodurch der Angriff wieder möglich wird. Zwei weitere Dragonblood-Angriffe bedienen sich eines Timing- bzw. Cache-Seitenkanals, um den PSK über einen Wörterbuchangriff zu ermitteln. Schließlich wurde ein Downgrade-Angriff entdeckt, der das Sicherheitsniveau auf die schwächste von Client und Access Point unterstützte Diffie-Hellman-Gruppe absenkt.

Einige der Schwächen lassen sich per Software entschärfen; entsprechende Sicherheitsupdates sollten zügig installiert werden. Ein Mischbetrieb von WPA3/WPA2 sollte unbedingt vermieden werden.

secorvo
security consulting

Europäische Hilfestellung

Der Europäische Datenschutzausschuss hat am 09.04.2019 Richtlinien zur Datenverarbeitung bei Diensten der Informationsgesellschaft verabschiedet und zur öffentlichen Konsultation gestellt. In dem 14-seitigen Papier erläutert der Ausschuss seine enge Auslegung des Art. 6 Abs. 1 b) DSGVO: Mit der Erforderlichkeit zur Vertragsdurchführung sollen nur solche Verarbeitungen personenbezogener Daten legalisiert werden, ohne die der Vertrag nicht erfüllt werden kann. Dabei seien auch die Erwartungen der Betroffenen zu berücksichtigen.

Analysen des Nutzerverhaltens, Sicherheitslogs, Speicherungen zu Gewährleistungszwecken oder aufgrund von Aufbewahrungspflichten seien nicht von Abs. 1 b) umfasst, sondern erforderten andere Rechtsgrundlagen. Zweifellos eine zutreffende Klarstellung. Daraus folgt jedoch, dass die Betroffenen gemäß Art. 12 ff DSGVO über diese zu informieren sind. Exzessive Verarbeitungen werden sich so kaum verhindern lassen – die Laienverständlichkeit der Datenschutzerklärung dürfte jedoch leiden.

Hambacher Manifest

Die 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat am 03.04.2019 unter anderem Anforderungen an die datenschutzgerechte Entwicklung von KI-Anwendungen unter dem Titel „Hambacher Erklärung zur Künstlichen Intelligenz“ verabschiedet. Die Anforderungen starten mit dem Grundsatz aus Art. 22 DSGVO, rechtlich relevante Entscheidungen nicht ausschließlich auf automatisierte Prozesse zu stützen sowie auch für Trainingsdaten das Zweckbindungsgebot zu beachten. Datenminimierung, die Entwicklung technischer und organisatorischer Standards, die klare Festlegung von Verantwortlichkeiten sowie der Anspruch, die Entwicklung auch politisch zu steuern und die regelmäßige Durchführung von Datenschutz-Folgenabschätzungen sind weitere Anforderungen.

Kein revolutionärer Wurf – zumal das Mantra der Transparenz nicht kritisch hinterfragt wird. Gerade bei KI-Anwendungen sind Zweifel angebracht, ob diese tatsächlich kurz, verständlich und für den Betroffenen nachvollziehbar dargestellt werden können – und ob dies der richtige Ansatz zum Schutz der Betroffenenrechte ist.

Secorvo News

200 Security News

Sie lesen gerade die 200. Ausgabe der Secorvo Security News. 800 Seiten mit rund 1.500 Nachrichten, die wir für Sie recherchiert, ausgewählt und formuliert haben, ungezählte fachliche Diskussionen und Tassen Kaffee liegen hinter uns. Die Security News haben mehr Leser als die meisten deutschen Fachzeitschriften im Gebiet Informationssicherheit und Datenschutz – und darauf sind wir auch ein kleines bisschen stolz.

Wir würden uns freuen, wenn Sie die Jubiläumsausgabe zum Anlass nähmen, uns in einem kurzen Kommentar zu verraten, was Sie uns schon immer einmal sagen wollten… Unter allen Einsendern verlosen wir die ersten zehn Exemplare der in Kürze erscheinenden dritten Auflage unseres Fachbuchs „Datenschutz und Informationssicherheit“.

T.I.S.P.-Zertifizierung

Kurzentschlossene können sich noch einen Platz auf dem T.I.S.P.-Seminar am **13.–17.05.2019** sichern. Die (über)nächste Gelegenheit zur Zertifizierung Ihrer Kenntnisse in der Informationssicherheit bieten wir am **14.–18.10.2019** (Achtung: nur noch vier freie Plätze, baldige Anmeldung empfohlen).

Wie souverän ist der Souverän?

Angesichts der wachsenden Komplexität von IT-Systemen, dem Eindringen der IT in immer mehr Lebensbereiche und der Zunahme der Verarbeitung personenbezogener Daten ist "digitale Souveränität" nicht mehr lediglich von mangelnder Medienkompetenz bedroht. Beim kommenden KA-IT-Si-Event am **06.06.2019** in Kooperation mit der Initiative Smart Ettlingen zeichnet Dirk Fox die Entwicklung des Internet vom "Schaufenster" zu einer Überwachungsinfrastruktur nach und zeigt auf, welche Verantwortung für die Erhaltung (oder womöglich die Wiederherstellung) von digitaler Souveränität auf die Softwareentwickler von heute und morgen zukommt – und welche Schritte dafür erforderlich sind. Im Anschluss folgt eine Diskussion zum Thema "Digitale Souveränität im internationalen Kontext". Danach haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (Anmeldung).

11. Tag der IT-Sicherheit

Für die Keynote des bereits elften Karlsruher „Tag der IT-Sicherheit“ konnten wir die polnische IT-Security-Expertin Paula Januszkiewicz („*Think and Act Like a Hacker to Protect Your Company's Assets*“) gewinnen. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V. findet am **11.07.2019** im Saal Baden der IHK Karlsruhe statt. Das vollständige Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2019	
06.-09.05.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
13.-17.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.-17.05.	European Identity & Cloud Conference 2019 (KuppingerCole Ltd., München)
19.-23.05.	Eurocrypt 2019 (IACR, Darmstadt)
21.-23.05.	16. Deutscher IT-Sicherheitskongress (BSI, Bonn)
22.-23.05.	20. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)
26.-30.05.	OWASP AppSec Tel Aviv 2019 (OWASP Foundation, Tel Aviv/ISR)
Juni 2019	
03.-05.06.	Entwicklertag 2019 (VKSI, GI, ObjektForum, Karlsruhe)
03.-04.06.	DuD 2019 (COMPUTAS Gisela Geuhs GmbH, Berlin)
05.-06.06.	BvD-Verbandstage 2019 (BvD e.V., Berlin)
13.-14.06.	Annual Privacy Forum 2019 (ENISA, EC DG Connect, Universität Wien, Rom/I)
17.-19.06.	4rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Stockholm/SWE)
24.-25.06.	T.I.S.P. Update Schulung (isits AG, Bochum)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Hans-Joachim Knobloch, Michael Knopp, Jannis Pinter, Friederike Schellhas-Mende.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Mai 2019



Kognitive Verzerrungen

Eine der an Einsichten reichste Lektüre der vergangenen Jahre war für mich die Veröffentlichung des Wirtschaftsnobelpreisträgers 2002, Daniel Kahneman: ‚Thinking, fast and slow' (‚Schnelles Denken, langsames Denken', 2011). Darin deckt der Psychologe Wirkmechanismen des menschlichen Denkens auf, die viele Wunderlichkeiten des Homo Rationalis (von ihm „kognitive Verzerrungen" genannt) verständlich machen.

Ein zentraler Mechanismus ist das Denken in Relationen. Wir kennen das von optischen Täuschungen: Identische Objekte erscheinen im Kontext kleinerer bzw. größerer Objekte unterschiedlich groß – selbst wenn wir um ihre gleiche Größe *wissen*, können wir sie nicht gleich groß *sehen*. Diese Relativität durchzieht unser gesamtes Denken. Der Mechanismus wird besonders offensichtlich bei Entscheidungen in Geldfragen: Nicht der absolute Preis, sondern das Verhältnis zu anderen Preisen ähnlicher Güter entscheidet. Das gilt vor allem, wenn eine Ware oder Leistung keinen allgemein anerkannten, „typischen" Preis besitzt: Eine Uhr für 1.400 € erscheint teuer neben einer für 99 €, aber günstig neben einer für 4.500 €.

Umgekehrt fällt es Menschen schwer, den Wert vieler „abstrakter Güter" wie Bildung, Gesundheit oder Freiheit einzuordnen. Damit erscheinen sie „unvergleichbar", denn sie lassen sich vom menschlichen Gehirn nicht in Relation zu anderen Gütern oder Werten setzen. Wie wertvoll ist unsere Privatsphäre? Und wie hoch der Verlust, wenn z. B. unsere E-Mail-Adresse bekannt wird?

Das ändert sich sofort, wenn ihnen ein Preis zugeordnet wird. Und vielleicht wird dies eines Tages das größte Vermächtnis der DSGVO sein: Über die von den Aufsichtsbehörden verhängten Ordnungsgelder erhält unsere Privatsphäre einen Wert, der sie vergleichbar macht. So wissen wir nun: Die Preisgabe von E-Mail-Adressen in einem Verteiler kostet 2.000 €. Fast so viel wie zwei iPhone XS.



Inhalt

Kognitive Verzerrungen

Security News

ZombieLoad und Firmwareschwachstellen

Spyware Hook

Log-Password-Leaks

Angreifbare Altlasten

Automatisieren statt Aufpassen

Arbeitszeiterfassung und Leistungskontrolle

Secorvo News

Neu: Der PKI-Blog

Wie souverän ist der Souverän?

11. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

ZombieLoad und Firmwareschwachstellen

Gleich zwei Mal machte der Chiphersteller Intel im Mai durch Schwachstellen auf sich aufmerksam. Am 14.05.2019 veröffentlichte Intel das Security Advisory INTEL-SA-00213, in dem mehrere kritische Schwachstellen in der Firmware beschrieben werden. Am selben Tag wurde eine neue Schwachstellenkategorie namens Microarchitectural Data Sampling (MDS) bekannt: Wird der Prozess eines Angreifers auf dem gleichen Kern wie ein Opferprozess ausgeführt, so kann der Angreifer Speicherbereiche des Opfers lesen. Im Kontext von Hyper Threading funktionieren derartige Angriffe besonders gut. Die Fallout, RIDL und ZombieLoad genannten Schwachstellen folgen den Schwachstellen Spectre und Meltdown: Schon wiederholt wurden Schwachstellen sowohl in den Intel CPUs als auch in den Management-Technologien (z. B. der Intel Management Engine) entdeckt. Ursache dieser Schwachstellen sind eine immer höhere Komplexität und Leistungsoptimierung auf Kosten der Sicherheit. So bringen moderne Plattformen diverse schlecht oder gar nicht dokumentierte Features mit, die die Angriffsfläche erhöhen. Für die aktuellen Schwachstellen stehen Sicherheitsupdates bereit, die unverzüglich eingespielt werden sollten.

Spyware Hook

Am 14.05.2019 wurde bekannt, dass die israelische Firma NSO Group eine kritische Schwachstelle in WhatsApp nutzte, um Spyware auf iOS- und Android-Smartphones zu installieren. Dazu genügte ein telefonischer Verbindungsversuch, der nicht einmal in der Anrufliste erscheint.

Kunden der auf Cyberwarfare spezialisierten Firma sind – eigenen Angaben zufolge – Regierungen und deren Sicherheitsbehörden, die damit Terrorismus bekämpfen. In jüngster Vergangenheit wurden Angriffswerkzeuge der NSO Group aber auch gegen Menschenrechtsaktivisten, Journalisten und mindestens einen Anwalt eingesetzt. Meldungen über ähnliche Angriffe, die ebenfalls in Verbindung zur NSO Group stehen, gab es bereits im August 2018.

Aber ganz unabhängig vom Geschäftsmodell des Unternehmens bleibt zu fragen, was von einem Unternehmen zu halten ist, dass entdeckte Sicherheitslücken zu eigenen Geschäftszwecken geheim hält – und damit wissentlich Milliarden Endgeräte weiter potentiellen Angriffen aussetzt.

Log-Password-Leaks

Passwörter sollen nur mit einer geeigneten Hash-Funktion und einem individuellen Salt geschützt gespeichert werden – das ist Best Practice, wie man u. a. beim NIST nachlesen kann. Auch Facebook, GitHub, Google und Twitter wissen das. Trotzdem hatten alle vier Unternehmen in jüngerer Vergangenheit Schwierigkeiten, das beim Umgang mit Nutzerpasswörtern zu beherzigen, wie zuletzt am 21.05.2019 von Google gemeldet: So wurden die eingegebenen Passwörter als „Beifang“ in Log-Dateien des Anbieters protokolliert. Bei Facebook hatten mehr als 20.000 Facebook-Mitarbeiter Zugriff auf diese Protokolle.

Zur Fehlerbehebung ist das Protokollieren von Anfragen äußerst nützlich, aber Passwörter haben darin nichts verloren und dürfen niemals im Klartext gespeichert werden. Dem Endnutzer bleibt nur darauf zu vertrauen, dass die Anbieter in dieser Hinsicht keine Fehler machen. Weil das aber ganz offensichtlich selbst bei großen Anbietern keine Selbstverständlichkeit ist, sollten Endnutzer für jeden Dienst ein anderes Passwort verwenden. Und gegen Vergessen hilft ein Passwortmanager.

Angreifbare Altlasten

Eine Standardinstallation von Windows 10 umfasst neben dem Edge-Browser noch heute den immer weniger gepflegten Internet Explorer (IE). Eine am 28.03.2019 veröffentlichte XXE-Schwachstelle beim Umgang mit MHTML-Dateien (*.mht) erlaubt es Angreifern, über eine manipulierte MHTML-Seite Dateien vom System des Opfers zu laden.

Aus dem Internet heruntergeladene Dateien werden unter Windows mit dem so genannten „Mark of the Web“ (MOTW) versehen – einem speziellen Attribut, welches eine Datei als nicht vertrauenswürdig einstuft und die weitere Verarbeitung einschränkt. Dadurch würde der Angriff normalerweise verhindert, doch der Mechanismus funktioniert nicht ordnungsgemäß beim Download mit Edge, da dieser die Zugriffsberechtigungen der heruntergeladenen Datei durch ein nicht dokumentiertes Sicherheits-Feature so verändert, dass niedrig privilegierte Prozesse wie die des IE die Dateiattribute nicht mehr lesen können. Anstatt die Datei in einem solchen Fall als „nicht vertrauenswürdig“ einzustufen, macht der IE das Gegenteil.

Offizielle Patches für diese Probleme gibt es bisher nicht und Microsoft kündigte lediglich an, dass eine Lösung in einer zukünftigen Version des Internet Explorers „in Erwägung gezogen“ werde. Bis dahin kann man sich vor solchen Angriffen nur schützen, indem man MHTML-Dateien standardmäßig mit einem anderen Programm als dem IE öffnet (z. B. einem Texteditor) oder den Internet Explorer deaktiviert. Alternativ hilft auch der Drittpartei-Patch von 0patch (ohne Gewähr).

Automatisieren statt Aufpassen

Anfang Mai konnten Firefox-Anwender weltweit keine Add-ons mehr ausführen, weil deren Code-Signatur als ungültig erkannt wurde: Das Zertifikat einer Intermediate-CA im Zertifikatspfad der Code-Signing-Zertifikate für Add-on Entwickler war am 04.05.2019 abgelaufen. Die Mozilla-Entwickler hatten als Validierungszeitpunkt den Termin gewählt, an dem das betreffende Add-on geladen wird – und nicht den Zeitpunkt, zu dem die Code-Signatur angebracht wurde. Microsofts Authenticode Code-Signaturverfahren nutzt dazu korrekter Weise Timestamps.

Noch blamabler ist, dass das Intermediate-CA-Zertifikat ohne eine rechtzeitige Erneuerung ablaufen konnte – zumal Mozilla das gleiche Malheur bereits drei Jahre zuvor unterlaufen ist. Dabei sollte die Erneuerung von Zertifikaten und CRLs wo immer möglich automatisiert und der Gültigkeitsstatus aktiv überwacht werden. Besser Aufpassen war noch nie eine gute Empfehlung.

Arbeitszeiterfassung und Leistungskontrolle

Mit Urteil C-55/18 vom 14.05.2019 verpflichtet der EuGH Arbeitgeber, die tägliche Arbeitszeit der Arbeitnehmer zu messen. Was der einen (insbesondere Gewerkschaften und Co.) Freud, da nun endlich die geleisteten Überstunden erfasst werden, ist der anderen Leid: Die Arbeitgeber fürchten einen Rückfall in Stechuhrzeiten, den Wegfall flexibler Arbeitszeitmodelle und Schwierigkeiten im Hinblick auf die Ruhezeiten. Datenschutzrechtlich stellt die Einführung von Systemen zur Zeiterfassung kein großes Problem dar: § 26 BDSG bietet dafür die notwendige Rechtsgrundlage.

Zugleich erwägen viele Unternehmen, Client-Monitoring-Systeme einzuführen, mit denen oft auch eine sehr einschneidende Kontrolle insbesondere der Arbeitnehmerleistung möglich ist. Da solche Systeme häufig automatisiert Entscheidungen treffen, wird nicht nur die Rechtsgrundlage des § 26 BDSG verlassen, sondern auch der Anwendungsbereich des Art. 22 DSGVO mit weitreichenden datenschutzrechtlichen Konsequenzen eröffnet. So müssen die Arbeitnehmer mindestens in die Verarbeitung einwilligen – ein stacheliges Unterfangen, da die Freiwilligkeit einer Einwilligung im Arbeitsverhältnis regelmäßig in Frage steht.

Damit ist klar, dass die EuGH-Entscheidung keineswegs als Freibrief für die Einführung von Leistungskontrollen missverstanden werden darf.

Secorvo News

Neu: Der PKI-Blog

Wer sich seit über fünfunddreißig Jahren mit Public Key Infrastrukturen (PKI) beschäftigt, hat einiges erlebt: Von den ersten RSA-Implementierungen auf PCs und Smartcards über das „Web of Trust" von Phil Zimmermans „Pretty Good Privacy" bis zur gesetzlichen Regulierung von „elektronischen Signaturen" und den manchmal bizarren Auswüchsen bei der praktischen Umsetzung. Inzwischen sind PKIs das Rückgrat vieler Sicherheitsmechanismen – und daher bei Fehlern auch gelegentlich Ursache weit reichender Sicherheitsprobleme. Seit Kurzem gewährt der Secorvo-PKI-Experte Hans-Joachim Knobloch einen Einblick in seine Erfahrungen und Erlebnisse rund um PKIs – in seinem eigenen PKI-Blog. Lesenswert.

Wie souverän ist der Souverän?

Angesichts der wachsenden Komplexität von IT-Systemen, dem Eindringen der IT in immer mehr Lebensbereiche und der Zunahme der Verarbeitung personenbezogener Daten ist „digitale Souveränität" nicht mehr lediglich von mangelnder Medienkompetenz bedroht. Beim kommenden KA-IT-Si-Event am **06.06.2019** in Kooperation mit der Initiative Smart Ettlingen zeichnet Dirk Fox die Entwicklung des Internet vom „Schaufenster" zu einer Überwachungsinfrastruktur nach und zeigt auf, welche Verantwortung für die Erhaltung (oder womöglich die Wiederherstellung) von digitaler Souveränität auf die Softwareentwickler von heute und morgen zukommt – und welche Schritte dafür erforderlich sind. Im Anschluss folgt eine Diskussion zum Thema „Digitale Souveränität im internationalen Kontext". Danach haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (Anmeldung).

11. Tag der IT-Sicherheit

Für die Keynote des bereits elften Karlsruher „Tag der IT-Sicherheit" konnten wir die polnische IT-Security-Expertin Paula Januszkiewicz (‚Think and Act Like a Hacker to Protect Your Company's Assets') gewinnen. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V. findet am **11.07.2019** im Saal Baden der IHK Karlsruhe statt. Das vollständige Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2019	
03.-05.06.	Entwicklertag 2019 (VKSI, GI, ObjektForum, Karlsruhe)
03.-04.06.	DuD 2019 (COMPUTAS Gisela Geuhs GmbH, Berlin)
05.-06.06.	BvD-Verbandstage 2019 (BvD e.V., Berlin)
06.06.	Wie souverän ist der Souverän? (KA-IT-Si, Karlsruhe)
13.-14.06.	Annual Privacy Forum 2019 (ENISA, EC DG Connect, Universität Wien, Rom/I)
17.-19.06.	4rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Stockholm/SWE)
Juli 2019	
11.07.	11. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
14.-17.07.	DFRWS USA 2019 (DFRWS, Portland/US)
16.-20.07.	PETS 2019 (University of Minnesota, Stockholm/SWE)

Fundsache

Der am 09.04.2019 veröffentlichte Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS) hätte besser acht Tage früher erschienen sollen: Streicht man von den kompakten neun Seiten die Formalia (Deckblatt, Adressangabe, Vorwort, Inhaltsverzeichnis, Beschreibung, Literaturverzeichnis, Abkürzungsverzeichnis) und die überflüssige Grafik, bleibt nur Seite sechs übrig. Und es ginge noch kompakter: "Mindeststandard: Wenn TLS verwendet wird, dann müssen die Vorgaben aus BSI TR-02102-2 eingehalten werden." Aha.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: André Domnick, Fabian Ebner, Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, Jannis Pinter, Friederike Schellhas-Mende, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Juni 2019



Der Wert des Flüchtigen

Wenn ich dieses Editorial verfasse weiß ich nicht nur, dass es viele Menschen lesen werden. Ich weiß auch, dass ich nicht wissen kann, wer genau es lesen wird – oder anders herum: Ich muss damit rechnen, dass es jeder Mensch lesen könnte. Auch Menschen, die mich nicht kennen, meine Äußerungen nicht in den Gesamtkontext einordnen werden oder können, vielleicht Sätze aus dem Zusammenhang reißen. Daher werde ich mich besonders um Unmissverständlichkeit bemühen, um die korrekte Verwendung von Begriffen und die Klarheit meiner Überlegungen. Das muss nicht gelingen – aber vor der Veröffentlichung werde ich überzeugt sein, dass ich es nicht klarer und unmissverständlicher schreiben konnte. Umgekehrt wird jeder Leser genau das wissen. Und mir daher jeden Satz und jede Äußerung auch zurechnen. Einmal in der Welt lässt sich ein solcherart veröffentlichter Gedanke nicht mehr zurücknehmen. Das ist auch bedeutsam, denn erst diese Ernsthaftigkeit verleiht ihm das nötige Gewicht.

Daneben (besser: davor und dahinter) gibt es aber auch das nichtöffentliche, gesprochene Wort: Dem kann dieses Gewicht nicht beigemessen werden. Und darf es nicht. Es muss zurücknehmbar bleiben, vorläufig und flüchtig. Dieser Schutz vor unerwarteter oder unerwünschter Kenntnisnahme durch Dritte ist essentiell: Denn wir benötigen den Raum des Vorläufigen und Flüchtigen, damit Gedanken und Überzeugungen im Diskurs reifen können. Der öffentliche Umgang mit privaten Äußerungen von Politikern (die hinsichtlich aller ihrer Äußerungen natürlich in einer besonderen Verantwortung stehen) macht manchmal vergessen, wie bedeutsam diese Flüchtigkeit für eine freie Gesellschaft ist.

Wer daher den Zugriff auf Daten von Sprachassistenten fordert, hat nicht nur den Datenschutz und die Unverletzlichkeit der Wohnung, sondern auch das Fundament einer freiheitlichen Ordnung nicht verstanden.



Inhalt

Der Wert des Flüchtigen

Security News

Magische Technologien

Dem Trustcenter ausgeliefert

Crypto Wars 2.0

Certificate Transparency

Private Videoüberwachungen

Sysmon 10

Alte Antwort, neue Bedeutung

Secorvo News

Secorvo@itsa

11. Tag der IT-Sicherheit

Veranstaltungshinweise

secorvo
security consulting

Security News

Magische Technologien

Ransomware ist derzeit eine der größten digitalen Gefahren für Unternehmen und Behörden. Sind die Daten erst einmal verschlüsselt, hilft in der Regel nur eine gelebte Disaster-Recovery-Strategie. Oft fehlt sie – und die Opfer wenden sich verzweifelt an Datenwiederherstellungs-Experten. Doch ohne bekannte Schwachstellen in der Ransomware hilft auch das nicht, denn die verwendeten starken Verschlüsselungsalgorithmen können nicht gebrochen werden. Mehrere US-amerikanische Data-Recovery-Firmen verfügen jedoch nach eigenen Angaben über „proprietäre Technologien", um die Daten zu entschlüsseln – wie kann das sein?

Wie Pro Publica am 15.05.2019 publizierte, besteht die magische „proprietäre Technologie" darin, unter der Hand das Lösegeld zu bezahlen... Die Firmen bieten den Opfern einen risikofreien Weg aus der Ransomware-Falle. Ransomware-Entwickler umwerben diese Firmen offenbar als vertrauenswürdige Mittelsmänner und bieten ihnen Vergünstigungen, Rabatte und Verlängerungen von Deadlines an. Lesson learned: „Magische Technologien" mag es geben – allerdings nicht in der Kryptografie.

Dem Trustcenter ausgeliefert

Auch Schadsoftware kann mit einer gültigen Code-Signatur versehen werden. Forscher veröffentlichten am 22.05.2019 eine auf den Daten von VirusTotal basierende Top-25-Liste der Trustcenter, mit deren Zertifikaten mutmaßliche Malware signiert wurde. Ganz oben: die Comodo CA. Deren neuer Betreiber Sectigo sperrte daraufhin am 24.05.2019 127 betroffene Zertifikate.

Wie am 30.05.2019 bekannt wurde, war darunter jedoch mindestens ein Code-Signing-Zertifikat eines legitimen Sectigo-Kunden, dessen CAD-Software von fünf der 70 Virenscanner fälschlich als Malware klassifiziert wurde. Nach der Sperrung beschwerten sich Anwender zuhauf beim Hersteller, dass ihre CAD-Software nicht mehr lief. Sectigo hat formal korrekt gehandelt: Nach Kapitel 4.9.1 der Baseline Requirements des CA/Browser-Forums muss ein Trustcenter ein Zertifikat nach spätestens fünf Tagen sperren, wenn „*The CA obtains evidence that the Certificate was misused*". Wie sorgfältig die Indizien zu prüfen sind, ist nicht genauer spezifiziert. Eine Haftung für fälschliche Sperrung ist nicht vorgesehen. Zwar hätten fünf Tage wohl gereicht, um den Sachverhalt mit dem betroffenen Kunden zu klären – das aber ist in diesem Fall offenbar unterblieben. Wer Zertifikate für geschäftskritische Zwecke nutzt, sollte also besser regelmäßig selbst den Sperrstatus der eigenen Zertifikate prüfen.

Crypto Wars 2.0

Verwendet man TLS mit Perfect Forward Secrecy (PFS) ist es auch bei Kenntnis des privaten Schlüssels unmöglich, aufgezeichnete TLS-Sitzungen nachträglich zu entschlüsseln. Aus Compliance-Gründen (Network Monitoring in internen Netzen) unterstützt das vom Europäischen Institut für Telekommunikationsnormen (ETSI) entwickelte ETS-Protokoll (vormals eTLS) PFS nicht. MITRE listet es daher seit dem 26.02.2019 auf Betreiben der Electronic Frontier Foundation (EFF) offiziell als Schwachstelle (CVE-2019-9191). Der Bankensektor, insbesondere die Industriegruppe BITS, versuchte schon während der Standardisierung TLS 1.3 durch die Entfernung von PFS zu schwächen. Webbrowser können ETS und TLS 1.3 nicht unterscheiden, da ETS PFS mit statischen Diffie-Hellman-Schlüsselpaaren realisiert.

Eine von derzeit vielen Bestrebungen, Krypto-Protokolle zu schwächen. So sollen beispielsweise Messenger-Dienste gesetzlich verpflichtet werden, Strafverfolgungsbehörden in Verdachtsfällen einen Zugriff auf die entschlüsselte Kommunikation zu ermöglichen. Keine neue Diskussion – und es gilt noch immer, was auch der Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) am 12.06.2019 publizierte: Backdoors schwächen nicht nur das Vertrauen der Nutzer in IT-Systeme, sondern können auch missbräuchlich genutzt werden. Keine gute Idee.

Certificate Transparency

Damit Zertifikate von Google Chrome als gültig anerkannt werden, müssen öffentlichen Zertifizierungsstellen diese seit dem 30.04.2018 vor der Ausstellung als *Precertificate* in mehrere öffentliche Certificate-Transparency-Protokolle schreiben. Ein echter Sicherheitsgewinn für die Web-PKI, denn nun kann jeder diese Protokolle durchsuchen – beispielsweise durch die Website crt.sh –, fehlerhafte Ausstellungen erkennen, melden und eine rasche Sperrung veranlassen.

So wurde am 16.04.2019 aufgedeckt, dass die französische Zertifizierungsstelle Certinomis unter anderem Zertifikate für nicht registrierte Domains und solche mit ungültigen Object Identifiers (OIDs) ausgestellt hatte. Wegen mehreren Verstößen gegen Baseline Requirements wird sie nun aus dem Root-Programm von Mozilla Firefox Version 69 entfernt; Certimonis-Zertifikate sind damit nicht mehr vertrauenswürdig. Auch die Zertifizierungsstellen Sectigo, SECOM und DigiCert sind betroffen: Sie haben Extended-Validation-Zertifikate (EV), die nur nach besonders sorgfältiger Überprüfung des Antragstellers ausgestellt werden dürfen und daher im Browser mit einer „grünen Adressleiste" belohnt

werden, teilweise mit „Default City“ als Städtenamen oder „Some-State“ als Staatsnamen ausgestellt. Die betroffenen Zertifikate wurden gesperrt.

Vielleicht gelingt es ja auf diesem Weg, das angekratzte Vertrauen in die Web-PKI zu kitten.

Private Videoüberwachungen

Das Bundesverwaltungsgericht hat am 27.03.2019 bestätigt, dass die Regelung zur Videoüberwachung im neuen § 4 BDSG mangels Reichweite der Öffnungsklausel der DSGVO nicht für private Stellen gilt. Private Videoüberwachungen sind allein nach Art. 6 Abs. 1 f) DSGVO (Rechtsgrundlage) und insbesondere Art. 13/14 DSGVO (Informationspflichten) zu beurteilen.

Die Entscheidung in der Sache – rechtswidrige Live-Überwachung einer Zahnarztpraxis – erging noch zur alten Rechtslage (§ 6b BDSG aF). Bei den Aussagen zu § 4 BDSG nF handelt es sich also streng genommen eher um ein *obiter dictum*: Das Gericht prüfte, ob eine Pflicht der Aufsichtsbehörde zur Überprüfung der Umsetzung besteht. Nach Überzeugung des Gerichts gelten die Öffnungsklauseln in Art. 6 Abs. 2, 3 DSGVO nur für hoheitliche Verarbeitungen. Für die Prüfung der Erforderlichkeit und Angemessenheit einer Überwachung dürfte es trotz der spezifischeren Ausführungen des § 4 BDSG weitgehend bei den bisherigen Maßstäben bleiben.

Sysmon 10

Das am 14.06.2019 aktualisierte Microsoft-Werkzeug Sysmon (v10.1) unterstützt mit 21 spezifischen EventIDs die Aufzeichnung detaillierter Logs des Laufzeitverhaltens eines Windowssystems (Server wie Clients). Für EventIDs 1 (ProcessCreate) und 7 (ImageLoad) wurde die Eigenschaft „Original FileName“ hinzugefügt, wodurch nun der aufrufende PE-Originaldateiname aufgezeichnet und nachvollziehbar wird. Die EventID 22 (DNSEvent DNS query) wurde ergänzt; sie wird erzeugt, wenn ein Prozess eine DNS-Abfrage ausführt, unabhängig davon, ob das Ergebnis erfolgreich ist oder fehlschlägt: sehr hilfreich bei der Vorfallsanalyse von Anomalien, Schadsoftware oder Datenexfiltrationen, da eine DNS-Protokollierung mit einer spezifischen Prozesszuordnung auf Urheber und Securityidentifier (SID) hinweist.

Diese Erkenntnisse gewinnt man allerdings nur, wenn Sysmon produktiv installiert ist. Mit einem eigenen Symon-Config-File lassen sich die laufenden Ereignisse (Events) in einer zentralen Logauswertung sammeln und auswerten.

Alte Antwort, neue Bedeutung

Am 13.06.2019 hat der Europäische Gerichtshof (EuGH) im Streit zwischen Google und der Bundesnetzagentur entschieden, dass GMail kein elektronischer Kommunikationsdienst nach § 3 Nr. 24 TKG bzw. RL 2002/21/EG ist. Definitionsmerkmal eines Kommunikationsdienstes sei, dass der Dienst ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht. Unstreitig übertragen E-Mail-Provider und andere Anbieter von vergleichbaren Internetdiensten (wie Messengerdienste) die Signale jedoch nicht selbst, sondern bedienen sich der durch Access-Provider angebotenen Infrastruktur.

Die Bedeutung der Entscheidung wird eingeschränkt durch die bevorstehenden Neuregulierungen der bereits bis Dezember 2020 umzusetzenden RL 2018/1972/EU und der ePrivacy-Verordnung. Beide Gesetzgebungen schaffen Rechtsrahmen, die direkt auf E-Mail-Dienste und vergleichbare Angebote zielen. In der Übergangszeit beschränkt das Urteil zwar einerseits u. a. staatliche Zugriffsrechte, andererseits verschärft es die Unsicherheit: Bisher wurde bezüglich des Telekommunikationsgeheimnisses und des Umgangs mit Verbindungsdaten regelmäßig Telekommunikationsrecht angewendet. Zugleich verdrängen die sehr allgemeinen DSGVO-Bestimmungen die Datenschutzbestimmungen des Telemediengesetzes – eine Situation, die der Gesetzgeber baldmöglichst klären sollte.

Secorvo News

Secorvo@itsa

Vom **08. bis 10.10.2019** ist Secorvo wieder auf der it-sa in Nürnberg vertreten. Am Stand 10.1-630 zeigen wir Ihnen u. a. ISMS ready2go und DSMS ready2go, unsere Lösungen für das Informationssicherheits- und Datenschutz-Management. Sie sind herzlich eingeladen, bereits vorab einen Termin mit uns zu vereinbaren. Gerne schicken wir Ihnen auch einen Registrierungscode, mit dem Sie Ihr kostenfreies E-Ticket (Tageskarte) ausdrucken können.

11. Tag der IT-Sicherheit

Für die Keynote des bereits elften Karlsruher „Tag der IT-Sicherheit“ konnten wir die polnische IT-Security-Expertin Paula Januszkiewicz (‚Think and Act Like a Hacker to Protect Your Company's Assets‘) gewinnen. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V. findet am **11.07.2019** im Saal Baden der IHK Karlsruhe statt. Das vollständige Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2019	
11.07.	11. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si)
14.-17.07.	DFRWS USA 2019 (DFRWS, Portland/US)
16.-20.07.	PETS 2019 (KTH Royal Institute of Technology, Stockholm/SWE)
August 2019	
03.-08.08.	Blackhat USA 2019 (Blackhat, Las Vegas/US)
08.-11.08.	DEF CON 27 (DEFCON, Las Vegas/US)
11.-13.08.	SOUPS 2019 (usenix, Kalifornien/US)
14.-16.08.	28th USENIX Security Symposium (usenix, Santa Clara/US)
18.-22.08.	Crypto 2019 (IACR, Santa Barbara/US)
September 2019	
17.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
23.-26.09.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.-27.09.	heise devSec 2019 (dpunkt-Verlag, Heidelberg)



Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Hans-Joachim Knobloch, Michael Knöppler, Michael Knopp, Jannis Pinter, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2019



Modell und Wirklichkeit

Seit Jahrhunderten erforschen Menschen die Welt. Sie erfanden die Gravitation, den Magnetismus und das Sonnensystem, um damit fallende Äpfel, ausgerichtete Kompassnadeln und kreisende Monde zu erklären und mathematisch zu beschreiben. Stieß dieses Wirklichkeitsmodell (z. B. durch den Nachweis der Konstanz der Lichtgeschwindigkeit) an Erklärbarkeitsgrenzen, wurde es flugs erweitert (Relativitätstheorie). Bis heute wissen wir jedoch nicht, ob es die Welt korrekt beschreibt. Die uneingeschränkte Geltung physikalischer Gesetze ist daher nur in diesem Wirklichkeitsmodell gesichert.

Ganz Ähnliches gilt für technische Lösungen. Sie lösen nie ein Wirklichkeitsproblem, sondern funktionieren nur in einem eingeschränkten Modell: So ist ein Auto nur unter bestimmten Voraussetzungen ein Fortbewegungsmittel – nicht unter Wasser, nicht in der Luft, nicht auf dem Mond (zumindest mit Verbrennungsmotor), und selten ohne Fahrweg oder bei Steigungen von über 30%. Leider vergessen wir das gelegentlich und wundern uns, wenn aus solchen Einschränkungen Risiken erwachsen. So zeigte eine israelische Forschergruppe am 23.06.2019, wie eine Drohne durch Vortäuschung von Verkehrszeichen ein Advanced Driver Assistance System (ADAS) beeinflussen kann. Und wenn das ADAS eines Tesla wie zuletzt am 01.03.2019 die Plane eines querenden LKW nicht als Hindernis erkennt, ist die Ursache höchstwahrscheinlich kein Programmierfehler, sondern eine Beschränkung des zu Grunde liegenden Wirklichkeitsmodells. Diese ergeben sich häufig implizit durch die Wahl einer technischen Komponente – so benötigt eine Bildauswertung Licht und Kontrast, ein Lasersensor nicht.

Dasselbe passiert mit Sicherheitslösungen, die oft versteckte Annahmen über das Angreiferverhalten enthalten. Skimming und Keyless-Go-Angriffe zeigen, dass diese nicht immer realistisch sind. Wir sollten daher von den Naturwissenschaften lernen und beginnen, die Wirklichkeitsmodelle unserer Lösungen präziser zu beschreiben.



Inhalt

Modell und Wirklichkeit

Security News

Was man nicht aufgibt...

Angst beflügelt den eilenden Fuß

Die Geister, die ich rief...

Was lange währt...

Stets ist die Sprache kecker als die Tat

Secorvo News

Easy – Certificates ready2go

Nächste Seminare

Hallo, hier spricht Deine Zahnbürste.

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Was man nicht aufgibt...

Die vor über 12 Jahren für Webserver eingeführten Extended Validation (EV) Zertifikate sollten Anwendern durch besonders gründlich geprüfte Zertifikatsanträge wieder Vertrauen in die durch Hacking-Vorfälle und Schludrigkeit in Verruf gekommene Web-PKI vermitteln. Dazu stellten Browser bei EV-Zertifikaten den geprüften Firmen- oder Organisationsnamen grün hinterlegt neben dem Vorhängeschloss in der Adresszeile dar („grüner Balken").

Doch schon seit iOS 12 (17.09.2018) heben Browser auf Apple-Mobilgeräten den Namen aus EV-Zertifikaten nicht mehr gesondert hervor. Auch Google Chrome wird ab Version 77, die am 10.09.2019 erscheint, die Hervorhebung komplett entfernen – seit Version 69 wird sie nur noch in grau statt grün dargestellt. EV-Zertifikate unterscheiden sich für den Endnutzer nicht mehr von DV- oder OV-Zertifikaten; der Mehrwert entfällt damit für Nutzer dieser Browser.

Diese Entwicklung entspricht der verbreiteten Einschätzung, dass EV-Zertifikate die in sie gesetzten Erwartungen nicht erfüllt haben und kein Plus an Sicherheit bieten. Google setzt stattdessen schon länger auf Certificate Transparency (SSN 6/2019). Auch durch die zunehmende Nutzung von Apps anstelle eines Browsers entfällt die Notwendigkeit der Darstellung von EV-Informationen. Statt EV-Zertifikate besonders zu kennzeichnen schlägt Mozilla mit Firefox Version 70 eine andere Richtung ein und brandmarkt unverschlüsselte HTTP-Webseiten als unsicher. HTTPS wird damit für Webseitenbetreiber endgültig zur Pflicht; die Mehrkosten für EV-Zertifikate kann man sich jedoch sparen.

Angst beflügelt den eilenden Fuß

Am 18.07.2019 schlug eine Schwachstellenmeldung Wellen: Fach- und Allgemeinpresse berichteten über eine kritische Sicherheitslücke im VLC Media Player, die einem Angreifer das entfernte Ausführen von Code ermöglichen würde. Untermauert wurde die Kritikalität durch einen CVSSv3 Score von 9.8. Losgetreten hatte sie CERT-Bund, die im BSI angesiedelte zentrale Anlaufstelle für Computersicherheitsvorfälle, nachdem MITRE den Schwachstellen-Identifier CVE-2019-13615 zugewiesen hatte. Wie sich herausstellte, handelte es sich gar nicht um eine Schwachstelle in VLC, sondern um eine in der von VLC verwendeten Bibliothek „libEBML", die bereits am 20.04.2018 mit Version 1.3.6 behoben worden war. VLC wird schon seit dem 29.05.2018 (Version 3.0.3) mit einer korrigierten „libEBML" ausgeliefert. Der Entdecker der Schwachstelle hatte eine Ubuntu-Version verwendet, die keine aktuelle Version der Bibliothek bereitstellte (deren Maintainer das Problem schnell behoben).

Ein Sicherheitsforscher, der eine nicht aktuelle Software analysiert, zwei offizielle Institutionen (MITRE und CERT-Bund), die ohne gründliche Prüfung eine kritische Schwachstelle anerkennen, Medien, die ohne tiefere Recherche voneinander abschreiben und die Community einer Linux-Distribution, die Sicherheitsaktualisierungen nicht zeitnah verfügbar gemacht hat – ein gefährlicher Cocktail, der Unternehmen vermeidbare Aufwände beschert hat.

Selbst die Änderung der Kritikalität der Schwachstelle ist nur schwer nachvollziehbar: Allein das NIST pflegt in der NVD eine umfängliche Änderungshistorie. CERT-Bund beschreibt die Änderungen vollkommen unzureichend und MITRE führt erst gar keine Historie. Und die Moral: Trau' keiner Nachricht, die Du nicht selbst überprüft hast...

Die Geister, die ich rief...

Das deutsche Vorratsspeicherungsgesetz ist nach den Urteilen des EuGH und der deutschen Obergerichte derzeit ausgesetzt und wird es auch noch auf absehbare Zeit bleiben. Allerdings hat sich der Europarat am 27.05.2019 für eine Vorratsdatenspeicherung zum Zwecke der Kriminalitätsbekämpfung ausgesprochen. Offenbar speichern Internet- und Telefonanbieter jedoch trotz der einschlägigen Rechtsprechung über Monate hinweg nicht abrechnungsrelevante Daten ihrer Kunden.

Um den Schutz des Fernmeldegeheimnisses aus Art. 10 Abs. 1 Grundgesetz zu gewährleisten, muss diese Art von Vorratsdatenspeicherung unterbunden werden. Wie wichtig das ist, zeigt ein aktueller Vorfall aus Dänemark: Das dänische Justizministerium gab am 02.07.2019 bekannt, dass ein IT-Fehler bei der Vorratsdatenspeicherung möglicherweise dazu geführt hat, dass Unschuldige verurteilt und Täter fälschlich freigesprochen wurden. Insgesamt müssen 10.700 Fälle von der inzwischen eingesetzten Expertenkommission überprüft werden.

Freiheit und Gerechtigkeit können auch unter die Räder einer gefährlichen Mixtur aus unkritischem Glauben von Strafverfolgern an die Verlässlichkeit technischer Nachweise und vorauseilendem Gehorsam bei Telekommunikationsanbietern hinsichtlich der, rechtsstaatliche Grenzen überdehnenden, Speicherung von Verbindungsdaten geraten.

Was lange währt...

Nach über sechsmonatiger Beta-Phase wurde am 28.06.2019 Version 2.1 der Burp Suite veröffentlicht. Als Proxy zwischen Web-Browser und -Server erlaubt sie das Mitschneiden, Analysieren und Mani-

pulieren von HTTP-Verkehr – ein unverzichtbares Werkzeug für Sicherheitsexperten und Web-Entwickler. Die lang erwartete Runderneuerung enthält sowohl in der (kostenfreien) Community- als auch in der Professional-Edition zahlreiche Verbesserungen: Der neue Crawler und die neue Scanning-Engine vereinfachen zusammen mit der dynamischen JavaScript-Analyse insbesondere automatisierte Tests. Auch das User Interface wurde an einigen Stellen stark überarbeitet – so wurden ein neues Dashboard und ein alternatives dunkles Farbschema integriert. HTTP-Antworten werden nun dank einer neuen Rendering-Ansicht unter Berücksichtigung von Stylesheets dargestellt. Die Burp Suite kann jetzt auch über eine REST-API aus anderen Anwendungen angesprochen werden, um beispielsweise Scans zu initiieren. Schließlich wurde auch die Performance verbessert.

Stets ist die Sprache kecker als die Tat

Datenschutzaufsichtsbehörden, Datenschutzkonferenz, Europäischer Datenschutzausschuss und Datenschutzverbände überschütten Unternehmen, Datenschutzbeauftragte und Verantwortliche derzeit mit Hinweisen, Orientierungshilfen und Stellungnahmen. Dabei hapert es aber gelegentlich an der inhaltlichen Konsistenz. Zwei aktuelle Beispiele:

Die Argumentation der Stellungnahme des HDBI vom 09.07.2019 zur Unzulässigkeit des Einsatzes von Office 365 in Schulen lässt sich durchaus auf Arbeitgeber übertragen. Als Lösung wird auf on-premise Angebote verwiesen. Zwar haben Rechtsbedenken gegen Office 365 durch das Ende der Deutschland-Cloud (SSN 3/2019) und eine niederländische Prüfung vom 07.11.2018 (SSN 4/2019), die erhebliche Datenschutzrisiken benennt (Zugriff auf personenbezogene Daten auf Grundlage des US Cloud Acts und ungeklärte Verwendung von Telemetrie-Daten durch Microsoft), neue Nahrung erhalten. Eine grundsätzliche Rechtswidrigkeit wurde bisher jedoch nicht festgestellt – und erscheint auch vor dem Hintergrund der geltenden EU-US Privacy Shield Vereinbarung juristisch fragwürdig.

Die neuen FAQ der bayerischen Landesdatenschutzaufsicht enthalten einen informationellen Rundumschlag – und verblüffen mit der Aussage, dass einerseits Google Maps, Google Fonts und allgemeine Captchas, sofern in der Datenschutzerklärung darüber informiert wird, in Webseiten eingebunden werden dürfen, andererseits aber ein rechtmäßiger Einsatz von Google Recaptcha eine Darlegung der Nutzerdatenverarbeitung durch Google erfordert. Die Zulässigkeit von Facebook Fanpages (SSN 4/2019) wird uneingeschränkt verneint.

Die Beispiele hinterlassen den Eindruck, dass die Aufsichtsbehörden sich mit einer eindeutigen Positionierung insbesondere zu amerikanischen Cloud-Angeboten schwer tun – und gelegentlich liebgewonnene Feindbilder die Argumentation überlagern.

Secorvo News

Easy – Certificates ready2go

Auch in internen Netzen wird immer häufiger TLS eingesetzt. Die Einrichtung und Erneuerung von Serverzertifikaten kann inzwischen auch ohne eigene PKI über eine Clientsoftware vorgenommen werden, die kompatibel mit öffentlichen Trustcentern ist. Mit Certificates ready2go, einer Entwicklung von Secorvo, übernimmt ein ACME-Proxy (SSN 3/2019) die Domain-Validierung und ermöglicht so auch Servern im gesicherten internen Netz den vollautomatisierten Bezug und die Erneuerung von Zertifikaten, beispielsweise von Let's Encrypt. Mit dem zugehörigen Dashboard Easy behalten Sie dabei den Überblick über den Status aller Ihrer internen Zertifikate. Zu sehen auf der it-sa 2019.

Nächste Seminare

Nach der Sommerpause startet das Seminarangebot von Secorvo in der letzten Septemberwoche (**23.–26.09.2019**) mit dem Zertifizierungsseminar TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.), gefolgt von T.I.S.P. (**14.–18.10.2019**, schnelle Anmeldung empfohlen) und IT-Sicherheit heute (**22.–24.10.2019**). Programme und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Hallo, hier spricht Deine Zahnbürste.

Ob zu Hause, in Fahrzeugen, Industrieanlagen oder Agrarbetrieben: IoT-Anwendungen sind heute nicht mehr wegzudenken und halten in nahezu allen Bereichen Einzug in unser Leben. Bis 2020 sollen laut Gartner 20 Milliarden vernetzte Geräte im Einsatz sein. Das Internet of Things eröffnet vielfältige Chancen, jedoch mangelt es häufig an Bewusstsein für Sicherheitsaspekte. Die sichere Kommunikation der unzähligen vernetzten Dinge untereinander ist dabei die größte Herausforderung.

Warum es für Unternehmen existentiell ist, ihre IoT-Devices und den Zugriff auf ihre IoT-Plattformen abzusichern und welche aktuellen Technologien dafür zur Verfügung stehen, erläutert beim kommenden KA-IT-Si-Event am **19.09.2019** Thorsten Gahrmann von der Nexus Group. Im Anschluss an den Vortrag haben Sie – wie gewohnt – Gelegenheit zum fachlichen und persönlichen Austausch bei unserem „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2019	
03.-08.08.	Blackhat USA 2019 (Blackhat, Las Vegas/US)
08.-11.08.	DEF CON 27 (DEFCON, Las Vegas/US)
11.-13.08.	SOUPS 2019 (usenix, Kalifornien/US)
14.-16.08.	28th USENIX Security Symposium (usenix, Santa Clara/US)
18.-22.08.	Crypto 2019 (IACR, Santa Barbara/US)
September 2019	
17.09.	Anwendertag IT-Forensik (Fraunhofer Institut SIT, Darmstadt)
19.09.	Hallo, hier spricht Deine Zahnbürste. (KA-IT-Si, Karlsruhe)
22.-24.09.	FIfFKon 2019 (FIfF e.V., Berlin)
23.-26.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.09.	Datenschutztag 2019 (COMPUTAS, Köln)
24.-27.09.	heise devSec 2019 (dpunkt.verlag, heise Developer, heise Security, Heidelberg)

Fundsache

Das NIST hat im Juni einen Entwurf für ein White Paper zur sicheren Softwareentwicklung veröffentlicht. Das White Paper hilft dabei, einen Software Development Life Cycle (SDLC) um Praktiken der sicheren Softwareentwicklung zu ergänzen. Kommentare können noch bis zum 05.08.2019 eingereicht werden.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Michael Knopp, Jannis Pinter, Friederike Schellhas-Mende, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

August 2019



Digitale Blockwarte

Manchmal kommen selbst dramatische Paradigmenwechsel verhuscht um die Ecke. So wissen wir zwar längst, dass ein Gerät, das seinen Standort über Satellitenortung oder WLAN-Accesspoints bestimmen kann, diese Information auch gelegentlich weitergibt. Natürlich dient das nie der Erstellung von Bewegungsprofilen, sondern ausschließlich anderen, unverdächtig nützlichen Zwecken, wie der Bestimmung der Verkehrsdichte, der exakten Berechnung der richtigen Kochzeit für das Frühstücksei oder der behütenden Aufsicht über den Nachwuchs. Charmant obendrein: Ortungsfunktion oder Gerät lassen sich ausschalten (ja, tatsächlich!), und schon sind wir zurück in steinzeitlicher Freiheit.

Damit könnte es allerdings bald endgültig vorbei sein. Wenn die Idee hinter Apples „Apple Tag" (angekündigt für iOS 13 auf der Entwicklerkonferenz am 03.06.2019) Schule macht, ist die Steinzeit abgelaufen. Und die Freiheit mit ihr. Wie so oft kommt die Überwachung im Schafspelz daher: Elektronische Geräte ohne Ortungs- und Mobilfunk-Chipsatz sollen von anderen, kommunikations- und GPS-fähigen Geräten via Bluetooth kontaktiert, die übermittelte Geräte-ID mit aktueller Ortsinformation angereichert und an Apple geschickt werden – damit verlorene oder gestohlene Devices einfacher und schneller wiedergefunden werden.

Welch zauberhafte Vorstellung: Dank Millionen digitaler Blockwarte müssen wir unsere Schlüssel, Hunde, Zahnbürsten oder Rasierapparate nie mehr suchen oder uns über entwendete Gadgets grämen – einfach ins Netz gucken, und schon wissen wir, wo sie sind. Und auch der Standort der Blockwarte ist jederzeit dokumentiert.

Schade nur, dass die Entwicklung ziemlich genau 30 Jahre zu spät kommt. Wie viel volkswirtschaftliches Vermögen hätte man damit im Ministerium für Staatssicherheit sparen können...

Und die Geschichte wäre vielleicht ganz anders verlaufen.



Inhalt

Digitale Blockwarte

Security News

Bluetooth-Downgrade

Kreditkarten-Upgrade

Heiße Schwachstelle

Komplexinetes

EuGH-Trend

Spiegelreflex-Trojaner

DSGVO-konforme Kamerafahrten

Forever Young

Secorvo News

Seminare

Hallo, hier spricht Deine Zahnbürste.

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Bluetooth-Downgrade

Ex- und Import von Verschlüsselungslösungen stießen in den 90er Jahren noch auf zahlreiche Restriktionen. Daher verwenden Bluetooth-Verbindungen bis heute getrennte Schlüssel für Integritätsschutz und Verschlüsselung. Während ersterer immer 128 bit lang ist, kann letzterer auf bis zu 8 bit verkürzt werden. Fast 20 Jahre dauerte es, bis ein internationales Forscherteam eine diesen Umstand nutzende Downgrade-Attacke entdeckte und am 14.08.2019 veröffentlichte: Ein Angreifer, der sich in die Schüsselaushandlung einschaltet, kann die Kommunikationspartner dazu bringen, einen 8 Bit Schlüssel zu verwenden und so die übertragenen Daten entschlüsseln.

Wer vertrauliche Daten (wie die Anschläge einer Tastatur oder Dokumente zum Drucken) und nicht nur die aktuelle Playlist via Bluetooth überträgt, sollte prüfen, ob die Hersteller beider Geräte Patches bereitstellen – oder doch zu einer kabelgebundenen Übertragung zurückkehren.

Kreditkarten-Upgrade

Auch bei einem am 29.07.2019 veröffentlichten Kreditkartenangriff mischt sich der Angreifer in die Aushandlung seiner beiden Opfer ein. So ermöglicht Visa inzwischen, am Point-of-Sale durch einfaches Auflegen der Kreditkarte zu bezahlen. Das Missbrauchsschäden bei gestohlenen Karten begrenzende Zahlungslimit (in Großbritannien £ 30) kann dabei durch die Man-in-the-Middle-Attacke auf ein Vielfaches erhöht werden.

Trotz des Proof-of-Concept will Visa nicht sofort etwas gegen die Schwachstelle unternehmen. Zwar kann ein Einzelschaden leicht im drei- oder vierstelligen Bereich liegen, doch dass organisierte Kriminelle zahlreiche Komplizen mit der erforderlichen Elektronik vor Ort auf „Einkaufstour" schicken, erscheint eher unwahrscheinlich. Daher dürfte Visa erst bei einem ohnehin fälligen Wechsel von Karten und Terminals eine sicherere Version ausrollen.

Heiße Schwachstelle

Eingebettete Systeme sind die jüngste Achillesferse der IT-Sicherheit. Da liegt es nahe, Betriebssysteme zu verwenden, die mit Fokus auf Sicherheit und Zuverlässigkeit entwickelt wurden, wie beispielsweise Wind Rivers marktführendes VxWorks. Umso schockierender ist daher eine Nachricht wie die vom 09.08.2019: Elf Schwachstellen wurden in VxWorks 6.9 gefunden, veröffentlicht unter anderem unter CVE-2019-12256. Besonders schlimm: Anwender wissen häufig gar nicht, ob sie betroffen sind oder nicht, denn bei vielen Lösungen wird das genutzte Betriebssystem nicht genannt.

Von vielen Herstellern werden bereits Updates zur Verfügung gestellt. Sie sollten, sofern die Systeme über Netzwerke erreichbar sind, dringend eingespielt werden. Und bei der Beschaffung neuer IoT-Geräte sollte zukünftig auf die Angabe der verwendeten IT-Komponenten geachtet werden.

Komplexinetes

Von Oktober bis Dezember 2018 wurde Version 1.13.4 der Open-Source-Anwendung Kubernetes einem Sicherheitsaudit unterzogen. Den Abschlussbericht veröffentlichte Kubernetes am 06.08.2019 im GitHub-Repository. Code-Qualität und Dokumentation der Container-Orchestrierungs-Lösung erhalten darin keine besonders gute Bewertung. So wurde beispielsweise die gleiche Programmlogik wiederholt implementiert anstatt auf zentrale Mechanismen zu setzen. Insgesamt wird Kubernetes als sehr komplex und reich an Abhängigkeiten eingestuft, was den Code wiederum besonders fehleranfällig macht. Daher überrascht es wenig, dass die Auditoren 37 Sicherheitslücken entdeckten, von denen fünf als hoch kritisch eingestuft wurden.

Das Beispiel zeigt erneut, dass übermäßig komplexe Lösungen ein Sicherheitsrisiko darstellen – und dass Open Source nicht automatisch bedeutet, dass existierende Schwachstellen von der Community selbst aufgedeckt werden. Korrekturen, die die Komplexität der Anwendung signifikant verringern, sind nachträglich nur schwer umsetzbar, da jene häufig aus grundsätzlichen Entwurfsentscheidungen resultiert. Ein Grund mehr, Security-Aspekte schon beim Design zu berücksichtigen.

EuGH-Trend

Der Europäische Gerichtshof (EuGH) hat am 29.07.2019 über die Verantwortung bei der Einbindung von Social Media Plugins entschieden (Rs. C-40/17). Ein Webseitenbetreiber war wegen eines Facebook Like-me Buttons und der daraus resultierenden Übermittlungen an Facebook Irland abgemahnt worden. Auch wenn es sich noch auf die EG-Datenschutz-Richtlinie und die Datenschutzrichtlinie für elektronische Kommunikation (RL 95/46/EG und 2002/58/EG) bezieht, bestätigt das Urteil einen bereits in der Entscheidung C-210/16 zu Facebooks Fanpages anklingenden Trend: Veranlasst oder ermöglicht der Webseitenbetreiber eine Datenverarbeitung durch einen Plattform- oder Dienstanbieter, tendiert der EuGH zur Annahme einer gemeinsamen Verarbeitung. Die daraus folgende

gemeinsame Verantwortung soll jedoch nur die Verarbeitungsphasen umfassen, für die Mittel und Zwecke gemeinsam bestimmt werden. Beide Beteiligte benötigen eine eigenständige Rechtsgrundlage, wobei der EuGH von der Erforderlichkeit einer durch den Webseitenbetreiber einzuholenden Einwilligung ausgeht. Informieren muss der Webseitenbetreiber nur über die gemeinsam verantwortete Verarbeitung.

Die Entscheidung ist insbesondere für Tracking-Pixel hochrelevant. Für Webseitenbetreiber ist die dargestellte Verantwortungsverteilung eine gute Nachricht. Offen bleibt, wie der Social-Media- oder Tracking-Anbieter seine über die gemeinsame Verarbeitung hinausgehende Nutzung begründen kann.

Spiegelreflex-Trojaner

Am 11.08.2019 zeigte Eyal Itkin auf der Defcon, wie sich der Markt für ein funktionierendes kriminelles Geschäftsmodell vergrößern lässt. So gelang es ihm unter Kombination mehrerer Schwachstellen einen Verschlüsselungstrojaner auf die Bilder von Canon-Kameras loszulassen (Demo). Dabei nutzte er die WLAN-Verbindung und das Picture Transfer Protocol (PTP). Nutzern der betroffenen Kameramodelle mit WLAN-Schnittstelle sei daher die Aktualisierung der Firmware und die Deaktivierung der WLAN-/NFC-Schnittstelle bei Nichtgebrauch ans Herz gelegt.

DSGVO-konforme Kamerafahrten

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) informierte am 30.07.2019 über die von Apple seit Juli 2019 auch in Deutschland vorgenommenen Aufnahmen von Straßenzügen und Gebäudefronten zur Aufwertung des Apple-eigenen Kartendienstes. Die damit einhergehenden datenschutzrechtlichen Fragen wurden erstmals mit dem vergleichbaren Dienst Google Streetview vor rund 10 Jahren beleuchtet.

Zur Sicherstellung der Betroffenenrechte wurden Maßnahmen eingeführt, die nun auch bei Apple umgesetzt werden, wie bspw. die vorherige Ankündigung von geplanten Kamerafahrten, die automatische Verpixelung von Gesichtern und Kfz-Kennzeichen, die Möglichkeit der Unkenntlichmachung des eigenen Hauses, die Widerspruchsmöglichkeit gegen die Verarbeitung sowie die Angabe von Beschwerdestellen für Betroffene. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) bewertet das Vorgehen als datenschutzkonform. Eine selten gelungene datenschutzrechtliche Zusammenarbeit zwischen einem amerikanischen Unternehmen und einer deutschen Aufsichtsbehörde.

Forever Young

Backdoors sind alte Bekannte (siehe SSN 12/2007 und SSN 01/2016) – und mächtige Ansatzpunkte für Angriffe. Bereits am 03.11.2003 wurde ein spektakulärer Ansatz für eine Backdoor im Linux-Kernel öffentlich, und erst kürzlich, am 26.07.2019, berichtete Bruce Schneier über die Verurteilung eines Mitarbeiters, der bei Siemens „logic bombs“ in Code eingebaut hatte.

Am 15.08.2019 wurde nun unter der CVE-2019-15107 die Existenz einer Hintertür in den Versionen 1.900 bis 1.920 des beliebten Admin-Tools webmin bekannt. Die Besonderheit gerade dieser Schwachstelle: Sie bestand offenbar seit April 2018 – und stattete Angreifer, die sie ausnutzten, mit hoch privilegierten Rechten aus. Ein weiteres Beispiel, dass gerade verbreitete Open Source-Lösungen besonders attraktiv (und zugleich anfällig) für derartige Angriffe sind.

Secorvo News

Seminare

Nach der Sommerpause startet das Seminarangebot von Secorvo in der letzten Septemberwoche (**23.–26.09.2019**) mit dem Zertifizierungsseminar TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.), IT-Sicherheit heute (**22.–24.10.2019**) und PKI (**18.–21.11.2019**). Für den T.I.S.P. (**14.–18.10.2019**) gibt es noch einen freien Platz; das nächste T.I.S.P.-Seminar folgt in der 48. Woche (**25.–29.11.2019**). Programme und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Hallo, hier spricht Deine Zahnbürste.

Ob zu Hause, in Fahrzeugen, Industrieanlagen oder Agrarbetrieben: IoT-Anwendungen sind heute nicht mehr wegzudenken und halten in nahezu allen Bereichen Einzug in unser Leben. Bis 2020 sollen laut Gartner 20 Milliarden vernetzte Geräte im Einsatz sein. Das Internet of Things eröffnet vielfältige Chancen, jedoch mangelt es häufig an Bewusstsein für Sicherheitsaspekte. Die sichere Kommunikation der unzähligen vernetzten Dinge untereinander ist dabei die größte Herausforderung.

Warum es für Unternehmen existentiell ist, ihre IoT-Devices und den Zugriff auf ihre IoT-Plattformen abzusichern und welche aktuellen Technologien dafür zur Verfügung stehen, erläutert beim kommenden KA-IT-Si-Event am **19.09.2019** Thorsten Gahrmann von der Nexus Group. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch bei unserem „Buffet-Networking“ – diesmal wieder mit Blick über die Dächer von Karlsruhe (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2019	
17.09.	Anwendertag IT-Forensik (Fraunhofer Institut SIT, Darmstadt)
19.09.	Hallo, hier spricht Deine Zahnbürste. (KA-IT-Si, Karlsruhe)
22.-24.09.	FIfFKon 2019 (FIfF e.V., Berlin)
23.-26.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.09.	Datenschutztag 2019 (COMPUTAS, Köln)
24.-27.09.	heise devSec 2019 (dpunkt.verlag, heise Developer, heise Security, Heidelberg)
Oktober 2019	
08.-10.10.	it-sa 2019 (NürnbergMesse GmbH, Nürnberg)
14.10.	Night of the Living Labs (FZI, Karlsruhe)
14.-18.10.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
15.10.	Swiss Cyber Storm 2019 (Swiss Cyber Storm Association, Bern/CH)
22.-24.10.	IDACON 2019 (WEKA-Akademie, München)
22.-24.10.	IT-Sicherheit heute - praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)

Fundsache

Am 24.07.2019 hat Netflix unter dem Titel „The Great Hack“ eine Dokumentation des Cambridge Analytica / Facebook-Skandals veröffentlicht.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Hans-Joachim Knobloch, Michael Knopp, Sarah Niederer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

September 2019



Das Vermächtnis

Vor exakt 2.300 Tagen erwirkte das FBI einen Haftbefehl gegen Edward Snowden – seitdem ist er auf der Flucht. Ein großes Opfer für den damals knapp 30-Jährigen. Jetzt hat er seine Geschichte veröffentlicht – auf Anhieb ein Bestseller. Was aber hat Snowden tatsächlich bewirkt?

Auf den ersten Blick wenig. Ende 2013 stellte die NSA ihr Utah Data Center fertig, mit einer Speicherkapazität, die die Archivierung und Analyse der gesamten weltweiten Datenkommunikation ermöglicht. Über den US Cloud Act sicherten sich die amerikanischen Geheimdienste am 06.02.2018 den Zugriff auf die Daten ausländischer Kunden von amerikanischen Unternehmen – ein (bislang folgenloser) Affront gegen das Privacy Shield-Abkommen mit der EU vom 02.02.2016. Derweil versucht das Bundesinnenministerium, deutschen Nachrichtendiensten „technische Datenerhebungen aus Wohnungen" zu ermöglichen – schließlich verfügen immer mehr Haushalte über freiwillig installierte Abhöranlagen: Alexa, Cortana, Siri und andere Sprachassistenten lassen grüßen.

Aber es gibt auch die andere Seite. So warnen Browser inzwischen vor Webseiten, die HTTP nicht oder mit veralteten TLS-Versionen schützen – rund 90% der Webkommunikation wird inzwischen verschlüsselt. Auch dank der Initiative „E-Mail made in Germany", einer Reaktion der deutschen E-Mail-Provider auf Snowdens Veröffentlichungen, schützen heute nur noch wenige E-Mail-Server die Kommunikation nicht via TLS vor dem Zugriff Dritter. Mehrere Messenger bieten vor Geheimdiensten sichere Ende-zu-Ende-Verschlüsselung. Sogar Microsoft und Apple versuchen die Daten ihrer Kunden dem NSA-Zugriff zu entziehen, indem sie die Schlüsselgenerierung in Kundenhand legen.

Jetzt gilt es, die Spurensammlung von Google und Co. zu begrenzen – sie sind inzwischen der Ansaugstutzen der NSA im Netz. Wenn uns das nicht gelingt ist Snowdens Vermächtnis verspielt.



Inhalt

Das Vermächtnis

Security News

Sichere(re)s DNS?

Identitätsdiebstahl via Auskunft

De-Anonymizer

SIM-Jack

Unzulässige Kekse

Renitenter Sündenbock

Secorvo News

Secorvo@it-sa

3. Auflage des T.I.S.P.-Buchs

Nächste Seminare

Möge das ISMS mit dir sein

Veranstaltungshinweise

secorvo
security consulting

Security News

Sichere(re)s DNS?

Gelingt es einem Angreifer die Namensauflösung einer Domäne zu manipulieren, kann er Nutzern gefälschte Webseiten „unterschieben". Eine wirksame Gegenmaßnahme ist die Einführung von DNS over TLS oder DNS over HTTPS (DoH), doch die läuft bislang zögerlich. Am 06.09.2019 kündigte Mozilla an DoH zum Default zu machen. Der Firefox-Browser enthält bereits einen DoH-Resolver, der künftig standardmäßig alle DNS-Anfragen verschlüsselt an einenn Resolver von Cloudflare senden soll.

Für komplexere Netzkonfigurationen sind allerdings Nebenwirkungen zu erwarten, bspw. bei Split-DNS (hier wird immer die externe Namensauflösung geliefert) oder Content-Filtering Blacklists. Firefox setzt Heuristiken ein, um solche Konfigurationen zu erkennen: Beim Start versucht Firefox, eine „Canary"-Domain aufzulösen; gelingt das nicht, wird DoH abgeschaltet. Schlägt später eine DOH-Anfrage fehl, wird das Betriebssystem befragt, und ist eine Enterprise Policy im Einsatz, ist DoH standardmäßig inaktiv. Vorsicht gilt auch, falls interne Domainnamen nicht offengelegt werden sollen. Administratoren sollten DOH in Firefox erforderlichenfalls deaktivieren.

Dubiose Hotspots oder Zensur betreibende Länder können mittels der Canary-Domain die DOH-Auflösung einfach „abschalten". Und beunruhigen kann auch, dass künftig Cloudflare alle DNS-Anfragen erhält, selbst wenn der Betreiber angibt, die Daten nur für 24 Stunden zu speichern. Monopolstellungen sind immer ein Risiko – in verschiedener Hinsicht.

Identitätsdiebstahl via Auskunft

Auf der Black Hat-Konferenz stellte der Sicherheitsforscher James Pavur am 08.08.2019 einen Social Engineering-Angriff vor, der sich Fehler bei der Umsetzung der datenschutzrechtlichen Auskunftspflicht von Unternehmen zu Nutze macht. Mittels einer selbst angelegten E-Mail-Adresse gab sich Pavur gegenüber mehr als 150 Unternehmen als seine Mitautorin Casey Knerr aus und bat um Auskunft über alle zu „ihr" verarbeiteten personenbezogenen Daten. Von den Unternehmen reagierten 72%; 23% antworteten gar nicht und 5% verweigerten jede Auskunft. Von den reagierenden Unternehmen übersandten 24% die Daten ohne jede Identitätsprüfung, weitere 16% verlangten leicht zu fälschende Identitätsnachweise (wie das Ausfüllen einer schriftlichen Erklärung, tatsächlich die betroffene Person zu sein).

Dabei sollte selbstverständlich sein, dass einem datenschutzrechtlichen Ersuchen erst nach hinreichend sicherer Identitätsprüfung nachgekommen wird, z. B. durch Versand an eine authentisierte Zustelladresse, ein Login in einem bestehenden Benutzerkonto oder die Vorlage eines von einer vertrauenswürdigen Instanz ausgestellten Identitätsnachweises.

De-Anonymizer

Personenbezogene Daten sind Informationen, die sich auf eine identifizierbare natürliche Person beziehen. Dabei sind für die Identifikation in der Regel weder Name noch Adresse erforderlich: Nach einer am 23.07.2019 in „nature" veröffentlichten Studie genügen bereits 15 demografische Attribute, um 99,98% der US-Bürger zu re-identifizieren. Für eine Anonymisierung reicht es daher in der Regel nicht, in einem Datensatz lediglich den Namen und die Adresse zu löschen. Mehr noch: Je aussagekräftiger die statistischen Angaben über eine Gruppe von Personen, desto höher ist die Wahrscheinlichkeit, dass eine Re-Identifizierung Einzelner möglich ist. Mit dem wachsenden Einsatz von künstlicher Intelligenz bei Big-Data-Auswertungen dürften zukünftig vermehrt vermeintlich anonyme Datensammlungen als Verarbeitung personenbezogener Daten zu bewerten sein.

SIM-Jack

Am 12.09.2019 veröffentlichte Cathal McDaid von AdaptiveMobile Security im firmeneignen Blog einen Post über die Schwachstelle Simjacker. Darüber können sich Angreifer mittels einer präparierten SMS in der SIM-Karte einnisten. Von dort können Informationen ausgelesen oder unbemerkt Telefonverbindungen aufgebaut werden, die das Gerät in eine Wanze verwandeln. Offenbar nutzen diese Schwachstelle Angreifer mehrerer Länder schon seit mindestens zwei Jahren. Die Schwachstelle bedroht jedes mobile Endgerät, auf dessen SIM-Karte (UICC) der Netzbetreiber die Software S@T Browser, eine Alternative zum klassischen SIM Toolkit, installiert hat. Sie soll in 30 Staaten mit insgesamt über einer Milliarde Einwohnern im Einsatz sein. Immerhin: Die Netzbetreiber Telekom, Vodafone und Telefónica teilten übereinstimmend mit, dass auf ihren Karten der S@T Browser nicht installiert ist.

Die Erfahrung zeigt, dass es in komplexen IT-Systemen selten nur einen einzigen Sicherheitsbug gibt. Daher gilt (nicht nur aus diesem Grund): Gelegentliches Ausschalten hilft.

Unzulässige Kekse

Cookie-Banner finden sich inzwischen auf fast allen Webseiten – oft sind sie jedoch datenschutzrecht-

lich unzureichend. Erst am 18.09.2019 wies der Landesbeauftragte für Datenschutz- und Informationsfreiheit (LfDI) Baden-Württemberg darauf hin, dass die Nutzung der Webseite keine rechtswirksame Einwilligung darstellt. Eine Studie der Ruhr-universität Bochum zeigt, dass die meisten untersuchten Cookie-Banner nicht nur nicht DSGVO-konform sind (86%), sondern auch psychologische Tricks anwenden, um Nutzer dazu zu bringen die gewünschte Einwilligung zu erteilen. Oft wird zudem nicht darüber informiert, dass die Daten an Dritte weitergegeben werden. Das LG Dresden urteilte am 11.01.2019, dass es nicht ausreicht, die Nutzer aufzufordern, Einstellungen im Browser vorzunehmen, die das Speichern von Cookies und die Übertragung von personenbezogenen Daten verhindern – auch dies eine verbreitete Unsitte.

Bereits im Cookie-Banner muss die Möglichkeit gegeben werden, die Verwendung von Cookies abzulehnen. Hier hilft eine kurze Beschreibung, welche Cookies was an wen übermitteln. Ausführliche Hinweise und Informationen können dann in einem gesonderten Cookie-Hinweis oder in der Datenschutzerklärung folgen. Eine gute Hilfe bei der Gestaltung bieten die FAQ des LfDI Baden-Württemberg.

Renitenter Sündenbock

Ransomware-Autoren haben ein neues Angriffsziel: US-amerikanische Kleinstädte, die nicht ausreichend gegen derartige Angriffe gewappnet sind. In der Not sind sie oft bereit, das geforderte Lösegeld zu zahlen. Am 10.06.2019 wurde Lake City (Florida) Angriffsopfer – und verlor 460.000 USD (42 BTC). Daraufhin entließ man am 21.06.2019 den IT-Direktor. Brian Hawkins jedoch verklagte am 09.08.2019 die Stadt: Er habe bereits 2017 gewarnt und auf die Anschaffung eines Cloud-basierten Backup-Systems gedrängt, was aus Kostengründen abgelehnt worden sei. Nach Überzeugung von Hawkins habe die Stadt damit entschieden, das Risiko eines Cyberangriffs zu akzeptieren. Solche essentiellen Entscheidungen sind im Rahmen des Risikomanagements zu dokumentieren, sonst kann man sich später nicht darauf berufen. Im Fall von Hawkins ist dies nicht geschehen – was ihn nun in Beweisnot bringt.

Secorvo News

Secorvo@it-sa

Besuchen Sie uns vom 08. bis 10.10.2019 auf der deutschen IT-Sicherheits-Leitmesse it-sa in Nürnberg. Unseren Stand finden Sie in Halle 10, Standnummer 10.1.-630. Wir zeigen unsere „ready2go"-Managementlösungen für Informationssicherheit (ISMSr2g), Datenschutz (DSMSr2g) und die Zertifikatsverwaltung (Easy). Am 09.10.2019 spricht um 10:45 Uhr Jörg Völker im Forum M10-Management über „Die Rückkehr der ISMS-Ritter".

Sie haben noch kein Ticket? Registrieren Sie sich mit unserem Gutscheincode **A411787** und Sie erhalten ein kostenfreies Tagesticket.

3. Auflage des T.I.S.P.-Buchs

Jetzt ist sie verfügbar – die gründlich überarbeitete und ergänzte dritte Auflage des T.I.S.P.-Begleitbuchs „Informationssicherheit und Datenschutz", ein Gemeinschaftswerk des gesamten Secorvo-Teams. Wir freuen uns sehr, dass der dpunkt.verlag die Herausgabe übernommen hat. Auf der Verlagswebseite finden sich ausgewählte Leseproben des 824 Seiten umfassenden Grundlagenwerks, das nun für 84,90 € im Buchhandel erhältlich ist.

Nächste Seminare

Die letzte Gelegenheit, bei der Sie sich in diesem Jahr Ihre Qualifikation und Erfahrung in der IT-Sicherheit zertifizieren lassen können, bieten wir Ihnen in der 48. Woche mit dem nächsten T.I.S.P.-Seminar (**25.–29.11.2019**) – von über 250 Teilnehmern mit 4,35 von 5 Punkten bewertet. In der Woche davor kommen PKI-Interessierte zum Zug: In nur vier Tagen vom Einsteiger zum Experten bei unserem PKI-Seminar (**18.–21.11.2019**), Rating: 4,3. Wir freuen uns auf Ihre Teilnahme!

Alle Programme, die Seminartermine 2020 und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Möge das ISMS mit dir sein

Die Etablierung von Informationssicherheit im Unternehmen gleicht oft dem Kampf der Star-Wars-Rebellen gegen die dunkle Seite der Macht – hier dem allzu sorglosen Umgang mit schützenswerten Informationen. Dabei hilft ein Informationssicherheits-Managementsystem (ISMS).

Damit sich der Aufbau und die Zertifizierung des ISMS jedoch nicht ähnlich lange hinziehen wie der Kampf gegen das Imperium empfiehlt es sich zielstrebig vorzugehen. Der Vortrag beim kommenden KA-IT-Si-Event am **24.10.2019** fasst die grundlegenden Anforderungen der ISO 27001 zusammen und stellt die konkrete Umsetzung und Zertifizierung beim Kirchlichen Rechenzentrum Südwestdeutschland (KRZ-SWD) vor.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Oktober 2019	
08.-10.10.	it-sa 2019 (NürnbergMesse GmbH, Nürnberg)
14.-18.10.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.10.	Night of the Living Labs (FZI Forschungszentrum Informatik, Karlsruhe)
15.10.	Swiss Cyber Storm 2019 (Swiss Cyber Storm Association, Bern/CH)
22.-24.10.	IDACON 2019 (WEKA-Akademie, München)
November 2019	
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
05.-06.11.	9. Handelsblatt Jahrestagung - Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
11.-15.11.	ACM CCS 2019 (ACM/SIGSAC, London/UK)
18.-21.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-22.11.	43. DAFTA (GDD, Köln)
25.-29.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-29.11.	DeepSec In-Depth Security Conference Europe (DeepSec, Wien/AT)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Benjamin Faller, Hans-Joachim Knobloch, Friederike Schellhas-Mende, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Oktober 2019



Rechenmagie

Wer die Liste der seit Inkrafttreten der DSGVO verhängten Datenschutz-Bußgelder durchsieht, wird von deren Spanne überrascht: Sie reicht von gerade einmal einhundert Euro bis zu deutlich dreistelligen Millionenbeträgen (Marriott, British Airways). Unvermeidlich drängt sich der Eindruck auf, dass die Bußgeldhöhe keiner einheitlichen Systematik folgt, sondern eher Beliebigkeit entspringt.

Bei genauerem Hinsehen wird deutlich, dass dies drei Ursachen haben dürfte: die noch geringe Erfahrung vieler europäischer Aufsichtsbehörden mit diesem gestärkten Sanktionsinstrument, die bisher eingeschränkte Abstimmung der Aufsichtsbehörden untereinander und die strukturell neue Ausrichtung der Bußgelder an der Leistungsfähigkeit des betroffenen Unternehmens.

Erkennbar ist, dass mit wachsender Erfahrung der Aufsicht auch die Höhe der Bußgelder steigt. Vor wenigen Wochen haben sich nun die deutschen Aufsichtsbehörden auf ein Berechnungsschema geeinigt, das die Bußgeldhöhe aus dem Unternehmensumsatz ableitet und mit einem Korrekturfaktor die Schwere des Verstoßes berücksichtigt sowie materielle Verstöße stärker als formelle ahndet.

Eine zu begrüßende Entwicklung zu mehr Transparenz und Nachvollziehbarkeit. Dennoch führen Rechenmodelle nicht automatisch zu gerechteren Ergebnissen. Daher ist der wichtigste Teil des Konzepts der letzte Punkt – die Berücksichtigung täterbezogener und wirtschaftlicher Umstände bei der endgültigen Bußgeldfestsetzung. Das ist keine Beliebigkeit durch die Hintertür, sondern räumt einen Ermessensspielraum ein, der bei besonnener Nutzung zu mehr Einzelfallgerechtigkeit führen kann als das Rechenschema.

Unternehmen müssen sich daran gewöhnen, dass derselbe Datenschutzverstoß zu verschiedenen Bußgeldern führen kann. Und die Aufsichtsbehörden müssen aufpassen, dass sie bei aller pseudo-objektiver Rechenmagie nicht das Augenmaß verlieren.



Inhalt

Rechenmagie

Security News

Unauffällige Erweiterungen

Freie Kekswahl

In Code We Trust

Entflammbarer Brandschutz

Rechenhilfe

Konkretisierungen

Secorvo News

Wissensauffrischung

Geliebter Feind – Enemy Mine

Alice und Bob im Wunderland

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Unauffällige Erweiterungen

Auf der CS3STHLM-Konferenz in Stockholm zeigte der Sicherheitsforscher Monta Elkins am 24.10. 2019, wie es ihm mit einem Budget von nur $200 gelang, eine Cisco ASA 5505 Firewall um eine Hardware-Backdoor zu erweitern. Der von ihm aufgelötete ATtiny85 greift über die serielle Schnittstelle die Passwortrücksetzung an und richtet eine Hintertür mit Administrationsrechten ein. Der etwa fingernagelgroße Mikrocontroller ist ohne Schaltplan kaum als zusätzliches Bauteil erkennbar. Der Angriff erinnert stark an die von Edward Snowden und Glenn Greenwald 2014 aufgedeckten Manipulationen der NSA an Cisco-Routern auf dem Postweg und Gerüchte über chinesische Hacker, die 2018 auf Mainboards des Herstellers Supermicro einen reiskorngroßen Chip ergänzt haben sollen. Derartige Manipulationen zeigen eindrucksvoll, dass zur Herstellung sicherer Produkte auch eine sichere Lieferkette gehört. Präpariert ein Angreifer originale Firewalls oder Server und verkauft sie dann beispielsweise über Amazon Marketplace, kann er manipulierte Geräte mit geringem Aufwand verbreiten.

Freie Kekswahl

Ein kollektives Stöhnen und Wehklagen der online-Werbebranche erschallte am 01.10.2019, nachdem der EuGH in der Rechtssache C-673/13 - Planet49-GmbH entschieden hatte, dass beim Besuch einer Webseite nur technisch notwendige Cookies – so genannte Session-Cookies – ohne Einwilligung gesetzt werden dürfen. Das Urteil ist EU-weit unmittelbar umzusetzen und anzuwenden. Die deutsche Umsetzung der „Cookie-Richtlinie“ im Telemediengesetz ist nicht rechtskonform und muss angepasst werden. Voreingestellte Häkchen gehören nun ebenso der Vergangenheit an wie konkludente Einwilligungen durch Weiternutzung einer Webseite mit impliziter Duldung.

Wirksame Einwilligungen setzen voraus, dass der Seitenbetreiber die Nutzer über Third-Party-Cookies, die er zu setzen wünscht, informiert. Erst wenn Nutzer die Möglichkeit haben, eine freiwillige Entscheidung für oder gegen die Cookies zu treffen, entspricht die Einwilligung den gesetzgeberischen Anforderungen. Das bedeutet für (fast) alle Unternehmen Handlungsbedarf bei der Anpassung der Cookie-Banner auf ihren Webseiten. Ansonsten geht man das Risiko ein, in das Visier der Aufsichtsbehörden und etwaiger Abmahner zu geraten. Es ist nur ein schwacher Trost, dass auch der EuGH nach Veröffentlichung des Urteils den eigenen Cookie-Banner mehrfach anpassen musste, bis er den Vorgaben des eigenen Urteils entsprach.

In Code We Trust

Der Turing-Award-Preisträger Ken Thompson illustrierte schon 1984 in seiner Dankesrede „Reflections on Trusting Trust“, wie ein manipulierter Compiler Backdoors in Programme einbauen kann, ohne dass dabei Spuren im Quellcode zurückbleiben. Die am 24.10.2019 veröffentlichte Kombination einer XXE- und einer Directory Traversal Schwachstelle im XML Language Server (aka lsp4xml) erreicht zwar nicht ganz das Ausmaß eines manipulierten Compilers. Durch die Verwendung der Komponente in XML-Plugins diverser Entwicklungsumgebungen (Eclipse, VS-Code, ...) drängt sich allerdings immer noch die gleiche Frage auf wie vor 35 Jahren: Können wir dem Code oder der Software trauen, die wir einsetzen um neue Software zu erstellen?

Ken Thompson kam zu dem Schluss, dass dies nicht möglich ist: „*You can't trust code that you did not totally create yourself.*“ Den kompletten Code inklusive Tools und Compiler selbst zu erstellen ist heute allerdings in den seltensten Fällen überhaupt und nur mit unvertretbar hohem Aufwand möglich. Allerdings sollte es zu den Minimaltugenden gehören, nur etablierte Werkzeuge mit aktuellem Versionsstand einzusetzen und niemals „blind“ Code(schnipsel) aus unbekannten Quellen zu verwenden.

Entflammbarer Brandschutz

Immer noch fordern Auditoren, Virenschutzprodukte auf Servern einzusetzen. Aber funktionieren solche Lösungen tatsächlich effektiv als Brandschutz, oder werden sie beim nächsten Feuer nicht eher zu Brandbeschleunigern? Denn eine Virenschutzlösung, die mit erhöhten Privilegien arbeitet, kann selbst zur mächtigen Bedrohung werden. Das zeigen am 19.10.2019 und 21.10.2019 gemeldete Schwachstellen (Trend Micro Anti Threat Toolkit) und Einbrüche bei Herstellern von Sicherheitslösungen (NordVPN, Avast) sowie zahlreiche zurückliegende Fälle (SSN 3/2004, SSN 5/2014, SSN 5/2016). Deshalb sollte bei der Entscheidung für eine solche Lösung die mögliche Fehlbarkeit der eingesetzten Produkte in Risiko- und Bedrohungsanalysen sowie Sicherheitskonzepten berücksichtigt werden.

Rechenhilfe

Am 16.10.2019 präsentierte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ihr Modell zur Berechnung von Bußgeldern für Verstöße nach Art. 83 Datenschutz-Grundverordnung (DSGVO). Die Bußgeldbemessung soll damit transparent, systema-

tisch nachvollziehbar und innerhalb der EU harmonisiert werden. Das Konzept nimmt die Bußgeldzumessung in fünf Schritten vor:

- Zuordnung des Unternehmens zu einer von insgesamt 20 Größenklassen
- Bestimmung des mittleren Jahresumsatzes der jeweiligen Größenklasse
- Ermittlung eines wirtschaftlichen Grundwertes (entspricht dem durchschnittlichen Tagessatz)
- Multiplikation dieses Grundwertes mit einem von der Schwere der Tatumstände abhängigen Faktor (1-6 für formelle und 1-12 für materielle Verstöße)
- Anpassung des ermittelten Wertes unter Berücksichtigung täterbezogener und z. B. wirtschaftlicher Umstände

Nach Auffassung der DSK bestärkt dieses Konzept durch die Anknüpfung an den Unternehmensumsatz die Umsetzung des Wunschs des Europäischen Gesetzgebers nach Wirksamkeit, Verhältnismäßigkeit und abschreckender Wirkung gemäß Art. 83 Abs. 1 DSGVO. Das Bußgeldmodell ist also durchaus darauf ausgelegt, den Bußgeldrahmen möglichst umfassend auszuschöpfen.

Konkretisierungen

Der Europäische Datenschutzausschuss (EDSA) hat am 08.10.2019 Version 2.0 der Richtlinie zur „Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung von Online-Diensten“ veröffentlicht. Die Richtlinie enthält vor allem Vorgaben zur Abgrenzung der Erlaubnistatbestände im Bereich Marketing und Online-Dienste. Sie begrenzen die Verarbeitungserlaubnis „Vertrag“ strikt auf die Prozesse, die nach Erwartung des Betroffenen zur Vertragserfüllung erforderlich sind. Bereits die Aufbewahrung von vertragsbezogenen Unterlagen zu Buchhaltungszwecken soll bspw. vor allem nach Vertragsende transparent auf die gesetzliche Pflicht (Art. 6 Abs. 1 c) DSGVO) gestützt werden. Zwecke wie Service-Verbesserung, Werbung in Verbindung mit dem Vertragsgegenstand oder Betrugsabwehr können über das berechtigte Interesse des Verantwortlichen begründet werden, nicht jedoch über den Vertrag. Gewarnt wird davor, Verarbeitungen, die ein Vertrag erforderlich macht, auf Einwilligungen zu stützen, da sich die Rechtsfolgen bezüglich Widerspruch, Löschpflichten u. a. erheblich unterscheiden. Datenverarbeitung beispielsweise zum Zweck individualisierter Werbung als Gegenleistung für ein Leistungsangebot einzufordern ist nach Auffassung des EDSA unzulässig.

Die Richtlinie macht wie die Orientierungshilfe der Datenschutzkonferenz deutlich, dass innerhalb von Verarbeitungsvorgängen nach Zwecken und Rechtsgrundlagen sorgfältig differenziert werden muss, dass diese Differenzierungen Teil der Datenschutzinformationen sein sollen und dass die Rechtsgrundlagen nicht abhängig von der Darstellung austauschbar sind.

Secorvo News

Wissensauffrischung

Schnellentscheidern bieten wir noch zwei Gelegenheiten in diesem Jahr, ihre Kenntnisse in der Informationssicherheit aufzufrischen und zu erweitern: Bei unserem T.I.S.P.-Seminar (**25.–29.11.2019**) sowie dem viertägigen Intensivseminar PKI (**18.–21.11.2019**). Eine Übersicht über alle angebotenen Seminare, Programme und die Termine im Jahr 2020 sowie die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Geliebter Feind – Enemy Mine

Fast täglich kann man in den Medien von Wirtschaftskriminalität, Wirtschaftsspionage und Cybercrime lesen. Was aber verbirgt sich konkret dahinter? Welche Tätertypen gibt es, und warum wird ein Mitarbeiter nach vielen Jahren Betriebszugehörigkeit auf einmal delinquent? Und was meinen Begriffe wie „wirtschaftskriminologisches Belastungssyndrom“ oder „Competitive Intelligence“? Wird man im eigenen Unternehmen mit einem solchen Vorfall konfrontiert, stellen sich viele Fagen: Was ist dem „internen Ermittler“ erlaubt und was nicht? Wann sollten Strafverfolgungsbehörden eingeschaltet werden? Und warum helfen Systeme wie ein IKS nur bedingt gegen Wirtschaftskriminalität?

Auf diese Fragen gibt Andreas Schäfer (VBK) auf dem nächsten KA-IT-Si-Event am **05.12.2019** Antworten und zeigt, wie Unternehmen sich im Vorfeld schützen und – im schlimmsten Fall – verteidigen können. Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (Anmeldung).

Alice und Bob im Wunderland

Zu einer Veranstaltung der ganz anderen Art laden wir Sie herzlich zusammen mit dem Forschungszentrum Informatik (FZI) am **14.11.2019** ein. Mit einem Vortrag von Tobias Schrödel über das Darknet und zahlreichen Live-Demos präsentiert Ihnen die IT-Sicherheitsregion Karlsruhe das „Wunderland der IT-Sicherheit“ im Karlsruher Palazzo. Lassen Sie sich von einem wunderbaren Abend verzaubern... Wir empfehlen eine schnelle Anmeldung, da die Zahl der Plätze begrenzt ist.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2019	
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
05.-06.11.	9. Handelsblatt Jahrestagung – Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
11.-15.11.	ACM CCS 2019 (ACM/SIGSAC, London/UK)
18.-21.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-22.11.	43. DAFTA (GDD, Köln)
25.-29.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-29.11.	DeepSec In-Depth Security Conference Europe (DeepSec, Wien/AT)
Dezember 2019	
03.12.	Black Hat Europe 2019 (Blackhat, London/UK)
05.-06.12.	8. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Berlin)
10.12.	GERMAN OWASP DAY 2019 (OWASP Foundation, Karlsruhe)

Fundsache

Nachdem der Heise-Verlag im Frühjahr 2019 Opfer eines Emotet-Angriffs wurde, hat er nicht den Deckmantel des Schweigens über diesen Vorfall gebreitet, sondern ist sowohl mit einer Aufarbeitung als auch einer FAQ zu diesem Thema an die Öffentlichkeit gegangen. Die Erkenntnisse sind lesenswert.



Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Michael Knöppler, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

November 2019



Denial of Service

Für viele Prediger der Digitalisierung sind vor allem personenbezogene Daten das „Öl" des 21. Jahrhunderts. Sehen wir einmal davon ab, dass das Bild ein wenig Schräglage hat (Daten sind keine in Jahrmillionen entstandene endliche Ressource), so ist die Botschaft doch klar: Die Rockefeller von morgen brauchen sehr, sehr viele Daten. Blöd nur, dass der ungebremsten Abschöpfung dieses Rohstoffs der Datenschutz entgegensteht. Daher forderte der damalige Bundesminister für Verkehr und digitale Infrastruktur, Alexander Dobrindt (CSU), in seinem „Strategiepapier Digitale Souveränität" (sic!) schon im März 2017 eine „neue Datenkultur: Weg vom Grundsatz der Datensparsamkeit hin zu einem kreativen, sicheren Datenreichtum." Und nicht nur er.

Dabei könnte sich das Problem von selbst erledigen. Zwar dürfen Daten ohne Zustimmung der Betroffenen nur unter drei Voraussetzungen verarbeitet werden: Ihre Verarbeitung ist zur Erfüllung eines Vertrags mit den Betroffenen erforderlich, der Verarbeiter hat ein (die schutzwürdigen Bedürfnisse der Betroffenen) überwiegendes, berechtigtes Interesse oder es gibt ein Gesetz, das die Verarbeitung vorschreibt – und mit Art. 8 der EU-Grundrechtscharta vereinbar ist. Daher bleibt oft nur, die Einwilligung der Betroffenen einzuholen.

Das haben die Datenverarbeiter inzwischen verstanden. Und holen Einwilligungen ein. In jeder App, auf jeder Webseite und in jedem Vertrag – selbst dann, wenn eine der oben genannten Voraussetzungen bereits erfüllt ist. Und die Betroffenen klicken und unterschreiben, so oft und ritualisiert, dass sie nicht nur die Datenschutzerklärung ignorieren, sondern die Bestätigung der Kenntnisnahme schon als bürokratische Zumutung empfinden.

So degeneriert der Königsweg der informationellen Selbstbestimmung zum Freibrief für jede Art der Verarbeitung. Kein Science-Fiction-Autor hätte sich das besser ausdenken können: Entscheidungs-Overload durch einen Denial-of-Service-Angriff auf den freien Willen.



Inhalt

Denial of Service

Security News

Doppelte Timing-Attacke

Mit OWASP wäre das nicht passiert

Rechtskonformes Tracking

Hungernde Haustiere

Tails 4.0

Teurer Datenfriedhof

Secorvo News

Enemy Mine – Geliebter Feind

Seminare 2020

Türchen für Türchen

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Doppelte Timing-Attacke

Unter dem Namen TPM-Fail publizierte ein internationales Forscherteam am 13.11.2019 eine Timing-Attacke, mittels derer sich private ECDSA-Schlüssel aus sicherheitszertifizierten Trusted-Platform-Modulen (TPMs) von Intel und STMicro extrahieren lassen. Bereits am 03.10.2019 hatten tschechische Forscher unter dem Namen Minerva eine verblüffend ähnliche Attacke u. a. gegen eine Smartcard von Athena veröffentlicht. Die Ähnlichkeit ist nicht zufällig – beide Arbeiten beziehen sich auf dieselbe Publikation aus dem Jahr 2011. Da beide Gruppen CVEs für ihre jeweiligen „Opfer" angemeldet hatten, bevor die andere Arbeit publiziert wurde, darf man von parallelen Entdeckungen ausgehen – und nicht von einem Plagiat.

Die Angriffe demonstrieren (wieder einmal), dass Sicherheitszertifikate für Produkte nur so viel wert sind wie die Sorgfalt bei deren Zertifizierung. Dabei sollte man auch das Kleingedruckte lesen: Die Anfälligkeit der Smartcard-Library gegen Seitenkanalangriffe war schon bei der Zertifizierung bekannt. Zertifiziert wurde daher nur die resistente Variante der ECDSA-Funktionen des Chip. Wenn aber ein Sicherheitschip Kryptofunktionen sowohl in einer „secure"- als auch in einer „fast"-Variante anbietet, welche wird ein Entwickler wohl nutzen?

Immerhin hat sich EdDSA als härtere Nuss im Vergleich mit ECDSA erwiesen: Die EdDSA-Erfinder erläuterten am 24.10.2018, dass dies kein Zufall ist. Gegen Seitenkanalangriffe hilft eben auch Prävention beim Entwurf des Kryptoverfahrens.

Mit OWASP wäre das nicht passiert

Am 25.10.2019 wurde eine lesenswerte Beschreibung von zwei kritischen Schwachstellen (CVE-2019-16663, CVE-2019-16662) im freien Netzwerktool rConfig veröffentlicht. Damit war es in den betroffenen Versionen möglich, aus der Ferne ohne Authentifizierung beliebige Kommandos als root-Benutzer auszuführen.

Hätten die Entwickler den schon im Herbst veröffentlichten Release-Candidate der OWASP API Security Top 10 gekannt und angewendet, wäre dieser Fehler zu vermeiden gewesen: Darin werden die API-Schwachstellen „Broken Authentication" und „Broken Object Level Authorization" behandelt, die bei rConfig ausgenutzt werden konnten.

Rechtskonformes Tracking

In enger Taktung erscheinen derzeit Nachrichten zum Thema Cookies, Webtracking und Einwilligung. Am 14.11.2019 veröffentlichten 12 Landesdatenschutzbeauftragte und der Bundesdatenschutzbeauftragte einen eindringlichen Hinweis unter der Überschrift „Personenbezogenes Webtracking nur mit Einwilligung". Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) wies in seiner Pressemitteilung explizit darauf hin, dass die „Hinweise des HmbBfDI zum Einsatz von Google Analytics" (sprich: seine eigenen) längst überholt und zurückgezogen seien: Ein Auftragsverarbeitungsverhältnis läge nach derzeitigem Sachstand dabei nicht vor.

Diese Pressemitteilungen müssen als Warnung an diejenigen verstanden werden, die sich noch nicht oder nicht ausreichend um einen DSGVO-konformen Einsatz ihrer Trackingtools und die DSGVO-gerechte Gestaltung der Cookie-Banner gekümmert haben. Am einfachsten ist es immer noch, gänzlich auf derartige Hilfsmittel – insbesondere unter Zuhilfenahme von Diensten Dritter – zu verzichten oder sie so lange abzustellen, bis ein DSGVO-konformer Einsatz gewährleistet ist.

Hungernde Haustiere

Mit der Futterstation FurryTail können Haustiere während der Abwesenheit der Bewohner per App mit passenden Futtermengen versorgt werden. Am 24.10.2019 publizierte die russische Sicherheitsforscherin Anna Prosvetova via Telegram (Account @theyforcedme) eine in fast 11.000 via Internet erreichbaren Geräten ausnutzbare Schwachstelle in der API bei der Autorisierungsprüfung, über die die Geräte von Unberechtigten ferngesteuert werden können.

Immer wieder werden in Smart-Home-Produkten elementare Schwachstellen entdeckt. Die Geräte werden möglichst billig von Drittanbietern für bekannte Marken entwickelt; auch die Tierfutterstation stammt nicht von Xiaomi selbst. Sicherheit ist dabei selten ein Qualitätskriterium. Durch die Internetanbindung solcher Geräte entstehen nicht nur neue Angriffsmöglichkeiten, sondern auch Geschäftsmodelle: Kann ein Unberechtigter die Futterausgabe remote blockieren, werden Haustierbesitzer erpressbar.

Tails 4.0

Die bereits in den SSN 06/2014 vorgestellte Distribution „Tails 1.0" für einen anonymen Internetzugriff wurde in der Zwischenzeit mehrfach überarbeitet. Am 22.10.2019 wurde die runderneuerte Version 4.0 veröffentlicht. Tails ermöglicht (wie Whonix) auch technisch weniger versierten Menschen eine einfache Nutzung des anonymen Tor-Netzwerks.

Version 4.0 verwendet Debian 10 als Plattform und aktuelle Anwendungen wie den Tor-Browser 9.0. Schwachstellen in den eingesetzten Softwarekomponenten wurden behoben. Für Nutzer ist wichtig, dass sie am System, am Browser und an den Plugins keine Veränderungen vornehmen, da sie sich sonst ggf. hierüber ungewollt zu erkennen geben. Tails kann von DVD, einem USB-Stick oder als virtuelle Maschine genutzt werden.

Teurer Datenfriedhof

Erst in den SSN 10/2019 haben wir das Thema Bußgeldbemessung bei Datenschutzverstößen thematisiert. Nun hat die Berliner Beauftragte für Datenschutz- und Informationssicherheit am 05.11.2019 gegen die Deutsche Wohnen SE das bisher höchste Bußgeld in Deutschland in Höhe von 14,5 Mio. € verhängt.

Schuld ist ein „Datenfriedhof" – und die unzureichende Trennung aufbewahrungspflichtiger von anderen personenbezogenen Daten. Werden personenbezogene Daten verarbeitet, muss jeweils geprüft werden, ob diese aufgrund steuerrechtlicher Vorgaben aufbewahrt werden müssen. Falls nicht, sind sie zu löschen, sobald sie für den Verarbeitungszweck nicht mehr erforderlich sind.

Bei der Anschaffung entsprechender Archivierungssysteme ist darauf zu achten, dass das System eine Löschung ermöglicht. Wer das versäumt, den kann die rechtswidrige Aufbewahrung wie im vorliegenden Fall teuer zu stehen kommen.

Secorvo News

Enemy Mine – Geliebter Feind

Fast täglich kann man in den Medien von Wirtschaftskriminalität, Wirtschaftsspionage und Cybercrime lesen. Was aber verbirgt sich konkret dahinter? Welche Tätertypen gibt es, und warum wird ein Mitarbeiter nach vielen Jahren Betriebszugehörigkeit auf einmal delinquent? Und was meinen Begriffe wie „wirtschaftskriminologisches Belastungssyndrom" oder „Competitive Intelligence"? Wird man im eigenen Unternehmen mit einem solchen Vorfall konfrontiert, stellen sich viele Fragen: Was ist dem „internen Ermittler" erlaubt und was nicht? Wann sollten Strafverfolgungsbehörden eingeschaltet werden? Und warum helfen Systeme wie ein IKS nur bedingt gegen Wirtschaftskriminalität?

Auf diese Fragen gibt Andreas Schäfer (VBK) auf dem nächsten KA-IT-Si-Event am 05.12.2019 Antworten und zeigt, wie Unternehmen sich im Vorfeld schützen und – im schlimmsten Fall – verteidigen können. Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (Anmeldung).

Seminare 2020

Mit einem T.I.S.P.-Seminar ist Ende November die Seminar-Saison 2019 bei Secorvo ausgeklungen. Im kommenden Jahr bieten wir Ihnen wieder zahlreiche Gelegenheiten, Ihre Kenntnisse in der IT-Sicherheit zu erweitern und Ihre Qualifikation zu zertifizieren. Das vollständige Programm mit allen Terminen und der Möglichkeit zur Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Türchen für Türchen

Kinder für das Thema Datensicherheit zu sensibilisieren und ihnen dabei spielerisch Verständnis für Verschlüsselungstechniken zu vermitteln ist das Ziel des Online-Adventskalenders „Krypto im Advent". Auch für diesen inzwischen fünften Kalender haben sich die Karlsruher IT-Sicherheitsinitiative und die Pädagogische Hochschule Karlsruhe wieder spannende Krypto-Rätsel für die Vorweihnachtszeit ausgedacht: Es gilt, alte und neue Verschlüsselungstechniken zu entdecken und dabei tolle Sachpreise zu gewinnen.



Schülerinnen und Schüler der Klassen 3 bis 6 können mit den Agenten Krypto und Kryptina und dem Agentenhund Kryptix im Zirkus auf Undercover-Mission gehen; Fortgeschrittene (7. bis 9. Klasse) helfen dem Agenten-Team, den Code des internationalen Agentenregisters zurück zu ergattern. Auch Schulklassen und Profis können miträtseln, letztere allerdings außer Konkurrenz. Anmeldungen sind ab sofort auf krypto-im-advent.de möglich – die Teilnahme ist wie immer kostenlos.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Dezember 2019	
03.12.	Black Hat Europe 2019 (Blackhat, London/UK)
05.12.	Geliebter Feind – Enemy Mine (KA-IT-SI, Karlsruhe)
05.-06.12.	8. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Berlin)
10.12.	GERMAN OWASP DAY 2019 (OWASP Foundation, Karlsruhe)
27.-31.12.	Chaos Communication Congress 36C3 (Chaos Computer Club, Leipzig)
Januar 2020	
20.-22.01.	Omnisecure 2020 (in TIME, Berlin)
21.-24.01.	AppSec California 2020 (OWASP Foundation, Santa Monica/US)>
31.01.-02.02.	ShmooCon 2020 (The Shmoo Group, Washington/US)

Fundsache

Das NIST Cybersecurity Framework v1.1 ist eine am 16.04.2018 publizierte Sammlung von nach Phasen (Identify, Protect, Detect, Respond, Recover) sortierten IT-Schutzmaßnahmen, die eine umfassende Hilfestellung zur Organisation der Informationssicherheit darstellt. Wertvoll sind auch die zusätzlichen Verweise, wo sich einzelne Maßnahmen in den bekanntesten Sicherheitsstandards wiederfinden.

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Friederike Schellhas-Mende

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Dezember 2019



Zauberlehrlinge

Walle! Walle manche Strecke, dass zum Zwecke Software fließe, und mit reichem, vollem Schwalle in den Rechner sich ergieße.

Das haben wir weder gewollt noch gemeint, als wir in den späten 90er Jahren regelmäßige Sicherheits-Patches forderten: Wer sich heute mit dem Internet verbindet, um einige wenige Sätze lange E-Mails abzurufen, wundert sich regelmäßig über sein rapide schrumpfendes Downloadkontingent. Denn nicht selten laden Rechner und Smartphones täglich Updates für Programme („Apps") und Betriebssystem im Umfang von mehreren Gigabyte – je Gerät in etwa das Volumen aller täglichen Twitter-Nachrichten zusammen, weltweit.

Kein Wunder, dass Bandbreiten knapp und Netze ständig überlastet sind. Herstellern und Providern kann das wohl recht sein – der ungebändigt steigende Datenhunger nährt ihre Geschäfte, und der Kunde zahlt, ohne zu bemerken, dass es gar nicht seine Nutzung ist, die den Datenverkehr verursacht. Dabei scheint das eine das andere zu befeuern: Die Frequenz, in der Apps heute aktualisiert werden, legt nahe, dass die Hersteller es mit der Sorgfalt nicht (mehr) so genau nehmen. Warum auch, wenn man schon morgen das nächste Update nachschieben und die (Sicherheits-) Tests auf den Kunden auslagern kann?

Und so sind wir dabei, das Verhältnis von Nutzdaten zum gesamten Datenvolumen rapide zu verschlechtern. Zum Glück sind da noch die Video-Streamer, sonst wären wir wohl schon deutlich unter der Ein-Prozent-Marke. Und während unsere Kinder freitags im Namen von Umwelt und Zukunft die Schule schwänzen, verbraten ihre Smartphones und die zugehörige Netzwerkinfrastruktur über 90% der Energie für die Übermittlung von Wegwerfcode, der schon bald durch ein Update ersetzt werden wird.

Diesmal ist es mit einem „*In die Ecke, Besen! Besen! Seids gewesen.*" des Meisters wohl nicht getan.



Inhalt

Zauberlehrlinge

Security News

Top 25 Software Errors

DSGVO-Erfahrungen

Responsible Disclosure

Schuld ist immer der Andere

German OWASP Day 2019

RSA-240 faktorisiert

DSGVO-konformes Win10

Secorvo News

... und noch nie zu fragen wagten.

Veranstaltungshinweise

Fundsache

Security News

Top 25 Software Errors

Neben dem bekannten CVE-System zur eindeutigen Identifizierung von konkreten, produktspezifischen Schwachstellen bietet die weniger bekannte „Common Weakness Enumeration“ (CWE) eine detaillierte Übersicht und Kategorisierung bekannter Fehler in Software. Die gefährlichsten werden in der Liste der „Top 25 Most Dangerous Software Errors“ geführt, die am 18.09.2019 zum ersten Mal seit acht Jahren neu erstellt wurde. Dafür wurden ca. 25.000 CVE-Einträge und deren Verknüpfungen zu CWE-Einträgen aus den vergangenen zwei Jahren ausgewertet. SQL Injections fielen dabei von Platz 1 auf Platz 6 zurück, während Cross-Site Scripting (XSS) und Out-of-Bounds-Speicherzugriffe (wie z. B. „Buffer Overflows“) die neue Liste anführen.

Die detaillierten Erläuterungen der Fehlertypen mit Code-Beispielen in mehreren Programmiersprachen und Vorschlägen für Gegenmaßnahmen aus unterschiedlichen Perspektiven sind eine empfehlenswerte Handreichung für jeden Software-Entwickler.

DSGVO-Erfahrungen

Am 06.11.2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) einen Erfahrungsbericht über die DSGVO-Umsetzung verabschiedet und Anfang Dezember veröffentlicht. Darin werden die Bereiche Informationspflichten, Recht auf Unterlagenkopien, Benennungspflicht des Datenschutzbeauftragten, Vorfallsmeldungen, Zweckbindung, Sanktionspraxis, Privacy by design, Direktwerbung, Profiling und einige eher die Zusammenarbeit der Behörden betreffende Fragen diskutiert. Zu einer Reihe von Regelungen werden Änderungsvorschläge gemacht.

Dabei wird deutlich, dass es sich um Erfahrungen der Aufsichtsbehörden handelt – der radikalste Vorschlag ist die Streichung der Meldepflicht des Datenschutzbeauftragten; die Veröffentlichungspflicht reiche aus. Der ausufernde Informationskatalog des Art. 13 f DSGVO soll bei zu erwartender Verarbeitung nur auf Verlangen erteilt werden. Weiter wird der Anstieg von Bagatellmeldungen beklagt – die in vielen Fällen entbehrliche 72-Stunden-Frist wird hingegen nicht thematisiert. Zwar wird der Bedarf eines Datenschutzmanagements festgestellt, aber dessen konkrete Ausgestaltung nicht diskutiert. Für das Profiling wird eine Verschärfung des Verbots aus Art. 22 DSGVO gefordert und für Art. 25 DSGVO (Privacy by design) eine Ausdehnung auf die Hersteller als Adressaten.

Insgesamt hätte man dem Bericht mehr Mut zur kritischen Vernunft, einen weniger eingeschränkten Blick sowie einen größeren Themenumfang gewünscht.

Responsible Disclosure

Am 09.12.2019 bat die Internet Engineering Task Force (IETF) um eine letzte Kommentierung des Drafts „A Method for Web Security Policies“. Dieser Internet-Standard spezifiziert die Informationen für Sicherheitsforscher, wie gefundene Schwachstellen bei den Betreibern gemeldet werden können. Die Ablage soll in einer Datei namens „security.txt“ erfolgen, die Webseitenbetreiber auf ihrem Webserver im Verzeichnis „/.well-known/“ ablegen. Vorgesehen sind neben den üblichen Kontaktdaten (E-Mail, Telefon) auch Bug-Bounty-Programme, und zwar sowohl solche des Betreibers als auch von Plattformen wie HackerOne oder Bugcrowd. Noch vor Verabschiedung des Standards bietet der Webdienst securitytxt.org bereits eine Funktion zum Erstellen einer solchen Datei und hilfreiche Hinweise zum Thema. Es wäre erfreulich, wenn sich diese Meldewegedokumentation in der Praxis durchsetzt.

Schuld ist immer der Andere

Am 05.12.2019 hat das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein den Volltext des Urteils des Bundesverwaltungsgerichts (BVerwG) vom 11.09.2019 veröffentlicht und in einer Pressemitteilung kommentiert. Kernpunkt war die Frage, ob der Betreiber einer Facebook Fanpage datenschutzrechtlicher Verantwortlicher ist oder nicht. Der im Rahmen des Vorabentscheidungsersuchens mit dieser Frage ebenfalls befasste EuGH hatte dies bereits am 05.06.2018 bejaht (SSN 07/2018). Das BVerwG hat nun in den Urteilsgründen klargestellt, dass es beim Betrieb der Fanpages nicht nur einen Fall der gemeinsamen Verantwortlichkeit sieht, sondern dass darüber hinaus auch der Betreiber der Facebook Fanpage verantwortlich im Sinne von Art. 2 lit. d) der Datenschutzrichtlinie ist. Weiter sei auch das BDSG alter Fassung unionsrechtskonform auszulegen, und deshalb sei auch der Betreiber einer Facebook Fanpage verantwortliche Stelle im Sinne des § 38 Abs. 5 BDSG a.F., unabhängig davon, ob im Rahmen einer gemeinsamen Verantwortlichkeit die Verantwortlichen in gleichem Maße Zugriff auf die personenbezogenen Daten haben.

Das Urteil bezieht sich allerdings auf die Rechtslage im Dezember 2011. Fanpage-Betreiber werden aber auch zukünftig Adressaten von ähnlichen Verfügungen sein können. Wie die Rechtmäßigkeit der Verarbeitungen durch Facebook nach aktueller Rechtslage zu beurteilen ist, bleibt im Urteil unbeantwor-

tet. Wer eine Facebook Fanpage betreibt, sollte sich jedoch seiner desbezüglichen Verantwortung bewusst sein und die notwendigen Maßnahmen zur Information der Betroffenen ergreifen sowie den Schutz der personenbezogenen Daten ernst nehmen.

German OWASP Day 2019

Am 10.12.2019 fand der German OWASP Day in Karlsruhe statt. Die gut besuchte und sehr gut organisierte Veranstaltung bot eine Reihe spannender und interessanter Vorträge. Besonders gut gefallen haben uns die Keynote von Christoph Kerschbaumer zu den verschiedenen Schichten der Firefox-Härtung und der von Jiska Classen sehr unterhaltsam vorgetragene Hack von Vorwerk-Staubsauger-Robotern. Empfehlenswert auch die von Franziska Bühler vorgestellte Möglichkeit von "ModDevOpsSec" – ein pragmatisches Vorgehen, wie man Security bei DevOps berücksichtigen und in das Ganze auch noch eine Web Application Firewall auf Basis von ModSecurity integrieren kann. So kann die Absicherung von Web Applikationen tatsächlich gut funktionieren.

RSA-240 faktorisiert

Am 02.12.2019 informierte eine Gruppe französischer Zahlentheoretiker um Emmanuel Thomé, dass ihnen die Faktorisierung von RSA-240 (795 bit) der RSA Factoring Challenge aus dem Jahr 1991 gelungen sei. Der Aufwand lag dank verbesserter Algorithmen rund 25% unter dem der Faktorisierung von RSA-232 (768 bit) vor ziemlich genau zehn Jahren (SSN 01/2010). Die Faktorisierungserfolge machen damit eine „Seitwärtsbewegung“ – und bleiben deutlich unter unserer Prognose aus dem Jahr 2002. Mit der Faktorisierung eines 1024-bit-Schlüssels (RSA-309) ist für das Jahr 2020 also eher nicht zu rechnen. Die Faktorisierung eines doppelt so langen, 2048-bit-RSA-Schlüssels (RSA-617) dürfte nach der Prognose nicht vor 2060 gelingen – wären da nicht die Quantencomputer, denen das (zumindest theoretisch) innerhalb von acht Stunden gelingen könnte, wie von Craig Gidney und Martin Ekera am 05.12.2019 beschrieben.

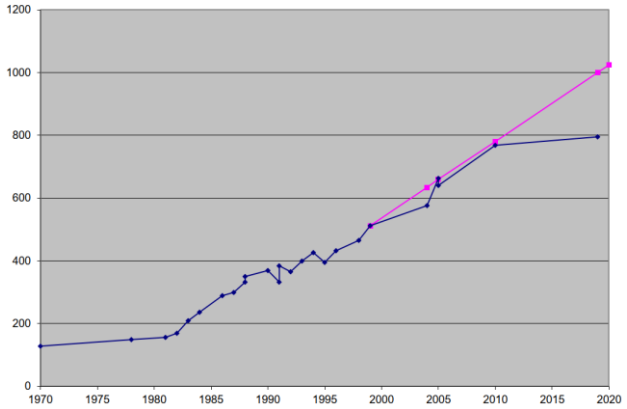


Abb.: Faktorisierungserfolge (blau), Prognose (rot)

DSGVO-konformes Win10

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat am 06./07.11.2019 ein Prüfschema zu Windows 10 veröffentlicht, das Verantwortliche in der Beantwortung der Frage unterstützt, ob Windows 10 DSGVO-konform eingesetzt wird.

Nach dem Prüfschema für Windows 10 und den zugehörigen wietergehenden technischen Hinweisen der DSK ist dafür insbesondere zu prüfen, ob eine Rechtsgrundlage für eine Übermittlung an Microsoft vorliegt. Da sich nicht alle Datenübermittlungen deaktivieren lassen, müssen erforderlichenfalls weitere technische und organisatorische Maßnahmen ergriffen werden, um unzulässige Übermittlungen zu unterbinden.

Secorvo News

... und noch nie zu fragen wagten.

Keine Novellierung des Datenschutzrechts hat eine solche Aufmerksamkeit bekommen wie die im Mai 2018 in Kraft getretene Datenschutz-Grundverordnung. Obwohl fast alles beim Alten geblieben ist, ist doch alles anders... und sind viele konkrete Fragen offen: Wann ist das Tracking von Webseitenbesuchern zulässig? Wie kann ein Unternehmen seine Informationspflichten angemessen erfüllen? Welche Datenschutzvorfälle sind meldepflichtig? Wie bestimmt sich die Höhe eines Bußgelds?

Zu diesen, weiteren und auch Ihren Fragen zur DSGVO und dem Datenschutz wird uns auf dem Jahresstart-Event der KA-IT-Si am **13.02.2019** Dr. Stefan Brink, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Rede und Antwort stehen. Wir freuen uns sehr auf diesen Termin, denn Dr. Brink ist für seine klaren Einschätzungen bekannt – und hoffen auf großes Interesse Ihrerseits.

Wir empfehlen eine frühzeitige Anmeldung.



Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2020	
20.-22.01.	Omnisecure 2020 (in TIME, Berlin)
21.-24.01.	AppSec California 2020 (OWASP Foundation, Santa Monica/US)
31.01.-02.02.	ShmooCon 2020 (The Shmoo Group, Washington/US)
Februar 2020	
19.-20.02.	30. ID:SMART Workshop (Fraunhofer Institut SIT, Darmstadt)
24.-25.02.	27. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
März 2020	
09.-12.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-20.03.	GI Sicherheit 2020 (Gesellschaft für Informatik, Göttingen)
25.-26.03.	secIT 2020 (Heise Medien, Hannover)

Fundsache

Das BSI bietet im Rahmen des Services BSI für Bürger eine Reihe von Erklärvideos an. Die anschaulich animierten Kurzfilme weisen auf wichtige Aspekte der IT-Sicherheit wie Backup, Browsersicherheit, Phishing und das Löschen von Daten auf Smartphones hin. Empfehlenswert.

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Fabian Ebner, Stefan Gora, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Christian Titze.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Januar 2020



Clear View

Eigentlich nicht überraschend, und doch ist die Empörung groß: Kashmir Hill, eine Reporterin der New York Times, löste am 18.01.2020 mit einem Bericht über Clearview AI einen Shitstorm aus. Die KI-Gesichtserkennung des Startups eines Australiers wird von mehr als 600 amerikanischen Strafverfolgungsbehörden genutzt – Claim: "Technology to help solve the hardest crimes". Lädt man ein Personenfoto hoch, durchsucht Clearview seine Datenbank mit rund drei Milliarden Bildern aus öffentlichen Quellen nach solchen, auf denen dieselbe Person abgebildet ist, und liefert die Bildquelle sowie, falls bekannt, den Namen und die Adresse der erkannten Person.

Die Technik dahinter ist kein Hexenwerk, sondern ein übliches biometrisches Gesichtserkennungsverfahren mit neuronalem Netz für die Ähnlichkeitssuche. Auch Microsoft bietet in Azure einen vergleichbaren Dienst. Neu ist bestenfalls die offenbar hohe Erkennungsrate. Da ist es kein großer Schritt zu einer Datenbrille, die auch gleich alle im Internet verfügbaren Informationen zu jeder erkannten Person anzeigt. So etwas gibt es bereits, und auch Clearview hat eine solche Brille entwickelt – will sie aber angeblich nicht auf den Markt bringen.

Gesichtserkennung, wie sie Clearview einsetzt, ist als Authentifikationsmechanismus bereits weit verbreitet; Apple bietet sie unter der Bezeichnung „Face ID" als Passwortersatz an. Und da sollten unsere Alarmglocken noch lauter anschlagen. Denn Gesichtserkennungssysteme berechnen aus dem Bild ein 3D-Modell des Gesichts, das mit Referenzwerten verglichen wird. Wer aber dieses Modell kennt (das sich aus jedem Personenfoto berechnen lässt), kann daraus schon heute täuschend echte Bilder erzeugen. Im Unterschied zu Passwörtern ist bei Gesichtserkennungssystemen allerdings ein „Passwortwechsel" nicht so einfach. Angesichts der Niedrigzinsen könnte es daher eine gute Idee sein, in Kliniken der plastischen Chirurgie zu investieren. Oder, besser noch, in die Unsichtbarkeits-Forschung.



Inhalt

Clear View

Security News

Fotos auf Facebook Fanpage

Überraschungsei WPA3

Querschnittsprüfung zur DSGVO

Presenter-Lücke

Amerikanische Inseln

Secorvo News

Wissen ist Macht

... und noch nie zu fragen wagten.

Veranstaltungshinweise

Security News

Fotos auf Facebook Fanpage

Mit Urteil vom 27.11.2019 hat das VG Hannover bestätigt, dass die niedersächsische Datenschutz-Aufsichtsbehörde (LfD Niedersachsen) zu Recht eine Verwarnung gegenüber einer Partei ausgesprochen hat, weil diese ohne Einwilligung Personenfotos auf ihrer Facebook Fanpage veröffentlicht hatte.

Demnach stellt die Veröffentlichung der Bilder einen Verstoß sowohl gegen Art. 6 Abs. 1 lit. e und f DSGVO als auch gegen §§ 22, 23 KUG dar. Für die Rechtmäßigkeit der Veröffentlichung fehlt die notwendige Einwilligung. Allein die Teilnahme an einer Veranstaltung stellt keine konkludente Einwilligungshandlung dar. Die Veröffentlichung auf einer Facebook Fanpage ist mit einer Veröffentlichung in Presseberichterstattungen nicht vergleichbar.

Soweit einzelne Personen aus Bildern hervortreten, ob nur als Beiwerk oder bei einer Bildberichterstattung über Menschenansammlungen wie Karnevalsumzüge o. ä., ist eine Interessenabwägung durchzuführen, um das Persönlichkeitsrecht der abgebildeten Personen zu wahren. Eine Veröffentlichung der Bilder auf Facebook steht diesem Interesse entgegen, da nicht kontrollierbar ist, wie die Bilder weiterverwendet werden. Damit hätte für eine rechtmäßige Veröffentlichung der Bilder eine Einwilligung der abgebildeten und hervortretenden Personen eingeholt werden müssen.

Vor der Veröffentlichung von Fotos auch öffentlicher Veranstaltungen in sozialen Netzwerken, bei denen einzelne Personen klar erkennbar sind, sollte demnach immer eine Einwilligung der Betroffenen eingeholt werden.

Überraschungsei WPA3

Am 06.01.2020 erschien das Linux-basierte Router-Betriebssystem OpenWRT in der neuen Hauptversion 19.07. Neben einer Vielzahl von Verbesserungen unterstützt OpenWRT auch erstmalig WPA3 (SSN 01/2018). Die im April 2019 entdeckten diversen Schwachstellen im Handshake-Protokoll von WPA3 Personal (SSN 04/2019) und die im August 2019 vorgestellten Seitenkanalangriffe, die bei Umsetzung der Sicherheitsempfehlungen der Wi-Fi Alliance gegen die vorherigen Angriffe möglich sind, wurden in der mit OpenWRT ausgelieferten Version von „hostapd“ alle bereits behoben.

Generell sollte vor dem Einsatz von WPA3 Personal überprüft werden, ob die bekannten Schwachstellen in der jeweiligen Implementierung bereits behoben sind. Wer WPA3 Enterprise nutzt, ist davon nicht betroffen, da hier SAE nicht zum Einsatz kommt.

Angesichts der bereits gefundenen Lücken sind weitere Nachbesserungen am WPA3-Standard nicht ganz unwahrscheinlich. Wer WPA3 nutzen möchte, sollte Firmware-Aktualisierungen im Auge behalten und einen Hersteller mit vertrauenswürdiger Update-Strategie wählen.

Querschnittsprüfung zur DSGVO

Die Landesbeauftragte für den Datenschutz Niedersachsen, Barbara Thiel, führte Ende Juni 2018 die bislang größte anlassunabhängige und branchenübergreifende Querschnittsprüfung zur Umsetzung der DSGVO durch. Die Überprüfung erfolgte anhand eines zehn Gliederungspunkte umfassenden Fragebogens zur Darstellung der Umsetzung der DSGVO, der nach rund 200 Einzelkriterien ausgewertet wurde. 50 ausgewählte mittelgroße und große Unternehmen hatten sich an der Befragung beteiligt.

Der 36seitige Abschlussbericht wurde am 05.11.2019 vorgestellt. Nur neun der Unternehmen erhielten die Bewertung grün („überwiegend zufriedenstellend“), 32 gelb („vereinzelter Handlungsbedarf“) und neun Unternehmen rot („erhebliche Defizite“). Vor allem der technisch-organisatorische Datenschutz und die Datenschutz-Folgenabschätzungen seien besorgniserregend.

Zwar ist die Verallgemeinerbarkeit der Ergebnisse angesichts der insgesamt rund 280.000 Unternehmen in Niedersachsen, davon knapp 21.000 mittlere und große (ab 2 Mio. € Umsatz), eher begrenzt. Dennoch dürfte nach wie vor ein sehr großer Teil der Unternehmen deutlichen Nachholbedarf beim Datenschutzmanagement haben.

Der Kriterienkatalog eignet sich als Leitfaden und sinnvolle Basis für interne Datenschutz-Audits zur Überprüfung des Reifegrads des Datenschutz-Managements, zumal Zertifizierungsmöglichkeiten aus Art. 42 DSGVO weiterhin nicht verfügbar sind.

Presenter-Lücke

Angriffe auf Funktastaturen und -mäuse sind lange bekannt (SSN 8/2016). Weniger bekannt ist, dass einige Hersteller die in den vergangenen Jahren u.a. von Matthias Deeg und Gerhard Klostermeier aufgedeckten Schwachstellen (siehe z. B. die Präsentation vom 24.10.2019) einfach ignorieren – und daher auch Nachfolgeprodukte anfällig sind.

Von den Sicherheitslücken sind auch Presenter betroffen. Zwar beherrscht der Sender nur wenige Tastencodes (Page Up, Page Down, F5, ...); der USB-Empfänger hingegen spielt Tastatur – und akzeptiert jeden Tastencode eines passenden Senders. Da

das Funkprotokoll weder Integritätsschutz noch Senderauthentifikation bietet, ist das Einspielen einer beliebigen Zeichenfolge (z. B. Öffnen der Commandozeile mit Windows+'R' und Start der PowerShell) mit einem 35 €-Dongle möglich. Gegen diesen bereits 2016 veröffentlichten Angriff sind (neben denen anderer Hersteller) auch die weit verbreiteten Presenter-Modelle R400, R700 und R800 von Logitech bis heute anfällig. Immerhin: Inzwischen bietet Logitech betroffenen Nutzern offenbar Ersatzempfänger über den Kundendienst.

Amerikanische Inseln

Seit dem 01.01.2020 gilt der California Consumer Privacy Act vom 23.09.2019, der für den Bundesstaat Kalifornien ein mit der DSGVO vergleichbares Datenschutzniveau schafft.

Das Gesetz fügt Datenschutzregeln in den US Civil Code ein (Sec. 1798.105 ff). Es ist anwendbar auf in Kalifornien niedergelassene oder tätige Unternehmen mit mehr als 25 Millionen US-Dollar Umsatz oder einer Datenverarbeitung, die mehr als 50.000 Verbraucher, Haushalte oder Geräte betrifft. Weiter sind Unternehmen umfasst, die ihren Umsatz mindestens zur Hälfte mit dem Verkauf personenbezogener Verbraucherdaten erzielen. Der Verbraucherbegriff ist dabei auf kalifornische Bürger beschränkt.

Das Gesetz hat ausdrücklich keine Schutzwirkung für die auf Europa gerichteten Geschäftsaktivitäten kalifornischer Unternehmen. Kern des Gesetzes ist ein Widerspruchsrecht gegen den Verkauf von Verbraucherdaten, eine umfangreiche aktive Informationspflicht und der DSGVO ähnliche Betroffenenrechte, v. a. ein Auskunftsrecht. Die Sanktionen betragen 2.500 USD für einfache und 7.500 USD für vorsätzliche Verstöße.

Im Vergleich zur DSGVO ist der Anwendungsbereich noch stark eingeschränkt und die Verarbeitung der Daten nicht auf rechtliche Erlaubnistatbestände limitiert. Dennoch stellt die Gesetzesanpassung eine deutliche Annäherung an europäische Datenschutzstandards dar. An der derzeitigen Rechtssituation bezüglich der Datenverarbeitung in den USA kann das Gesetz eines einzelnen Bundesstaates, zudem mit beschränktem Anwendungsbereich, nichts ändern. Aber es ist wenigstens ein derzeit seltener Grund für verhaltenen Optimismus.

Secorvo News

Wissen ist Macht

Im Jahr 2020 bieten wir Ihnen wieder mehrere Gelegenheiten, Ihre Kenntnisse in der Informationssicherheit auszubauen oder durch ein T.I.S.P.- oder T.P.S.S.E.-Zertifikat bestätigen zu lassen.

Den Anfang macht ein „Klassiker": Unser ständig weiterentwickeltes und aktualisiertes PKI-Seminar (**09.–12.03.2020**). „Für mich bildet das bei Ihnen angeeignete Wissen zusammen mit den aufwändig gestalteten Seminarunterlagen eine zentrale Arbeitsgrundlage im PKI Umfeld", urteilte jüngst ein Seminarteilnehmer. Es folgt der „TeleTrusT Professional for Secure Software Engineering" – ein „informatives und interaktives Seminar mit einem sehr guten Verhältnis von Theorie und Praxis", so eine Teilnehmerbewertung (**16.–19.03.2020**). Und mit der Vorbereitung auf das nächste T.I.S.P.-Seminar (**11.–15.05.2020**) können Sie bereits jetzt mit der aktuellen dritten Auflage des Begleitbuchs zum T.I.S.P. beginnen, das wir Ihnen unmittelbar nach Eingang Ihrer Anmeldung zusenden.

Alle Termine, Programme und die Möglichkeit zur Online-Anmeldung finden Sie hier.

… und noch nie zu fragen wagten.

Keine Novellierung des Datenschutzrechts hat eine solche Aufmerksamkeit bekommen wie die im Mai 2018 in Kraft getretene Datenschutz-Grundverordnung. Obwohl fast alles beim Alten geblieben ist, ist doch alles anders… und sind viele konkrete Fragen offen: Wann ist das Tracking von Webseitenbesuchern zulässig? Wie kann ein Unternehmen seine Informationspflichten angemessen erfüllen? Welche Datenschutzvorfälle sind meldepflichtig? Wie bestimmt sich die Höhe eines Bußgelds?

Zu diesen, weiteren und auch Ihren Fragen zur DSGVO und dem Datenschutz wird uns auf dem Jahresstartevent der KA-IT-Si am **13.02.2020** Dr. Stefan Brink, Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg, Rede und Antwort stehen. Wir freuen uns sehr auf diesen Termin, denn Herr Dr. Brink ist für seine klaren Einschätzungen bekannt – und hoffen auf großes Interesse Ihrerseits.

Wir empfehlen eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2020	
31.01.-02.02.	ShmooCon 2020 (The Shmooh Group, Washington/US)
Februar 2020	
13.02.	KA-IT-Si Event "... und noch nie zu fragen wagten." (KA-IT-Si, Karlsruhe)
19.-20.02.	30. ID:SMART Workshop (Fraunhofer Institut SIT, Darmstadt)
24.-25.02.	27. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg
März 2020	
09.-12.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-20.03.	GI Sicherheit 2020 (Gesellschaft für Informatik e.V., Göttingen)
25.-26.03.	secIT 2020 (Heise Medien, Hannover)
25.-27.03.	DFRWS EU Conference (DFRWS, Oxford/UK)
31.03.-03.04.	Blackhat Asia 2020 (Blackhat, Singapur/SIN)
31.03.-02.04.	IT-Sicherheit – praxisnah und aktuell (Secorvo, Karlsruhe)



Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2020



Von der IT lernen

Selten, dass der Mensch etwas von der Informationstechnik lernen kann. In der Regel ist es umgekehrt: Vom einfachen Algorithmus bis zur künstlichen Intelligenz versucht die IT, vom Menschen zu lernen.

Aber im Umgang mit Viren kennt sich die Informationstechnik inzwischen aus – seit dem ersten Computer-Virus aus dem Jahr 1984 sind sie eine ständige Bedrohung. Computer-Viren mutieren zudem weit schneller als Grippeviren, und die Infektionswege haben durch immer weitere Schnittstellen und die zunehmende Vernetzung der Systeme ständig zugenommen. Trotzdem ist bis heute ein „GAU“ ausgeblieben.

Das Erfolgskonzept der Virenabwehr in der Informationstechnik ist die Reaktion auf verschiedenen Ebenen. Am einfachsten lässt es sich in fünf Schritten beschreiben:

1. Expertenanalyse des Virus direkt nach erstem Auftreten
2. Unverzügliche und umfassende Information über Infektionswege, Schad-Funktion und wirksame erste Gegenmaßnahmen
3. Sensibilisierung der Nutzer für Symptome und Infektionswege
4. Blockade einzelner Infektionswege (z. B. durch Updates)
5. Isolation befallener Systeme

Tatsächlich eignen sich nicht alle Maßnahmen, die gegen Computerviren helfen, auch für Menschen, wie das Neuaufsetzen des Betriebssystems oder das Formatieren der Festplatte.

Allerdings gilt auch für „echte“ Viren: Keine Panik. Ausbreitung und Schäden lassen sich eindämmen. Ruhe bewahren – aber zugleich alle riskanten Tätigkeiten vermeiden. Und immer wieder gründlich die Hände scannen – pardon: waschen.



Inhalt

Von der IT lernen

Security News

Gemeinsam verantwortlich

Audit? Aber sicher!

Keep it simple

Erpressung „on top“

IT-Grundschutz 2020

Conditio sine qua non

Mixed Content

Secorvo News

Secorvo Seminare

EaSy mit Microsoft-PKI

„Ich seh' etwas, was Du nicht siehst…“

Veranstaltungshinweise

Security News

Gemeinsam verantwortlich

Bereits im Datenschutz-Tätigkeitsbericht 2019 legte der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI), Dr. Stefan Brink dar, dass angesichts der aktuellen Rechtslage insbesondere im Bereich Social Media Unklarheiten bei der Gemeinsamen Verantwortlichkeit bestehen. Am 06.02.2020 informierte der LfDI via Pressemitteilung über einen für öffentliche Stellen erstellten Anforderungskatalog der Aufsichtsbehörde. Danach riskiert die einen solchen Dienst einsetzende verantwortliche Stelle von der Aufsichtsbehörde in die Pflicht genommen zu werden, wenn die Anforderungen nach Art. 26 DSGVO vom Plattformbetreiber nicht angeboten und auch auf Anforderung des Nutzers nicht umgesetzt werden.

Der Anforderungskatalog sollte auch von Unternehmen geprüft werden, da die Anforderungen der Aufsichtsbehörde übertragbar sind. Wer in einem solchen Fall auf die Nutzung von Social-Media-Diensten nicht verzichtet, muss sich darüber im Klaren sein, dass er damit das Risiko eines Bußgeld bewehrten DSGVO-Verstoßes in Kauf nimmt.

Audit? Aber sicher!

Wie wichtig es ist, bei Security-Audits auf Qualität zu achten, haben im Februar die Audits zweier Wahl-Apps aus den USA gezeigt. So legte ein von Pro Publica in Auftrag gegebenes Security-Audit offen, dass die bei den Vorwahlen in Iowa verwendete Wahl-App von „elementaren Sicherheitsproblemen" betroffen ist, über die u. a. eine Manipulation der Anzahl der Stimmen möglich gewesen wäre. Der Hersteller behauptet, die App wäre zuvor „mehreren rigorosen Sicherheitstests durch eine Drittpartei" unterzogen worden. Auch die bereits mehrfach in den USA eingesetzte Wahl-App „Voatz" hat erhebliche Sicherheitsmängel, wie Forscher des MIT am 13.02.2020 mitteilten. Die Schwachstellen erlauben einem Angreifer Stimmen zu manipulieren, Stimmabgaben zu unterdrücken oder zu erkennen, für wen ein Wähler gestimmt hat. Auch für Voatz gab es laut Hersteller in der Vergangenheit diverse Sicherheitsaudits.

Security-Audits sollte man grundsätzlich von qualifizierten, idealerweise auch zertifizierten Auditoren nach anerkannten Prüfstandards durchführen lassen. Damit werden die Ergebnisse vergleichbar – und Vorfälle wie die oben genannten sollten seltene Ausnahmen sein.

Keep it simple

Am 28.01.2020 hat Linus Torvalds WireGuard in den Hauptzweig des Linux-Kernels aufgenommen. WireGuard realisiert ein neuartiges VPN-Protokoll, das einfacher, sicherer und performanter sein will als die VPN-Standards OpenVPN und IPsec.

Mit nur etwa 4.000 Zeilen Quellcode (loc) ist die Komplexität von WireGuard deutlich geringer als die von OpenVPN und OpenSSL (70.000 bis 600.000 loc) oder IPSec (400.000 loc). Damit sinkt die Fehleranfälligkeit und das Auditieren des Quelltextes wird erheblich erleichtert. Durch die Beschränkung auf das absolute Minimum – beispielsweise wird nur eine einzige Cipher Suite unterstützt und statt X.509-Zertifikaten kommen wie bei SSH Schlüsselpaare zum Einsatz – bietet WireGuard nicht denselben Funktionsumfang wie OpenVPN; das könnte eine Hürde bei der Durchsetzung sein. Aus Sicherheitssicht ist WireGuard jedoch ein Schritt in die richtige Richtung – denn Komplexität ist einer der großen Feinde der IT-Sicherheit.

Erpressung „on top"

Dass man Ransomware für die Betroffenen noch unangenehmer gestalten kann, haben die Macher der „MAZE"-Ransomware um den 05. und 09.12.2019 unter Beweis gestellt. Dafür kombinierten sie zwei schon lange von Cyberkriminellen genutzte „Geschäftsmodelle", um den Zahlungsdruck zu erhöhen: Zunächst werden die Daten gestohlen und wie üblich verschlüsselt. Kommt der Betroffene der Zahlungsaufforderung nicht nach, werden die gestohlenen Daten in kleinen Häppchen im Internet veröffentlicht. Besonders verheerend kann das angesichts hoher DSGVO-Bußgelder sowohl für Unternehmen als auch für Privatpersonen sein.

Wer bereits Maßnahmen zum Schutz vor Ransomware (SSN 02/2016 und SSN 04/2016) ergriffen hat und eine solide, getestete Disaster-Recovery-Strategie mit Backups umsetzt, sollte sich daher besser nicht zufrieden zurücklehnen und das Thema „Data Loss Prevention" aus den Augen verlieren...

IT-Grundschutz 2020

Das BSI hat – wie geplant – am 01.02.2020 die 2020er Edition des IT-Grundschutz-Kompendiums veröffentlicht. Mit der Umstellung der IT-Grundschutz-Kataloge auf das IT-Grundschutz-Kompendium verfolgte das BSI das Ziel, die Aufwände für die Konzepterstellung zu reduzieren und die Praktikabilität bei der Umsetzung zu erhöhen (SSN 8/2018) – aus der Praxis können wir bestätigen, dass das gelungen ist.

Neu in der Edition 2020 sind die Bausteine „CON.8 Software-Entwicklung" sowie „NF.5 Raum sowie

Schrank für technische Infrastruktur"; die weiteren Änderungen sind klar aufgeführt. Alte Zöpfe, wie die Anforderung, regelmäßig das Kennwort zu wechseln – „Die Passwörter SOLLTEN in angemessenen Zeitabständen geändert werden." (ORP.4.A8) – wurden bei der Gelegenheit auch abgeschnitten. Aus unserer Sicht ist die neue Fassung eine weitere Verbesserung dieses wichtigen Referenzwerkes der IT-Sicherheit.

Conditio sine qua non

In der Automobilbranche sind Anforderungen an die IT-Sicherheit wie eine TISAX-Zertifizierung mittlerweile Standard. Andere Branchen ziehen nach: So wurde in einer europaweiten Ausschreibung im Bereich Krankenkassen/Sozialdienste (Unterstützungsdienstleistungen Fallbearbeitung) von den Bietern ein ISMS-Zertifikat nach DIN EN ISO 27001 gefordert. Eine Bietergemeinschaft wurde ausgeschlossen, obwohl eines der Mitglieder zertifiziert war. Daraufhin hatte ein anderes, nicht zertifiziertes Mitglied den Ausschluss vor dem Bundeskartellamt angegriffen. Dieses wies den Nachprüfungsantrag jedoch bereits am 19.07.2019 zurück.

Das Beispiel zeigt, dass nach einer langen Phase der Zurückhaltung inzwischen auch in Deutschland ein ISMS zunehmend zum Stand der Technik gezählt und von Anbietern erwartet wird.

Mixed Content

Am 06.02.2020 kündigte Joe DeBlasio vom Chrome Security Team im Google Security Blog an, dass Chrome zukünftig Schritt für Schritt Mixed-Content-Downloads verhindern wird. Damit werden von verschlüsselten Seiten keine unverschlüsselten Downloads mehr möglich sein. Dies setzt die Ende 2019 angekündigten Bestrebung fort, Mixed Content in Chrome komplett zu blockieren. Dass dieses Vorgehen bei Herstellern problematische Umgehungsstrategien provozieren kann, hat 2018 der Sennheiser-Fall gezeigt (SSN 11/2018).

Entwickler sollten dennoch prüfen, ob ihre Anwendungen Mixed-Content-Downloads durchführen und diese auf HTTPS umstellen. In der Praxis beobachten wir insbesondere in Unternehmensnetzen noch vergleichsweise oft unverschlüsselte Kommunikation. Da diese in aktuellen Browsern zukünftig weiteren Beschränkungen unterliegen wird, erscheint auch hier der Umstieg auf HTTPS angebracht.

Secorvo News

Secorvo Seminare

Wenige Tage noch bis zum „TeleTrusT Professional for Secure Software Engineering" – einem interaktiven Seminar mit großem Praxisteil zur sicheren Softwareentwicklung (**16.–19.03.2020**). Und im Mai folgt das nächste T.I.S.P.-Seminar (**11.–15.05.2020**) – wer bereits jetzt mit der Vorbereitung anhand des jüngst aktualisierten Begleitbuchs zum T.I.S.P. beginnen möchte, sollte sich einfach anmelden – das Begleitbuch wird Ihnen umgehend zugesendet (Programme und Online-Anmeldung).

EaSy mit Microsoft-PKI

Unsere Zertifikatsmanagement-Lösung Certificates ready2go – EaSy erhält im nächsten Release (April 2020) die Möglichkeit zur Anbindung einer Active Directory Enterprise CA. Über das EaSy Enrollment-Gateway können ACME Clients wie der bekannte Certbot für interne Server öffentlich gültige Zertifikate bei Trustcentern wie Let's Encrypt & Co. beziehen und automatisch erneuern – und künftig auch intern gültige Zertifikate bei einer vorhandenen Microsoft-PKI. Für die internen Zertifikate entfällt die Beschränkung auf öffentlich registrierte Servernamen; die Enterprise CA kann Zertifikate auch für bspw. „intranet.local" erstellen (Kontakt).

„Ich seh' etwas, was Du nicht siehst…"

Das kommende KA-IT-Si-Event am 26.03.2020 dreht sich um die Sichtbarmachung des Unsichtbaren: Die Sicherheit eines Verfahrens oder Protokolls kann man nämlich nicht durch einfaches Hinsehen erkennen, wie Professor Dr. Jörn Müller-Quade (KIT) zeigen wird. Schlimmer noch: Sie ist keine funktionale Eigenschaft und kann daher auch nicht durch einfaches Testen festgestellt werden.

Dem begegnet die Kryptographie mit mathematischen Beweisen, mit denen nachgewiesen wird, dass ein Verfahren in einem bestimmten Modell unter präzise beschriebenen Voraussetzungen eine ebenso präzise definierte Sicherheitseigenschaft erfüllt. Unterschiede zwischen dem (vereinfachenden) Modell und der Wirklichkeit können dazu führen, dass auf die Implementierung eines als sicher bewiesenen Systems so genannte Seitenkanalangriffe möglich sind. Noch gravierender ist, dass nicht ohne weiteres nachprüfbar ist, ob ein reales technisches System auch wirklich die modellierte Sicherheitslösung umsetzt. Ein Ansatz, diesem Problem zu begegnen, ist *Auditable Security* – ein Konzept, das durch den modularen Aufbau von Systemen eine Überprüfung bestimmter Eigenschaften durch eingehende visuelle Inspektion zu ermöglichen versucht.

Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2020	
16.-19.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-20.03.	GI Sicherheit 2020 (Gesellschaft für Informatik e.V., Göttingen)
25.-26.03.	secIT 2020 (Heise Medien, Hannover)
25.-27.03.	DFRWS EU Conference (DFRWS, Oxford/UK)
31.03.-03.04.	Blackhat Asia 2020 (Blackhat, Singapur/SIN)
April 2020	
21.-22.04.	Datenschutztage 2020 (FFD, Wiesbaden)
21.-22.04.	Security Forum 2020 (Hagenberger Kreis, Hagenberg/AT)
Mai 2020	
06.-07.05.	BvD Verbandstag 2020 (BvD e.V., Berlin)
10.-14.05.	Eurocrypt 2020 (IACR, Zagreb/HRV)
11.-15.05.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
12.-15.05.	European Identity & Cloud Conference 2020 (KuppingerCole Ltd., München)



Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: André Domnick, Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, Sarah Niederer, Friederike Schellhas-Mende, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2020



Panikresistenz

Seit drei Wochen befindet sich die Welt im Ausnahmezustand. Für Sicherheits- und Datenschutzbeauftragte ist das eine harte Belastungsprobe – denn angesichts der drohenden Überlastung unseres Gesundheitssystems und der teilweise existenziellen Auswirkungen des „Social Distancing" auf die wirtschaftliche Situation vieler Unternehmen stehen Datenschutz und Sicherheit derzeit hinter anderen Prioritäten zurück.

An keinem Thema wird das gerade deutlicher als an der Diskussion über ein Handy-Tracking zur Kontaktnachverfolgung. Zwar wurden die Verkehrs- und Standortdaten am 25.03.2020 doch nicht auf dem Altar des „Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite" geopfert – aber wohl nur, weil der Gesetzgeber in letzter Sekunde verstand, dass die Daten der Mobilfunknetze viel zu ungenau sind, um feststellen zu können, ob der Abstand zweier Smartphone-Nutzer zueinander kleiner als zwei Meter ist: Eine einzelne Funkzelle kann schließlich eine Fläche mit einem Durchmesser von bis zu 35 km abdecken.

Nun aber wird es spannend. Denn die derzeit diskutierte „Corona-App", die via Bluetooth Kontaktpersonen registriert und nach einem positiven Corona-Test alle bis zu 20 Tage zurückliegenden Kontakte informiert, erfordert die freiwillige Mitwirkung der Smartphone-Nutzer: Auch die Kontaktperson benötigt die App, und flächendeckend funktioniert das System erst mit mindestens 60% aller Bürger.

Anders als die Tracking-Lösungen, die in China, Polen oder Israel eingesetzt werden, soll die App anonym arbeiten – aber die Warnung zentral absetzen. Man darf gespannt sein, wie dieser Zielkonflikt gelöst wird – und ob man die Chance für „Privacy by Design" auch diesmal verspielt. Denn Anonymität ist tatsächlich möglich – erfordert aber eine dezentrale Datenhaltung, Verschlüsselung und wechselnde Pseudonyme. Das Ergebnis wird zeigen, wie panikresistent unser Grundrechtsverständnis wirklich ist.



Inhalt

Panikresistenz

Security News

Datenschutz-Abmahnung

Kritische Leitsystem-Lücken

Wiederbelebungsversuch

Datenschutz und Social Media

Apple begrenzt Zertifikatsgültigkeit

Benachrichtigungspflicht

Secorvo News

Rezensenten gesucht

RaSy/DaSy mit LDAP-Anbindung

Veranstaltungshinweise

secorvo
security consulting

Security News

Datenschutz-Abmahnung

Am 27.02.2020 entschied das OLG Stuttgart, dass Unternehmen wegen fehlender Datenschutzerklärungen abgemahnt werden können. Das Gericht musste zunächst klären, ob § 13 Telemediengesetz oder die Datenschutz-Grundverordnung (DSGVO) anzuwenden war. Letztere genießt Vorrang, da sie die EU-Datenschutz-Richtlinie ersetzt hat. Nach Auffassung des Gerichts handelt es sich bei den Vorschriften der DSGVO um Marktverhaltensregeln – nur dann ist eine Abmahnung nach dem Wettbewerbsrecht (UWG) möglich. Da Art. 80 DSGVO nicht abschließend regelt, wie Verstöße gegen die DSGVO rechtlich durchzusetzen sind, sind außerdem Wettbewerbsverbände klagebefugt.

Wer keine Datenschutzerklärung auf seiner Webseite vorhält, verstößt damit nicht nur gegen seine (Informations-) Pflichten aus Art. 13 DSGVO, sondern auch gegen § 3a UWG, da die Erfüllung von Informationspflichten einen Wettbewerbsbezug aufweist: Kommt man seinen Informationspflichten nicht nach, macht man sich das Leben (zu) leicht, deshalb darf abgemahnt werden. Es wäre nicht überraschend, wenn diese Rechtsprechung zukünftig auf unvollständige Datenschutzerklärungen ausgeweitet wird – hier können also Abmahnungen von Wettbewerbern drohen.

Kritische Leitsystem-Lücken

Sicherheitsforscher der Kaspersky Lab Security Services hatten bereits am 28.12.2019 auf dem Chaos Computer Congress (36c3) gravierende Lücken im Prozessleitsystem Siemens SPPA-T3000 offengelegt, das hauptsächlich in Kraftwerken eingesetzt wird. Am 21.02.2020 veröffentlichten sie nun ein White Paper mit Details. In diversen Komponenten des T3000 entdeckten sie sowohl veraltete Software-Versionen (wie Windows Server 2003) als auch Schwachstellen in den T3000-Anwendungen, Standardpasswörter und gravierende Konfigurationsfehler. Die Angriffsfläche ist dabei vergleichsweise groß: Angreifer können zentrale Komponenten übernehmen, Informationen extrahieren, Rechte erweitern und somit schlimmstenfalls die vollständige Kontrolle über ein Kraftwerk gewinnen. Hierfür ist jedoch eine Verbindung zum internen Leittechnik-Netz notwendig, die normalerweise den Zutritt zur Anlage erfordert. Allerdings wird manchmal aus anderen Netzen Zugriff auf die Leittechnik-Netze gestattet.

Siemens hatte schon im Dezember ein Advisory veröffentlicht und viele der Schwachstellen in Updates beseitigt. Allerdings werden diese nach unserer Erfahrung häufig nicht oder erst stark verzögert eingespielt. Die Forscher veröffentlichten zusätzlich Anweisungen und Tools für T3000 Assessments, mit denen das Vorhandensein einiger der Schwachstellen festgestellt und deren Ausnutzung vermieden werden können. Bei bedachtem Vorgehen wird von einer solchen Prüfung der Betrieb nicht beeinträchtigt.

Wiederbelebungsversuch

Am 21.02.2020 hat Kroatien einen neuen Entwurf für die ePrivacy-Verordnung – die die ungeliebte Cookie-Richtlinie ersetzen soll – an die Delegationen der anderen EU-Mitgliedstaaten versandt, nachdem der vorherige Entwurf (SSN 6/2019) gescheitert war. Ein „vereinfachter" Text soll nun mit der DSGVO in Einklang gebracht werden. Dieser Versuch besteht vor allem darin, Einwilligungen durch das berechtigte Interesse an der Datenverarbeitung zu ersetzen. Beim berechtigten Interesse wird wie in der DSGVO eine Interessenabwägung vorgenommen.

Kroatien macht dabei für das Tracking Vorschläge, wann ein berechtigtes Interesse ausreichen soll und welche Interessen der Verbraucher dem entgegenstehen können. Bei der Abwägung ist zu berücksichtigen, ob der Endnutzer vernünftigerweise damit rechnen kann, dass der Verantwortliche dessen personenbezogene Daten verarbeitet. Dabei wird auf die Vorgaben der DSGVO Bezug genommen.

Im Hinblick auf die Rechtsprechung des Europäischen Gerichtshofs (EuGH), der nicht zuletzt in der Planet-49-Entscheidung (SSN 10/2019) den Schwerpunkt auf die Erteilung von Einwilligungen gelegt hat, muss man sich fragen, warum die Ansätze des EuGH im Hinblick auf das Verhältnis von Einwilligung und berechtigtem Interesse nicht berücksichtigt und nicht einmal in der Begründung angesprochen werden.

Datenschutz und Social Media

Der LfDI Rheinland-Pfalz hat am 06.03.2020 einen neuen Handlungsrahmen für öffentliche Stellen im Umgang mit Social-Media-Plattformen bereitgestellt. Anhand des EuGH-Urteils zu Facebook-Fanpages, des anschließenden Urteils des Bundesverwaltungsgerichts zur Möglichkeit der Datenschutzaufsichtsbehörden, sich statt an Facebook auch an den Fanpage-Betreiber zu halten und ergänzenden Beschlüssen der Datenschutzkonferenz führt das Papier die Anforderungen an Behörden-Präsenzen bei Social-Media-Plattformen aus. Für den rechtskonformen Betrieb benötigt man zunächst eine Rechtsgrundlage für die Weitergabe von Daten an den Social-Media-Anbieter, i.d.R. eine Nutzer-Einwilligung. Der LfDI akzeptiert eine Einwilligung re-

gistrierter Nutzer gegenüber dem Social-Media-Anbieter, sofern diese auf ausreichender Transparenz beruht; nicht registrierte Nutzer müssten gesondert einwilligen oder ausgeschlossen werden.

Eine weitere Anforderung ist eine transparente Vereinbarung des Betreibers mit dem Plattformanbieter nach Art. 26 DSGVO. Diese muss Antworten auf alle Fragen aus dem DSK-Beschluss vom September 2018 bieten, was die aktuelle Facebook-vereinbarung z. B. zu Löschfristen der Daten nicht erfüllt. Weiter sind die Informationspflichten aus Art. 13 DSGVO zu erfüllen und es wird ein Datenschutz-Konzept für das Angebot gefordert.

Die Forderungen sind auf private Stellen übertragbar. Fazit: Derzeit kann kein Social-Media-Angebot datenschutzkonform betrieben werden. Abhilfe könnten nur die Plattform-Anbieter schaffen.

Apple begrenzt Zertifikatsgültigkeit

Beim Treffen des CA/Browser Forums in Bratislava am 19./20.02.2020 kündigte Apple an, ab September 2020 keine neu erstellten TLS-Zertifikate mehr zu akzeptieren, die länger als 13 Monate (398 Tage) gültig sind. Die am 03.03.2020 veröffentlichte Regelung bezieht sich nicht nur auf den Safari-Browser, sondern auf alle Apps, die TLS-Funktionen eines Apple-Geräts nutzen – vom Mac bis zur Apple Watch. Betroffen sind ausschließlich öffentliche Zertifikate, die unterhalb der im Apple-Ökosystem vorinstallierten Root CAs ausgestellt wurden. Wer eine interne PKI betreibt, kann weiterhin länger gültige Zertifikate nutzen.

Apple widersetzt sich mit der neuen Regelung dem Ergebnis der Abstimmung SC22 des CA/Browser Forums vom September 2019, das eine Kürzung der maximalen Zertifikatsgültigkeit für öffentlich gültige TLS-Zertifikate auf 13 Monate abgelehnt hatte. Apple setzt die Verkürzung nun beim Endnutzer durch und erzwingt somit einen neuen de-facto Standard bei allen Webseitenbetreibern, die mit Apple-Geräten kompatibel bleiben wollen.

Aus Sicherheitssicht ist Apples Regelung zu unterstützen, da einerseits Webseitenbetreiber gedrängt werden, aktuelle Zertifikate mit ggf. angepassten Krypto-Standards zu nutzen und ihr Zertifikatsmanagement besser zu automatisieren, sowie andererseits die Risiken durch die häufig laxe (Nicht-)Nutzung von Sperrprozessen zeitlich begrenzt werden. Allerdings ist zu befürchten, dass andere Browser-Hersteller nachziehen und Abstimmungen im CA/Browser Forum durch eigene Wild-West-Regelungen unterminieren.

Wer öffentlich gültige Zertifikate nutzt, kann mit ACME das Zertifikatsmanagement automatisieren. Für interne Systeme unterstützt Sie dabei unsere Lösung Certificates ready2go.

Benachrichtigungspflicht

Datenschutzvorfälle müssen, sofern ein Risiko für die Rechte und Freiheiten der Betroffenen nicht ausgeschlossen werden kann, innerhalb von 72 h der Aufsichtsbehörde gemeldet werden (Art. 33 DSGVO). 2019 kam es allein in Baden-Württemberg zu 1.824 Meldungen, wie Dr. Stefan Brink (LfDI) am 13.02.2020 in seinem Vortrag bei der Karlsruher IT-Sicherheitsinitiative verriet. Und das ist wahrscheinlich nur die Spitze des Eisbergs. Ein zweiter Hinweis war aber noch wichtiger: Die Aufsichtsbehörde erwartet, sofern besondere personenbezogene Daten (wie medizinische) von dem Vorfall betroffen sind, eine unverzügliche Benachrichtigung der Betroffenen nach Art. 34 DSGVO.

Secorvo News

Rezensenten gesucht

Entschleunigung ist eine wichtige Voraussetzung dafür, dass Menschen sich nicht nur um Dringendes, sondern auch um Wichtiges kümmern. Wie zum Beispiel Weiterbildung. Im Oktober 2019 erschien die dritte, überarbeitete und erweiterte Auflage unseres Handbuchs „Informationssicherheit und Datenschutz“, zugleich Begleitbuch zum T.I.S.P.-Seminar, im dpunkt.verlag. Es zählt zu den umfassendsten Darstellungen des Themengebiets. Oder, wie ein Leser schrieb: „*Ich war auf der Suche nach einem Lehrbuch, das einerseits die Grundlagen umfassend abdeckt und andererseits eine gewisse technische Tiefe aufweist, was bei vielen amerikanischen Werken rund um die CISSP-Zertifizierung leider nicht der Fall ist. Das Buch erfüllt diese Anforderungen ganz hervorragend und ist für den Einsatz in der Hochschullehre sehr gut geeignet sowie als Schulungsunterlage für Praktiker und als Nachschlagewerk.*“ Für die Neuauflage suchen wir noch Rezensenten – und können dafür über eine (begrenzte) Anzahl von Freiexemplaren verfügen. Wir freuen uns auf Ihre Kontaktaufnahme.

RaSy/DaSy mit LDAP-Anbindung

Ende März 2020 erschien RaSy/DaSy, das in *ISMS ready2go* und *DSMS ready2go* integrierte Tool zur Durchführung von Risikoanalysen und Datenschutzfolgenabschätzungen (DSFA), in Version 1.5. Die darin neu geschaffene Möglichkeit, Nutzer über eine Anbindung an ein LDAP-Directory wie beispielsweise Microsofts Active Directory (AD) hinzuzufügen, vereinfacht die Administration deutlich. Das überarbeitete Design erleichtert zudem den täglichen Umgang mit RaSy/DaSy.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2020	
21.-22.04.	Datenschutztage 2020 (FFD Forum für Datenschutz, Wiesbaden)
Mai 2020	
06.-07.05.	BvD Verbandstag 2020 (BvD e.V., Berlin)
11.-15.05.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
12.-15.05.	European Identity & Cloud Conference 2020 (KuppingerCole Ltd., München)
13.-14.05.	21. Datenschutzkongress (EUROFORUM, Berlin)
Juni 2020	
02.-03.06.	a-i3/BSI-Symposium 2020 (a-i3, Bochum)
15.-16.06.	DuD 2020 (COMPUTAS, Berlin)
Juli 2020	
08.07.	Security Cruise (Connecting Media, Karlsruhe)
09.07.	12. Tag der IT-Sicherheit (KA-IT-Si, IHK, CyberForum, KASTEL, Karlsruhe)
14.-18.07.	PETS 2020 (University of Minnesota, Montréal/CAN)
19.-21.07.	DFRWS USA 2020 (DFRWS, Memphis/US)



Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Christian Titze.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2020



Imagine

Stellen Sie sich einmal vor – rein hypothetisch – ein neuer Virus bräche aus. In China. Ein Computervirus, meine ich.

Und stellen Sie sich weiter vor, er besäße unschöne Eigenschaften: Er ist hochansteckend und besitzt eine Inkubationszeit von einigen Tagen, in denen er sich aber weiter verbreitet. Bricht er aus, dann richtet er bei 5-10 % der befallenen Geräte erhebliche Schäden an – von der Löschung des Datenbestands und der installierten Software bis hin zu irreparablen Hardware-Defekten. Jüngere Geräte sind offenbar weniger stark betroffen.

Dabei nutzt er alle Schwächungen des „Immunsystems" wie sicherheitskritische Fehler in veralteter Software oder unbedachte Konfigurationen. Offenbar verwendet er alle Arten von Kontakten mit anderen Rechnern zur Verbreitung: USB-Sticks, SD-Karten, Bluetooth-, WLAN- und Internetverbindungen. Befallene Rechner können bisher nur über die Symptome identifiziert werden; da der Virus sein Erscheinungsbild ändert, ist er für Virenscanner „unsichtbar".

Da sich der Virus nun auch in Deutschland ausbreitet, Sicherheitsexperten zur Schadensbegrenzung knapp sind und bisher keine wirksamen Schutzmaßnahmen zur Verfügung stehen, sperrt die Bundesregierung internationale Datenverbindungen. Rechner dürfen Räume nur noch in unvermeidlichen Fällen verlassen und nur innerhalb des Unternehmens oder der eigenen Wohnung miteinander verbunden werden (LAN). Sie müssen einen Mindestabstand von 1,5 m zu anderen Rechnern einhalten und außerhalb geschlossener Räume in Metallbehältern transportiert werden...

Das klingt ein wenig wie Selbstmord aus Angst vor dem Tod. Und selbst wenn der Vergleich mit der aktuellen Situation hinkt (denn schließlich geht es dort um den Schutz von Leib und Leben): Ein wenig mehr Paranoia hier und etwas mehr Augenmaß dort könnten keinesfalls schaden.



Inhalt

Imagine

Security News

MASVS 1.2

CWE für Hardware-Schwächen

Gefährliche Browser-Helfer

Neu im Telemediengesetz

Dauerbrenner DS-Erklärung

Corona-Orientierungshilfe

Secorvo News

Wiederaufnahme des Seminarbetriebs

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

MASVS 1.2

Nach zahlreichen Überarbeitungen wurde am 17.03.2020 Version 1.2 des Mobile Application Security Verification Standard (MASVS) von OWASP gleich in acht Sprachen veröffentlicht. Analog zum etablierten ASVS für Web-Anwendungen definiert der MASVS einen Sicherheitsstandard aus verschiedenen Anforderungen an mobile Apps. In Anbetracht der häufigen Berichterstattung über verwundbare Apps war ein solcher Standard überfällig.

Der MASVS unterscheidet drei aufeinander aufbauende Prüf-Niveaus/Level: Der Basis-Level 1 wird in Level 2 um Defense-in-Depth-Anforderungen und in Level „R" um Maßnahmen gegen Reverse Engineering erweitert. Je nach Schutzbedarf der App sollte der gewünschte Level entsprechend festgelegt werden. In acht Bereichen wird im Standard beschrieben, welche Anforderungen beispielsweise an Architektur, Datenschutz und sichere Kommunikation gestellt werden.

Ergänzt wird der MASVS zukünftig um die Version 1.2 des Mobile Security Testing Guide (MSTG). Der MSTG beschreibt Prüfpunkte für die Sicherheitsanforderungen des MASVS und kann somit im Rahmen eines Pentests eingesetzt werden. Da Apps meist mit Web-Services im Backend kommunizieren und deren Sicherheit im Rahmen des MASVS nicht betrachtet wird, sollte die Prüfung des Gesamtsystems auch die Web-Services umfassen. Hierbei empfiehlt sich eine Vorgehensweise auf Basis des OWASP Testing Guide und Prüfung der API Security Top 10.

CWE für Hardware-Schwächen

Bisher war die Common Weakness Enumeration (CWE) eine Sammlung und Kategorisierung häufiger Fehler in Software, die zu Sicherheitsschwachstellen führen können (SSN 12/2019). Am 24.02.2020 sind mit Version 4.0 häufige Fehler im Hardware-Design neu hinzugekommen; zusätzlich gibt es eine für die sichere Softwareentwicklung wertvolle „Software Development"-Sicht auf die Schwächen, welche die vorherigen Architektur- und Entwicklungs-Sichten kombiniert.

Aus Sicherheitssicht besonders zu begrüßen ist die Integration von Hardware-Schwächen in die CWE. Dieser Schritt unterstreicht eine Entwicklung, die wir in der vergangenen Zeit vermehrt beobachten konnten: Nachdem Software-Sicherheit sich inzwischen als ein wichtiges und zunehmend höher priorisiertes Qualitätsmerkmal etabliert hat, wird der Allgemeinheit die Fehlbarkeit von Hardware immer bewusster – nicht zuletzt aufgrund von medial wirksamen Schwachstellen wie Meltdown und Spectre (SSN 02/2018). Bisher spielte die Sicherheit bei der Entwicklung von Hardware eher eine untergeordnete Rolle. Wichtigere Parameter waren Performance, Effizienz und Kosten. Dass Hardware-Fehler unter Umständen alle anderen Sicherheitsmaßnahmen kompromittieren können, haben verschiedene Schwachstellen eindrucksvoll demonstriert. Beispielsweise war ein Fehler im Nvidia Tegra Prozessor in frühen Nintendo Switch Konsolen dafür verantwortlich, dass diese ohne eine Möglichkeit zur Behebung mit Homebrew-Firmware bespielt werden konnten. Auch Apple hat in jüngster Vergangenheit Bekanntschaft mit Hardware-Schwachstellen gemacht: Der checkra1n-Exploit für iPhones wurde inzwischen auf den in Macs zu findenden T2-Chip „portiert". Und Intels „Converged Security and Management Engine" (CSME) ist ebenfalls von einer nicht behebbaren Schwachstelle betroffen. Wir empfehlen daher auch bei Hardware-Entwicklung die Nutzung der CWE und die Durchführung expliziter Risikobetrachtungen.

Gefährliche Browser-Helfer

Als kleine Alltagshelfer erleichtern „Browser Extensions" und andere Plugins vielerlei Aufgaben. Doch merke: Erweiterungen sind Computerprogramme und können Schaden anrichten. Sie dürfen zudem meist mit nur wenigen Klicks auch von niedrig privilegierten Nutzern installiert werden und stammen oft aus intransparenten Quellen.

Wie Brian Krebs am 03.03.2020 berichtete, war eine Browser Extension verantwortlich dafür, dass die Webseite des „Blue Shield of California" von verschiedenen Sicherheitsprodukten als bösartig eingestuft wurde. Ein Mitarbeiter, der die Webseite aktualisierte, hatte in seinem Webbrowser die Erweiterung „Page Ruler" installiert. Als einst nützliches Tool mit über 400.000 Installationen wurde sie vor wenigen Jahren vom Entwickler verkauft und injiziert seitdem im Hintergrund bösartigen JavaScript-Code in Webseiten, während diese über ein CMS wie WordPress oder Joomla gepflegt werden.

Wie häufig das Problem bösartiger Erweiterungen ist, zeigt ein Blick auf Googles Chrome Web Store: Im Februar 2020 wurden 500 bösartige Erweiterungen entfernt, im April 2020 nochmals fast 50 – und das ist wahrscheinlich nur die Spitze des Eisbergs. Wie schon beim Umgang mit Docker-Images und Programmbibliotheken (SSN 03/2019) empfehlen wir auch bei Plugins einen minimalistischen Ansatz: Installieren Sie nur solche Plugins, die Sie unbedingt benötigen und die von vertrauenswürdigen Entwicklern aus offiziellen Quellen stammen. In größe-

ren Umgebungen empfiehlt sich ein Whitelisting-Ansatz: Konfigurieren Sie Webbrowser so, dass nur erlaubte Plugins installierbar sind. Eine vollständige Deaktivierung von Plugins sollte hingegen gut abgewogen werden, da viele Plugins Ihre Sicherheit und Privatheit im Web verbessern.

Neu im Telemediengesetz

Am 03.04.2020 hat die Bundesregierung mit dem Gesetzesentwurf zur Umsetzung der 2018 überarbeiteten Richtlinie über audiovisuelle Mediendienste (AVMD-RL) im Telemediengesetz das Gesetzgebungsverfahren eröffnet; jetzt ist der Bundesrat am Zug. Der Entwurf verankert neben dem bisherigen Telemedienrecht neue Pflichten für Anbieter von Webseiten zum Abruf von Video-Sendungen und Videosharing-Plattformen in den neuen §§ 10a ff TMG. Dazu gehören ein Beschwerdeverfahren, das Videosharing-Plattform-Anbieter ihren Nutzern bereitstellen müssen, und ein entsprechendes Abhilfeverfahren bezüglich rechtswidriger Inhalte. Weiter werden eine Verpflichtung zum Einsatz von Nutzungsbedingungen und eine Datenschutzregelung für den Umgang u. a. mit Altersverifikationsdaten eingeführt.

Auch wenn Ziel des Gesetzes die Richtlinienumsetzung ist, überrascht doch, dass trotz wiederholter TMG-Änderungen seit Geltung der DSGVO noch immer keine Anpassung der §§ 13 ff TMG erfolgt, obwohl diese schon lange von Aufsichtsbehörden und Lehre als unzureichend angesehen werden.

Dauerbrenner DS-Erklärung

Das Spannungsverhältnis zwischen Transparenz und Verständlichkeit von Datenschutzerklärungen erhält weiteres Futter. Der Erwägungsgrund 39 der DSGVO verlangt Verständlichkeit in einer klaren und einfachen Sprache. Aufsichtsbehörden und Gerichte scheinen sich jedoch derzeit eher in Richtung Detaillierung zu bewegen. So wandte sich die dänische Datenschutzaufsichtsbehörde am 11.02.2020 in einer Entscheidung gegen das Dänische Meteorologische Institut gegen gängige Cookie-Banner: Die Einwilligung über ein einheitliches „Akzeptieren“ oder „Ok“ sei nicht ausreichend für eine freiwillige Einwilligung. Vielmehr müsse in unterschiedliche Verarbeitungszwecke granular und einzeln eingewilligt werden. Das Angebot einer detaillierten Auswahl nach einem weiteren Klick sei intransparent. Auch müsse eine Gesamtablehnung mit einem Klick möglich und genauso schnell auffindbar sein. Mit anderem Bezug, aber möglicherweise richtungsweisend urteilte das OLG Köln am 19.02.2020, dass allein der 80seitige Umfang der AGB bei einem komplexen Geschäftsmodell wie PayPal nicht zur Intransparenz und mangelnder Einbeziehung führe. Bei Internetgeschäften sei es dem Nutzer überlassen, wie lange er sich mit den Bedingungen befasse.

Für Datenschutzerklärungen (56 Seiten von Samsung) wurde dies auch schon umgekehrt bewertet (SSN 06/2016). Die „Wahrheit“ dürfte wohl in der Mitte liegen.

Corona-Orientierungshilfe

Der Europäische Datenschutzausschuss (EDSA) hat in seiner 24. Sitzung am 24.04.2020 seine bisherigen Empfehlungen zum Umgang mit Gesundheitsdaten während einer Pandemie ergänzt und Orientierungshilfen zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken im Kontext des Covid-19 Ausbruchs angenommen.

Eine erste Ergänzung betrifft die Erleichterung internationaler Datentransfers zu Forschungszwecken in Drittstaaten. Hier soll auf die Ausnahmen des Art. 49 DSGVO zurückgegriffen werden, wenn andere Garantien des Datenschutzniveaus nicht zur Verfügung stehen.

Bezüglich der Tracking-Tools zur Ausbreitungsüberwachung verweist der EDSA auf die Flexibilität der DSGVO, die den Datenbedarf zur Epidemie-Bekämpfung bereits vorsehe. Die Orientierungshilfe setzt sich intensiv mit der Gestaltung erforderlicher Einwilligungen auseinander. Weitere Anforderungen betreffen Anonymisierung und Löschfristen sowie den angemessenen Schutz der Daten, wenigstens durch Pseudonymisierung oder Verschlüsselung.

Insgesamt betont der EDSA, dass trotz der Ausnahmesituation die Datenschutzbestimmungen der DSGVO umgesetzt werden können und müssen.

Secorvo News

Wiederaufnahme des Seminarbetriebs

Den aufgrund der Pandemie-Verordnungen des Landes Baden-Württemberg bis Ende Mai eingestellten Seminarbetrieb werden wir nach der Sommerpause wieder aufnehmen. Da viele Teilnehmer ihre Anmeldung verschoben haben, ist die Mindestteilnehmerzahl schon jetzt bei einigen Seminaren erreicht – wir empfehlen daher eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Hinweis: Wegen der derzeitigen Pandemie-Einschränkung finden einige der genannten Veranstaltungen möglicherweise nicht oder in anderer Form statt.

Mai 2020	
06.-07.05.	BvD Verbandstag 2020 (BvD e.V., Berlin)
12.-15.05.	European Identity & Cloud Conference 2020 (KuppingerCole Ltd., München)
13.-14.05.	21. Datenschutzkongress (EUROFORUM, Berlin)
Juni 2020	
02.-03.06.	a-i3/BSI-Symposium 2020 (a-i3, Bochum)
15.-16.06.	DuD 2020 (COMPUTAS, Berlin)
Juli 2020	
14.-18.07.	PETS 2020 (University of Minnesota, Montréal/CAN)
19.-21.07.	DFRWS USA 2020 (DFRWS, Memphis/US)

Fundsache

Privacy Captcha gibt es zwar schon seit 2014, aber seit Spätsommer 2019 in neuem Gewand und gerade derzeit für einen sicheren Versand schützenswerter Daten bei unsicheren Kommunikationskanälen zu empfehlen.

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Michael Knopp, Sarah Niederer, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Mai 2020



Unterirdisch

Die Londoner „Tube“, benannt nach den Röhren, durch die die Untergrundbahnen fahren, ist die älteste U-Bahn und mit mehr als 270 Stationen an über 400 km Schienenstrecke noch heute das drittgrößte U-Bahn-Netz der Welt.

Der Eröffnung am 09.01.1863 ging jedoch ein erbittertes Ringen voraus. 17 Jahre hatte der Jurist *Charles Pearson* für den Bau gekämpft. Zwar erstickte London damals im Pferdedroschkenverkehr, aber Eisenbahnen waren noch eine junge Technik – erst 1838 hatte *Isambard Kingdom Brunel* die erste Eisenbahnstrecke erbaut. Doch der nur 6,5 km lange erste U-Bahn-Abschnitt wurde allen Widrigkeiten zum Trotz ein riesiger Erfolg: Im ersten Betriebsjahr beförderte die Tube bereits 9,5 Mio. Fahrgäste. Daher folgten bald weitere Linien; heute nutzen über 3 Mio. Menschen die Tube am Tag – fast 1,2 Milliarden im Jahr.

Drei Jahre Bauzeit und 1,3 Mio. Pfund kostete der Bau; für die damalige Zeit ein gigantisches Projekt. Aber es wurde rechtzeitig begonnen, bevor Bebauungsdichte und Kanalisation ein solches Querschnittsprojekt unmöglich gemacht hätten. Der erste Abschnitt konnte fast komplett in offener Bauweise errichtet werden. Wer heute eine U-Bahn plant, muss trotz aller technischen Errungenschaften wie Tunnelbohrmaschinen mit ganz anderen Hindernissen und Kosten kalkulieren. 320 Mio. Euro kostete das nach 14 Jahren Bauzeit am 08.08.2009 eröffnete, 1,8 km lange U-Bahn-Sackgässchen (U55) ins Berliner Regierungsviertel (177 Mio. €/km), und mehr als eine Milliarde Euro wird der knapp 3,4 km lange Stadtbahn-Tunnel in Karlsruhe bei der Fertigstellung 2021 nach 11jähriger Bauzeit voraussichtlich verschlungen haben (294 Mio. €/km).

Mit U-Bahnen verhält es sich offenbar wie mit dem Datenschutz: Auch der benötigt engagierte, idealistische Vorkämpfer, die nicht so leicht aufgeben – und je später man mit der Umsetzung beginnt, desto aufwändiger und teurer wird es am Ende.



Inhalt

Unterirdisch

Security News

Präventive Kontaktdaten

Corona-App und Datenschutz

Zuverlässige Corona-App?

Corona-Patientendatendatenschutz

Videokonferenzen & Datenschutz

Secorvo News

Herbstseminare

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Präventive Kontaktdaten

Seit dem 04.05.2020 atmet die Republik auf: Viele Dienstleistungen wie Friseur- oder Restaurantbesuche, die wochenlang verboten waren, sind zumindest eingeschränkt wieder zugelassen. Diese Einschränkungen haben es allerdings aus datenschutzrechtlicher Sicht in sich: Je nach Bundesland muss man nun seine Kontaktdaten (Name, Anschrift und Telefonnummer) hinterlassen bzw. werden diese von den Anbietern erfasst. Es sei denn, man wechselt in das „richtige" Bundesland: Nicht überall ist die Kontaktdatendokumentation vorgeschrieben, da es keine bundeseinheitliche Regelung gibt. Auch die Vorgaben zur Art und Weise der Erfassung und Verarbeitung, der Dauer der Aufbewahrung (vier bis sechs Wochen) und der Löschung der Daten sind uneinheitlich. In einem Bundesland muss der Besucher sogar (zwingend) sein Einverständnis zur Erhebung der Kontaktdaten erteilen – hier hat der Verordnungsgeber offenbar das Prinzip der datenschutzrechtlichen Einwilligung nicht verstanden. Einig ist man sich immerhin darin, dass das Aushängen oder Auslegen von Listen keine probate Form der Datenerfassung ist.

In manchen Bundesländern sind die Regelungen zur Kontaktnachverfolgung in einer einheitlichen Corona-Verordnung niedergelegt, in anderen gibt es für jedes Gewerbe getrennte Verordnungen. So wird beispielsweise in der ab dem 02.06.2020 gültigen Fassung der Verordnung des Baden-Württembergischen Kultus- und des Sozialministeriums über Sportstätten der nun wieder zulässige Betrieb von Schwimm- und Hallenbädern sowie Thermal- und Spaßbädern geregelt. Neben der Bereitstellung einer Aufsichtskraft für das Einhalten der Grundsätze des Infektionsschutzes muss der Betreiber solcher Einrichtungen dem Gesundheitsamt oder der Ortspolizeibehörde über die Besucher Auskunft geben können. Diese Angaben umfassen Namen und Vornamen, Datum und Uhrzeit (Beginn und Ende) des Besuchs, eine Telefonnummer oder Adresse. Die Daten sind vier Wochen nach der Erhebung zu löschen. Betriebe, die sich einen Onlineshop leisten können, werden mit der Erfüllung der Anforderungen an die Datenerhebung weniger Probleme haben; alle anderen haben mit Besucherschlangen und Papierbergen zu rechnen. Mit dem Grundsatz der Datensparsamkeit haben die Anforderungen wenig gemein.

Bleibt die (vage) Hoffnung, dass damit anonyme Schwimmbad- und Restaurantbesuche nicht der Vergangenheit angehören – und die Listen nicht zum Standard werden. Schließlich könnte ja eine zweite Infektionswelle kommen – und da wäre es doch praktisch, auf diese Daten zurückgreifen zu können...

Corona-App und Datenschutz

Nach vielen Warnungen hat die Bundesregierung am 26.04.2020 den Schwenk auf eine freiwillige, dezentrale App-Lösung zur Kontaktverfolgung und Infektionseindämmung vollzogen. SAP und die Deutsche Telekom sollen die App nun bis Mitte Juni fertigstellen. Viele Politiker möchten weitere Lockerungen der Kontaktbeschränkungen mit der Einführung einer solchen App verknüpfen, um bei Neuinfektionen mögliche weitere Betroffene zukünftig schneller und mit weniger Aufwand informieren zu können.

Mit der Hinwendung zu einem datenschutz-freundlicheren, dezentralen Konzept sind die Herausforderungen jedoch noch nicht gelöst. Es bleibt eine pseudonyme Datenverarbeitung durch den Anbieter, zu der Rechtsgrundlage, Verantwortlichkeit und Sicherheit zu bestimmen sind. An der Einwilligung des Nutzers als Rechtsgrundlage hat bereits der EDSA Zweifel geäußert. Kritisch wird diesbezüglich die Freiwilligkeit sein. Diese besteht nur, wenn Eingriffslockerungen wie Restaurantbesuche auch von privater Seite nicht von der App-Nutzung abhängig gemacht werden.

Ungeklärt sind zudem die Folgen von Kontaktwarnungen. Ist der Nutzer dadurch zur Quarantäne verpflichtet, hat er einen sofortigen Testanspruch oder besteht sogar eine Testpflicht? Gilt der Nutzer nach einer Warnung als „in Kontakt mit einem Infizierten" und werden die App-Daten damit zum Beweismittel gegen den Nutzer?

Diese Fragen erfordern ein Begleitgesetz, denn für eine diesbezügliche Verordnung gibt das Infektionsschutzgesetz selbst bei weitester Dehnung keine Ermächtigung her. Einen sehr bedenkenswerten Gesetzentwurf hat eine Privatinitiative bereits vorgelegt. Die Verfügbarkeit der App wird dadurch jedoch weiter verzögert, denn im Unterschied zu einer Verordnung unterliegen Gesetze demokratischen Entscheidungsprozessen.

Zuverlässige Corona-App?

Unabhängig von der datenschutz-konformen Gestaltung der Corona-App stellt sich die grundlegendere Frage, ob eine derartige App die in sie gesetzten Erwartungen auch technisch erfüllen kann. Die vorgeschlagenen Lösungen basieren überwiegend auf der Signalstärkemessung mittels *Bluetooth Low Energy Beacons*, beispielsweise mit den Google und Apple APIs. Leider sind derartige Messungen physikalisch bedingt trotz Kalibrierungen sehr ungenau und werden durch Faktoren wie die Antennenform,

den Gerätetyp und die Umgebung stark beeinflusst. Nicht ohne Grund werden bei der Entfernungsmessung (z. B. mit GPS) nicht die Signalstärken, sondern die sehr viel präziseren Zeitdifferenzen zwischen dem Senden und Empfangen verwendet.

Tatsächlich kann auch die Exposition nicht verlässlich festgestellt werden, da sich Smartphones in der Regel nur beim Telefonieren in Gesichtsnähe befinden und sonst meist in einer Hosen-, Hand- oder Jackentasche stecken oder irgendwo herumliegen. Bluetooth-Signale werden zudem von Vorhängen, Plexiglasscheiben und dünnen Wänden nicht abgeschwächt. Daher sind häufige Fehlerkennungen zu erwarten – sowohl *false positives* (Kontakteinträge, auch wenn die Personen wirksam voreinander geschützt waren) als auch *false negatives* (keine Kontakteinträge, weil z. B. die Smartphones weiter voneinander entfernt waren als die Personen oder das Signal abgeschirmt wurde).

Die Messungen sind daher prinzipiell unzuverlässig und können nur Hinweise geben. Zudem könnten Angreifer mittels starker Signale die App täuschen und einer großen Zahl von Personen einen Kontakt mit einem Corona-Infizierten vorspielen. So ließe sich beispielsweise ein ganzes Unternehmen vorsätzlich in Quarantäne schicken. Weitere Angriffsmöglichkeiten sind das Kopieren fremder Identitäten oder Falschmeldungen zu positiven Tests.

Zwar ist die Forderung nach staatlichem Schutz vor der Corona-App zu begrüßen, aber auch darüber lassen sich die technisch bedingten Unzulänglichkeiten und die genannten Angriffsvektoren nicht ausräumen. So deutet alles darauf hin, dass der praktische Nutzen der App im besten Fall eher gering sein dürfte – und im schlimmsten sogar die negativen Folgen überwiegen.

Corona-Patientendatenschutz

Einige Gesundheitsämter haben sich in den vergangenen Wochen offenbar „vorsorglich" mit Schreiben an die Kliniken ihrer Region gewandt und diese zur unverzüglichen Fax-Übermittlung aller Entlassungsberichte von mit Corona-Viren infizierten Patienten aufgefordert. Tatsächlich lässt sich aus dem Infektionsschutzgesetz jedoch keine solche Ermächtigung ableiten. Die Gesundheitsämter müssen sich, wenn sie diagnostische Daten benötigen, direkt an die betroffenen Patienten wenden. Denn auch eine Pandemie entbindet Kliniken nicht von der ärztlichen Schweigepflicht, und sie entzieht den Betroffenen auch nicht ihre Persönlichkeitsrechte.

Eine Übermittlung von Patientendaten an die Gesundheitsämter ist damit regelmäßig nicht nur ein Verstoß gegen geltendes Datenschutzrecht, sondern nach § 203 Strafgesetzbuch eine Verletzung von Privatgeheimnissen – und damit eine Straftat. Werden die Patientendaten dann auch noch per Fax übermittelt, kann dies zudem als ein mindestens fahrlässiger Verstoß gegen Sicherungspflichten gewertet werden.

Videokonferenzen & Datenschutz

Die Berliner Beauftragte für Datenschutz hatte am 08.04.2020 auf der Webseite ihrer Behörde eine „Checkliste zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen" bereitgestellt. Darin wies sie darauf hin, dass die Dienste Microsoft Teams, Skype Communications und Zoom Video Communications „die aufgeführten Bedingungen nicht erfüllen."

Microsoft veröffentlichte daraufhin am 06.05.2020 eine Stellungnahme, in der sich das Unternehmen gegen diese Einschätzung von Teams und Skype wehrt. Unterschiedliche Medien berichten in diesem Zusammenhang von einer Abmahnung von Microsoft gegenüber der Berliner Beauftragten für Datenschutz. Kurz darauf war das Dokument der Datenschutzaufsicht nicht mehr abrufbar.

Dabei ist nicht etwa der Inhalt des Dokuments unzutreffend. Vielmehr wurde von der Aufsichtsbehörde nicht begründet, warum genau die genannten Produkte die Anforderungen nicht erfüllen. Seit dem 22.05.2020 ist eine überarbeitete Version 1.3 der Checkliste verfügbar, in der die Behörde weiterhin fordert, kurzfristig eingesetzte „nicht datenschutzgerechte Lösungen" so bald wie möglich abzulösen, aber auch ankündigt, „in Kürze eine ausführlichere Übersicht mit detaillierteren Angaben zu verschiedenen gängigen Anbietern von Videokonferenz-Diensten zu erstellen."

Doch wie findet man bis dahin geeignete datenschutzrechtlich zulässige Produkte? Auf die Tests von Institutionen wie der Stiftung Warentest kann man sich dabei wohl eher nicht stützen – Testsieger waren am 13.05.2020 Microsoft Teams und Skype, trotz eines „befriedigend" beim „Basisschutz persönlicher Daten".

Secorvo News

Herbstseminare

Den aufgrund der Pandemie-Verordnungen des Landes Baden-Württemberg eingestellten Seminarbetrieb werden wir wie geplant nach der Sommerpause wieder aufnehmen. Da viele Teilnehmer ihre Anmeldung verschoben haben, ist die Mindestteilnehmerzahl schon jetzt bei einigen Seminaren erreicht – wir empfehlen Ihnen daher eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2020	
02.-03.06.	a-i3/BSI-Symposium 2020 (a-i3, Bochum)
15.-16.06.	DuD 2020 (COMPUTAS, Berlin)
Juli 2020	
08.07.	Security Cruise (Connecting Media, Karlsruhe)
14.-18.07.	PETS 2020 (University of Minnesota, Montréal/CAN)
19.-21.07.	DFRWS USA 2020 (DFRWS, Memphis/US)
August 2020	
01.-06.08.	Blackhat USA 2020 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 28 (Defcon, Las Vegas/US)
09.-11.08.	SOUPS 2020 (usenix, Boston/US)
12.-14.08.	29th USENIX Security Symposium (usenix, Boston/US)
16.-20.08.	Crypto 2020 (IACR, Santa Barbara/US)

Fundsache

Im April 2020 veröffentlichte das CrypTool-Entwicklerteam Release 2020.1 der Version 2 des bewährten Kryptographie-Lerntools. Es enthält zahlreiche Verbesserungen, Ergänzungen und Korrekturen – darunter auch ein Tutorial für die Differentielle Kryptoanalyse. Die neue Version wird im Dezember bei unserem Adventsrätsel „Krypto im Advent“ zum Einsatz kommen.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2020



Friendly Fire

Es ist nicht lange her, da galten Phishing-Angriffe als IT-Dilettanten-Test: Wer auf die holprigen, in schlechtem Englisch verfassten Aufforderungen hereinfiel und PIN und TAN für sein Konto preisgab, der konnte sich der Schadenfreude seiner Umgebung sicher sein. Die von solchen Angriffen verursachten Schäden blieben daher überschaubar, auch, weil die deutschen Banken technisch gegensteuerten: 2016 summierten sie sich auf gerade einmal 8,7 Mio. Euro.

Aber die Phisher lernten schnell, dass mit „digitalem Social Engineering" auch ganz andere Summen abgerufen werden können: Ob CEO Fraud, Verschlüsselungs-Trojaner oder Credential Phishing – alle diese Angriffsformen basieren im Kern darauf, den Empfänger mit einer halbwegs plausiblen Geschichte zu einer Schaden verursachenden Reaktion zu verleiten. Entscheidender Auslöser ist am Ende ein Klick – auf einen Link, einen Login-Knopf oder eine Online-Überweisung.

Zwar gibt es probate Mittel, um die Authentizität einer E-Mail oder eines Anrufs zu überprüfen, auf die auch ausgefuchste Angreifer keinen Einfluss haben: die interne Rückfrage, die Prüfung der Rufnummer oder E-Mail-Adresse, das Vier-Augen-Prinzip. Eine solche Aufdeckung digitaler „Enkel-Tricks" fordert jedoch Aufmerksamkeit und gesundes Misstrauen von den IT-Nutzern. Leider sind wir seit Jahren (SSN 01/2012) dabei, ihnen gerade dies abzugewöhnen.

E-Mail-Clients, die nur den vom Absender wählbaren Sendernamen statt der E-Mail-Adresse anzeigen, Online-Anbieter, die für den Rechnungsversand oder das User-Management beliebige Second-Level-Domains nutzen und Marketing-Abteilungen, die Klickraten durch HTML-formatierte E-Mails mit verdeckten Links in die Höhe zu treiben versuchen: All dies stumpft Aufmerksamkeit und Misstrauen ab. Schutz vor Täuschungsangriffen werden wir daher nicht allein durch Mitarbeiter-Sensibilisierung erreichen – auch Hersteller, Marketingabteilungen und die interne Kommunikation müssen ihren Teil der Verantwortung erkennen.



Inhalt

Friendly Fire

Security News

IT-Sicherheit 2.0

Cookies - nur mit Einwilligung

Ungewolltes Phishing-Training

Aus für Google Analytics

Thunderspy

DSGVO-konforme Auskünfte

Universalität der Grundrechte

Secorvo News

T.P.S.S.E. und T.I.S.P.

Termine zum Vormerken

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

IT-Sicherheit 2.0

Mitte Mai wurde ein Referentenentwurf des Innenministeriums für das „IT-Sicherheitsgesetz 2.0“ mit Stand vom 07.05.2020 öffentlich. Zwar kann sich bis zur Gesetzesverabschiedung noch sehr viel ändern, doch verdient der Entwurf aufgrund seiner zahlreichen Neuerungen Aufmerksamkeit. So erhält das BSI neue Aufgaben, u. a. die Förderung des Verbraucherschutzes und die Entwicklung eines „Stands der Technik“ bzgl. der sicherheitstechnischen Anforderungen an IT-Produkte. Es soll zur allgemeinen Meldestelle für Sicherheitsrisiken in der Informationstechnik werden und selbst aktiv nach Sicherheitslücken von öffentlich erreichbaren IT-Systemen suchen dürfen, auch mittels simulierter Angriffe.

Den Betreibern kritischer Infrastrukturen auferlegte Pflichten werden ausgeweitet auf „Unternehmen von besonderem öffentlichen Interesse“, die durch Rechtsverordnung noch genauer zu bestimmen sind. Im Telemediengesetz (TMG) soll u. a. eine Anzeigepflicht bei Angriffen und Datenverlusten gegenüber dem Bundeskriminalamt ergänzt werden. Ein interessantes Detail ist auch die Verlängerung der Speicherdauer für Protokolldaten der Systeme des Bundes auf bis zu 18 Monate. Und nicht zuletzt werden die Sanktionen bei Verstößen auf DSGVO-Niveau angehoben.

Die Rolle des BSI wird durch den Gesetzesentwurf deutlich erweitert. Der Entwurf enthält zahlreiche Regelungen, die erhebliche Auswirkungen auf IT-Vorhaben zahlreicher Unternehmen haben werden. Die Umsetzungsfristen, soweit vorgesehen, liegen bei nur einem Jahr – ein wichtiger Grund, das Gesetzgebungsverfahren aufmerksam zu verfolgen.

Cookies - nur mit Einwilligung

Am 28.05.2020 hat der Bundesgerichtshof nach der Planet49-Entscheidung des EuGH (SSN 10/2019) nun auch ein Urteil in Sachen Cookies gefällt. Das Ergebnis ist wenig überraschend: Das Setzen von Cookies ist nur zulässig, wenn der Betroffene zuvor eingewilligt hat. Die Auffassung, dass hiervon technisch erforderliche Cookies nicht betroffen sind, teilt der BGH mit dem EuGH. Am meisten Aufsehen erregt der BGH mit seiner Auslegung des § 15 Abs. 3 Satz 1 TMG: Obwohl darin dem Wortlaut nach von einem Widerspruch die Rede ist, hat nach Überzeugung des BGH auch hier eine Einwilligung vorzuliegen.

Damit steht unzweifelhaft fest: Möchte ein Webseitenbetreiber neben technisch notwendigen Cookies und ähnlichen Technologien auch solche einsetzen, die z. B. dem Marketing dienen, benötigt er die Einwilligung des Seitenbesuchers. Klarheit darüber, wie solche Einwilligungen in der Praxis auszusehen haben, gibt es jedoch weiter nicht.

Ungewolltes Phishing-Training

Am 02.04.2020 sperrte Linksys die Konten aller „Smart-Wi-Fi“-Nutzer, nachdem bekannt geworden war, dass Angreifer über so genannte Credential-Stuffing-Attacken die Kontrolle über eine Vielzahl von Benutzerkonten erlangt hatten. Dazu probieren Angreifer aus früheren Leaks bekannte Benutzernamen und Passwörter in anderen Anwendungen aus.

Die – an sich begrüßenswerte – proaktive E-Mail von Linksys, in der die Kunden zur Rücksetzung des Passworts aufgefordert wurden, wurde jedoch nicht von einer bekannten Linksys-Domäne, sondern von subscribermanagement@linksys-email.com verschickt – typisches Merkmal einer Phishing-E-Mail. Ein vermeidbarer sicherheitskritischer Fehler: Misstrauische Nutzer werden nicht auf diese E-Mail reagiert haben, andere wurden verunsichert und einige werden wieder einmal gelernt haben, dass es doch nicht weh tut, auf zweifelhafte E-Mail-Links zu klicken.

Kein Einzelfall, wie unsere Praxiserfahrung zeigt. E-Mails mit anhängenden Bestellungen im PDF-Format ohne Begleittext, Faxe mit anderer Ortsvorwahl als die des Absenders, kryptische Servernamen und Aufforderungen, ein Benutzerkonto zu aktivieren, die von unternehmensfremden Domains verschickt werden. Vermeintliche Kleinigkeiten, die mittelfristig jedoch große Schäden verursachen können. Denn der nächste Phishing-Angriff kommt bestimmt.

Aus für Google Analytics

Die Datenschutzkonferenz hat am 12.05.2020 ihre Hinweise zum Einsatz von Google Analytics aktualisiert und die Orientierungshilfe für Anbieter von Telemedien ergänzt. In der ausdrücklich nicht abschließenden Beurteilung werden der Widerrufs-Button von Google und die Einordnung als Auftragsverarbeitung „beerdigt“. Zudem wird klargestellt, dass Google unabhängig von anonymize_IP regelmäßig mit personenbezogenen Daten arbeitet. Die Datenschutzkonferenz betrachtet die Nutzung von Analytics daher als Fall der gemeinsamen Verantwortung (Art. 26 DSGVO).

Die Nutzung von Analytics könne in der Regel nicht aus einem berechtigten Interesse abgeleitet werden, sodass eine Einwilligung der Nutzer erforderlich ist. Die Information der Betroffenen muss beinhalten, dass Google die gesammelten Daten zu „beliebigen eigenen Zwecken“ verwendet, die Daten unter Zugriff staatlicher Stellen in den USA verarbeitet und darlegen, welche Zwecke damit von Google verfolgt werden. Dazu wird auf die Leitlinien für Transparenz des EDSA vom 11.04.2018 verwiesen.

Keine dieser Anforderungen erfüllt Analytics derzeit: Es gibt kein Vertragsangebot von Google zur gemeinsamen Verantwortung, und auch technisch genügt Analytics den Anforderungen der DSK nicht. Eine informierte Einwilligung kann auch der Seitenanbieter nicht beisteuern. In aller Klarheit und Kürze: Die Nutzung von Google Analytics ist in Europa derzeit nicht rechtskonform möglich.

Thunderspy

Intels Thunderbolt-Technologie setzt sich immer weiter durch; viele Notebooks bringen bereits entsprechende Ports mit. Technisch werden dabei der DisplayPort für die Bildübertragung und PCI Express (PCIe) für eine performante Datenübertragung kombiniert. Zurzeit wird Version Thunderbolt 3 verbreitet, die die Funktionen von USB 3.1 umfasst, also den Anschluss von USB-Geräten und Ladefunktionen bietet. So eignet es sich ausgezeichnet als Docking-Port. Da PCIe auf der Basis von Direct Memory Access (DMA) arbeitet, kann darüber auf den Hauptspeicher des Computers zugegriffen werden. Um das unberechtigte Auslesen sensibler Daten und Manipulationen des Systems zu verhindern, haben Hersteller DMA Remapping und Thunderbolt Security entwickelt; darüber kann man einzelne Geräte (z. B. Docks) für PCIe autorisieren.

Nach unserer Erfahrung wird Thunderbolt Security in vielen Unternehmen jedoch deaktiviert, weil der Verwaltungsaufwand hoch ist. Der Sicherheitsforscher Björn Ruytenberg hat am 17.04.2020 in einem Paper mehrere Schwachstellen des Protokolls veröffentlicht, die es erlauben, die Sicherheitsfunktionen zu umgehen. Nach Einschätzung des Autors lassen sich die Schwachstellen kaum in Software beheben. Wer den Thunderbolt Port nutzt, sollte daher auf die Vertrauenswürdigkeit des Geräts achten.

DSGVO-konforme Auskünfte

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, hat aufgrund zahlreicher Beschwerden die Berechnungsmethoden von Wirtschaftsauskunfteien zur Einstufung der Kreditwürdigkeit von Unternehmen und Privatpersonen überprüft. Die Pressemitteilung vom 05.06.2020 lässt aufhorchen: Nach den Grundsätzen für die Verarbeitung personenbezogener Daten gemäß DSGVO müssen die Daten u. a. „sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein“, Art. 5 Abs. 1 lit. d DSGVO. Gegen diesen Grundsatz haben Wirtschaftsauskunfteien offenbar teilweise verstoßen: So wurden Bonitätsbeurteilungen bei nicht vorliegenden Informationen z. B. auf Basis von Annahmen getroffen. Dies führte dazu, dass Kreditrahmen niedriger eingestuft wurden. Bewertungen sind jedoch nur dann rechtmäßig, wenn die Richtigkeit der genutzten Daten (und damit der Bewertung selbst) sichergestellt ist.

Universalität der Grundrechte

Am 19.05.2020 hat das Bundesverfassungsgericht über die Auslandsfernaufklärung des Bundesnachrichtendienstes im Ausland geurteilt und Teile des BND-Gesetzes für verfassungswidrig erklärt. Im Urteil stellt das BVerfG klar, dass sich deutsche Staatsgewalt auch an die Grundrechte (im Verständnis von Abwehrrechten, z. B. zum Schutz vor staatlichen Abhörmaßnahmen) halten muss, wenn sie Wirkungen außerhalb des deutschen Staatsgebietes erzeugt, und auch dann, wenn keine deutschen Bürger betroffen sind.

Dieses Urteil wird bei der Gesetzgebung zu generell grenzüberschreitenden Sachverhalten wie Datenschutz, Rechtsfragen des Internet, Medienrecht usw. künftig stets zu beachten sein. Damit steht es in eklatantem Kontrast zum amerikanischen Grundrechtsverständnis, wie es beispielsweise im US CLOUD Act (SSN 3/2019) zum Ausdruck kommt.

Secorvo News

T.P.S.S.E. und T.I.S.P.

Im September bieten wir Ihnen wieder die Möglichkeit, Ihre Kenntnisse und Kompetenzen in der IT-Sicherheit zu aktualisieren – und zu zertifizieren: für das Teilgebiet des sicheren Software-Engineerings (T.P.S.S.E., **14.–17.09.2020**) und das Zertifikat als Information Security Professional (T.I.S.P., **21.–25.09.2020**). Zur Vorbereitung erhalten Sie nach Ihrer Anmeldung unser Begleitbuch „Informationssicherheit und Datenschutz“, das im vergangenen Herbst in dritter Auflage im dpunkt-Verlag erschienen ist.

Termine zum Vormerken

Am 08.07.2020 bietet KA-IT-Si-Partner Connecting Media die zweite SecurityCruise – diesmal auf der „MS Digital“. Spannende Vorträge, Workshops und spezielle Talkrunden mit den größten IT-Security-Anbietern im deutschsprachigen Raum erwarten Sie. Für KA-IT-Si-Partner und –Unterstützer gibt es das Steuermannpaket zum Vorteilspreis von 45 €. Schicken Sie bei Interesse eine kurze E-Mail an info@ka-it-si.de und wir senden Ihnen den Rabattlink zu.

Derweil freuen wir uns darauf, unsere KA-IT-Si-Veranstaltungen im zweiten Halbjahr 2020 wieder aufzunehmen. Notieren Sie sich gerne schon einmal die geplanten Termine in Ihrem Kalender: 24.09.2020 | 22.10.2020 | 12.11.2020 | 10.12.2020. Wir beginnen im September mit einem spannenden Vortrag zum „Mythos der Enigma“ von Johann Grathwohl, IT-Security-Architekt bei CONITAS.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2020	
08.07.	Security Cruise (Connecting Media, Karlsruhe)
14.-18.07.	PETS 2020 (University of Minnesota, Montréal/CAN)
19.-21.07.	DFRWS USA 2020 (DFRWS, Memphis/US)
August 2020	
01.-06.08.	Blackhat USA 2020 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 28 (Defcon, Las Vegas/US)
07.-11.08.	SOUPS 2020 (usenix, Boston/US)
12.-14.08.	29th USENIX Security Symposium (usenix, Boston/US)
17.-21.08.	Crypto 2020 (IACR, Santa Barbara/US)
September 2020	
14.-17.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
22.09.	Datenschutztag 2020 (COMPUTAS. Köln)

Fundsache

Das *Border Gateway Protocol* (BGP) ist ein zentraler Bestandteil des Internet-Routings. Wie unsicher BGP ist, haben in den letzten Jahren verschiedene „Fehlkonfigurationen" z. B. von chinesischen, pakistanischen oder russischen Internet Service Providern gezeigt. Cloudflare hat mit der Website „Is BGP Safe Yet?" am 17.04.2020 eine Art „digitalen Pranger" eingerichtet, der ISPs animieren soll, Sicherheitsmechanismen wie die kryptographische Validierung von Routing-Informationen zu nutzen.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2020



Menschenrecht Anonymität

Menschen urteilen täglich. Vieltausendfach. Über Menschen. Wir müssen das tun, um angemessen auf unser Umfeld zu reagieren. Aber diese Urteile sind nie zutreffend und nur selten gerecht, denn es sind verkürzende, vereinfachende Bewertungen, die wir auf der Grundlage sehr begrenzter Detailkenntnis vornehmen. Das ist jedoch unvermeidlich – schließlich sind wir begrenzte Wesen: Kein Mensch, kein Richter könnte von sich behaupten, alle für ein Urteil relevanten Fakten und Hintergründe zu kennen. Doch da wir handeln müssen, müssen wir auch mit Halbwissen urteilen.

Und genau hier beginnt das Dilemma. Je mehr wir wissen, desto schwerer fällt es uns, ein Urteil zu fällen. Entgegenstehende Fakten trüben den Blick, lassen die Konturen von schwarz und weiß, von richtig und falsch unscharf werden. Das mag einer der Gründe sein, warum Vorurteile und generalisierte Bewertungen etwas bestechend Verlockendes an sich haben: Sie sind klar, rein, einfach – leider aber (fast) immer falsch. Denn sie zeichnen ein überscharfes (Zerr-) Bild der Wirklichkeit, das die komplexe, vielschichtige „Wahrheit" bestenfalls in einer ganz bestimmten Perspektive widerspiegelt.

Können wir einen Menschen mit irgendeiner Information in Verbindung bringen, fällen wir also unvermeidlich ein (wahrscheinlich ungerechtes) Urteil – sogar dann, wenn die Information unzuverlässig, sachfremd oder in diesem Kontext irrelevant ist. Genau deshalb brauchen wir Anonymität: Sie allein schafft einen urteilsarmen Raum, in dem neutraler Respekt und unvoreingenommener Umgang zwischen Menschen möglich wird. Und damit freie Entfaltung.

Am 10.07.2020 machte ein Beitrag auf netzpolitik.org das polnische Startup PimEyes bekannt, das aus im Internet verfügbaren Bildern biometrische Daten von mehr als 900 Mio. Gesichtern gewonnen haben will. Es bietet Gesichtsidentifikation für jedermann – der Anfang vom Ende der Anonymität. Wer aber anonyme Räume zerstört, schafft freie Entfaltung ab.



Inhalt

Menschenrecht Anonymität

Security News

Ende des Privacy Shields

Bußgeld für die AOK

Lunchgate

DSFA für CWA

Bundesgenossen

Videokonferenzsysteme – revisited

Wieder einmal Störerhaftung

Secorvo News

Endlich wieder... Seminare

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Ende des Privacy Shields

Der Europäische Gerichtshof hat am 16.07.2020 – wie von europäischen Datenschutzexperten erwartet – den Kommissionsbeschluss zum EU-US-Privacy Shield für ungültig erklärt. Auch die Standardvertragsklauseln werden im Urteil sehr kritisch beurteilt und dürften als Rechtsgrundlage für viele der bisher über das Privacy Shield legitimierten Verarbeitungen in den USA ausscheiden: Mit Rechtsvorschriften wie dem CLOUD Act (SSN 3/2019) garantiere das amerikanische Recht nach Auffassung des EuGH keinen dem EU-Recht äquivalenten Schutz personenbezogener Daten.

Damit hat der EuGH der Verarbeitung europäischer personenbezogener Daten in den USA, aber auch durch Töchter amerikanischer Unternehmen in Europa eine deutliche Absage erteilt – wer es dennoch tut, ist in der Nachweispflicht. Das wird auch aus den FAQ des europäischen Datenschutzausschusses zum Urteil deutlich, die dieser am 23.07.2020 veröffentlichte. Sollten die Aufsichtsbehörden nun gezielt Verarbeitungen personenbezogener Daten europäischer Bürger durch amerikanische Unternehmen mit Bußgeldern ahnden, dürfte eine Schockwelle durch Online-Marketing-Abteilungen schwappen.

Bußgeld für die AOK

Am 30.06.2020 teilte der Baden-Württembergische Beauftragte für Datenschutz und Informationssicherheit mit, dass seine Behörde gegen die AOK Baden-Württemberg ein Bußgeld in Höhe von 1,24 Mio. € verhängt hat. Im Zusammenhang mit Gewinnspielen hatte die AOK personenbezogene Daten erhoben und zu Werbezwecken verwendet; in mehr als 500 Fällen lag die dafür notwendige Einwilligung jedoch nicht vor. Bei der Bußgeldbemessung (SSN 10/2019) wurden das kooperative Verhalten der Krankenkasse, ihre Bedeutung für das Gesundheitssystem sowie die Belastung durch die Corona-Pandemie berücksichtigt. Wie hoch wäre es wohl ausgefallen, wenn diese begünstigenden Faktoren nicht vorgelegen hätten?

Angesichts unzureichender, aber immerhin vorhandener Maßnahmen und eines vergleichsweise geringen Anteils an rechtswidriger Werbeverwendung erscheint die Bußgeldhöhe kaum verhältnismäßig. Doch steigt damit der Druck auf Unternehmen, ihre Datenschutzumsetzung in der Praxis wirksamer zu überwachen.

Lunchgate

Die Sicherheitsfirma modzero veröffentlichte am 07.07.2020 eine Schwachstelle in der um eine Kontaktdatenfunktion erweiterte Tisch-Reservierungs-App des Schweizer Startups Lunchgate. Dem Bericht „Mit Webapps gegen COVID-19“ zufolge handelt es sich dabei um eine sogenannte Insecure Direct Object Reference, durch die alle erfassten Daten öffentlich einsehbar waren. Dabei fiel auf, dass Lunchgate die Kontaktdaten mindestens 21 statt der maximal zulässigen 14 Tage speichert. Lesen bildet: Ein Blick in die OWASP Cheat Sheets, hier konkret in das Insecure Direct Object Reference Prevention Cheat Sheet, hätte den Entwicklern geholfen, diese Lunchgate-Affäre zu vermeiden.

DSFA für CWA

Als die Corona-Warn-App (CWA) am 16.06.2020 zur Nutzung bereitgestellt wurde, hatte das Robert-Koch-Institut (RKI) erst vier Tage zuvor die zugehörige Datenschutz-Folgenabschätzung (DSFA) abgeschlossen. Der 117 Seiten lange Bericht dürfte eine der bislang meistdiskutierten und am besten durchleuchteten DSFA seit dem Inkrafttreten von Art. 35 DSGVO sein. Er orientiert sich am Standard-Datenschutzmodell (SDM) und berücksichtigt sämtliche in Art. 35 Abs. 7 DSGVO vorgegebenen Inhaltsbestandteile. So sind der Ablauf aus Nutzersicht, die Systemarchitektur, die Funktionsweise, die rechtliche Bewertung, die Analyse der Risiken für die Betroffenen und die getroffenen Maßnahmen ausführlich dokumentiert.

Dennoch werden dem Bericht datenschutzrechtliche Unerfahrenheit, Zielverfehlung (Legitimation statt Risikominimierung) und erhebliche Lücken attestiert, bspw. bei der Betrachtung der verwendeten Serverkomponenten und der möglichen Verknüpfung der Positivschlüssel mit den IP-Adressen bei der Übermittlung. Weitere Kritikpunkte sind das Ausklammern der Risiken durch das nicht kontrollierbare *Exposure Notifikation Framework* (ENF) von Apple und Google, durch das bestimmte Verarbeitungsschritte fremddiktiert werden, oder die Methodik der Risikobetrachtung. Die teilweise berechtigten Kritikpunkte erscheinen jedoch angesichts der Umstände (politischer Druck, Zeitdruck, vermeintliche Bedeutung der App) entschuldbar – zumal die öffentliche Diskussion über die Datenschutzkonformität der CWA zweifelsfrei dem Datenschutz gedient hat.

Bundesgenossen

Das Bundeskartellamt hat am 01.07.2020 den Abschlussbericht zur bereits im Dezember 2017 begonnenen Sektoruntersuchung zu Smart-TVs vorgelegt. Anlass der Untersuchung war der Verdacht auf erhebliche, dauerhafte Verstöße gegen verbrau-

cherrechtliche Vorschriften - mit einem Schwerpunkt beim Datenschutz.

Der Bericht dokumentiert erhebliche Datenschutzmängel wie zu pauschal bezeichnete Rechtsgrundlagen und Zwecke (bspw. „Verbesserung der angebotenen Dienste“), zu komplexe, unverständliche und zugleich undifferenzierte Datenschutzerklärungen, fehlende Angaben zu den verarbeiteten Daten, mangelnde Datensicherheit oder unerlaubte Werbung.

Dank des 9. Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) hat das Kartellamt seit dem 08.07.2017 mit § 32e Abs. 5 GWB die Befugnis zur Prüfung von Wirtschaftszweigen auf die Einhaltung von Verbraucherschutzrecht. Zuletzt hatte sich das Bundeskartellamt im Februar 2019 bereits mit dem Datenschutz bei Facebook beschäftigt (SSN 2/2019). Sollten weitere derartige Berichte folgen, könnte das Bundeskartellamt zu einem relevanten Player im Datenschutz werden.

Nun sind die Datenschutzaufsichtsbehörden aufgerufen, die im Bericht festgestellten Mängel aufzugreifen, dessen Untersuchungstiefe über viele Betrachtungen der Aufsichtsbehörden deutlich hinausgeht.

Videokonferenzsysteme – revisited

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat am 03.07.2020 vier einander ergänzende Dokumente zu Videokonferenzsystemen, darunter eine ausführliche Bewertung führender Angebote (u. a. GoToMeeting, Jitsi, Google Meet, Teams, Skype, WebEx und Zoom) samt Handlungsempfehlungen für Unternehmen und Behörden vorgelegt und damit ihre erste Stellungnahme vom 08.04.2020 (SSN 5/2020) ergänzt.

Der Checkliste zufolge soll vor jeder Videokonferenz geprüft werden, ob nicht eine Telefonkonferenz ausreicht. Weiter sollen selbst betriebene Dienste vorgezogen werden, da die vorhandenen Angebote überwiegend als „nicht rechtskonform einsetzbar“ eingestuft werden. Dabei wird zum einen auf das (derzeit für solche Telemediendienste noch nicht anwendbare) Telekommunikationsgeheimnis verwiesen; zum anderen geht die Prüfung davon aus, dass das organisierende Unternehmen grundsätzlich Auftragsverarbeitungsverträge schließen müsse – und diese würden für Teams, Google Meet und Co. nicht ausreichend angeboten.

Nicht näher analysiert wird allerdings, ob die Voraussetzungen für eine Auftragsverarbeitung überhaupt regelmäßig vorliegen. Hieran bestehen Zweifel, denn nicht jedes der Angebote muss als Dienst mit fester Nutzeranmeldung betrieben werden. Und selbst dann ist fraglich, warum die damit verbundene Übermittlung dienstnotwendiger Daten nicht zu rechtfertigen sein soll. Die Untersuchung reiht sich damit leider in eine Reihe durch die Corona-Krise ausgelöster, überhasteter Stellungnahmen zu Videokonferenzsystemen ein, auch wenn die mit deren Einsatz verbundene grundsätzliche Problematik nicht in Abrede zu stellen ist.

Wieder einmal Störerhaftung

Seit dem 3. Gesetz zur Änderung des Telemediengesetzes (TMG), das die Störerhaftung von WLAN-Betreibern durch die Neufassung von § 8 TMG begrenzen sollte, ist es um Filesharing-Urteile ruhig geworden. Daher sorgte die (noch nicht rechtskräftige) Verurteilung einer älteren Dame, die nach eigenen Angaben einen offenen WLAN-Knoten betrieben aber selbst nicht genutzt hatte, durch das Amtsgericht Köln vom 08.06.2020 für Aufsehen. Um den Erstattungsanspruch abzuwehren hätte sie nach Auffassung des Gerichts konkrete Nutzer im fraglichen Zeitpunkt benennen müssen.

Eine Rückkehr zur Störerhaftung ist trotz dieses Urteils zum Glück nicht zu fürchten. Allerdings ist es keine gute Entwicklung, dass durch subtile Differenzierungen des Klägers unkundige WLAN-Betreiber ohne anwaltliche Vertretung – wie in diesem Fall – Gefahr laufen, verurteilt zu werden.

Secorvo News

Endlich wieder... Seminare

Nach langer Pause können wir Ihnen im September wieder die Möglichkeit bieten, Ihre Kenntnisse und Kompetenzen in der IT-Sicherheit zu aktualisieren – und zu zertifizieren: für das Teilgebiet des sicheren Software-Engineerings (T.P.S.S.E., **14.–17.09.2020**) und das Zertifikat als TeleTrust Information Security Professional (T.I.S.P., **21.–25. 09.2020**).

Zur Vorbereitung auf das Seminar und die T.I.S.P.-Prüfung erhalten Sie nach Ihrer Anmeldung unser Begleitbuch „Informationssicherheit und Datenschutz“, das im vergangenen Herbst in dritter Auflage im dpunkt-Verlag erschienen ist – und sich inzwischen zahlreicher positiver bis begeisterter Kritiken erfreut. Wer also noch eine Sommerlektüre sucht...

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2020	
06.-09.08.	DEF CON 28 (Defcon, Las Vegas/US)
07.-11.08.	SOUPS 2020 (usenix, Boston/US)
12.-14.08.	29th USENIX Security Symposium (usenix, Boston/US)
17.-21.08.	Crypto 2020 (IACR, Santa Barbara/US)
September 2020	
07.-11.09.	IEEE European Symposium on Security and Privacy (IEEE Computer Society, Genua/IT)
14.-17.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
21.-22.09.	Security of Things World (we.CONECT Global Leaders GmbH, Berlin)
21.-25.09.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
22.09.	Datenschutztag 2020 (COMPUTAS. Köln)
24.09.	IT-Sicherheitsrechtstag (TeleTrusT e.V., Berlin)
29.09.-01.10.	IT-Sicherheit - praxisnah und aktuell (Secorvo, Karlsruhe)
29.09.-02.10.	Blackhat Asia 2020 (Blackhat, Singapur/SIN)

Fundsache

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe hat am 16.06.2020 den Umsetzungsbericht 10 Jahre „KRITIS-Strategie“ veröffentlicht. Der bietet vertiefte Einblicke in die Risikobewertung und den Schutz der verschiedenen Sektoren kritischer Infrastrukturen.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2020



Vermintes Terrain

Bei manchen Gelegenheiten sollte man zurückhaltend sein, Kenntnisse in der IT-Sicherheit oder dem Datenschutz durchblicken zu lassen. Zum Beispiel beim Abendessen mit Freunden. Eine der sich nach einem solchen „Coming Out" geradezu schicksalhaft ergebenden Fragen, die jeden noch so zauberhaften Abend irreparabel pulverisieren kann, ist – pars pro toto – diese hier: „Ist Whatsapp eigentlich sicher?"

Wo soll man da anfangen – und was lieber verschweigen? Dass die Kontaktdaten des Smartphones an Whatsapp übertragen werden? Dass eine solche Übermittlung von Daten Dritter in die USA rechtswidrig ist? Dass Whatsapp sich die Rechte an allen Inhalten übertragen lässt? Dass Whatsapp nach eigenen Angaben Ende-zu-Ende-Verschlüsselung realisiert? Dass man diese Behauptung nicht sicher bestätigen kann – schließlich könnte es ja eine „Hintertür" geben? Dass verlinkte Inhalte nicht in die Verschlüsselung eingeschlossen sind? Dass Whatsapp-Videochats ohnehin unverschlüsselt übertragen werden? Dass das vielleicht gar nicht die wichtigste Frage ist, da die Verbindungsdaten ein „digitales Bewegungsbild" liefern? Dass Whatsapp zum Facebook-Konzern gehört – und dass für diesen Verbindungsdaten ohnehin wertvoller sind als Kommunikationsinhalte? Dass „ich hab' ja nichts zu verbergen" das denkbar ignoranteste Argument gegen Datenschutz ist? Dass „Soziale Netzwerke" keine Sozialkontakte ersetzen sollten? Dass Bewegung für die Entwicklung der Sprösslinge besonders wichtig ist – und zwar nicht nur für die Daumen? Und – spätestens hier werden Sie mit hoher Wahrscheinlichkeit enthauptet – dass die Vermittlung von Digitalkompetenz und der damit einhergehenden „digitalen Souveränität" wichtiger sein sollte als die Befürchtung sozialer Ausgrenzung, und es sich daher lohnt, sich dem Anpassungsdruck entgegenzustellen?

Wissen kann manchmal einsam machen.



Inhalt

Vermintes Terrain

Security News

Folgen von „Schrems II"

Alt und anfällig...

Qualifikation des DSB

Listen to the Key

Out of Scope

Vergissmein(nicht)?

Secorvo News

KA-IT-Si-Stammtisch

Secorvo Seminare

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Folgen von „Schrems II“

Nach dem Urteil des EuGH zur Ungültigkeit des EU/US Privacy-Shield (C-311/18) vom 16.07.2020 hat Google mit ersten Hinweisen zur Neugestaltung seiner Datenübermittlungen in die USA reagiert und erweitert seine Vertragsbedingungen für Werbeprodukte und Google Analytics um Standardvertragsklauseln. Zudem kann der Anwender bei Beauftragung aktuell entweder die Variante "Auftragsverarbeitung" für verschiedene Dienste, darunter Analytics, oder unabhängige Verantwortung ankreuzen. Die Einordnung als gemeinsame Verantwortung der DSK vom 12.05.2020 wird damit nicht umgesetzt. Google hält seine Anwender zudem zum Einholen von Einwilligungen der Nutzer an, stellt hierzu auch Hilfen zur Verfügung und verweist auf seine Informationen zur Datennutzung.

Diese Reaktion wird von Max Schrems und der neu gegründeten Initiative „My Privacy is None of Your Business“ als unzureichend angesehen. Um die Aufsichtsbehörden zur Urteilsdurchsetzung zu zwingen hat die Initiative daher Seiten großer Unternehmen gescannt und Beschwerden über die fortgesetzte Nutzung eingereicht; inzwischen liegen Beschwerden gegen 101 Unternehmen in 30 EU-Staaten vor.

Auch die Haltung der deutschen Aufsichtsbehörden ist eindeutig, wie u. a. die Stellungnahme des LfDI Baden-Württemberg vom 25.08.2020 belegt. „Retten“ lässt sich die Situation wohl allein durch eine technische Beschränkung der Datenverarbeitung auf Europa und eine aufklärende Erneuerung der Informationen zur Datennutzung seitens Google – oder den konsequenten Verzicht auf die Nutzung dieser Dienste.

Alt und anfällig...

E-Mails dominieren weltweit sowohl die private als auch die Unternehmenskommunikation. Das dabei verwendete „Simple Mail Transfer Protocol“ (SMTP) feierte in diesem Monat seinen 38. Geburtstag – und stammt aus einer Zeit, in der Sicherheitsmechanismen noch nicht zu den Kernfunktionen eines Protokolls zählten. Passenderweise stellten drei Forscher am 06.08.2020 auf der Blackhat USA 18 Angriffe auf E-Mail-Sender-Authentisierung vor und zeigten, wie anfällig E-Mail-Infrastrukturen auch mit nachträglich eingebauten Sicherheitsmechanismen wie SPF, DKIM und DMARC sind. Sicherheitsaufsätze stoßen auch hier an ihre Grenzen.

Angriffe mit gefälschten Absendern zählen derzeit zu den erfolgreichsten Wegen, Schadsoftware zu verbreiten, wie der unlängst wiederbelebte Emotet demonstriert. Aufgrund der veralteten Architektur wird E-Mail auch mit Sicherheitsaufsätzen auf lange Zeit unsicher bleiben. Daher müssen neben technischen Schutzmaßnahmen vor allem auch die Menschen über die Fallstricke von E-Mail aufgeklärt werden.

Qualifikation des DSB

Das Landesarbeitsgericht (LAG) Mecklenburg-Vorpommern hat am 25.02.2020 über die Abberufungsvoraussetzungen eines Datenschutzbeauftragten (DSB) entschieden. Dabei traf es eine Reihe von Feststellungen zu den erforderlichen Qualifikationen und zum Pflichtumfang des DSB. Zur Qualifikation stellt das LAG fest, dass ein Volljurist mit Rückgriff auf technisches Personal zur Klärung von Fragen ohne weiteres über die erforderliche Fachkenntnis verfügt bzw. Datenschutzrecht korrekt anwenden kann.

Bezüglich der Pflichten war streitig, ob der DSB durch eine unterbliebene Verarbeitungsbeanstandung und einen Hinweis im Januar 2018, die DSGVO könne erst mit Geltung umgesetzt werden, seine Pflichten verletzt habe. Hierzu führt das LAG aus, dass ein DSB bei mehreren Betrieben und umfangreicher Datenverarbeitung zwangsläufig Prioritäten setzen muss. Durch Schulungen, Bearbeitungen von Anfragen und Mitwirkung in entsprechenden Unternehmensgremien hat er seine Pflichten erfüllt. Für die Einhaltung des Datenschutzes ist letztlich das Unternehmen verantwortlich. Dies galt auch für die Vorbereitungen zur Umsetzung der DSGVO.

Die Position des DSB wird durch das Urteil gestärkt, gleichzeitig werden die Anforderungen an seine Tätigkeit auf eine realistische Erwartung beschränkt. Als Orientierung für die Aufgabenbeschreibung bietet das Urteil hilfreiche Bezüge.

Listen to the Key

In ihrem am 24.08.2020 als Videoaufzeichnung erschienenen Vortrag von der HotMobile 2020 stellten Sicherheitsforscher der National University of Singapore einen neuen Angriff auf physische Schließsysteme vor. Die Forscher konnten zeigen, dass Angreifer neben dem bekannten Lockpicking auch das Geräusch eines ins Schloss geschobenen Schlüssels analysieren können. Denn aus dem z. B. mittels Smartphone-Mikro aufgezeichneten Geräusch der Pins beim Einschieben lässt sich das Profil des Schlüssels errechnen und ein passender Nachschlüssel fräsen – vorausgesetzt, der Angreifer kennt den Typ von Schloss und Schlüssel und der Schlüssel wird mit gleichmäßiger Geschwindigkeit eingeschoben. Eine App, die aus einer Audio-Aufnahme automatisch Nachschlüssel erzeugt, liegt also immerhin noch in einiger Ferne.

Bei dem Angriff handelt es sich um einen typischen Seitenkanalangriff. Darüber lassen sich häufig auch gute „primäre“ Schutzmechanismen umgehen: So kann beispielsweise ein grundsätzlich sicheres Kryptoverfahren einem Angreifer über Laufzeit- oder Spannungsunterschiede bei der Berechnung die Rekonstruktion des Schlüssels oder Klartextes ermöglichen. Solche Angriffe wurden u. a. bei der Mifare DESFire-Karte gezeigt. Andere Seitenkanalangriffe sind ein Passwortdiebstahl durch Aufzeichnung der Tippgeräusche oder Wärmebildaufnahmen der Tastatur. Die Härtung gegen Seitenkanalangriffe ist allerdings eine herausfordernde Angelegenheit.

Out of Scope

Dass beauftragte Einbrüche – ob digital als Penetrationstest oder physikalisch beispielsweise als Bestandteil eines Red-Team-Assessments – immer auch mit Risiken verbunden sind, hat der Fall zweier amerikanischer Penetrationstester eindrucksvoll gezeigt. Als diese am Abend des 11.09.2019 im Rahmen eines größeren, vom Staat Iowa beauftragten Assessments zum Testen des Alarmsystems durch eine offene Tür in das Dallas County Courthouse in Iowa eingedrungen waren, verließen sie das Gebäude in Handschellen – obwohl sie die schriftliche Freigabe für das Assessment mit sich führten und sich gegenüber den Beamten identifizieren konnten. Nach mehr als fünf Monaten rechtlichen Trubels wurden die Pentester Ende Januar 2020 freigesprochen. Eine Zusammenfassung der gesamten Geschichte mitsamt „Lessons learned“ gaben die beiden nun auf der Blackhat 2020.

Hilfreich war, dass ihr Arbeitgeber Coalfire sich unermüdlich für die beiden Mitarbeiter einsetzte. Um ähnliche Vorfälle zu vermeiden, rät Coalfire Auftraggebern und Pentestern, Vereinbarungen zum Ablauf eines Assessments immer schriftlich zu dokumentieren und die zugehörigen Vertragsunterlagen im Vorfeld von Juristen überprüfen zu lassen.

Auch klassische Penetrationstests können mit ähnlichen Risiken verbunden sein, wie der Fall von Rob Fuller zeigt: Durch einen winzigen Schreibfehler im vom Kunden genannten IP-Adressblock wurde das falsche Unternehmen angegriffen. Obwohl es in diesem konkreten Fall ohne negative Folgen blieb (und sogar zu einem neuen Kunden führte), hätten auch hier rechtliche Konsequenzen drohen können. Die eindeutige Klärung des Auftragsumfangs und der Zielobjekte („In Scope“/„Out of Scope“) muss deshalb zentraler Bestandteil einer jeden Vereinbarung zu einem Security Assessment sein.

Vergissmein(nicht)?

Der Bundesgerichtshof (BGH) entschied am 27.07.2020 bezüglich zweier Verfahren, wann Suchergebnisse durch Google zu löschen sind. Im ersten Fall konnte der Betroffene nicht erreichen, dass direkt auf ihn beziehbare Daten entfernt werden, da die Grundrechtsabwägung keinen Vorrang seines Schutzinteresses ergab. Das zweite Verfahren wurde ausgesetzt und mit weiteren Fragen an den Europäischen Gerichtshof (EuGH) für eine Vorabentscheidung eingereicht. Darin muss die Frage beurteilt werden, ob Google – nach Auffassung der Kläger – inhaltlich falsche Artikel eines Unternehmens über die Betroffenen löschen muss.

Im Urteil C-507/17 vom 24.09.2019 beschied der EuGH, dass Betreiber nicht verpflichtet sind, Auslistungen in sämtlichen Versionen ihrer Suchmaschinen vorzunehmen, sondern diese auf alle mitgliedstaatlichen Versionen beschränkt werden können. Aufgrund nationaler Datenschutzstandards können die Behörden eines Mitgliedsstaates jedoch eine Löschung in allen Versionen verlangen. Auch daraus wird deutlich, dass das in Art. 17 der DSGVO verankerte Recht auf „Vergessenwerden“ immer für den konkreten Einzelfall betrachtet werden muss.

Secorvo News

KA-IT-Si-Stammtisch

Aufgrund der nach wie vor geltenden Auflagen im Veranstaltungsbereich können wir unsere KA-IT-Si-Events nicht wie gewohnt durchführen. Daher möchten wir mit unserem ersten „KA-IT-Si-Stammtisch“ am **Donnerstag, 24.09.2020**, ab 18 Uhr im Biergarten der „Ersten Fracht“ in Karlsruhe (direkt gegenüber dem Hauptbahnhof) eine Plattform für den Austausch bieten.

Dort erwarten Sie vier verschiedene Thementische mit Andreas Sperber von aramido (Penetrationstests – das Was und Wie), Dr. Ingmar Baumgart vom FZI (Vulnerability Disclosure), Dirk Fox von Secorvo (Phishing-Awareness) und Oliver Winzenried von WIBU-Systems (Karlsruher „House of IT-Security“ und die zukünftige IT-Security Coworking Area). Die Ansprechpartner werden die Diskussionen mit einer kurzen Einführung in das Thema anstoßen.

Bei Interesse reservieren wir Ihnen gerne einen Platz an Ihrem ausgewählten Thementisch. Bitte melden Sie sich dafür bis Dienstag, 22. September 2020 an (keine Teilnahmegebühr, Bewirtungskosten exklusive).

Secorvo Seminare

Eine Terminübersicht, ausführliche Programme und die Möglichkeit zur Online-Anmeldung finden Sie auf unserer Webseite.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2020	
07.-11.09.	IEEE European Symposium on Security and Privacy (IEEE Computer Society, Genua/IT)
14.-17.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
21.-22.09.	Security of Things World (we.CONECT Global Leaders GmbH, Berlin)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
22.09.	Datenschutztag 2020 (COMPUTAS. Köln)
24.09.	IT-Sicherheitsrechtstag (TeleTrusT e.V., Berlin)
29.09.-01.10.	Informatik 2020 (GI Gesellschaft für Informatik, Karlsruhe)
29.09.-02.10.	Blackhat Asia 2020 (Blackhat, Singapur/SIN)
Oktober 2020	
12.-14.10.	ISSE 2020 (IEEE, Wien/A)
13.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH
22.-23.10.	heise devSec 2020 (dpunkt.verlag, heise Developer, heise Security, Heidelberg

Fundsache

Der Vortrag My Cloud is APT's Cloud: Investigating and Defending Office 365 zeigt bekannte und weniger bekannte Angriffe auf Microsofts Cloud-Lösungen auf, die in Zeiten von Covid-19 immer mehr an Bedeutung gewonnen haben.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2020



Wehret den Anfängen

Ganz gleich ob im Verein, im Unternehmen oder in einer Behörde: Fehler in und mangelnde Aktualität von Namens- und Adresseinträgen verursachen Jahr für Jahr Millionenkosten. Sendungen erreichen ihr Ziel nicht, Personen werden mehrfach in Datenbanken geführt und zusammengehörende Vorgänge werden nicht miteinander verknüpft. Ein teures Ärgernis.

Diesem Missstand will nun das Registermodernisierungsgesetz (mehr dazu in diesen SSN) amtlicherseits einen Riegel vorschieben: Zukünftig sollen Bundesbürger in über 50 öffentlichen Registern einheitlich unter ihrer Steuer-ID geführt werden. Doppelte Datenhaltung und komplizierte Identifikationen („Wie schreibt sich doch gleich Ihr Name?“) sollen damit der Vergangenheit angehören.

Ein kühner Traum. Und eine fragwürdige Hoffnung – ist doch ein Tippfehler in einer Nummer kaum unwahrscheinlicher als ein Fehler in der Namensangabe und dabei weit schwieriger zu entdecken; mit dem Risiko für den Betroffenen, dass die Ursache für einen solchen fehlerhaften Eintrag in einer Datenbank nicht so leicht nachvollziehbar ist.

Wirklich bedenklich aber ist der Zweck des Gesetzes selbst. Eine einheitliche Identifikation vereinfacht die Verknüpfung und Zusammenführung von Angaben aus unterschiedlichen Datensammlungen. Datenschützer nennen das „Profilbildung“: Es ist genau die Art „angereicherten Wissens“ über Menschen, vor der das Grundrecht der informationellen Selbstbestimmung den Einzelnen schützen soll. Ein ungutes Gefühl hinterlässt auch die Verwendung einer abstrakten Nummer statt des Namens für die eindeutige Identifikation einer Person. Das gab es schon einmal in Deutschland; damals war es Teil eines systematischen Prozesses der Entwürdigung und Verdinglichung von Menschen. Einen Sieg der Bürokratie über die Unordnung sollten wir auch aus diesem Grund verhindern.



Inhalt

Wehret den Anfängen

Security News

Keine Biometrie zur Zeiterfassung

Schlüsselkasten

KISS

Darf ich mal sehen?

Einwilligungs-Standards

Totgesagte leben ewig

Secorvo News

Seminarbetrieb wieder aufgenommen

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Keine Biometrie zur Zeiterfassung

Das Landesarbeitsgericht Berlin-Brandenburg hat in einem nun veröffentlichten Urteil vom 04.06.2020 die Anforderungen an den Einsatz von Biometrie im Arbeitsverhältnis konkretisiert und elektronische Fingerabdrücke bei der Zeiterfassung für nicht erforderlich und damit unzulässig erklärt.

Bereits das erstinstanzliche Gericht hatte die für den Fingerabdruckabgleich gespeicherten „Minuten" als biometrische Daten gemäß Art. 9 Abs. 1, 4 Nr. 14 DSGVO eingeordnet. Demzufolge sei nach der Eignung zunächst zu prüfen, ob kein gleich wirksames, das Persönlichkeitsrecht weniger beeinträchtigendes Mittel existiere. Trotz der vorgetragenen abstrakten Manipulationsgefahr hat das LArbG Chipkarten oder Tokensysteme als gleich wirksam angesehen und damit die Erforderlichkeit im Kontext der betrieblichen Zeiterfassung verneint. Erst wenn die Erforderlichkeit bejaht worden wäre, hätten die vorgetragenen Schutzmaßnahmen (Nichtauslesbarkeit, Pseudonymisierung u.a.) im Rahmen einer Abwägung berücksichtigt werden können.

Das Urteil konkretisiert die Prüfanforderungen an den Einsatz von biometrischen Merkmalen. Bei der Zutrittskontrolle für besonders schutzbedürfte Bereiche bspw. kann der Biometrieeinsatz weiter gerechtfertigt sein, nicht jedoch lediglich zur Vermeidung vermuteter sonstiger Manipulationsgefahren.

Schlüsselkasten

Kryptografische Schlüssel müssen zufällig gewählt werden – für Computer ist das eine Herausforderung. DiceKeys kündigte am 19.08.2020 an, endlich eine Lösung für dieses Dauerproblem gefunden zu haben: rein mechanisch – durch würfeln. Für 25 US$ wird ein spezieller Würfelsatz im Kasten geliefert. Das Ergebnis kann mit einer App abfotografiert werden, sodass man den 192-bit-Schlüssel weiterverwenden kann. Den Schlüssel schützt man, indem man den Kasten mit den Würfeln möglichst feuerfest hinterlegt. Unterhaltsam ist dies in einem Video dargestellt.

KISS

Am 02.09.2020 erlangte ein Feature der auf jedem modernen Windows-Rechner standardmäßig installierten Microsoft Malware Protection traurige Bekanntheit: Über das Programm „MpCmdRun.exe" konnten mit der Option „-DownloadFile" Dateien heruntergeladen werden. Ein Angreifer könnte dies z. B. im Rahmen eines „Living off the Land"-Angriffs (LOL) nutzen. Darunter wird der Missbrauch von auf einem System bereits vorhandenen Funktionen und Programme für bösartige Zwecke verstanden. In den vergangenen Jahren nahm die Zahl der LOL-Angriffe laut Symantec deutlich zu. Angriffe über solche „Seitentüren" sind oft einfach; auch hinterlässt ein Angreifer meist weniger Spuren, löst mit niedrigerer Wahrscheinlichkeit Alarme aus und kann über längere Zeit unentdeckt agieren. Anfang 2020 hatten die Entwickler der 49 kB großen Ragnar Locker Ransomware diese für einen LOL-Angriff genutzt, indem sie sie in einer 282 MB großen MicroXP-basierten virtuellen Maschine versteckten.

Ob und warum das Download-Feature in der Microsoft Malware Protection notwendig ist, teilte Microsoft nicht mit. Mittlerweile ist die Funktion offenbar wieder deaktiviert: So ergaben Tests von Secorvo, dass Downloadversuche verschiedenster Dateien von Microsoft Defender selbst als Angriffsversuch („Trojan:Win32/MpUtilAbuse.A") erkannt wurden. Bleibt zu hoffen, dass unnötige Features von Microsoft in Zukunft gleich weggelassen werden, anstatt sie im Nachhinein als Trojaner zu identifizieren...

Minimalismus als Grundprinzip für Container, Bibliotheken (SSN 03/2019) und (Browser-)Plugins (SSN 04/2020) hilft auch gegen LOL-Angriffe: Die Angriffsfläche wird reduziert, die Angriffsresilienz erhöht. Lassen Sie weg, was nicht unbedingt nötig ist.

Darf ich mal sehen?

Am 03.09.2020 hat die Datenschutzkonferenz (DSK) ihre neue Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen" veröffentlicht. Darin werden im Wesentlichen die 2019 vom European Data Protection Board in einer Leitlinie zusammengefassten Grundsätze übernommen. Interessant aus deutscher Sicht sind vor allem die Ausführungen zur Überwachung von Beschäftigten: Hier werden die wichtigsten rechtlichen Rahmenbedingungen erläutert, die ihre Rechtsgrundlage im BDSG haben. Enthalten ist auch eine Checkliste, die auf den ersten Blick zwar hilfreich erscheinen mag, deren Umsetzung dann aber doch entsprechende technische und rechtliche Kenntnisse erfordert. Dies ist insbesondere deshalb wichtig, weil Videoüberwachungssysteme nicht ohne Datenschutz-Folgenabschätzungen eingesetzt werden dürfen.

Wenn Sie also ein Videoüberwachungssystem installieren möchten oder bereits betreiben, sollten Sie sich dringend informieren, ob die in der Regel durchzuführende Interessenabwägung zu Ihren Gunsten ausgeht und ob die Anlage auch sonst den gesetzlichen Anforderungen entspricht.

Einwilligungs-Standards

Mit der seit dem 15.08.2020 zur Verfügung stehenden zweiten Auflage des Transparency & Consent Frameworks (TCF 2.0) hat das Interactive Advertising Bureau ein ambitioniertes Konzept für die Gestaltung datenschutzrechtlicher Einwilligungen auf Webseiten vorgelegt – und mit Google gleich einen zugkräftigen Teilnehmer gewonnen.

Das TCF legt fest, welche Informationen über die Datenverarbeitung mitgeteilt werden müssen und wie die Einwilligungen an die „Vendors" weitergeleitet werden. Dabei wird das Zusammenwirken von veröffentlichenden Seitenbetreibern, Werbetreibenden, Betreibern von Werbenetzen und Plattformen sowie Einwilligungs-Tools beschrieben (*Consent Management Platform*). Herz des Konzepts ist, wie sichergestellt werden soll, dass neben den Seitenbetreibern auch die Werbeinhaltsanbieter einen Nachweis der Nutzer-Einwilligung erhalten.

Das TCF 2.0 erweitert die „Cookie-Einwilligungen" auf im Hintergrund aktive Marketingdienstleister wie bspw. Google. Google unterstützt den Standard, setzt bei seinen Kunden die Anwendung aber bislang nicht voraus und betrachtet die eigenen Nutzungsrichtlinien als strenger.

Die Standardisierung der Informationen und deren Darstellung wäre allein bereits ein beachtlicher Erfolg angesichts der Schwierigkeiten jedes Seitenanbieters, aussagekräftige Datenschutzerklärungen zu erstellen. Allerdings betrachtet das TCF die Rolle von Seitenbetreibern, die selbst Werbenetze nutzen, und deren diesbezügliches Tracking nicht ausreichend.

Totgesagte leben ewig

Mit dem als Entwurf vorliegenden Registermodernisierungsgesetzes (RegMoG) will die Bundesregierung die Digitalisierung der öffentlichen Verwaltung voranbringen. Danach sollen über 50 Register der öffentlichen Verwaltung reformiert werden, darunter Melde-, Personenstands-, Personalausweis-, zentrales Fahrerlaubnis-, Bundeszentralregister und das Versichertenverzeichnis der Krankenkassen.

Zentrales Element des RegMoG ist die Einführung eines eindeutigen und veränderungsfesten Ordnungsmerkmals – die Steuer-ID. Dagegen hat sich am 26.08.2020 die Datenschutzkonferenz (DSK) ausgesprochen, auch gegen die Einführung einer anderen einheitlichen Identifikationsnummer für natürliche Personen in öffentlichen Registern.

Gegen die Steuer-ID spricht nach der DSK bereits deren völlige Loslösung aus ihrer steuerlichen Zweckbindung, gegen ein einheitliches Merkmal überhaupt die Gefahr der Bildung von umfassenden Persönlichkeitsprofilen. Bereits 1983 hat das Bundesverfassungsgericht im „Volkszählungsurteil" das Schaffen eines einheitlichen Personenkennzeichens als Vorstufe von Total- oder Teilabbildern der Persönlichkeit als mit der Würde des Menschen nicht vereinbar angesehen. Die DSK schlägt sektorspezifische Kennzeichen nach dem Vorbild Österreichs vor, die das Bundesinnenministerium allerdings mit Verweis auf deren Komplexität ablehnt.

Die Gesetzesbegründung beschreibt die Möglichkeiten der Profilbildung ausschließlich als Vorzüge und belegt damit bereits selbst ausführlich die absehbare Verfassungswidrigkeit.

Secorvo News

Seminarbetrieb wieder aufgenommen

Im September hat Secorvo nach sechsmonatiger Pause wieder die ersten Seminare (unter Beachtung aller Infektionsschutzauflagen) durchgeführt – sehr zur Freude aller Teilnehmer.

Im November bieten wir Ihnen zwei weitere Gelegenheiten, Ihre Kenntnisse und Kompetenzen in der IT-Sicherheit zu aktualisieren – und zu zertifizieren:

Das Grundlagen- und Vertiefungsseminar Public-Key-Infrastrukturen (PKI) (**09.–12.11.2020**) und das Zertifizierungsseminar TeleTrusT Information Security Professional – T.I.S.P. (**16.–20.11.2020**).

Zur Vorbereitung auf das T.I.S.P.-Seminar und die anschließende Prüfung erhalten Sie nach Ihrer Anmeldung unser Begleitbuch „Informationssicherheit und Datenschutz", das im vergangenen Herbst in dritter Auflage im dpunkt-Verlag erschienen ist – und sich inzwischen vieler positiver bis begeisterter Kritiken erfreut. Vielleicht suchen Sie ja auch noch nach einer Lektüre für die nun wieder längeren Herbstabende...

Ausführliche Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter

https://www.secorvo.de/seminare

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Oktober 2020	
12.-14.10.	ISSE 2020 (IEEE, Wien/A)
13.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
22.-23.10.	heise devSec 2020 (dpunkt.verlag, heise Developer, heise Security, Heidelberg)
27.-28.10.	IDACON 2020 (WEKA-Akademie, München)
November 2020	
03.-04.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
09.-13.11.	ACM CCS 2020 (ACM/SIGSAC, Orlando/US)
09.-12.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
09.-12.11.	Black Hat Europe 2020 (BlackHat, London/UK)
13.-15.11.	FIfFKon20 (FIfF, Berlin)
16.-20.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
18.-20.11.	44. DAFTA (GDD, Köln)
19.-20.11.	DeepSec 2020 (DeepSec, Wien/AT)

Fundsache

Am 25.08.2020 veröffentlichte der TeleTrusT-Arbeitskreis „Security by Design“ eine Handreichung zu Design-Prinzipien und Security-Anforderungen an digitale Produkte. Auf 15 Seiten werden wesentliche Punkte kompakt und verständlich dargestellt sowie Handlungsempfehlungen für Hersteller, Anbieter und Betreiber gegeben.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2020



Deep Fakes

Seit Jahrzehnten durchzieht eine zentrale Frage die IT-Sicherheit: Wie kann ein IT-System zuverlässig feststellen, ob eine natürliche Person, die sich am System anmeldet, tatsächlich diejenige ist, die sie zu sein behauptet? Dass Passwörter zwar die vielleicht einfachste, aber keineswegs ideale Lösung für dieses Problem sind, wissen wir seit Langem. Besser ist die Prüfung verschiedener Merkmale wie der Besitz eines Tokens (Smartcard, EC-Karte, ...) oder der Zugang zu einem E-Mail-Account bzw. einem Telefonanschluss. Auch die Analyse biometrischer Daten mittels Fingerabdruckscannern, Stimm- oder Gesichtserkennung verbreitet sich dank deren technischer Weiterentwicklung (und aller Kritik zum Trotz).

Während Authentifikationen dadurch zuverlässiger, aber auch immer (zeit-)aufwändiger werden, erzeugt die Weiterentwicklung der Verfahren zugleich ein ganz neues Problem. Denn von der Extraktion eindeutiger Erkennungsmerkmale ist der Weg zur Synthese oft nicht besonders weit. Bilder (Gesichter) und Filme (Bewegungen) lassen sich heute auf beeindruckende Weise digital nachbilden. Durch den Einsatz lernender Algorithmen wird inzwischen auch die Fälschung des gesprochenen Worts zum Kinderspiel. So lassen sich nicht nur Inhalt, Wortwahl und Satzbildung imitieren (eindrucksvoll demonstriert von „The New Yorker“ im Jahr 2017 mit einer synthetisch erzeugten Rede von Donald Trump). Mit „Voice-Cloning“-Systemen wie Replica oder Lyrebird kann man inzwischen auch das gesprochene Wort selbst täuschend echt technisch erzeugen.

Daher könnten uns in unserer immer stärker medial vermittelten Wirklichkeit, in der auch persönliche Kontakte zunehmend per Telefon, Chat oder Video gepflegt werden, schon bald die in der „analogen Welt“ bewährten Erkennungsmechanismen verloren gehen. Bevor wir glauben, dass wir einen Kommunikationspartner tatsächlich sehen oder hören, warten wir womöglich in nicht allzu ferner Zukunft lieber erstmal dessen Passworteingabe ab.



Inhalt

Deep Fakes

Security News

Microsoft und der Datenschutz

Dark Pattern

Täteropfer

Sichere Online-Wahlen?

Windows Open Source

Jäger und Sammler

Secorvo News

Rätsel lösen und Preis gewinnen

Seminarangebot 2021

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Microsoft und der Datenschutz

Heftige Kritik erntete Baden-Württemberg für seinen Plan, Microsoft Office 365 in Schulen einzuführen. Kultusministerin Eisenmann wurde dafür am 28.09.2020 mit dem Big Brother Award 2020 ausgezeichnet. Bei der Bewertung sind sich jedoch auch die Datenschutz-Aufsichtsbehörden uneins: Die Datenschutzkonferenz beschloss am 23.09.2020 mit knapper Mehrheit die vorläufige, auf Verträgen vom Januar 2020 beruhende Einschätzung, Microsoft Office 365 sei derzeit nicht datenschutzkonform einsetzbar. Darauf reagierten die Landesdatenschutzbeauftragten des Saarlandes, Hessens, Bayerns und Baden-Württembergs am 02.10.2020 mit einer abweichenden gemeinsamen Stellungnahme, nach der sie zwar im Hinblick auf das EuGH-Urteil Schrems II erhebliches Verbesserungspotenzial sehen, die Frage jedoch ohne Anhörung von Microsoft und die Berücksichtigung aktueller Vertragsanpassungen für nicht entscheidungsreif halten. Der LfDI Baden-Württemberg, Dr. Brink, kündigte am 30.10.2020 an, das Pilotprojekt des Landes zur Einführung von Microsoft Office 365 an Schulen zu begleiten.

So viel ist jedoch klar: Beim Abschluss von Microsoft-365-Verträgen sollten die folgenden Punkte unbedingt schriftlich fixiert werden:

- Daten werden nur auf Servern innerhalb der EU gespeichert.
- Microsoft ist Auftragsverarbeiter und nimmt keine Rechte in Anspruch, die zur Verantwortlichkeit des Auftraggebers zählen (wie die Kontrolle über Unterauftragsverarbeiter etc.).
- Die Konfiguration ist so zu wählen, dass Daten nur übertragen werden, wenn es (aus Sicht des Verantwortlichen) tatsächlich notwendig ist.
- Datenübermittlungen in Länder ohne geeignetes Datenschutzniveau sind nur bei Vorliegen geeigneter Garantien erlaubt – dafür genügen die Standardvertragsklauseln ohne zusätzliche Schutzmaßnahmen regelmäßig nicht.

Bei Verträgen mit US-Anbietern besteht weiterhin das bisher ungelöste Problem des Cloud Acts, der amerikanische Unternehmen verpflichtet, US-Behörden auch den Zugriff auf solche Daten zu ermöglichen, die in Rechenzentren außerhalb der USA verarbeitet werden.

Dark Pattern

Am 07.09.2020 veröffentlichte das Bundesministerium für Justiz und Verbraucherschutz die Studie „Innovatives Datenschutz-Einwilligungsmanagement“, die die Ausgestaltung, Nutzerfreundlichkeit und Rechtskonformität von Einwilligungsmanagement-Modellen und Verbesserungsmöglichkeiten bewertet. Danach zielen viele Modelle darauf ab, Verbraucherinnen und Verbraucher mittels so genannter Dark Pattern zu einer Einwilligung in Trackingmechanismen zu bewegen. Dieses Vorgehen kann strafrechtliche Relevanz besitzen: Nach § 42 Abs. 2 Nr. 2 BDSG ist mit bis zu zwei Jahren Freiheitsstrafe bedroht, wer sich personenbezogene Daten durch unrichtige Angaben erschleicht.

Unternehmen sollten daher genau prüfen, ob das auf der Webseite gewählte Verfahren zur Einwilligung Nutzern eine „echte“ Wahl lässt. Der Studie zufolge sind Nutzer durchaus bereit ihre Einwilligung zu erteilen – vorausgesetzt, sie wurden ordentlich informiert.

Täteropfer

Das US Treasury Department's Office of Foreign Assets Control (OFAC) warnte am 01.10.2020 in einem Advisory vor Zahlungen – auch durch Dritte – an Ransomware-Erpresser (SSN 06/2019) wegen möglicher Verstöße gegen Bestimmungen bestehender Handels- und Wirtschaftssanktionen. US-Bürgern sind bspw. nach dem International Emergency Economic Powers Act (IEEPA) oder dem Trading with the Enemy Act (TWEA) Zahlungen an Personen oder Institutionen untersagt, die sich auf der OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) befinden.

Entsprechende europäische Regelungen sind die EU-Verordnungen Nr. 2580/2001 und Nr. 881/2002. In Deutschland werden Verstöße nach den §§ 17 ff AWG geahndet, die auch „leichtfertiges Handeln“ einbeziehen: Eine Zahlung an den zunächst vermutlich unbekannten Erpresser kann dies erfüllen.

War ein Ransomware-Angriff erfolgreich, stehen Unternehmen (ohne aktuelles Backup) vor einem Dilemma: Die Chance auf ein schnelles, wenn auch nicht gesichertes Wiedererlangen der Daten und Unterbleiben der teilweise angedrohten Veröffentlichung (SSN 2/2020) gegen das mit einer Lösegeldzahlung verbundene Sanktionsrisiko. Lösbar erscheint dies nur durch Prävention: So hat z. B. die Cybersecurity and Infrastructure Security Agency (CISA) zusammen mit dem Multi-State Information Sharing & Analysis Center (MS-ISAC) am 30.09.2020 hierfür ein gemeinsames Dokument zum Umgang mit Ransomware veröffentlicht.

Sichere Online-Wahlen?

Am 30.09.2020 hat das BSI einen Entwurf der Technischen Richtlinie BSI TR-03162 vorgelegt, die

IT-sicherheitstechnische Anforderungen an eine Online-Wahl für Verwaltungsräte der Sozialversicherungen festlegt. Die Vorgaben sind schlüssig und definieren unter Rückgriff auf verschiedene BSI-Vorgaben wie das IT-Grundschutz-Kompendium und die IT-Grundschutz-Standards verpflichtende Anforderungen. Dabei werden die verschiedenen Phasen einer Wahl berücksichtigt und auch weitere Technische Richtlinien des BSI referenziert.

Nicht explizit betrachtet werden jedoch konkrete Anforderungen an die Absicherung von Anwendung und Anwendungskomponenten. Für das benannte Modellprojekt mag das ausreichen – die Einhaltung der für politische Online-Wahlen geltenden Wahlrechtsgrundsätze des Grundgesetzes (siehe die Ausarbeitung des Deutschen Bundestages zu Online-Wahlen vom 03.03.2014) kann die Richtlinie jedoch nicht garantieren.

Windows Open Source

Kurz vor dem 19. Geburtstag von Windows XP am 25.10.2020 postete ein anonymer Nutzer am 23.09.2020 auf 4chan unter /g/ eine Quellcode-Sammlung von Windows XP SP1, Windows Server 2003 RTM, Windows 2000 und weiteren älteren Windows-Betriebssystemen. Sie besteht aus früheren Quellcode-Leaks, die zum Teil seit Längerem in privaten Foren ausgetauscht wurden. Trotz einiger fehlender Komponenten konnten daraus funktionierende Windows-Versionen kompiliert werden.

Die mediale Aufmerksamkeit führte zu neuen Funden im Quellcode. So entdeckte ein Twitter-Nutzer die Root Signing Keys für Benutzerzertifikate in Microsofts NetMeeting. Und die für die EternalBlue-Schwachstelle (CVE-2017-0144) verantwortliche Funktion war schon zu Erscheinen von Windows XP mit einem Kommentar versehen, der vor dem gefährlichen Verhalten warnte.

Der Quellcode könnte ein gefundenes Fressen für White- und Blackhat-Hacker sein: So enthalten aktuelle Windows-Versionen zweifellos zahlreiche „alte“ Code-Fragmente oder ganze Komponenten. Der Sicherheitsforscher Tavis Ormandy demonstrierte im August 2019 sicherheitskritische Schwachstellen, die in fast allen Windows-Versionen der letzten Jahrzehnte enthalten waren. Zwar hatten zahlreiche Unternehmenskunden über Microsofts „Shared Source Initiative“ schon lange Zugriff auf den Code, aber die allgemeine Verbreitung könnte die Aufdeckung bisher versteckt gebliebener Schwachstellen kurzzeitig beflügeln.

Jäger und Sammler

Am 06.10.2020 hat der Europäische Gerichtshof zum dritten Mal zur Vorratsdatenspeicherung (diesmal in Großbritannien, Belgien und Frankreich) geurteilt. Darin bestätigt er erneut, dass eine anlasslose und undifferenzierte Speicherung von Verkehrs- und Standortdaten der Telekommunikation einen schweren Eingriff in die Grundrechte der Betroffenen darstellt. Dennoch wird die Anordnung einer Vorratsdatenspeicherung nicht vollständig ausgeschlossen; es bedarf allerdings einer tatsächlichen, gegenwärtigen oder vorhersehbaren Gefahrenlage, etwa eines unmittelbar bevorstehenden oder erfolgten Angriffs auf die nationale Sicherheit. Auch die Bekämpfung schwerer Kriminalität erfordert mindestens das Bestehen von Rechtsschutzmöglichkeiten für die Betroffenen. Die Urteile gründen auf der grundrechtskonformen Auslegung der Datenschutz-Richtlinie für elektronische Kommunikation (2002/58/EG) und legen den Spielraum für eine eventuelle Verordnung zur elektronischen Kommunikation (ePrivacy-Verordnung) fest. Ob die Regelungen der §§ 113b ff TKG dem standhalten darf bezweifelt werden: Das Urteil könnte also auch Folgen für die Rechtslage in Deutschland haben.

Secorvo News

Rätsel lösen und Preis gewinnen

Vor fünf Jahren ging „Krypto im Advent“ – eine Initiative von Secorvo in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe – mit über 1.000 Anmeldungen an den Start. Im vergangenen Jahr begeisterte der Online-Adventskalender, der Kinder und Jugendliche spielerisch an Verschlüsselungstechniken heranführt, bereits mehr als 3.500 Teilnehmer. Dabei gilt es, täglich spannende Verschlüsselungs-Rätsel zu lösen, um einen von über 200 Sachpreisen zu gewinnen.

Auch Schulklassen und Profis können miträtseln, letztere allerdings außer Konkurrenz. Anmeldungen sind ab sofort auf Krypto-im-Advent.de möglich – die Teilnahme ist wie immer kostenlos.

Seminarangebot 2021

Wir hoffen Ihnen im kommenden Jahr unsere Präsenzseminare wieder in der bekannten Qualität anbieten zu dürfen. Alle Seminarthemen, Termine und Programme finden Sie unter

https://www.secorvo.de/seminare

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2020	
03.-04.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
09.-13.11.	ACM CCS 2020 (ACM/SIGSAC, Orlando/US)
09.-12.11.	Black Hat Europe 2020 (BlackHat, London/UK)
13.-15.11.	FIfFKon20 (FIfF, Berlin)
18.-20.11.	44. DAFTA (GDD, Köln)
19.-20.11.	DeepSec 2020 (DeepSec, Wien/AT)
30.11.-01.12.	Cybersecurity 2020 (Handelsblatt/EUROFORUM, Berlin)
Februar 2021	
01.-02.02.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
02.-03.02.	17. Deutscher IT-Sicherheitskongress (BSI, virtuell)
18.-19.02.	OWASP Global AppSec (OWASP, Dublin/IRL)
22.-26.02.	T.I.S.P. TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-25.02.	secIT 2021 (Heise Medien, Hannover)

Fundsache

Am 09.10.2020 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Bericht zur Lage der IT-Sicherheit in Deutschland vorgelegt. Dabei wird die wachsende Verbreitung und Zunahme von Schadprogrammvarianten als die auch zahlenmäßig größte Bedrohung für die Informationssicherheit deutlich.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

November 2020



Unter den Wolken

Luftaufnahmen haftet etwas Magisches an. Vielleicht, weil sie aus einer Perspektive aufgenommen werden, die wir Menschen aus eigener Kraft nicht einnehmen können – es grüßt der ewige Traum vom Fliegen. Diese Faszination ist es wohl auch, die Menschen auf Türme, Berge und zu Ballonfahrten und Fallschirmsprüngen treibt.

Doch diese bislang seltenen Bilder werden selbstverständlicher: Dank leistungsstarker Servo-Motoren, verbesserter Batterie-, Funk- und Kameratechnik sowie hochwertiger GPS-, Beschleunigungs- und Gyro-Sensoren liefern mit Videokameras bestückte Drohnen heute Aufnahmen, die zuvor bestenfalls aus Hubschraubern möglich waren.

Und das weckt Begehrlichkeiten. Drohnenflüge kosten nur einen mikroskopischen Teil eines Hubschrauberflugs, können fast überall gestartet werden und liefern Bilder in Echtzeit – perfekte Voraussetzungen für eine großflächige Überwachung des öffentlichen Raums. Im April wurden in Düsseldorf Drohnen zur Überwachung der Einhaltung der Corona-Kontaktbeschränkung eingesetzt.

Mitte November brachte die Firma DJI die Kamera-Drohne „mini 2“ auf den Markt: Mit nur 239 g darf sie von jedermann geflogen werden, überträgt Full-HD-Aufnahmen über eine Distanz von bis zu 10 km und erreicht eine Fluggeschwindigkeit von über 57 km/h. Bei einer Flugdauer von bis zu 30 Minuten und einer maximalen Flughöhe von 4.000 m ist der Wirkungskreis gewaltig. Die Motoren sind schon aus wenigen Metern Entfernung nicht mehr zu hören – und die nur 14 cm lange Drohne kaum noch zu erkennen.

Die Anschaffung eines Polizeihubschraubers kostet rund 5,8 Mio. €, Betriebs- und Flugkosten sowie die Pilotenausbildung nicht gerechnet. Für diesen Betrag erhält man – ohne Preisverhandlung – rund 13.000 Mini-Drohnen: für jeden vierten Bundespolizisten eine.

Schöne neue Überwachungswelt.



Inhalt

Unter den Wolken

Security News

Vorsicht bei Gesundheits-Apps

Spurenarm Surfen

Verräterische Uploads

Github Code Scanning

Datenschutz in Videokonferenzsystemen

Hallo Admin

Secorvo News

Adventsrätsel

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Vorsicht bei Gesundheits-Apps

Neben sogenannten „Medical Apps“ aus dem Lifestyle- und Wellness-Bereich wurden am 06.10.2020 die ersten „Gesundheits-Apps“ zugelassen, die es vom Arzt auf Rezept gibt und deren Kosten von den gesetzlichen Krankenversicherungen übernommen werden. In das DiGA-Verzeichnis aufgenommen werden die Apps ohne weitere sicherheits- und datenschutzrechtliche Prüfung durch die zuständigen Behörden nach einem an die CE-Kennzeichnung angelehnten „Fast-Track“-Verfahren: Die Hersteller geben eine Erklärung ab, in der sie versichern, dass sie die gesetzlichen Vorgaben einhalten. Dieses kursorische Verfahren bewertet der Landesbeauftragte für Datenschutz und Informationsfreiheit Rheinland-Pfalz kritisch – bei den ersten angebotenen „Apps auf Rezept“ wurden bereits erhebliche Sicherheits- und Datenschutzlücken festgestellt. Eine Überprüfung durch die zuständige Aufsichtsbehörde, das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), fand erst im Nachgang statt. Wer solche Apps verschrieben bekommt oder freiwillig nutzen möchte, sollte sich zuvor genauer mit den Einstellungen beschäftigen. Blindes Vertrauen in solche Anwendungen ist jedenfalls nicht zu empfehlen.

Spurenarm Surfen

Wer im Internet „surft“ hinterlässt Spuren – unvermeidlich beim Anbieter der aufgerufenen Seite und fast immer zusätzlich bei eingebundenen Trackern, Werbeseitenanbietern, Diensten, Icons von Social Networks oder Schriftarten. Zwar dürfen IP-Adresse und Zugriffszeitpunkt nur mit Einwilligung der Betroffenen übermittelt und von den Empfängern zu eigenen Zwecken wie der Gewinnung von Werbe-Profilen genutzt werden – aber darum kümmern sich viele Anbieter wenig.

Schutz gegen solcherart unerwünschtes Tracking bieten nicht nur die Datenschutz-Grundverordnung, sondern auch Browser-Einstellungen und die Nutzung von Browser-Erweiterungen. Sie begrenzen das Tracking auf den Seitenanbieter, sperren lästige Werbeeinblendungen aus und verkürzen so, ganz nebenbei, die Ladezeiten von Webseiten merklich. Aber Achtung: Man sollte nur Browser-Erweiterungen installieren, denen man vertraut, sonst holt man sich leicht statt eines Privatsphärenschützers einen Spionagehelfer in den Browser (SSN 04/2020).

Bei den Browser-Einstellungen empfiehlt es sich, zumindest so genannte „Third-Party Cookies“ zu deaktivieren. Empfehlenswerte Browser-Erweiterungen sind beispielsweise der Privacy Badger oder HTTPS Everywhere der EFF. ClearURLs entfernt Tracking-Bestandteile aus URLs. Mit Decentraleyes werden lokale Ressourcen statt solcher von einem zentralen Content Delivery Network (CDN) injiziert. uBlock Origin blockiert nicht nur lästige Werbeeinblendungen sondern auch bösartige und gefährliche Domänen. Und wer sein Netzwerk bereits auf DNS-Ebene von einem dedizierten Gerät aus filtern möchte, dem empfiehlt sich Pi-hole. Zu guter Letzt kann man über „Cover Your Tracks“ (ehemals Panopticlick) prüfen, wie eindeutig der „Fingerprint“ des eigenen Browsers ist und was man dagegen tun kann.

Verräterische Uploads

Am 18.05.2020 berichtete die Investigativ-Journalismus-Webseite „bell¿ngcat“, wie mittels einer Bier-Bewertungs-App Militärpersonal identifiziert und vertrauliche Dokumente gefunden werden können: Manche der in Untappd hochgeladenen und mit einer Örtlichkeit (wie z. B. einer Bar) verknüpften Fotos des getrunkenen Bieres zeigen neben dem Bierglas Militärausweise, Kreditkarten und Militärdokumente. Jedes Besucher-Profil besitzt zudem eine „Timeline“ der Örtlichkeiten, an denen die Person bereits ein Foto hochgeladen hat. So konnten sogar geheime oder inoffizielle Militärbasen identifiziert und chronologische Abläufe von Reisen zwischen Militärbasen und privaten Aufenthaltsorten rekonstruiert werden.

Ähnliches erlaubt die „Heatmap“ der Fitness-App Strava: Wie Nathan Ruser bereits am 27.01.2018 erkannte, kann diese genutzt werden, um Militärbasen zu erkennen und detailliert zu kartographieren. Bereits am 08.07.2018 berichtete bell¿ngcat, wie dank der Fitness-App von Polar das Haus und die Jogging-Gewohnheiten eines hochrangigen Militäroffiziers einer Nuklearwaffenbasis herauszufinden waren – samt vollem Namen.

Auch Bewertungen auf Google Maps oder Amazon bieten Einblick in Aufenthaltsorte, Vorlieben und Gewohnheiten von Personen. Wenn diese Angaben z. B. über die Suche nach Benutzernamen, Aufenthaltsorten, Freunden, Bekannten oder Verwandten mit Daten anderer sozialer Netzwerke wie Swarm korreliert werden, ergibt sich schnell ein aussagekräftiges Gesamtbild.

Für Sammelpunkte, die Ernennung zum „Local Guide“ oder „Top Reviewer“ machen Menschen ihr Leben öffentlich und sich selbst zum freiwillig gläsernen Menschen. Beim nächsten Joggen, Biertrinken oder Bewerten sollte man vielleicht darüber nachdenken, ob man diese Spuren wirklich hinterlassen möchte.

Github Code Scanning

Nachdem Github am 18.09.2019 das Code-Analyse-Unternehmen Semmle übernommen hat, bietet Github auf Basis der CodeQL-Technologie seit dem 30.09.2020 auf Github automatisierte Code Scans an. Diese Funktionen wie Scans auf Schwachstellen im Code und den Abhängigkeiten oder auch die Suche nach hartkodierten Geheimnissen sind sowohl für Enterprise-Modelle als auch über öffentliche Repositories verfügbar. Sobald Änderungen am Code in ein Repository hochgeladen werden, können entsprechende Code Scans automatisch durchgeführt und Schwachstellen zeitnah ausfindig gemacht werden. Eine einfache Möglichkeit, Schwachstellen aufzudecken ohne in komplexe Technologien oder teure Werkzeuge investieren zu müssen. Insbesondere für finanziell häufig klamme Open-Source-Projekte ist dieses Angebot ein Mehrwert. Erste Erfahrungsberichte bestätigen das: Durch die Anpassungsmöglichkeiten an die jeweiligen Anwendungsumgebungen war es im Jenkins-Projekt möglich, sieben Schwachstellen in verschiedenen Plug-Ins zu identifizieren, die generische Code Scanner nicht finden konnten.

Datenschutz in Videokonferenzsystemen

Mit der zunehmenden Nutzung von Web- bzw. Videokonferenzen seit Beginn der Corona-Pandemie haben sich viele Datenschutzaufsichtsbehörden zu deren Zulässigkeit und zu den an diese zu stellenden Datenschutzanforderungen geäußert. Mit der neuen Orientierungshilfe der Datenschutzkonferenz (DSK) vom 23.10.2020 fassen die Aufsichtsbehörden nun (endlich) ihre Auffassung zusammen. Darin wird weiterhin von einem Auftragsverarbeitungsverhältnis zum Anbieter ausgegangen; dafür führt das Papier als neue Rolle die des „Veranstalters“ als Verantwortlichem ein. Für den Austausch von bspw. Gesundheitsdaten soll zuvor eine Einwilligung eingeholt werden, der Kommunikationskanal wird zur eigenständigen Inhaltsverarbeitung erklärt.

Mit der Checkliste zur Orientierungshilfe können Unternehmen überprüfen und dokumentieren, ob das von ihnen eingesetzte Tool den Anforderungen der Aufsichtsbehörden entspricht oder ob Nachbesserungsbedarf besteht, etwa bzgl. der vertraglichen Nutzungsgrundlagen, Betroffeneninformationen oder der technischen Einstellungen. Dabei erscheinen die Antworten auf die Checkpunkte durch die bekannten Einschätzungen der DSK bereits determiniert, sodass die Verantwortlichen lediglich zum bereits vorbestimmten Ergebnis (Unzulässigkeit) geführt werden. Die in ersten Stellungnahmen teilweise eklatanten Begründungsmängel setzen sich auch in den gemeinsamen Papieren abgeschwächt fort, daher ist der tatsächliche Nutzen leider begrenzt.

Hallo Admin

Am 10.11.2020 berichtete der Sicherheitsforscher Kevin Backhouse vom Github Security Lab, wie man mit einer einfachen Methode Administrator-Privilegien in der Desktop-Variante von Ubuntu 20.04 erlangen konnte. Hierfür leitete der Sicherheitsforscher die Datei „.pam_environment“ auf „/dev/zero“ um. Nach Änderung einer Benutzereinstellung (wie z. B. der genutzten Sprache) versucht der Hintergrunddienst „accounts-daemon“ die umgeleitete Datei einzulesen und landet in einer Endlosschleife. Danach kann der Dienst (durch ein eingebautes Sicherheits-Feature, das den Zugriff auf sensible Dateien verhindern soll) von einem normalen Benutzer zum Absturz gebracht werden.

Bei der nächsten Anmeldung wird der Benutzer dann von GNOME mit dem Dialog zur erstmaligen Einrichtung eines Administrator-Accounts begrüßt – da der Login-Manager nicht mit dem „accounts-daemon“ kommunizieren kann, nimmt er an, es gäbe keine Benutzer auf dem System.

Die Sicherheitslücke zeigt eindrucksvoll, wie sämtliche Schutzmaßnahmen sehr einfach durch das Versetzen des Systems in einen Ausnahmezustand umgangen werden konnten. Eine schöne Metapher für viele Sicherheitslücken – sind es doch oft Sonderfälle, die ausgenutzt werden können. Diese funktionieren übrigens auch beim Menschen: Versetzt man jemanden durch Zeitdruck, Androhung von Konsequenzen, Schmeicheleien o. ä. in einen Ausnahmezustand, fällt er auf Social Engineering herein.

Secorvo News

Adventsrätsel

Am 01.12.2020 startete die sechste Staffel des Adventsrätsels „Krypto im Advent“, einer Initiative von Secorvo in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe. Sie führt jährlich rund 4.000 Kinder und Jugendliche spielerisch an Verschlüsselungstechniken heran. Dabei gilt es, über 24 Tage spannende Verschlüsselungs-Rätsel zu lösen, um einen der über 250 Sachpreise zu gewinnen.

Auch Schulklassen und Profis können miträtseln, letztere allerdings außer Konkurrenz. Anmeldungen sind auch nach dem 01.12. noch möglich (Krypto-im-Advent.de); die Teilnahme ist kostenlos.

Erzählen Sie es weiter – und rätseln Sie gerne mit!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2021	
01.-02.02.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
02.-03.02.	17. Deutscher IT-Sicherheitskongress (BSI, virtuell)
18.-19.02.	OWASP Global AppSec (OWASP, Dublin/IRL)
22.-26.02.	T.I.S.P. TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-25.02.	secIT 2021 (Heise Medien, Hannover)
März 2021	
03.-04.03.	Future Security 2021 (Fraunhofer VVS, Nürnberg)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Fundsache

Europol veröffentlichte am 05.10.2020 den Bericht "Internet Organised Crime Threat Assessment" (IOCTA): aktuelle Bedrohungen durch die organisierte Kriminalität auf gut 60 Seiten. Aufgeführt werden konkrete Beispiele wie die „Versteigerung“ geraubter Daten und Schwierigkeiten, z. B. auch in Deutschland die Infrastruktur von „Bulletproofed“-Hostern zu stören. Durchaus empfehlenswert, um sich einen Überblick über die aktuelle Bedrohungslage zu verschaffen und gegebenenfalls die eigenen Schutzmaßnahmen anzupassen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Dezember 2020



Beweislastumkehr

Am 26.11.2020 hat die Datenschutzkonferenz der deutschen Aufsichtsbehörden (DSK) einen Beschluss zur Datenschutzkonformität von Windows 10 Enterprise gefasst. Das Dokument liest sich – selbst (oder gerade) für einen „in der Wolle gewaschenen" Datenschützer – äußerst befremdlich.

In aller Ausführlichkeit wird zunächst festgehalten, dass Microsoft mehrfach versichert hat, dass Windows 10 bei Konfiguration der Telemetrie-Stufe „Security" keine Telemetriedaten (Daten über das Nutzungsverhalten) an Microsoft übermittelt. Mit Bezugnahme auf eine (dem Beschluss beiliegende) BSI-Untersuchung vom Januar 2020 kommt die DSK zu dem Ergebnis, dass „Verantwortliche nicht abschließend von ihrer (...) Prüf- und Nachweispflicht für den datenschutzkonformen Einsatz von Windows 10 hinsichtlich der Übermittlung von Telemetriedaten" entlastet werden können. Dabei kommt die referenzierte BSI-Untersuchung zu dem Schluss, dass „sich keine Hinweise ergeben, dass Windows 10 Enterprise (...) Daten an Microsoft übertragen hat, die aus h. S. ein Risiko oder das Offenlegen vertrauenswürdiger Informationen darstellen. Insbesondere konnte keine Übertragung von Telemetriedaten an Microsoft beobachtet werden."

Für ihr Urteil genügte der DSK, dass eine bestimmte Verbindung „nicht im Klartext analysiert werden konnte" – mithin die Möglichkeit besteht, dass Microsoft entgegen der anderslautenden Zusicherungen darüber doch Telemetriedaten übermitteln *könnte*. Das Verdikt wirkt wie eine merkwürdige Gemengelage aus Skepsis, Vorurteilen und Unterstellungen – und wird viel Unsicherheit hervorrufen. Warum sich die Aufsichtsbehörden hier so in Stellung bringen, während zeitgleich Millionen Webseiten und Milliarden Apps offensichtlich rechtswidrig Nutzerdaten erheben und (nicht nur) in die USA übermitteln, dürfte auch Datenschützern schwer zu vermitteln sein.



Inhalt

Beweislastumkehr

Security News

Besenrein

Cookie-Einsatz im Fokus

Gefährliche Ignoranz

Neue Datenschutzklauseln

Spy in the Middle

Identifikation bei Auskunftsanfrage

Windows 10 und die Daten

Vorsatz 2021: Keine unnötigen Risiken

Veranstaltungshinweise

secorvo
security consulting

Security News

Besenrein

Am 07.07.2020 veröffentlichte The Register einen exklusiven Artikel darüber, wie Cyberkriminelle mehr als 240 Subdomänen existierender Organisationen übernehmen konnten. Ursächlich dafür waren Subdomänen mit verwaisten DNS-Einträgen, die auf zwischenzeitlich aufgegebene Azure-Ressourcen zeigten. Die Angreifer erstellten Ressourcen mit denselben Namen neu und empfingen anschließend den gesamten Datenverkehr, der für die noch im DNS hinterlegte Subdomäne bestimmt war.

Offensichtlich ist das Problem so groß, dass Microsoft am 29.09.2020 in der Netzwerksicherheitsdokumentation für Azure einen Artikel zur Verhinderung von Subdomain-Übernahmen ergänzte.

Merke: Auch in der Cloud betriebene Assets sollten einem kontrollierten Lebenszyklus unterliegen – Stichwort „Cloud Asset Management" – und am Ende „besenrein" abgeschlossen werden. Außerdem sollte man nicht davon ausgehen, dass in der Cloud betriebene Ressourcen „auto-magisch" sämtliche Konfigurationen selbst vornehmen und „einfach funktionieren". Bester Beweis dafür sind die seit Jahren immer wieder entdeckten falsch konfigurierten und damit für die ganze Welt zugänglichen AWS S3 Buckets.

Cookie-Einsatz im Fokus

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat am 25.11.2020 seinen Bericht zur Prüfung des Einsatzes von Cookies und Drittdiensten auf niedersächsischen Webseiten veröffentlicht. Die geprüften Webseiten genügten – wenig überraschend – nicht den Anforderungen der DSGVO, der Gerichte und der Aufsichtsbehörden. Häufig kommen so genannte „Consent Tools" zum Einsatz, die die Lage eher verschlimmern als verbessern: Einwilligungen werden häufig nicht wirksam eingeholt, Widerrufsmöglichkeiten fehlen ganz und die zur Verfügung gestellten Informationen zum Tracking sind mangelhaft. Dabei blieb bei der Prüfung gänzlich unbeachtet, dass es neben Cookies auch andere Tracking-Technologien gibt, an die die gleichen Anforderungen zu stellen sind.

Das Risiko, wegen unzureichender „Consent Banner" mit einem Bußgeld belegt zu werden, steigt: Europaweit häufen sich die Berichte über entsprechende Verfahren der Aufsichtsbehörden. Die Handreichung der niedersächsischen Aufsichtsbehörde gibt verständliche Hinweise, was möglich und erlaubt ist.

Gefährliche Ignoranz

Am 06.12.2020 veröffentlichte der Sicherheitsforscher Oskars Vegeris Details zu einer am 31.08.2020 an Microsoft gemeldeten kritischen Schwachstelle in Microsoft Teams. Sie konnte zur Ausführung beliebigen Codes aus der Ferne genutzt werden – plattformübergreifend. Nötig war dafür allein eine bösartige Chat-Nachricht. Die Schwachstelle war „wurmbar", d. h. es konnte Schadcode geschrieben werden, der sich selbstständig weiter verbreitet. Sie wurde Ende Oktober 2020 geschlossen – still und heimlich, da es sich bei Teams um ein sich „selbst aktualisierendes Produkt" handelt, und ohne CVE-Eintrag. Belohnt wurde der Sicherheitsforscher nicht für seinen Fund, da der Desktop-Client nicht Teil des Bug-Bounty-Programms ist – die Schwachstelle also „out of scope" war.

Ein beliebtes, aber gefährliches Vorgehen, da es die Finder kritischer Schwachstellen künftig motivieren könnte, solche Funde direkt auf dem Schwarzmarkt zu verkaufen oder zu veröffentlichen. Das sollte Microsoft eigentlich wissen: 2018 hatte die Sicherheitsforscherin „SandboxEscaper" nach einer ähnlichen Erfahrung mit Microsoft mehrere Zero-Day-Schwachstellen samt Exploit-Code auf Twitter und GitHub veröffentlicht.

Neue Datenschutzklauseln

Die Europäische Kommission hat am 13.11.2020 einen Entwurf für neue Standardvertragsklauseln, die zugehörige Angemessenheitsentscheidung und Leitlinien zur Verwendung zur öffentlichen Konsultation vorgelegt. Die Neugestaltung war bereits durch sich verändernde Übermittlungskonstellationen, vor allem aber durch das Schrems-II Urteil erforderlich geworden.

Der vorgelegte Entwurf ersetzt und vereinheitlicht die bisherigen drei Varianten der Standardvertragsklauseln. Dafür werden innerhalb der Entwurfsklauseln vier Module gebildet: Modul 1 für die Übermittlung zwischen Verantwortlichen, Modul 2 für Auftragsverarbeiter, Modul 3 für Unterbeauftragungen durch Auftragsverarbeiter und Modul 4 für die Zusammenführung von personenbezogenen Daten, die der EU-Auftragsverarbeiter erhebt, mit Daten des Verantwortlichen aus einem Drittstaat. Die anwendbaren Regelungen ergeben sich aus der anfänglichen Festlegung der Konstellation. Die Umsetzungsfrist für den Übergang zu den neuen Klauseln soll ein Jahr ab Verabschiedung betragen.

Dem Schrems-II Urteil wird durch die verankerte Pflicht zur Prüfung der Umsetzbarkeit, entsprechende Meldepflichten und Kündigungsvorbehalte Rechnung getragen. Die Erneuerung der in die Jahre

gekommenen Standardvertragsklauseln war überfällig. Ansätze zur Lösung der Problematik von zu weit gehenden oder ungenügend kontrollierten staatlichen Zugriffen (Stichwort „US CLOUD Act“) enthalten die Klausel-Entwürfe jedoch nicht.

Spy in the Middle

Am 08.12.2020 veröffentlichte Cloudflare, wie der Konzern künftig durch Einsatz von „Oblivious DNS over HTTPS“ (ODoH), einem in Kooperation mit Apple und Fastly entwickelten Protokoll, die Anonymität von Anfragen mittels DNS over HTTPS (DoH) verbessern will. DoH ermöglicht die Namensauflösung über TLS-gesicherte HTTP-Verbindungen und war wegen der Nachvollziehbarkeit des Surfverhaltens durch Cloudflare in die Kritik geraten (SSN 09/2019). Bei ODoH ist die DNS-Anfrage verschlüsselt, sodass der Proxy-Anbieter den Inhalt nicht mitlesen kann. Weder der DNS-Anbieter noch der Betreiber des Proxy-Servers kann eine Anfrage einem Nutzer zuordnen – solange der Proxy-Betreiber nicht mit dem DNS-Anbieter kooperiert.

Dass DNS dringend Sicherheits- und Privatsphären schützende Funktionen wie Verschlüsselung benötigt, steht außer Frage. Mit welcher Technologie dies erfolgen wird, ist jedoch noch offen. TLS und HTTPS liegen zwar aus konzeptioneller Sicht auf dem falschen OSI-Layer, aber eine in der Praxis getestete und weit verbreitete Technologie ist erfahrungsgemäß sicherer als die Entwicklung eines neuen Protokolls. Auch ist die großflächige Änderung der bestehenden DNS-Infrastruktur z. B. in Form von Erweiterungen wie DNSSEC in der Praxis schwierig. Ähnlich der Entwicklung von Programmierbibliotheken ist es einfacher, bei den Nutzern eine neue „Bibliothek“ (ODoH) zu installieren, als eine bestehende Infrastruktur zu ändern.

Identifikation bei Auskunftsanfrage

Das Verwaltungsgericht Berlin entschied am 31.08.2020, dass bei einem Auskunftsersuchen eine „qualifizierte Form“ der Identifikation nur dann verlangt werden kann, wenn „begründete Zweifel“ an der Identität des Antragstellers bestehen. So sehen es auch § 59 BDSG und Art. 12 Abs. 6 DSGVO vor. Dem BayObLG genügt jedoch laut Beschluss vom 18.11.2020 bei einem schriftlichen Antrag auf Auskunft nicht, dass sich der Antragsteller mit vollständigem Namen und Geburtsdatum identifiziert. Dass auch die korrekte Adresse bekannt war, wie der Schriftwechsel mit den Gerichten zeigt, half auch nicht weiter. Vor Gericht und auf hoher See – ist man in Gottes Hand.

Windows 10 und die Daten

Am 26.11.2020 hat die Datenschutzkonferenz einen Beschluss zur Datenschutzkonformität der Telemetriefunktionen von Windows 10 Enterprise gefasst. Die Bewertung geht auf eigene Laboruntersuchungen einer DSK-Arbeitsgruppe und eine Analyse des BSI vom Januar 2020 zurück.

Die Übermittlung der Telemetrie-Daten an Microsoft kann auch personenbezogene Daten zum Nutzungsverhalten beinhalten, deren Übermittlung durch das verantwortliche Unternehmen v. a. gegenüber Arbeitnehmern einer Rechtsgrundlage und bei Übermittlung in Drittstaaten gesonderter Regelungen bedarf. Die Untersuchungen kommen zu dem Ergebnis, dass die geprüften Windows-Versionen die Deaktivierung der Telemetrieübermittlung grundsätzlich ermöglichen. Die DSK sieht die Microsoft-Kunden als Verantwortliche in der Nachweispflicht bzgl. der sicheren Unterbindung von Übermittlungen. Probleme bereitet hier die Ansteuerung eines Microsoft-Endpunktes in allen Einstellungsvarianten, der möglicherweise für eine dynamische Konfiguration der Telemetrieeinstellungen verwendet werden kann. Die diesbezüglichen Zusicherungen von Microsoft werden als nicht ausreichend angesehen. Für Windows Pro und Home besteht derzeit keine Deaktivierungsmöglichkeit.

Es drängt sich die Frage auf, wie Verantwortliche auch bei vergleichbaren Anwendungen regelmäßig eigenständig über die Zusicherungen der Anbieter hinaus nachweisen sollen, dass keine derartigen Übermittlungen an die Software-Anbieter stattfinden.

Vorsatz 2021: Keine unnötigen Risiken

Meldungen wie die vom 19.11.2020 über eine Sicherheitslücke im Server-Backend der Corona-Warn-App lassen sich unterschiedlich interpretieren: Laut Projekt belegt sie, dass „der Open-Source- sowie Community-Prozess einwandfrei funktioniert“; nach der Beschreibung der Entdeckung auf GitHub war es hingegen ein Zufallsfund. Sie fiel auf, als ein Scanner auf Basis des (in SSN 11/2020 beschriebenen) GitHub-integrierten Scanners trainiert wurde. Eines jedenfalls zeigt der Fall: Selbst kritisch in der Öffentlichkeit stehende Software kann Fehler enthalten. Daher empfehlen wir für 2021 einen grundlegenden Sicherheitsmechanismus: Unnötige Risiken vermeiden! Wer sein Auto öffnen lassen möchte, indem das Auto das Handy fragt, ob der Fahrzeughalter gerade vor ihm steht – bitte. Für sicherheitsbewusste Technik-Nutzer sollte aber eine Möglichkeit bestehen, einen solchen potenziell fehlerhaften Zugangsmechanismus zu deaktivieren.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2021	
01.-04.02.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, virtuell)
02.-03.02.	17. Deutscher IT-Sicherheitskongress (BSI, virtuell)
18.-19.02.	OWASP Global AppSec (OWASP, Dublin/IRL)
22.-26.02.	T.I.S.P. TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-25.02.	secIT 2021 (Heise Medien, Hannover)
März 2021	
03.-04.03.	Future Security 2021 (Fraunhofer VVS, Nürnberg)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2021



Gretchenfrage

Die nicht unerwartete Außerkraftsetzung des Privacy Shields durch den EuGH hat eine Welle von Vertragsneugestaltungen und viel Unsicherheit ausgelöst. Darf man personenbezogene Daten noch von US-Unternehmen verarbeiten lassen? Und wenn ja: wie?

Dabei gerät zunehmend die entscheidende Frage aus dem Blick. Denn worum geht es im Kern? Wir möchten einem fremden Dritten Daten anvertrauen, für die wir verantwortlich sind – und es, Vertrag hin oder her, auch bleiben. Die von der DSGVO geforderten vertraglichen Vereinbarungen und technisch-organisatorischen Zusicherungen, die wir mit dem Verarbeiter abschließen, sind dabei nur ein Instrument, um die Vertrauenswürdigkeit des Dritten zu untermauern. Sie sollten selbstverständlich sein.

Denn jedes Vertrauen braucht Fundierung: langjährige Zusammenarbeit, eigene Inspektion (Audits), Prüfung durch anerkannte Institutionen (Zertifikate), klare Vereinbarungen und rechtliche Absicherungen. Und selbst dann ist ein wenig verbleibende Skepsis kein Fehler.

Doch vertrauensbildende Maßnahmen erfordern die tiefere Beschäftigung mit Dienst und Dienstleister – keine gute Überlebensbedingung in einer schnelllebigen Zeit. Daher mutiert unser immer blinderes Vertrauen in die IT (in Programme, in Dienste und in Dienstleister) zu Vertrauensseligkeit. Ein perfekter „Nährboden“ für Täuschung und Betrug, siehe Enron, FlowTex oder Wirecard.

Während nicht nur unsere Abhängigkeit von der IT sondern auch die von kaum noch austauschbaren Diensten wächst, schrumpft zugleich das Fundament, auf dem Zusammenarbeit immer gründen sollte: solides Vertrauen. Wer seine Risiken beherrschen will, sollte sich daher häufiger die Frage stellen: Vertraue ich diesem Dienst, dieser Software wirklich? Und wenn die Antwort kein klares „Ja“ ist, sollte man sich besser damit beschäftigen. Oder zumindest nicht verwundert die Augen aufreißen, wenn der Blindflug schief geht.



Inhalt

Gretchenfrage

Security News

Datenschutz im Homeoffice

DNSpooq

Post-Brexit-Datenschutz

Unerwünschte Anrufe

BSI-Standard zu BCM 2.0

BND im Visier

CrypTool in Java

Secorvo News

Secorvo-Seminare

Krypto-at-Home

Veranstaltungshinweise

secorvo
security consulting

Security News

Datenschutz im Homeoffice

Am 27.01.2021 trat die SARS-CoV-2-Arbeitsschutzverordnung (Corona-ArbSchV) des Bundesministeriums für Arbeit und Soziales in Kraft, befristet bis zum 15.03.2021. Nach § 2 Abs. 4 „hat der Arbeitgeber den Beschäftigten im Fall der Büroarbeit oder vergleichbaren Tätigkeiten anzubieten, diese Tätigkeiten in deren Wohnung auszuführen, wenn keine zwingenden betriebsbedingten Gründe entgegenstehen“. Homeoffice kann Telearbeit oder mobiles Arbeiten sein – in jedem Fall trägt der Arbeitgeber die datenschutzrechtliche Verantwortung. Dabei sind besondere Schutzmaßnahmen angezeigt. Die Checkliste des Bayerischen Landesamts für Datenschutzaufsicht kann dabei eine Hilfestellung sein.

Aus rechtlicher Perspektive ist die Norm problematisch, weil die Begrifflichkeiten des § 2 Abs. 4 teilweise unbestimmt sind. Was ist unter „zwingenden betriebsbedingten Gründen“ zu verstehen? Genügt es bereits, wenn im Homeoffice dem Datenschutz nicht hinreichend Rechnung getragen werden kann? Dann könnten sich fast alle Arbeitgeber auf den Ausnahmetatbestand berufen, denn eine gleichwertig sichere Infrastruktur ist zuhause selten gegeben.

DNSpooq

Ende Januar 2021 veröffentlichten Sicherheitsforscher von JSOF unter dem Namen DNSpooq sieben Schwachstellen für den DNS-Server dnsmasq, der in eingebetteten Systemen wie Routern und IoT-Geräten weit verbreitet ist. Meist übernimmt er darin die Rolle des DNS-Forwarders und leitet Namensanfragen zur Auflösung an DNS-Server weiter; die Antworten hält er in einem Cache vor. in einem Whitepaper erläutern die Forscher, wie die gefundenen Schwachstellen kombiniert werden können, um gefälschte Einträge in diesen Cache einzuschleusen. Damit tritt dieser Cache-Poisoning-Angriff in die Fußstapfen des 2008 von Dan Kaminski gezeigten Angriffs auf DNS. Die Angriffe können über das Internet, aus dem lokalen Netz oder sogar vom Browser des Opfers aus erfolgen.

Dagegen schützen würde der flächendeckende Einsatz von HSTS oder DNSSEC, die jedoch noch viel zu selten eingesetzt werden. Doch auch in der DNSSEC-Implementierung von dnsmasq entdeckten die Forscher Buffer Overflows, die es einem Angreifer ermöglichen könnten, Server aus der Ferne zu übernehmen. Von den Schwachstellen sind mehr als 40 Hersteller betroffen, von denen einige bereits aktualisierte Software zur Verfügung stellen. Doch ist zu vermuten, dass viele eingebettete Geräte verwundbar bleiben, da sie keine Updates erhalten. Schlimmstenfalls muss man die Geräte ersetzen. Wer Sicherheits-Schrott kauft, kauft oft zweimal.

Post-Brexit-Datenschutz

Am 01.01.2021 begann die Übergangsfrist von vier Monaten, innerhalb derer die Übermittlung von personenbezogenen Daten in das Vereinigte Königreich Großbritannien und Nordirland noch als Übermittlung innerhalb der EU behandelt werden darf (siehe Art. FINPROV.10A Abs. 4 b) des Handels- und Kooperationsabkommens vom 30.12.2020). Sofern weder die EU noch Großbritannien widersprechen, kann die Übergangsfrist um weitere zwei Monate verlängert werden.

Anschließend wird das Vereinigte Königreich in Bezug auf die Übermittlung von personenbezogenen Daten ein Drittland sein. Dann wird es zusätzlicher Garantien (Art. 44 ff DSGVO) für die Datenübermittlung bedürfen. Diese könnten in einem das Vereinigte Königreich betreffenden Angemessenheitsbeschluss (Art. 45 DSGVO) bestehen. Auch ohne Angemessenheitsbeschluss kann die Datenübermittlung zulässig sein, wenn ein Vertrag nach den Standardvertragsklauseln geschlossen wird. Dabei kann es allerdings erforderlich sein, dass deren effektive Einhaltung durch weitere Maßnahmen sichergestellt wird.

Unerwünschte Anrufe

Am 04.01.2021 teilte die Bundesnetzagentur mit, dass sie gegen den Betreiber eines Call-Centers ein Bußgeld in Höhe von 145.000 Euro verhängt hat. Dessen Anrufe dienten u. a. der Neukundenakquise für einen Pay-TV Anbieter. Weder Call-Center noch Auftraggeber hatten vor dem Kauf der Adressdaten geprüft, ob die angeblich erteilten Werbeeinwilligungen auch tatsächlich vorlagen. Dies ist aber im B2C-Bereich unerlässliche Voraussetzung für datenschutz- und wettbewerbsrechtlich zulässige Werbeanrufe. Auch im B2B-Bereich werden die Grenzen der mutmaßlichen Einwilligung von den Gerichten sehr eng gesteckt. Adresskauf und Auftrag entbinden den Werbetreibenden nicht von der Pflicht, die Einwilligungen nachzuweisen.

Vor einer anderen Art unerwünschter Anrufe, auch als Vishing (Voice Phishing) bezeichnet, warnte das FBI am 14.01.2021 in einer PIN (Private Industry Notification)-Warnung: Durch Anrufe über VoIP-Systeme wird versucht, ähnlich wie mit Links in Phishing-Mails, Angestellte dazu zu verleiten, Webseiten zu besuchen, auf denen Zugangsdaten abgefischt werden. Ähnliche Angriffe gibt es seit Jahren im privaten Bereich (z. B. von angeblichen Mitarbei-

tern des Microsoft-Support) – eine offenbar nach wie vor erfolgreiche Masche.

BSI-Standard zu BCM 2.0

13 Jahre nach der Veröffentlichung des IT-Grundschutz-Standards 100-4: Notfallmanagement hat das BSI am 19.01.2021 dessen grundlegende Überarbeitung als Community Draft BSI 200-4 Business Continuity Management (BCM) publiziert. Der Standard gibt auf 298 Seiten neben einer theoretischen Einordnung der verschiedenen BCM-Aspekte praktische Hilfestellung für den schrittweisen Aufbau eines BCM. Beispielsweise ist eine Abgrenzung zwischen BCM und IT-Service-Continuity-Management (ITSCM) hilfreich, um falsche Erwartungen zu vermeiden.

Ähnlich wie beim modernisierten IT-Grundschutz im Standard 200-2 werden verschiedene Ausbaustufen eines BCM vorgestellt und deren Vorteile und Grenzen beschrieben. Diese Ausbaustufen erlauben einen Einstieg mit überschaubaren Aufwänden. Vor dem Hintergrund verschärfter Anforderungen an die Notfallvorsorge ist diese aktualisierte Handreichung sehr zu begrüßen. Fazit: Lesenswert.

BND im Visier

Der Europäische Gerichtshof für Menschenrechte (EGMR) hat am 11.01.2021 eine Beschwerde der Organisation „Reporter ohne Grenzen“ und des Rechtsprofessors Niko Härting aus dem Jahr 2017 gegen die Überwachungspraktiken des Bundesnachrichtendienstes (BND) angenommen. Die Beschwerde betrifft die Befugnisse nach dem G10-Gesetz und die Frage, ob gegen die Überwachung von E-Mail, Post und Telekommunikation effektive Rechtsmittel zur Verfügung stehen.

Nun muss die Bundesregierung Stellung nehmen, inwieweit tatsächlich Nachrichten der Beschwerdeführer abgefangen wurden und ob ihnen ein effektives Rechtsmittel zur Verfügung gestanden hat, denn die vorbefassten Gerichte hatten einen direkten Nachweis der Beobachtung von den Beschwerdeführern verlangt.

Das anstehende Verfahren entbehrt nicht einer gewissen Ironie, da der EuGH in seinem Schrems-II Urteil wegen genau solcher Einblicksbefugnisse ohne adäquaten Rechtsschutz ein angemessenes Datenschutzniveau in den USA verneint und mit den geäußerten Zweifeln an dessen Herstellbarkeit mittels Standardvertragsklauseln große Rechtsunsicherheit geschaffen hat.

CrypTool in Java

Das erfolgreiche CrypTool-Projekt, das Professor Esslinger aus Siegen seit mehr als 20 Jahren mit einem Team ehrenamtlicher Mitwirkender vorantreibt, hat Ende November 2020 die Java-Version des Kryptologie-Lernprogramms publiziert. Sie ergänzt das Windows-CrypTool 2 um eine vom Betriebssystem unabhängige Version. Mit Release 2020.1 war es im März 2020 um zahlreiche Funktionen (wie zum Beispiel einem visualisierten Tutorial zur Differentiellen Kryptoanalyse) erweitert worden.

Secorvo News

Secorvo-Seminare

Trotz der erfreulicherweise sinkenden Infektionszahlen ist derzeit schwer vorhersehbar, wann wir unsere Präsenz-Seminare wieder durchführen können – noch sind Hotels und Gastronomie geschlossen. Dennoch planen wir.

Sofern auch Sie planen möchten, können Sie Ihre Seminarteilnahme gerne buchen – selbstverständlich stornieren wir Ihre Buchung kostenfrei, wenn Ihnen die Teilnahme oder uns die Durchführung des Seminars aufgrund der Pandemie-Maßnahmen nicht möglich sein sollte.

Im September 2020 konnten wir unsere Infektionsschutzmaßnahmen noch auf mehreren Seminaren erfolgreich umsetzen: Durch eine Begrenzung der maximalen Teilnehmerzahl, interne „Wegführungen“, Lüftungspausen und Desinfektionsmaßnahmen sorgen wir während der Seminare für einen wirksamen Infektionsschutz.

Krypto-at-Home

Über 4.700 Schülerinnen und Schüler sowie ältere Kryptografie-Fans tauchten im Advent 2020 in die Welt der Verschlüsselung ein: Ein erneuter Teilnahmerekord bei unserem Online-Adventskalender "Krypto im Advent".

Als Beitrag der KA-IT-Si zum Home-Schooling haben wir nun die 36 Rätsel (und Lösungen) zusammengefasst und zum Download und Nachrätseln unter www.krypto-im-advent.de bereitgestellt. Perfektes Lernmaterial – nicht nur für den Informatik-Unterricht in den siebten Klassen. Verraten Sie es gerne weiter!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2021	
02.-03.02.	17. Deutscher IT-Sicherheitskongress (BSI, virtuell)
22.-26.02.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-25.02.	secIT 2021 (Heise Medien, virtuell)
März 2021	
15.-18.03.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, virtuell)
23.-25.03.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-21.04.	Datenschutztage 2021 (FFD Forum für Datenschutz, Mainz)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
27.-30.04.	BvD Verbandstag 2021 (BvD, Berlin)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Milena Jutz, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Februar 2021



Die schlechte gute Nachricht

Der 13.05.2019 dürfte in die Annalen des Heise-Verlags eingegangen sein. An diesem Montag schlug „Emotet“ im Verlagsnetz ein und bewies, dass auch ein technisch kompetentes und sicherheitsbewusstes Unternehmen zum Opfer werden kann. Anders als die meisten Emotet-Geschädigten ging der Verlag an die Öffentlichkeit und berichtete in schonungsloser Offenheit über den Vorfall, die eigenen Fehler und seine „Lessons learned“. Was dabei deutlich wurde: Die Hacker nutzten jeden Fehler und jede noch so kleine Nachlässigkeit, um sich nach ihrem Eindringen im Netz festzusetzen.

2014 hatte „Emotet“ begonnen, seine Trojaner-Infrastruktur zu einer Art „Cloud-Service für Angreifer“ auszubauen. Mit gut gemachten Spear-Phishing-Angriffen, die aus den E-Mails anderer Opfer konstruiert wurden, und bösartigen Makros in angehängten Office-Dateien hatte sich die Gruppe Zugang zu zigtausend IT-Systemen von Privatpersonen, Unternehmen und Behörden verschafft und „vermietete“ die Zugänge an Kriminelle zur Einschleusung von Online-Banking-Malware oder Verschlüsselungstrojanern.

Am 27.01.2021 meldete das Bundeskriminalamt, das seit 2018 gegen Emotet ermittelt hatte, dass es zusammen mit Europol deren Infrastruktur „ausgehoben“ habe. Die Zerschlagung stelle „eine wesentliche Verbesserung der Cybersicherheit in Deutschland dar“. Also „Ende gut, alles gut“? Ist das wirklich so? Seit Anfang Februar wertet das BSI die auf den Emotet-Servern entdeckten Credentials aus, die die Trojaner bei ihren Opfern „eingesammelt“ hatten, und informiert die betroffenen Unternehmen. Dabei zeigt sich, dass das erfolgreiche „Einnisten“ von Emotet in tausenden Unternehmen offenbar nicht einmal bemerkt worden war – zigtausend „Schläfer“-Rechner warteten noch immer auf ihren Einsatz.

Das ist keine gute Nachricht. Denn durch das Ausschalten eines einzelnen Angreifers verbessert sich die Cybersicherheit natürlich nicht. Sondern nur durch einen wirksameren Schutz der IT-Systeme.



Inhalt

Die schlechte gute Nachricht

Security News

„Human Supply Chain” Attack

Troja-X

Rechtmäßigkeit der Verarbeitung

Grundschutz-Kompendium 2021

Verzagte Neuregelung

Selbstverständliche Best Practices

Secorvo News

PKI, T.P.S.S.E. und T.I.S.P.

Lesen bildet

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

„Human Supply Chain" Attack

Am 05.02.2021 versuchten Angreifer, in einer Wasseraufbereitungsanlage in Oldsmar (Florida) die chemische Zusammensetzung des Wassers zu verändern. Der Angriff wurde von einem Mitarbeiter erkannt, der die Mauszeigerbewegungen und eine Misstrauen erweckende Veränderung des Natriumhydroxid-Anteils bemerkte. Daraufhin setzte er diesen zurück und meldete den Vorfall. Einem Advisory des Massachusetts Department of Environmental Protection zufolge erfolgte der Angriff über einen TeamViewer-Zugang; drei Tage zuvor hatte es Datenleaks gegeben, die auch Credentials für die Wasseraufbereitungsanlage in Oldsmar enthielten.

Der Vorfall macht deutlich, wie wichtig es ist, dass kritische Industrial Control Systems nicht nur erfahrenes Personal und bspw. Intrusion-Detection-Systeme oder SIEM einsetzen, sondern auf diversitären Architekturen basieren. Eine Infrastruktur, die an verschiedenen Stellen getrennte Systeme verwendet, erlaubt es, gefälschte Werte, die (ähnlich wie bei Stuxnet) über ein kompromittiertes System eingespielt werden, auf Plausibilität zu prüfen und Abweichungen zu erkennen.

Zusätzlich empfehlen wir allen Betreibern kritischer Systeme die Beachtung gängiger Best Practices: So sollten Management-Schnittstellen nicht nach außen exponiert und Remote-Zugänge – falls überhaupt erforderlich – bestmöglich abgesichert werden. Hierzu gehört das Erzwingen starker Authentifizierungsmechanismen bspw. über eine Multi-Faktor-Authentifizierung und die strenge Kontrolle des Ursprungs der Authentifizierungs-Anfrage (Einschränkung auf IP-Bereiche und Geräte). Auch eine bedarfsabhängige Aktivierung des Remote-Zugangs verringert die Angriffsfläche. Passwörter sollten zudem nicht nur stark sein, sondern dürfen auch nicht geteilt werden, da sonst eine Zuordnung zu Benutzern und ein differenziertes Berechtigungsmanagement unmöglich sind.

Troja-X

Das 2019 gestartete europäische Projekt Gaia-X soll eine europäische Dateninfrastruktur der Zukunft entwickeln, die eine europaweite „digitale Souveränität" von Unternehmen und Geschäftsmodellen ermöglicht. Es soll sich an sieben Leitprinzipien ausrichten, zu denen insbesondere der „europäische Datenschutz" und „Offenheit und Transparenz" zählen. Bislang haben sich dem Projekt über 300 Organisationen aus ganz Europa angeschlossen.

Ob das Projekt mehr ist als politisches Marketing muss sich jedoch noch erweisen. So löste am 18.11.2020 eine Mitteilung der Nachrichtenagentur Dow Jones News über die Beteiligung des amerikanischen Big-Data-Unternehmens Palantir, der Cloud-Anbieter Microsoft, Amazon und Google sowie des chinesischen Unternehmens Huawei Diskussionen aus – sollte Gaia-X europäische Unternehmen und Behörden doch gerade von Anbietern unabhängig machen, deren Sicherheits- und Datenschutzniveau aufgrund staatlicher Eingriffsbefugnisse wie dem US-CLOUD Act in Zweifel stehen. Mit zu viel Offenheit wird aus Gaia-X jedenfalls bald ein Troja-X.

Rechtmäßigkeit der Verarbeitung

In einem am 11.01.2021 veröffentlichten Beschluss stellt das Verwaltungsgericht (VG) Wiesbaden fest, dass bei der Bearbeitung eines Löschbegehrens immer „erneut" die Rechtmäßigkeit der Datenverarbeitung nach Art. 6 DSGVO zu prüfen sei. Die ist sowohl vor Beginn einer Datenverarbeitung als auch anschließend regelmäßig zu prüfen; dasselbe gilt für die Angemessenheit der festgelegten Löschfrist.

Erreicht eine verantwortliche Stelle ein Löschbegehren, hat sie nach Auffassung des VG zunächst zu prüfen, ob die Voraussetzungen für eine rechtmäßige Datenverarbeitung noch vorliegen – und erst dann, ob diese dem Löschersuchen entgegenstehen. Anderenfalls ist die Verarbeitung ohnehin zu beenden und sind die Daten zu löschen.

Grundschutz-Kompendium 2021

Am 01.02.2021 veröffentlichte das BSI die jährliche Überarbeitung und Erweiterung des IT-Grundschutz-Kompendiums. Auf den ersten Blick überrascht der neue Baustein „INF.11 Allgemeines Fahrzeug". Da moderne Fahrzeuge eher einem Rechenzentrum mit vier Rädern ähneln, ist es jedoch sinnvoll, daran IT-Sicherheitsanforderungen zu stellen.

Nicht in diese Edition geschafft hat es der Baustein „SYS.1.2.3: Windows Server 2019", der bereits als Community Draft vorliegt. Die Verschiebung des Bausteins „APP.6 Allgemeine Software", der bisher auf anderer Ebene (CON.4) angesiedelt war, ist zu begrüßen; daraus ergeben sich Vorteile bei der Modellierung und den Soll-Ist-Vergleichen. Und der ehemalige Katalogbaustein „B 5.25 Allgemeine Anwendungen" hat nun einen Nachfolger; das hilft bei Migrationen.

Wie gewohnt sind alle im Kompendium vorgenommenen Verbesserungen systematisch in einem Änderungsdokument zusammengefasst. Das vereinfacht die Fortschreibung von IT-Sicherheitskonzepten. Fazit: Klasse.

Verzagte Neuregelung

Das Bundeskabinett beschloss am 10.02.2021 nach Eingang von 31 Stellungnahmen einen Entwurf für ein „Gesetz zur Regelung des Datenschutzes [...] in der Telekommunikation und bei Telemedien“ (TTDSG). Das Gesetz soll die bislang im Telekommunikationsgesetz (TKG) geregelten Datenschutzbestimmungen in einem Gesetz mit dem teilweise neu zu regelnden Datenschutz des Telemediengesetzes (TMG) zusammenführen. Die Anpassung des TKG setzt (verspätet) die europäische Richtlinie 2018/1972 über einen Kodex für elektronische Kommunikation vom 11.12.2018 um.

Der Entwurf enthält in § 24 eine neue Einwilligungsregelung zur Verwendung von Cookies und bereits im Endgerät gespeicherten Informationen. Die bisherigen Regelungen zum technischen und organisatorischen Datenschutz aus § 13 TMG werden teilweise gekürzt, dafür wird ein Auskunftsverfahren für Bestands- und Nutzungsdaten von Telemediendiensten umfangreich neu geregelt.

Was der Entwurf versäumt ist die Abgrenzung und Neuaufteilung der Pflichten zwischen Telekommunikations- und Telemediendiensten, für die die neuen Begriffsbestimmungen des Kodex für elektronische Kommunikation einen Ansatzpunkt bieten. So ist es beispielsweise an der Zeit, E-Mail-, Messenger- und Videokonferenzdienste als interpersonelle Kommunikationsdienste neu einzuordnen. Stattdessen kreist der Entwurf um neue Eingriffsbefugnisse und Datenschutzeinschränkungen.

Selbstverständliche Best Practices

Über Sinn und Unsinn von (immer wieder neuen) IT-Sicherheits-Checklisten kann man trefflich streiten. Das trifft auch auf die vom Bayrischen Landesdatenschutzbeauftragten bereits am 27.05.2020 veröffentlichte fünfseitige Checkliste zur „Cybersicherheit für medizinische Einrichtungen“ zu.

Sie ist eine übersichtliche Zusammenstellung geeigneter Schutzmaßnahmen. Allerdings sollte nicht der Eindruck entstehen, dass die Liste alle, nicht einmal alle wesentlichen Anforderungen abdeckt. Wie in der Einleitung angemerkt liegt der Fokus auf der Verfügbarkeit der verarbeiteten (personenbezogenen) Daten und weniger auf den in diesem Kontext mindestens ebenso wichtigen Zielen Integrität und Vertraulichkeit.

Die zahlreichen Verweise auf das IT-Grundschutz-Kompendium sind zweifellos sinnvoll, werfen aber die Frage auf, ob die Checkliste eher als „Lesehilfe“ für medizinische Einrichtungen gedacht ist, die sich die Mühe einer gründlichen Auseinandersetzung mit dem IT-Grundschutz ersparen möchten. Viele der in der Checkliste aufgeführten Punkte sind zudem simple Selbstverständlichkeiten („Empfehlung zur Vermeidung leicht zu erratender Passwörter oder Passwortbestandteile“), andere muten etwas merkwürdig an („Kenntnis der zuständigen Datenschutzaufsichtsbehörde“ – die sollte spätestens beim Lesen der Checkliste bekannt sein).

Hilfreicher erscheint die vom TeleTrusT Bundesverband IT-Sicherheit e. V. am 04.02.2021 in erweiterter Fassung (v1.8) veröffentlichte Handreichung zum „Stand der Technik in der IT-Sicherheit“ – mit 98 Seiten deutlich umfangreicher als die bayerische Checkliste, aber dafür eine umfassendere Zusammenstellung geeigneter technisch-organisatorischer Maßnahmen (TOMs).

Secorvo News

PKI, T.P.S.S.E. und T.I.S.P.

Unsere beiden Zertifizierungsseminare zum „TeleTrusT Information Security Professional“ (**03.–07.05.2021**) und zum „TeleTrusT Professional for Secure Software Engineering“ (**26.–29.04.2021**) sowie das Vertiefungsseminar zu Public-Key Infrastrukturen (**19.–22.04.2021**) hoffen wir wieder in bewährter Form und unter Einhaltung der Abstandsregelung als Präsenzveranstaltung durchführen zu können. Das Programm und die Möglichkeit zur Online-Anmeldung finden Sie auf unserer Webseite. Teilnehmer des T.I.S.P.-Seminars erhalten nach Anmeldung zur Vorbereitung das T.I.S.P.-Begleitbuch „Informationssicherheit und Datenschutz“ zugesandt.

Lesen bildet

Der Ausfall zahlreicher Abendveranstaltungen hat die Bücherkäufe ansteigen lassen. Da wollen wir Sie nicht alleine lassen und laden Sie herzlich ein zum „1. Literarischen Kabinett“ der Karlsruher IT-Sicherheitsinitiative am 25.03.2021 um 18 Uhr (Teams). Sie werden zahlreiche Werke der Weltliteratur kennenlernen, die Sicherheits- und Datenschutzexperten gelesen haben müssen. Fünf Bücher werden wir etwas ausführlicher vorstellen – und freuen uns nicht nur auf Ihre Anmeldung, sondern auch über eine persönliche Rückmeldung: Welche Bücher gehören unbedingt auf diese Liste? Und: Haben Sie Lust, Ihr eigenes Lieblingsbuch, das Sie im Hinblick auf IT-Sicherheit oder Datenschutz nachdenklich oder betroffen gemacht hat, kurz in 10 Minuten vorzustellen? Dann schreiben Sie uns.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2021	
15.-18.03.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, virtuell)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-22.04.	Datenschutztage 2021 (FFD Forum für Datenschutz, Mainz/virtuell)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Mai 2021	
03.-07.05.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
04.-07.05.	Blackhat Asia 2021 (Blackhat, virtuell)
12.05.	SecurityCruise (Connecting Media, Karlsruhe)
19.-21.05.	BvD Verbandstage 2021 (BvD, virtuell)
19.-20.05.	22. Datenschutzkongress (EUROFORUM, virtuell)

Fundsache

Datenschutz-Unterstützung für Vereine: Mit DS-GVO.clever bietet der LfDI Baden-Württemberg seit kurzem eine effiziente und effektive Hilfestellung für Vereine bei der Erstellung ihrer Datenschutzhinweise.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Milena Jutz, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

März 2021



Hoheitsverhältnisse

Allen früheren Unkenrufen zum Trotz geht Deutschland „in die Cloud“: Spätestens seit Beginn der Pandemie schmelzen die ursprünglichen Bedenken deutscher Unternehmen wie Eis in der Sonne. Zugleich werden immer mehr Dienste (nur noch) Cloud-basiert angeboten.

Womöglich liegt das Cloud-Problem auch an ganz anderer Stelle als bisher diskutiert. Sicher, man muss dem externen Hoster seiner Daten vertrauen. Aber das galt schon, als Cloud-Dienste noch „Outsourcing“ hießen. Geändert hat sich aber, dass auch die Software „gemietet“ und vom Anbieter bereitgestellt wird. Und mit dem Versprechen, immer die aktuelle Version zur Verfügung gestellt zu bekommen, verschiebt sich die Hoheit über den Einsatz neuer Funktionen vom Nutzer zum Anbieter.

Wer in den vergangenen zwölf Monaten Microsoft Teams genutzt hat, konnte die kontinuierliche Weiterentwicklung der Videokonferenz-Software live miterleben: Fast täglich ändern sich Qualität und Details, oft zum Besseren – aber Einfluss hat der Kunde („Mieter“) darauf nicht. So bietet Teams seit Kurzem eine Transkriptions-Option: Auf Mausklick wird das gesprochene Wort in Text umgesetzt und als Untertitel angezeigt. Bisher funktioniert das nur bei amerikanischem Englisch halbwegs überzeugend. Aber das sind zweifellos Kinderkrankheiten, so wie die Tatsache, dass man zwar in den Einstellungen „Mich automatisch in Besprechungsuntertiteln und Transkriptionen identifizieren“ deaktivieren kann – Teams diese Einstellung aber im Hintergrund automatisch wieder aktiviert.

Ohne Zustimmung (und sogar gegen den Willen) des „Mieters“ überträgt Microsoft also die dem Fernmeldegeheimnis unterliegenden Inhalte der Telekommunikation an eine KI in der Cloud. Das fühlt sich ein wenig so an, als ließe ein Vermieter mal eben die Schlafzimmerwand durch eine transparente Glasscheibe ersetzen. Willkommen in der schönen neuen Welt.



Inhalt

Hoheitsverhältnisse

Security News

Meldepflicht bei Schwachstellen

Datenschutzkonformes Faxen?

Vom Pinguin zum Kaiserpinguin

Wieder Videokonferenzen

Anspruch auf Negativauskunft

Streitige Bußgelder

Secorvo News

PKI-Seminar online

Heute schon gehackt?

Veranstaltungshinweise

secorvo
security consulting

Security News

Meldepflicht bei Schwachstellen

Am 05.03.2021 wies das BSI auf eine schwerwiegende Sicherheitslücke bei Microsoft Exchange hin. Anschließend äußerten sich verschiedene Datenschutzaufsichtsbehörden zu der Frage, ob die Anfälligkeit für eine solche Schwachstelle meldepflichtig ist. Zunächst ist vom Unternehmen eine Bewertung des Risikos für die (möglicherweise) Betroffenen vorzunehmen. Wird bei einer technischen Überprüfung der Systeme festgestellt, dass die Schwachstelle ausgenutzt wurde, muss – da sind sich die Aufsichtsbehörden einig – eine Meldung erfolgen. Ist keine Kompromittierung feststellbar und gibt es keine Hinweise darauf, dass ein Abfluss von personenbezogenen Daten stattgefunden hat, dann ist eine Meldung nach Art. 4 Nr. 12 DSGVO jedoch nicht zwingend.

Datenschutzkonformes Faxen?

Immer wieder wird diskutiert, ob der Versand personenbezogener Daten via Telefax datenschutzkonform ist. Am 01.03.2021 hat sich die Landesbeauftragte für Datenschutz und Informationsfreiheit von Bremen in einer Stellungnahme nun eindeutig positioniert und den Versand von Faxen als grundsätzlich datenschutzrechtlich unzulässig bewertet: Insbesondere wegen der zunehmenden Verwendung von Internet-Technologien und Computerfaxen sei der Versand nicht sicherer als eine Postkarte oder eine unverschlüsselte E-Mail.

In technischer Hinsicht „hinkt" der Vergleich jedoch erheblich. So ist heute für E-Mails – Edward Snowden sei Dank – eine Punkt-zu-Punkt-Verschlüsselung zwischen E-Mail-Servern Standard. Außerdem besteht bei Computerfaxen nicht mehr die Gefahr, dass ein Fax in allgemein zugänglichen Räumen eingeht und so von Unbefugten gelesen werden kann. Und schließlich nutzt die Faxübermittlung dieselbe Technologie wie ein Telefonat – die nach wie vor dem Telekommunikationsgeheimnis unterliegt. Insofern ist den Landesaufsichtsbehörden zuzustimmen, die hier etwas mehr Augenmaß anlegen: Es kommt darauf an, geeignete Sicherheitsmaßnahmen zu ergreifen. Dazu kann auch gehören, zu prüfen, ob es sicherere Möglichkeiten für den Versand eines Schriftstücks gibt.

Vom Pinguin zum Kaiserpinguin

Am 12.03.2021 veröffentlichten Sicherheitsforscher von GRIMM drei Schwachstellen im Linux Kernel, die kombiniert zu einer lokalen Erweiterung der Benutzerrechte (*Local Privilege Escalation*, LPE) führen können. Das Besondere an den Schwachstellen ist, dass sie seit 15 Jahren im für iSCSI und RDMA genutzen „ib_iser"-Kernelmodul stecken, das auf nicht speziell gehärteten Systemen auch von niedrig privilegierten Benutzern zur Laufzeit nachgeladen werden kann. Ein Proof of Concept Exploit ist bereits verfügbar und kann genutzt werden, um auf bestimmten Red Hat-, CentOS- und Fedora-Systemen Root-Rechte zu erlangen. Auch auf Debian- und Ubuntu-Systemen kann der Exploit funktionieren, erfordert allerdings einige Vorbedingungen wie z. B. am System angeschlossene RDMA-Hardware.

Die Schwachstelle hebelt auf vielen Linux-Systemen das Berechtigungskonzept komplett aus. Die entsprechenden Sicherheitsaktualisierungen sollten daher schnellstmöglich installiert werden. Zudem sollten weitere restriktive Maßnahmen getroffen werden, die auch ohne entsprechende Patches vor einer Ausnutzung geschützt hätten: Auch Linux-Systeme sollten so gehärtet sein, dass von einem (einfachen) Benutzer nur explizit erlaubter Code ausgeführt werden darf, beispielsweise mithilfe von grsecurity. Im konkreten Fall hätte das ein Nachladen des obskuren Kernelmoduls verhindert. Eine umfassende Überprüfung vorhandener Härtungsmaßnahmen ist z. B. mit dem freien Tool Lynis möglich.

Wieder Videokonferenzen

Die Berliner Landesdatenschutzbeauftragte hat nach den Erstauflagen von März und Juli 2020 ihre Bewertungsübersicht zu Videokonferenzangeboten im Ampelsystem am 18.02.2021 erneuert. Weiterhin stehen die Zeichen für alle größeren Anbieter auf rot. Unverändert wird die rechtliche Bewertung weitgehend auf die Vertragslage, vor allem das Vorliegen eines ausreichenden Auftragsverarbeitungsvertrages gestützt.

Damit setzt die Aufsichtsbehörde die Einstufung als Auftragsverarbeitung weiter unbegründet voraus; nur knapp wird auf künftige Änderungen durch die TKG-Novelle zur Umsetzung des Europäischen Telekommunikationskodex (siehe SSN 2/2021) eingegangen, auf das geplante TTDSG gar nicht.

Nach geltendem Recht sind Videokonferenzangebote Telemediendienste, je nach Konstellation auch schlicht Dienstleistungen. Zu begründen ist mindestens für Arbeitgeber die Übermittlung von Anmeldedaten an die Dienste. Doch Auftragsverarbeitung setzt eine weisungsgebundene Verarbeitung im Interesse und für Zwecke des Auftraggebers voraus. Da dies in vielen Fällen kaum konstruierbar ist, kann ein beanstandungsfreier AV-Vertrag kaum zustande kommen.

Unabhängig davon sind allerdings die regelmäßigen Transparenzprobleme bezüglich der Verarbeitung eine offene Flanke. Dieses Problem wird erst lösbar, wenn die Anbieter eine eigene, regulierte Stellung erhalten, die zu einer legitimen Übermittlung der Nutzungsdaten führt. Mit Geltung des aktuellen TKG-Entwurfs würden Videokonferenzdienste als „interpersonelle Kommunikationsdienste" unter das TKG und damit auch unter das neue Telekommunikationsdatenschutzrecht fallen. Dank gesetzlicher Rechtsgrundlage würde damit u. a. für Verkehrsdaten die Auftragsverarbeitung ohnehin entfallen.

Anspruch auf Negativauskunft

Am 03.02.2021 hat das AG Lehrte (Niedersachsen) entschieden, dass Betroffene nach Art. 15 Abs. 1.1. und 2. HS DSGVO das Recht haben, vom Verantwortlichen zu verlangen, dass dieser ihnen bestätigt, keine personenbezogenen Daten der Betroffenen zu verarbeiten. Kommt der Verantwortliche dem nicht nach, so hat er, wenn der Betroffene den Gerichtsweg einschlägt, die Kosten des Verfahrens zu tragen, deren Höhe sich nach dem vom Gericht festgelegten Streitwert bemisst.

Streitige Bußgelder

Nachdem bereits im November letzten Jahres mit dem Bußgeld gegen 1&1 ein hohes Bußgeld drastisch reduziert wurde, hat das LG Berlin nun mit Beschluss vom 18.02.2021 auch das Rekordbußgeld gegen die „Deutsche Wohnen SE" (15 Mio. €) aufgehoben. Noch ist das Verfahren offen, da die Staatsanwaltschaft Berlin Beschwerde eingelegt hat.

Anders als im 1&1-Fall (Verhältnismäßigkeit der Bußgeldhöhe) ist die Ursache diesmal ein rechtlich umstrittener Verfahrensfehler: Im Konflikt stehen hier Art. 83 DSGVO, der Bußgelder gegenüber den Verantwortlichen (juristischen Personen) vorsieht, und § 30 OWiG, der dafür ein Organverschulden voraussetzt. Da die Berliner Aufsichtsbehörde den Fall jedoch bereits vor Inkrafttreten der DSGVO angestoßen hatte, ist verwunderlich, dass sie diesbezüglich keine Ausführungen vorgelegt und offenbar nicht ermittelt hat. Für das Landgericht hätte sich allerdings die Frage einer Vorlage an den EuGH stellen müssen.

Zwar kann der Fall nicht als Argument für gute Erfolgschancen von Rechtsmitteln gegen hohe Datenschutz-Bußgelder herangezogen werden. Absehbar ist jedoch, auch wenn die endgültige Entscheidung noch auf sich warten lassen wird, dass die Aufsichtsbehörden künftig stärker das persönliche Verschulden von Geschäftsführungen und anderer Gesellschaftsorgane im Blick haben werden.

Secorvo News

PKI-Seminar online

Angesichts der großen Teilnahmezahlen bei unseren jüngsten Online-Events werden wir im April erstmals auch eines unserer Seminare online durchführen: Noch gibt es freie Plätze für das Seminar „Public Key Infrastrukturen – Grundlagen, Vertiefung, Realisierung„ vom **19. bis 22.04.2021** - Theorie und vertiefte Praxis mit unseren PKI-Experten. Das Seminar ist als Weiterbildung zur T.I.S.P.-Rezertifizierung anerkannt.

Das vollständige Programm und die Anmeldung finden Sie unter www.secorvo.de/seminare. Wir freuen uns auf Ihre Teilnahme!

Heute schon gehackt?

Sie wollten schon immer einmal wissen, wie „Hacking" eigentlich funktioniert? Dann tauchen Sie gemeinsam mit uns in die Welt des Server-Hackings ab! Lernen Sie auf dem nächsten **KA-IT-Si-Event** am **29.04.2021** ab 18 Uhr, wie Hacker, Sicherheitsforscher und Penetrationstester Schwachstellen finden und ausnutzen.

Fast jedes Unternehmen besitzt heutzutage eine IT-Infrastruktur, die in irgendeiner Weise mit dem Internet verbunden ist. Jede solche Anbindung kann ein Einfallstor für Angreifer darstellen. Anhand einer Live-Demonstration zeigen wir Ihnen, wie über das Internet erreichbare Systeme geprüft werden können und in welche Richtungen sich ein Penetrationstest in nachgelagerten Schritten weiter entwickeln kann. Zusätzlich werden Grenzen und Beschränkungen von Penetrationstests aufgezeigt, die dabei helfen können, das Mittel „Penetrationstest" als Sicherheitsmaßnahme besser zu verstehen und zu bewerten.

Bitte melden Sie sich **bis Freitag, 23.04.2021** für diese Veranstaltung an. Alle Teilnehmer erhalten auch diesmal wieder vorher eine kleine Überraschung per Post von uns.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, virtuell)
20.-22.04.	Datenschutztage 2021 (FFD Forum für Datenschutz, Mainz/virtuell)
Mai 2021	
03.-07.05.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
04.-07.05.	Blackhat Asia 2021 (Blackhat, virtuell)
12.05.	SecurityCruise (Connecting Media, Karlsruhe)
19.-21.05.	BvD Verbandstage 2021 (BvD, virtuell)
19.-20.05.	22. Datenschutzkongress (EUROFORUM, virtuell)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Milena Jutz, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2021



Lesen bildet.

Häufig sind es Schriftsteller, die technische und gesellschaftliche Entwicklungen lange zuvor erahnen und beschreiben; manchmal prägen sie damit den gesellschaftlichen Diskurs der Technikfolgen. Kein Wunder, werden doch die theoretischen Möglichkeiten oft erst durch eine realistische Erzählung konkret vorstellbar. Gelingt es einem Autor dabei, in seiner Geschichte – meist einer Dystopie – die zentralen Fragen aufzuwerfen, kann eine solche Erzählung mehr Grundverständnis vermitteln als hundert Vorträge.

Das gilt vielleicht ganz besonders für den Datenschutz und die Informationssicherheit, leiden beide doch unter demselben Dilemma: Je erfolgreicher der Schutz, desto abstrakter und unkonkreter die Gefahr. Aus einer Diskussion mit Datenschutz- und Datensicherheitsexperten in Süddeutschland entstand daher kürzlich die folgende, zweifellos nicht vollständige Liste von zehn belletristischen Werken, die die Bedeutung von Datenschutz und Datensicherheit in besonders beeindruckender Weise konkret werden lassen:

1. George Orwell: 1984 (1948)
2. Clifford Stoll: Das Kuckucksei / Cuckoo's Egg (1989)
3. Robert Harris: Enigma (1995)
4. John Katzenbach: Der Patient (2006)
5. Jeffery Deaver: Der Täuscher (2009)
6. Marc Elsberg: Blackout (2012)
7. Dave Eggers: Der Circle (2013)
8. Marc Elsberg: ZERO (2014)
9. Marc-Uwe Kling: Quality Land (2017)
10. Andreas Eschbach: NSA (2018)

Einige werden Ihnen zweifellos bekannt sein. Die Lektüre der anderen legen wir Ihnen wärmstens ans Herz. Und wenn Sie das nächste Mal gefragt werden, warum Datenschutz oder Datensicherheit bloß so wichtig genommen werden: Empfehlen Sie einfach – ein Buch.



Inhalt

Lesen bildet.

Security News

Urheberzensur

Warnung vor IT-Produkten

Kryptotrojaner ohne Lösegeld

TKG novelliert

Secorvo News

Enigma zum Selberdrucken

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Urheberzensur

Am 11.03.2021 hat die „Clearingstelle Urheberrecht im Internet“ (CUII) ihre Arbeit aufgenommen. Ihr gehören Urheberrechtsvertreter (wie der Börsenverein des deutschen Buchhandels oder der Verband der Filmverleiher) sowie die größten deutschen Internet-Zugangsprovider an. Ihr Ziel: Die Ahndung von Urheberrechtsverletzungen im Internet in Gestalt von DNS-Sperren durch die Provider.

Voraussetzung für die Beantragung der Sperrung einer „strukturell urheberrechtsverletzenden Webseite“ (SUW) ist, dass die Inanspruchnahme des Webseitenbetreibers durch den Rechteinhaber keine Erfolgsaussichten hat, dieser aber „zumutbare Maßnahmen“ zur Aufdeckung der Identität des Webseitenbetreibers unternommen hat.

Die Entscheidung über eine Sperrung trifft ein Prüfausschuss einstimmig, den ein „unbefangener Vorsitzender“ mit Befähigung zum Richteramt leitet. Vor der Sperrung durch die Provider wird die Einhaltung der Netzneutralitätsvorgaben (EU 2015/2120) durch die Bundesnetzagentur geprüft. Ein sechsköpfiger Steuerkreis überwacht die Arbeit der CUII und beschließt über den Verhaltenskodex, in dem Antrags- und Sperrverfahren beschrieben sind.

Diese „Notwehrmaßnahme“ der Urheberrechtsinhaber hinterlässt trotz der Selbstbeschränkung auf jährlich maximal 200 Anträge einen schalen Beigeschmack, entscheidet doch ein privates Gremium statt unabhängiger Gerichte über die Zugänglichkeit von Webseiten – und damit über die Grundrechte Dritter, wie der Verfassungsblog am 24.03.2021 kritisierte.

Auch die Rolle der Bundesnetzagentur bleibt nebulös, denn sie ist „durch Briefwechsel“ nichtöffentlich vereinbart und schließt offenbar eine inhaltliche Prüfung der Sperrempfehlung nicht ein. Ein Verfahren also, bei dem sich erst erweisen muss, ob die Trennlinie zu „sonstigen unerwünschten Webseiten“ (SUW) klar gezogen bleibt.

Warnung vor IT-Produkten

Dürfen (Datenschutz-) Aufsichtsbehörden vor dem Einsatz bestimmter IT-Produkte warnen, wenn hierzu datenschutzrechtliche Bedenken bestehen? Die Zwischenergebnisse zu dieser Frage hat der Arbeitskreis (AK) “Grundsatz der DSK zu den Rahmenbedingungen für aufsichtsbehördliche Produktwarnungen der Datenschutzkonferenz” (DSK) bereits am 09.11.2020 in einem noch abzuschließenden Gutachten vorgestellt. Dabei wird auch die Frage beleuchtet, ob sich die aufsichtsrechtliche Legitimation aus Art. 57 Abs. 1 lit. b i.V.m. Art. 58 Abs. 3 lit. b DSGVO ergibt. Das Gutachten kommt zu dem Zwischenergebnis, dass eine Warnung unter drei Voraussetzungen rechtens sei:

- Richtigkeit der Information,
- Sachlichkeit der Information und
- Berücksichtigung des Verhältnismäßigkeitsgrundsatzes (Erforderlichkeit und Angemessenheit).

Überdies bestehe die Notwendigkeit der Überprüfung einer zeitlichen Befristung der Produktwarnung, die sich insbesondere aus § 40 Lebensmittel- und Futtermittelgesetzbuch (LFGB) ergebe. Noch nicht abschließend bewertet ist die Frage, ob den betroffenen Herstellern vor Publikation die Möglichkeit einer Stellungnahme gewährt werden sollte.

Noch gibt es zahlreiche offene Fragen. So werden nicht alle Aufsichtsbehörden dieselbe Einschätzung vertreten. Und welche Bewertungsmaßstäbe und -kriterien werden zu Grunde gelegt, um Einheitlichkeit und Vergleichbarkeit zu schaffen? Diese Fragen sollen auf der nächsten Datenschutzkonferenz am 28./29.04.2021 geklärt werden.

Trotz des offensichtlichen Nutzens einer im Idealfall einheitlichen Bewertung der Aufsichtsbehörden sind grundsätzliche Bedenken angebracht. Denn an Lebensmittelwarnungen werden sehr hohe Anforderungen gestellt, die weit über die des DSK hinausgehen: So müssen „hinreichende Anhaltspunkte dafür vorliegen, dass von einem Erzeugnis eine Gefährdung für die Sicherheit und Gesundheit ausgeht oder ausgegangen ist“. Ob Anhaltspunkte für eine Gefährdung beispielsweise bei den von der Berliner LDSI inkriminierten Videokonferenz-Lösungen (SSN 3/2021) vorliegen, muss ernsthaft bezweifelt werden.

Kryptotrojaner ohne Lösegeld

Danny Palmer beschrieb am 25.03.2021 auf ZDnet, wie die Firma Spectra Logic einen Kryptotrojaner loswurde – ohne Lösegeld zu bezahlen. Zwei Dinge waren dafür erforderlich: Die Entscheidung der Geschäftsführung gegen eine Lösegeldzahlung und eine IT-Abteilung, die bis zum Umfallen Überstunden machte, um die Firma wieder „ans Laufen“ zu bringen. Nach acht Tagen waren zumindest die wichtigsten Systeme wieder betriebsbereit. Das mutet an wie ein Königsweg – doch vor dem erleichterten Aufatmen sollte man zunächst drei Fragen beantworten:

- Wie würde Ihre Geschäftsführung entscheiden – für oder gegen eine Lösegeldzahlung?

- Gibt es in Ihrer IT-Abteilung Bereitschaftsregelungen für Notfälle? Können externe Dienstleister eingebunden werden – und wenn ja: welche und wie?
- Kennen Sie Ihre kritischen Prozesse und Systeme? Wie viele Tage würden Sie voraussichtlich benötigen, um die IT für die wesentlichen Geschäftsprozesse wiederherzustellen? Ab welcher Dauer ist ein IT-Ausfall existenzbedrohend?

Wer sich auf eine Selbstmedikation im Falle eines erfolgreichen Kryptotrojaner-Angriffs vorbereiten will, sollte sich dabei an Standards wie dem BSI-Standard 200-4 orientieren – und seine Backup- und Notfall-Pläne auch üben. So realistisch wie möglich. Und sie vor allem ausdrucken, damit der Kryptotrojaner sie nicht mitverschlüsselt.

TKG novelliert

Am 22.04.2021 wurde die Novelle des Telekommunikationsgesetzes (TKG) verabschiedet. Wer gehofft hatte, dass damit Klarheit hinsichtlich der rechtlichen Behandlung von Videokonferenzen geschaffen würde, wurde enttäuscht. Aber es ist ein Trend erkennbar, der zumindest für das in Abstimmung befindliche Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) hoffen lässt. Mit den Regelungen über die sog. Universaldienste (§§ 78 ff. TKG) wird klar, dass die Ausweitung des Fernmeldegeheimnisses (§ 88 TKG) auf Anbieter von sog. Over-the-top-Diensten näher rückt.

Damit wäre die Forderung der Aufsichtsbehörden nach Auftragsverarbeitungsverträgen hinfällig: Die Verantwortlichkeit für die Sicherheit der Dienste läge bei den Dienstanbietern und nicht bei den Nutzern; zuständige Kontrollinstanz wäre die Bundesnetzagentur. Diese Entwicklung ist aus unserer Sicht dringend geboten und wird bereits seit langem gefordert (siehe z. B. das ZEW-Gutachten von Prof. Thomas Fetzer, Universität Mannheim, aus dem Jahr 2016).

Secorvo News

Enigma zum Selberdrucken

Die ENIGMA zählt zweifellos zu den faszinierendsten Verschlüsselungsverfahren in der Geschichte der Kryptografie. Berühmt wurde sie nicht nur durch ihre bedeutende Rolle im Zweiten Weltkrieg, sondern vor allem auch durch ihre geniale Entschlüsselung unter Mitwirkung des Informatik-Pioniers Alan Turing.



Enigma I aus dem 3D-Drucker (Foto: Prof. Wiest)

Seit 2017 rekonstruieren Studierende der Hochschule der Medien in Stuttgart im Projekt „ENIGMA R.D.E." diese berühmteste Chiffriermaschine der Welt, von der nur wenige Originalgeräte erhalten sind, im 3D-Druckverfahren. Ziel ist eine Konstruktionsanleitung, mit der Laien für unter 300 € Materialkosten ein funktionierendes Gerät in Originalmaßen anfertigen können. Das Projekt wurde 2019 mit dem Landeslehrpreis des Ministeriums für Wissenschaft, Forschung und Kunst Baden-Württemberg ausgezeichnet.

Die Veröffentlichung der Anleitung ist für den Spätsommer 2021 geplant. Bei unserem kommenden KA-IT-Si-Event am **20.05.2021** dürfen Sie bereits einen Blick auf ein funktionierendes Modell werfen: Prof. Wiest wird von der bewegten Geschichte des Projekts berichten, gibt Einblicke in die Besonderheiten des Nachbaus und entschlüsselt selbstverständlich auch live Geheimbotschaften mit seiner ENIGMA.

Diesmal erhalten Sie kurz vor dem Event nicht nur eine kleine Stärkung per Post von uns, sondern auch Ihre ganz persönliche Enigma, damit Sie die Nachricht des Referenten entschlüsseln können. Lassen Sie sich überraschen! Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen – nach den überwältigenden Teilnehmerzahlen der letzten Events auch diesmal online – und kostenlos (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2021	
04.-07.05.	Blackhat Asia 2021 (Blackhat, virtuell)
17.-20.05.	Security Cruise (Connecting Media, virtuell)
19.-21.05.	BvD Verbandstage 2021 (BvD, virtuell)
19.-20.05.	22. Datenschutzkongress (EUROFORUM, virtuell)
20.05.	Enigma zum Selberdrucken (KA-IT-Si, virtuell)
Juni 2021	
08.06.	Datenschutztag 2021 (COMPUTAS, Berlin)>
09.-11.06.	Entwicklertag 2021 (VKSI, GI, ObjektForum , virtuell)
14.-15.06.	DuD 2021 (COMPUTAS, Berlin)
17.-18.06.	Annual Privacy Forum 2021 (ENISA, DG Connect, Católica University of Portugal, virtuell)

Fundsache

Neben Kali Linux gibt es weitere Linux-Distributionen, die einen umfassenden Werkzeugkasten für Penetrationstester bieten, wie beispielsweise BlackArch und Parrot OS. Von letzterer erschien am 28.03.2021 Version 4.11. Zu den Änderungen zählen sowohl eine Vielzahl aktualisierter und besser kurierter Hacking-Werkzeuge als auch der Umstieg auf eine LTS-Version. Auch ARM-Architekturen werden wieder unterstützt. Wer in der Vergangenheit Schwierigkeiten mit Kali hatte, dem sei Parrot OS ans Herz gelegt – unseren Erfahrungen nach ist Parrot OS an einigen Stellen gepflegter, zuverlässiger und stabiler.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Mai 2021



Zweck verfehlt

Am vergangenen Samstag erhielt ich im Zusammenhang mit einer Erbschaftsangelegenheit ein Schreiben von einem Finanzinstitut, bei dem ich bisher kein Kunde war. Betreff: „Datenschutzhinweise“. Sie ahnen, was beilag: Fünf eng bedruckte Seiten „zur Kenntnisnahme und für Ihre Unterlagen“. Immerhin nur fünf, dachte ich fast erleichtert.

Ähnliche Schreiben wurden seit Inkrafttreten der DSGVO millionenfach versandt. Sie dienen der Erfüllung der Informationspflicht aus Art. 13 DSGVO: Danach müssen Betroffene zu Beginn einer Verarbeitung erfahren, welche personenbezogenen Daten zu welchen Zwecken verarbeitet werden.

Ein wichtiges Prinzip des Datenschutzes: Transparenz. Nur: In dieser Umsetzung degeneriert es zur Farce, zu einer gigantischen Vergeudung von Ressourcen – denn gelesen werden solche Seiten wohl von den wenigsten Empfängern. Das sehen offenbar auch die Absender so: Das Schreiben beginnt mit den Worten „… aufgrund rechtlicher Bestimmungen der Datenschutz-Grundverordnung erhalten Sie …“. Nicht etwa: „… mit diesem Schreiben möchten wir Sie über die Verarbeitung Ihrer folgenden personenbezogenen Daten informieren.“ Oder gar: „… für die Abwicklung unseres Vertrags müssen wir personenbezogene Daten von Ihnen verarbeiten. Der folgenden tabellarischen Übersicht können Sie entnehmen, zu welchen Zwecken wir welche Angaben erheben – und wann wir sie löschen.“

Darüber hätte ich mich tatsächlich gefreut: Eine übersichtliche Darstellung auf einer Seite, der ich auf einen Blick entnehmen kann, welche Daten konkret erfasst werden – und wann sie wieder aus den Systemen verschwinden. Stattdessen: Reichlich allgemeine Formulierungen über mögliche Verarbeitungen, die dem Art. 13 formal genügen mögen – mich aber weitgehend im Unklaren darüber lassen, welche Daten denn nun konkret von mir verarbeitet werden.

Aber vielleicht weiß das ja auch dort niemand so ganz genau.



Inhalt

Zweck verfehlt

Security News

Fragmentation meets Exploitation

IT-Sicherheitsgesetz 2.0

Auslegungssache

IT-Grundschutz-Kompendium

Volatility v3

Secorvo News

Live Hacking – Grundlagen von Pentests

KA-IT-Si für alle

12. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Fragmentation meets Exploitation

Am 11.05.2021 veröffentlichte das Team um den Sicherheitsforscher Mathy Vanhoef (bekannt von den KRACK- oder Dragonblood-Angriffen) mit FragAttacks eine neue Gruppe von Schwachstellen in Wi-Fi-Netzen. Bei den neuen Schwachstellen handelt es sich um drei Design- sowie diverse Implementierungsfehler. Betroffen sind allen relevanten Wi-Fi-Standards (u. a. WPA2 und WPA3) sowie Geräte zahlreicher Hersteller.

Die Design-Schwachstellen sind schwierig auszunutzen, da sie u. a. die Mitwirkung des Benutzers voraussetzen. Die Lücken in den Implementierungen sind vom praktischen Standpunkt aus schwerwiegender: Sie sind leichter ausnutzbar und erlauben es, Systeme in internen Netzen anzugreifen, ohne die Verschlüsselung brechen zu müssen. Hierzu bedienen sich die Forscher fragmentierter Authentisierungspakete. Der fehlerfreie Umgang mit fragmentierten Daten ist ein komplexes Problem und verursacht immer wieder Schwachpunkte in Kommunikationsprotokollen.

In einem neunmonatigen Disclosure-Prozess wurden die Schwachstellen an die Hersteller kommuniziert. Die meisten Hersteller sind derzeit noch mit der Behebung der Schwachstellen beschäftigt, wobei in vielen Fällen Updates der Firmware notwendig sind. Einzelne Hersteller haben bereits Patches veröffentlicht.

Wer die Angriffe nachvollziehen und eigene Geräte auf Verwundbarkeit testen will, findet entsprechende Tools auf Github. Sofern für eingesetzte Komponenten noch keine Patches verfügbar sind, sollte – bspw. unter Berücksichtigung der Funkausleuchtung – die Relevanz für die eigene Organisation geprüft und entschieden werden, wie man mit der Schwachstelle umgeht. Eine Vorstellung weiterer Details zu den Angriffen ist auf der Konferenz Black Hat USA zu erwarten.

IT-Sicherheitsgesetz 2.0

Am 07.05.2021 hat der Bundesrat den Gesetzesentwurf des Bundestages zur Überarbeitung des IT-Sicherheitsgesetzes angenommen. Nach Veröffentlichung im Bundesgesetzblatt wird das Gesetz aller Kritik zum Trotze in Kraft treten. Neben einigen gravierenden, das BSI betreffenden Änderungen gibt es nun größeren Handlungsbedarf bei den Betreibern Kritischer Infrastrukturen. So werden die Einführung von „Systemen zur Angriffserkennung“ sowie detailliertere Meldungen zur Pflicht und die „Siedlungsabfallentsorgung“ zu einem neuen Sektor der Kritischen Infrastrukturen.

Um in dem Paragrafendschungel den Überblick zu behalten empfehlen wir einen Blick in die Plattform OpenKRITIS, die neben anderem eine gute Übersicht über die Änderungen anbietet.

Auslegungssache

Ist die Übermittlung personenbezogener Daten in Drittstaaten zulässig, wenn die Betroffenen informiert eingewilligt haben oder die Übermittlung zur Erfüllung eines Vertrags erforderlich ist? Art. 49 DSGVO sieht solche Ausnahmetatbestände vor, die jedoch von den Aufsichtsbehörden mit Verweis auf eine Leitlinie des Europäischen Datenschutzausschusses (EDSA) vom 25.05.2018 bislang sehr restriktiv ausgelegt werden.

Im Zweifel ist jedoch immer der Wortlaut des Gesetzes maßgeblich. So sind nach Prof. Thomas von Danwitz, Richter am Europäischen Gerichtshof (EuGH) und Berichterstatter für das „Schrems-II“-Urteil, die Ausnahmeregelungen des Art. 49 DSGVO „noch nicht hinreichend ausgelotet“ (siehe seine Stellungnahme auf dem Europäischen Datenschutztag vom 28.01.2021).

Damit ist Art. 49 DSGVO jedoch kein „Freibrief“ für jede Datenübermittlung: Für jeden Fall, in dem weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien bestehen, ist die Erforderlichkeit zu prüfen – beispielsweise also, ob keine Dienstleister aus der EU die Verarbeitung übernehmen können.

IT-Grundschutz-Kompendium

Das BSI verkündete am 19.05.2021 im IT-Grundschutz-Newsletter die Veröffentlichung weiterer Umsetzungshinweise zur Edition 2021 des IT-Grundschutz-Kompendiums. Darin wird aufgezeigt, wie die Anforderungen aus dem jeweiligen IT-Grundschutz-Baustein des Kompendiums erfüllt werden können.

Die Ergänzungen betreffen insbesondere die Schicht "IND" (Industrielle IT): IND.1 Prozessleit- und Automatisierungstechnik, IND.2.1 Allgemeine ICS-Komponente, IND.2.2 Speicherprogrammierbare Steuerung (SPS), IND.2.4 Maschine und IND.2.7 Safety Instrumented Systems.

Für die praktische Umsetzung der Bausteine wird die Lektüre der Hinweise wärmstens empfohlen.

Volatility v3

Bereits am 01.02.2021 wurde Volatility, das Standardwerkzeug für die forensische Hauptspeicheranalyse, nach einer eineinhalbjährigen Betaphase in einer stabilen Version 3 (Release V3-1.0.1) auf

GitHub veröffentlicht. In den seither vergangenen Monaten wurden weitere Fehler behoben und die Stabilität der neuen Funktionen verbessert.

Die Grundausstattung an Plugins ist im Vergleich mit der bisherigen Version V2.6.1 allerdings noch deutlich reduziert. So unterstützt Volatility V2.61 allein für Windows 113 Plugins, das Release V3-1.0.1 umfasst lediglich 44. Dennoch empfiehlt sich der Einsatz der neuen Version: Mit der Umstellung auf Python 3 wurden parallele Threads eingeführt, wodurch bisher sehr zeitintensive Plugins wie z. B. „strings" (Mapping von Strings auf Speicheradressen) oder „yarascan" (Prüfung des Hauptspeichers mit YARA-Regeln) wesentlich schneller abgearbeitet werden. Das ersparte z. B. bei der Untersuchung 64-GB-großer Hauptspeicherabzüge von MS Exchange im Kontext des APT-HAFNIUM-Angriffs im März 2021 z. T. mehrstündige Laufzeiten – bei einem akuten, kritischen Angriff ein echter Gewinn für die Verteidiger in den Unternehmen.

Eine weitere wichtige Funktion ist die automatisierte Unterstützung der Generierung spezifischer Windows-Profiles, die sich häufig nach NTOS-Kernel-Subversion unterscheiden. Bisher konnten lediglich Fachleute neue Profile erstellen.

Secorvo News

Live Hacking – Grundlagen von Pentests

Online-Formate können lebendige Seminare mit direktem Erfahrungsaustausch nur begrenzt ersetzen. Dafür haben sie große Stärken bei Demonstrationen und praktischen Übungen: Da bieten sie ein unmittelbareres Erleben und die Möglichkeit zum Training am gewohnten eigenen System.

Der große Erfolg einer Abendveranstaltung zum gleichen Thema im April hat uns daher motiviert, ein Ein-Tages-Online-Mitmach-Seminar für Sie zu entwickeln: In unserem „Live-Hacking-Lab" weisen unsere Penetrationstest-Experten Sie in die Grundlagen der Schwachstellensuche ein. Dabei führen Sie unter unserer Anleitung an realitätsnah konfigurierten, verwundbaren Laborsystemen gängige Methoden zur Identifikation von Schwachstellen praktisch durch – ganz bequem an Ihrem eigenen Arbeitsplatz.

Neben diesem Einblick in die Praxis des „Ethical Hackings" zeigen wir Ihnen die Möglichkeiten und Grenzen von Penetrationstests. Das Schulungskonzept spiegelt die langjährige Erfahrung der Referenten wider – von Praktikern für Praktiker.

Das Seminar bieten wir an am **23.06.2021** und am **14.07.2021**. Programm und Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

KA-IT-Si für alle

Erstmals haben wir in diesem Jahr Veranstaltungen der Karlsruher-IT-Sicherheitsinitiative (KA-IT-Si) in einem Online-Format durchgeführt. Die Resonanz war überwältigend: Mehr als 650 Datenschutz- und Datensicherheitsexperten haben an den bisherigen vier Abendveranstaltungen teilgenommen.

Auch wenn wir so bald wie möglich zu unseren Präsenzveranstaltungen mit lebendigem Buffett-Networking zurückkehren werden: Wir wollen auch zukünftig eine Möglichkeit zur „virtuellen" Teilnahme bieten, nicht zuletzt um die Veranstaltungen bundesweit „besuchbar" zu machen. Wenn Sie interessiert sind, freuen wir uns, wenn Sie sich in den Einladungsverteiler eintragen.

12. Tag der IT-Sicherheit

Auch der jährliche "Karlsruher Tag der IT-Sicherheit", eine Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V., wird in diesem Jahr als virtuelle Veranstaltung stattfinden, verteilt auf drei Abende. Den Einstieg bildet jeweils ein kurzer Blick in die Forschungs- und Gründerszene der Informationssicherheit, gefolgt von einem vertiefenden Fachvortrag:

1. Abend – Donnerstag, **01.07.2021**, 18 Uhr

10 Jahre Kompetenzzentrum KASTEL – ein Ausblick auf die IT-Sicherheit der Zukunft.
Prof. Dr. Jörn Müller-Quade (KIT)

Aus der Sicht eines Hackers. *Tim Schmidt (KIT)*

2. Abend – Donnerstag, **08.07.2021**, 18 Uhr

Einfach.Sicher.Machen. Transferstelle IT-Sicherheit im Mittelstand. *Stephanie Ziegler (KIS)*

Modernes DNS: Datenschutz mit Nebenwirkungen.
Prof. Dr. Rainer W. Gerling

3. Abend – Donnerstag, **15.07.2021**, 18 Uhr

Elevator Pitch: StartUps IT-Security.
Jun.-Prof. Dr. Christian Wressnegger (Poison Ivy) und *Mirko Ross (asvin)*

Cookies, Tracking, Analysen.
Friederike Schellhas-Mende (Secorvo)

Im Anschluss an die Vorträge bieten wir die Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit den Referenten und anderen Teilnehmern. Wir freuen uns auf drei kurzweilige und interessante Abende mit Ihnen! (Anmeldung)

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2021	
08.06.	Datenschutztag 2021 (COMPUTAS, Berlin)
09.-11.06.	Entwicklertag 2021 (VKSI, GI, ObjektForum , virtuell)
14.-15.06.	DuD 2021 (COMPUTAS, Berlin)
17.-18.06.	Annual Privacy Forum 2021 (ENISA, DG Connect, Católica University of Portugal, virtuell)
23.06.	Live Hacking Lab – Grundlagen Penetrationstest (Secorvo, virtuell)
Juli 2021	
01.07.	12. Tag der IT-Sicherheit, 1. Abend (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
08.07.	12. Tag der IT-Sicherheit, 2. Abend
12.-14.07.	PETS 2021 (University of Minnesota, virtuell)
12.-16.07.	DFRWS USA 2021 (DFRWS, virtuell)
14.07.	Live Hacking Lab – Grundlagen Penetrationstest (Secorvo, virtuell)
15.07.	12. Tag der IT-Sicherheit, 3. Abend
31.07.-05.08.	Blackhat USA 2021 (Blackhat, Las Vegas/US)

Fundsache

Am 15.04.2021 veröffentlichte der LfDI Baden-Württemberg ein Video zum Löschen von Daten samt Musterverzeichnis von Verarbeitungstätigkeiten mit integriertem Löschkonzept. Ein guter Einstieg.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2021



Erpressbar

Ransomware-Angriffe, bei denen die Daten der Opfer verschlüsselt und erst nach Zahlung eines Lösegelds wieder zur Entschlüsselung freigegeben werden, sind in den vergangenen Monaten zu einem beachtlichen Unternehmensrisiko herangewachsen. So hat nicht nur die Zahl der Angriffe, sondern auch die Höhe der Lösegeldforderungen erheblich zugenommen.

Seit etwa zehn Jahren sind Ransomware-Angriffe verbreitet. Da die Angreifer häufig genug Lösegeldzahlungen von den betroffenen Unternehmen erhalten, sind die Angriffe nicht nur finanziell sehr attraktiv, sondern werden auch erhebliche Summen in die Weiterentwicklung der Angriffssoftware investiert.

Die von einem Angriff betroffenen Unternehmen und Institutionen sind dabei allerdings nicht nur Opfer eigener Versäumnisse wie unzureichender Schutzmaßnahmen, fehlender Updates oder lückenhafter Backup- und Notfall-Konzepte, sondern auch der Schwachstellen in erworbener Software: Gäbe es diese Lücken nicht, wären Ransomware-Angriffe vergleichsweise selten erfolgreich.

Dennoch sind Schadensersatzforderungen an diese „Mitverursacher" schwierig, denn die Angreifer verwischen ihre Spuren: Meist ist nicht oder nur mit sehr viel forensischem Aufwand feststellbar, auf welchem Weg das Eindringen in die Systeme gelungen ist. Kein Wunder, wollen die Täter ihr technisches Vorgehen doch noch bei weiteren Opfern erfolgreich praktizieren – und obendrein die von ihnen entwickelte Angriffssoftware vor „Piraterie" schützen.

Damit bleibt Unternehmen und Behörden nur eines: Sich darauf einzustellen, dass – allen Schutzmaßnahmen zum Trotz – ein Ransomware-Angriff passieren kann. Und dafür zu sorgen, dass Angriffe schnell erkannt werden, Backups nicht verschlüsselt werden und ein Neuaufsetzen der Infrastruktur in kurzer Zeit gelingt. Diesen Weg sollte nur scheuen, wer über ausreichend Rücklagen verfügt.



Inhalt

Erpressbar

Security News

Konzertierte Aktion

Parallel-Welten-Netze

Alles auf Anfang

Zoom-Benchmark

Bann für Banner

E-Privacy-Richtlinie umgesetzt

Secorvo News

Teamverstärkung

Secorvo Seminare

12. Tag der IT-Sicherheit

Veranstaltungshinweise

secorvo
security consulting

Security News

Konzertierte Aktion

Die deutschen Datenschutz-Aufsichtsbehörden haben am 02.06.2021 die Durchführung einer koordinierten Prüfung internationaler Datentransfers personenbezogener Daten angekündigt. Damit soll den Anforderungen des Europäischen Gerichtshofs aus seiner Schrems-II-Entscheidung vom 16.07.2020 zur Durchsetzung verholfen werden: So dürfen weder das „Privacy Shield" noch die Standardvertragsklauseln ohne „wirksame zusätzliche Maßnahmen" als Rechtsgrundlage herangezogen werden.

Dazu werden ausgewählte Unternehmen zunächst mit abgestimmten Fragebögen zu Bewerberportalen, konzerninternem Datenverkehr und Tracking angeschrieben; außerdem stehen Mailhoster und Webhoster auf der Liste der Aufsichtsbehörden. Auch wenn zunächst nur ein (geringer) Teil der rund 3,3 Mio. deutschen Unternehmen angeschrieben werden wird, lohnt ein Blick in die Fragebögen, die u. a. von der Webseite des virtuellen Datenschutzbüros abgerufen werden können: Sie zeigen, welche Prüfpunkte im Fokus der Aufsichtsbehörden stehen.

Parallel-Welten-Netze

Seit einiger Zeit werden über "LoRaWAN" (Long Range Wide Area Network) IoT-Geräte über Funkverbindungen mit kleiner Reichweite zu Weitverkehrsnetzen mit geringer Bandbreite zusammengeschlossen. Am 08.06.2021 aktivierte Amazon USA ein bereits 2019 angekündigtes neues Feature von Amazon-Echo- und -Ring-Geräten, das diese LoRaWAN-Technik in Kombination mit BLE (Bluetooth Low Energy) nutzt: Bei schlechter Verbindung zum eigenen WLAN verbinden sich Amazon-Geräte via Amazon Sidewalk nun automatisch mit anderen Amazon-Geräten in der Umgebung, um eine Netzverbindung zu erhalten. Konkret redet der eigene Amazon-Lautsprecher oder die Ring-Kamera dann nicht mehr mit dem gerade schlecht verfügbaren WLAN-Router, sondern z. B. mit dem Echo-Gerät des Nachbarn. Dieses fungiert als „Bridge" zum Internet und stellt dafür 80 kbit/s seiner Bandbreite zur Verfügung.

Ähnliche Ansätze gab es bereits in der Vergangenheit mit Hotspots einiger ISPs. Dabei stellten private Router zusätzlich ein Gastnetzwerk zur Verfügung, über das andere Kunden desselben Providers Zugriff zum Internet erhielten. Der große Unterschied liegt allerdings darin, dass derartige Hotspots durch ein dediziertes Netzwerk-Gerät aufgespannt werden (Router), das über entsprechend segmentierende Sicherheitsfunktionen dafür sorgt, dass die Nutzer des Hotspots den eigenen Geräten nichts anhaben können.

Ob sich Lautsprecher und Kameras als Netzwerk-Barrieren eignen, sollte trotz ggf. sogar guter Spezifikation gründlich getestet werden. Und selbst dann stellt die reine Bereitstellung der Schnittstelle einen neuen Angriffsweg dar. Sobald die Funktion auch in Deutschland aktiviert wird, sollte man daher entscheiden, ob man Pioniernutzer dieser neuen Lösungen sein möchte – oder die Option in der Konfiguration lieber deaktivieren.

Alles auf Anfang

Von der Europäischen Kommission wurden am 04.06.2021 neue Standardvertragsklauseln für die DSGVO-konforme vertragliche Regelung des internationalen Austauschs personenbezogener Daten beschlossen und vom Europäischen Parlament verabschiedet. Darin wurde der durch die Cookies-II-Rechtsprechung entstandene Änderungsbedarf berücksichtigt.

Auch wenn die bisher gültigen Standardvertragsklauseln noch bis Ende September 2021 abgeschlossen werden können, ist es wichtig zu wissen, dass diese nur noch bis Ende Dezember 2022 verwendet werden dürfen. Bis dahin müssen sämtliche Verträge auf die neuen Standardvertragsklauseln umgestellt sein.

Zoom-Benchmark

Das Center for Internet Security (CIS) ist bekannt für Hardening Guides/Benchmarks zu Betriebssystemen, Webservern oder Datenbanken. Inzwischen gibt es auch Guides für Anwendungen und Cloud-Lösungen wie Zoom oder Azure – denn auch Cloud-Dienste sollte man restriktiv konfigurieren. Die Benchmarks sind in der Regel recht ausführlich und unterscheiden die Anforderungen u. a. nach Level 1 und Level 2. Einstellungen des Level 1 sollten in den meisten Fällen problemlos umsetzbar sein; bei Level 2 ist ggf. je Einstellung im Einzelfall eine Prüfung erforderlich.

Zur automatisierten Prüfung werden vom CIS mit Kosten verbundene Werkzeuge bereit gestellt: für den regelmäßigen Einsatz und wiederholte Compliance-Prüfungen eine gute Lösung. Testen kann man dies bspw. für Zoom über Test-Skripte, die Ende Mai 2021 auf Github zur Verfügung gestellt wurden.

Bann für Banner

Am 31.05.2021 hat die Stiftung noyb (my privacy is None of YOur Business) von Datenschutzaktivist Max Schrems den Cookie-Bannern pressewirksam den Kampf angesagt. Allen Cookie-Bannern? Nein,

nur solchen, die genervten Nutzern nicht die richtigen Auswahlmöglichkeiten lassen. noyb will über 500 Unternehmen anschreiben, bei denen nicht rechtmäßige Cookie-Banner festgestellt wurden, und droht mit einer Datenschutzbeschwerde bei der zuständigen Aufsichtsbehörde.

Da Webseiten nur selten korrekte Cookie-Banner verwenden, könnte eine beträchtliche Anzahl von weiteren Beschwerden die (von Schrems sicher erhoffte) Folge sein. In der Regel werden mindestens die Anforderungen an den Widerspruch für erteilte Einwilligungen (genauso einfach wie die Erteilung) gar nicht oder nicht korrekt umgesetzt.

Dabei kann man in den Leitlinien des European Data Protection Board nachlesen, wie es richtig geht. Großen Nachbesserungsbedarf sieht auch das ULD bei der länderübergeifenden Datenschutz-Prüfung von Medien-Webseiten. Wer es genau wissen will, dem sei der Vortrag „Cookies, Tracking, Analysen“ von RAin Friederike Schellhas-Mende (Secorvo) auf dem kommenden Karlsruher Tag der IT-Sicherheit am 15.07.2021 ans Herz gelegt (siehe unten).

E-Privacy-Richtlinie umgesetzt

Das schon lange erwartete „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien“ (TTDSG) wurde endlich am 28.05.2021 im Bundestag und tags darauf im Bundesrat beschlossen. Mit diesem Gesetz, das zusammen mit dem novellierten Telekommunikationsgesetz (TKG) am 01.12.2021 in Kraft tritt, wird die E-Privacy-Richtlinie der EU vor allem hinsichtlich der Cookies umgesetzt. Geregelt werden der digitale Nachlass und insbesondere das Thema Cookies und Einwilligungen. Das Gesetzt enthält in § 25 die Vorgabe, dass eine Einwilligung in das Setzen von Cookies immer dort notwendig ist, wo es sich nicht um technisch notwendige Cookies handelt, die beispielsweise zum Betrieb der Webseite erforderlich sind. Interessant ist § 26, in dem die Grundlage für Einwilligungsverwaltungsdienste gelegt wird. Diese Regelung muss aber noch mittels einer Verordnung konkretisiert werden.

Bei der Umsetzung sollte beachtet werden, dass nicht alles, was für den Nutzer komfortabler auch besser ist: Die Möglichkeit zur zentralen Speicherung und Verwaltung von Einwilligungen bei Treuhändern erscheint verlockend, bringt aber neue Risiken mit sich. Auch die Einwilligung über Voreinstellungen des Internetbrowsers sollte sehr kritisch betrachtet werden, wenn man eine Eindämmung der Bannerflut erreichen will. Völlig außer Acht geblieben sind leider die Anforderungen an die Gestaltung der Cookie-Banner; hier ist erster Nachbesserungsbedarf erkennbar.

Secorvo News

Teamverstärkung

Seit dem 01.07.2021 verstärkt Milan Burgdorf, Diplom-Jurist mit mehrjähriger Berufserfahrung als Informationssicherheitsbeauftragter das Secorvo-Team. Herzlich willkommen!

Secorvo Seminare

Nachdem die Infektionszahlen erwarten lassen, dass im Spätsommer die Durchführung von Präsenzseminaren wieder möglich sein wird, bieten wir das erfolgreiche T.I.S.P.-Seminar vom **20.09. bis 24.09.2021** (schnelle Buchung empfohlen) und vom **22.11. bis 26.11.2021** an. Das Programm und die Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

12. Tag der IT-Sicherheit

Der jährliche "Karlsruher Tag der IT-Sicherheit", eine Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V., findet in diesem Jahr als virtuelle Veranstaltung statt – verteilt auf drei Abende. Der erste Abend mit Prof. Dr. Jörn Müller-Quade (Leiter der Forschungsgruppe „Kryptografie und Sicherheit“ am KIT) und dem White-Hat-Hacker Tim Schmidt am 01.07. stieß bereits auf großen Zuspruch. Es folgen:

2. Abend – Donnerstag, **08.07.2021**, 18 Uhr

Einfach.Sicher.Machen. Transferstelle IT-Sicherheit im Mittelstand. *Stephanie Ziegler (KIS)*

Modernes DNS: Datenschutz mit Nebenwirkungen. *Prof. Dr. Rainer W. Gerling*

3. Abend – Donnerstag, **15.07.2021**, 18 Uhr

Elevator Pitch: StartUps IT-Security.
Jun.-Prof. Dr. Christian Wressnegger (Poison Ivy) und *Mirko Ross (asvin)*

Cookies, Tracking, Analysen.
Friederike Schellhas-Mende (Secorvo)

Im Anschluss an die Vorträge bieten wir die Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit den Referenten und anderen Teilnehmern. Wir freuen uns auf drei kurzweilige und interessante Abende mit Ihnen! (Anmeldung)

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2021	
01.07.	12. Tag der IT-Sicherheit, 1. Abend (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
08.07.	12. Tag der IT-Sicherheit, 2. Abend
12.-14.07.	PETS 2021 (University of Minnesota, virtuell)
12.-16.07.	DFRWS USA 2021 (DFRWS, virtuell)
15.07.	12. Tag der IT-Sicherheit, 3. Abend
31.07.-05.08.	Blackhat USA 2021 (Blackhat, Las Vegas/US)
August 2021	
05.-09.08.	DEF CON 29 (DEFCON, Las Vegas/US)
08.-10.08.	SOUPS 2021 (usenix, Vancouver/CAN)
11.-13.08.	30th USENIX Security Symposium (usenix, Vancouver/CAN)
15.-19.08.	Crypto 2021 (IACR, Santa Barbara/US)
September 2021	
07.-09.09.	6th IEEE European Symposium on Security and Privacy (IEEE, Wien/AUT)
14.-15.09.	D•A•CH Security (Institut für Verteilte Intelligente Systeme, syssec, München))
20.-24.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
28.-30.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2021



Die Bäume und der Wald

Je tiefer wir in den Schutz der immer komplexeren Informationstechnik eintauchen, desto eher laufen wir Gefahr das große Bild aus den Augen zu verlieren. Treten wir also einen Schritt zurück.

Besonders zwei Entwicklungslinien sind es, die sich gerade deutlich abzeichnen. Die eine: Mit der zunehmenden Digitalisierung entstehen zahlreiche neue Risiken, die oft erst nach einem Vorfall erkannt werden, so wie Anfang Juli beim Ransomware-Vorfall im Landratsamt Anhalt-Bitterfeld. Der Landrat rief den Katastrophenfall aus: Wochenlang konnten im Landkreis weder Wohngeld noch Sozialhilfe gezahlt, Mitarbeitergehälter überwiesen oder Fahrzeuge angemeldet werden.

Die zweite Entwicklungslinie zeigt, wie wenig wir bisher der ersten gewachsen sind – und wie unverstanden der Zusammenhang noch ist. Denn wie in einer Parallelwelt zeigte die CDU die Forscherin Lilith Wittmann beim LKA an, nachdem diese am 11.05.2021 eine hoch kritische Sicherheitslücke in der CDU-Connect-App entdeckt und dem CERT-Bund gemeldet hatte. Schon am 18.05.2009 wies das BVerfG eine Beschwerde gegen den „Hackerparagrafen" § 203c StGB zurück, der immer wieder die bspw. datenschutzrechtliche Ahndung der Verbreitung von Programmen mit Sicherheitslücken verhindert –wie sollte man auch eine solche Lücke dokumentieren, ohne ein Programm zu verwenden, das sie ausnutzt? Und am 08.06.2021 lehnte es eine Beschwerde gegen die Geheimhaltung von Zero-Day-Exploits durch deutsche Sicherheitsbehörden ab – genau damit entwickelt die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) seit 2017 Software zur Telekommunikationsüberwachung.

Klar ist: Unsere Zukunft wird digital sein. Funktionieren wird sie nur, wenn sie sicher ist. Daher muss die systematische Beseitigung von Sicherheitslücken unser aller Ziel sein. Auch das der Sicherheitsbehörden. Die Geheimhaltung und Verbreitung solcher Lücken gehört geahndet – nicht deren Aufdeckung oder Dokumentation.



Inhalt

Security News

UK ist sicheres Drittland

Ransomware-Hotfix

Ransomware Readiness

Grenzen des One-Stop-Shop

MS PKI under attack

Ersatz für Cookie-Banner?

Secorvo News

Secorvo Seminare

Irren ist kryptografisch

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

UK ist sicheres Drittland

Aufatmen in vielen Unternehmen: Entgegen den Bedenken des EU-Parlaments hat die EU-Kommission am 28.06.2021 den Angemessenheitsbeschluss für Großbritannien (UK) angenommen. Damit gilt UK nun als sicheres Drittland mit angemessenem Datenschutzniveau, obwohl der Investigatory Powers Act dem britischen Geheimdienst ähnlich viele Befugnisse einräumt wie den US-amerikanischen Diensten der FISA 702, der EO 12333 und der CLOUD Act. Die UK-GDPR basiert auf den europäischen Standards und übernimmt wesentliche Teile der DSGVO. Darin enthalten sind aber auch Ausnahmeregelungen zu Zwecken der Einwanderungskontrolle, was neben den unkontrollierten Zugriffen durch die Geheimdienste für Bedenken gesorgt hat.

Der Angemessenheitsbeschluss hat eine Laufzeit von sechs Jahren, kann aber durch die Kommission jederzeit eingeschränkt oder auch komplett aufgehoben werden.

Ransomware-Hotfix

Am 02.07.2021 gelang es Angreifern der Ransomware-Gruppe REvil mittels einer Zero-Day-Schwachstelle zahlreiche Installationen der Softwareverteilungsplattform Kaseya VSA zu kompromittieren. Die Cloud-Plattform des Herstellers konnte offenbar rechtzeitig abgeschaltet werden; die On-Premise-Instanzen diverser Kunden wurden jedoch übernommen und lieferten eine als Hotfix getarnte Ransomware an die verwalteten Systeme aus. Die Erpresser forderten anschließend von Kaseya die Rekordsumme von 70 Mio. Dollar für die Entschlüsselung der betroffenen Systeme. Bei vielen Unternehmen kam es zu Einschränkungen des IT-Betriebs.

Der Angriff veranlasste US-Präsident Joe Biden, Wladimir Putin am 09.07.2021 aufzufordern, gegen die mutmaßlich aus Russland stammende Gruppe REvil vorzugehen. Offenbar gerieten die Angreifer unter Druck: Am 05.07.2021 senkten sie ihre Forderung überraschend auf 50 Mio. Dollar, und am 13.07.2021 verschwanden ihre Webseiten. Ob die Gruppe untergetaucht ist oder ob es sich um eine Aktion der Ermittlungsbehörden oder der Geheimdienste handelt, ist nicht bekannt. Allerdings teilte Kaseya am 23.07.2021 mit, dass man von einer „vertrauenswürdigen Drittpartei" einen Generalschlüssel erhalten habe.

In den vergangenen Jahren erfolgen vermehrt Angriffe über die „Supply Chain", so wie der Solarwinds-Hack vom vergangenen Dezember. Bei solchen Angriffen werden mit einer Schwachstelle zahlreiche Kunden gleichzeitig kompromittiert, trotz ansonsten angemessener Schutzmaßnahmen. Daher sollte für administrative Werkzeuge ein besonders hohes Schutzniveau greifen.

Ransomware Readiness

Am 30.06.2021 veröffentlichte die amerikanische Cybersecurity & Infrastructure Security Agency (CISA) ein neues Modul für das Cyber Security Evaluation Tool (CSET). CSET ist eine Desktop-Software für Windows, die umgesetzte Schutzmaßnahmen im Netzwerk prüft. Mit dem neuen Modul Ransomware Readiness Assessment (RRA) wird überprüft, wie gut eine Organisation technisch und organisatorisch vor Ransomware-Vorfällen geschützt ist und ob sie sich von einem Vorfall absehbar erholen kann.

In einem ersten Test machte das Modul einen guten Eindruck – es eignet sich auch für Organisationen, die einen ersten Überblick gewinnen wollen, da sie noch nicht so genau wissen, was beim Thema „Schutz vor Ransomware" zu beachten ist. Vorausgesetzt, man scheut die Installation einer 1 GB großen EXE-Datei nicht, die einen kompletten Microsoft IIS Express zum Anzeigen einer Webseite mitbringt. Nehmen Sie vorsichtshalber eine virtuelle Maschine – denn auch bei Tests kann man sich etwas einfangen.

Grenzen des One-Stop-Shop

Bisher konnten nationale Aufsichtsbehörden bei angezeigten Verstößen gegen die DSGVO nicht direkt gegen Unternehmen mit Firmensitz in einem anderen europäischen Mitgliedsstaat vorgehen, weil entsprechend Art. 56 DSGVO die Federführung einer solchen Untersuchung bei der Aufsichtsbehörde des Sitzlandes liegt. Im unternehmens- oder steuerrechtlichen Kontext ist dieses Zuständigkeitsprinzip als „One-Stop-Shop" bekannt.

In der Vergangenheit stellte dieses Prinzip beispielsweise die deutschen Aufsichtsbehörden vor erhebliche Probleme, wenn sie mögliche Verstöße von großen Internet-Konzernen untersuchen wollten, die ihren Sitz in Irland haben.

Der EuGH hat nun am 15.06.2021 bestätigt, dass nach Art. 55 DSGVO eine nationale Aufsichtsbehörde einen Verstoß gegen die DSGVO selbst verfolgen kann, sofern sie das Verfahren der Zusammenarbeit und Kohärenz nach Art. 60 DSGVO eingehalten hat. Allerdings – und das ist neu – stellt der EuGH klar, dass die nationale Behörde zur wirksamen Anwendung der DSGVO den angeblichen Verstoß weiter untersuchen darf, wenn die federführende Aufsichtsbehörde nicht mit ihr zusammenarbeitet.

Eine lesenswerte Zusammenfassung des Urteils findet sich in der EuGH-Pressemitteilung.

MS PKI under attack

Via Advisory warnte Microsoft am 23.07.2021 vor einem „PetitPotam" getauften NTLM-Angriff auf den Zertifikatsdienst der Microsoft-PKI, mit dem ein Angreifer sich Nutzer-Berechtigungen verschaffen kann. Die Ursache ist – wieder einmal – übertriebene Abwärtskompatibilität: Da Microsoft NTLM per Default-Einstellung unterstützt, dürften von der Schwachstelle sehr viele Microsoft-PKIs betroffen sein. Die wirksamste (und simpelste) Schutzmaßnahme ist daher auch, die NTLM-Authentifikation mindestens auf Domain-Controllern zu deaktivieren – ohnehin eine gute Idee, um sich vor weiteren noch unentdeckten Bugs zu schützen. Falls das nicht gewünscht ist, sollte man zumindest den Web-Enrollment-Dienst der Windows-PKI deaktivieren oder ihm, wenn er gebraucht wird, NTLM verbieten. Der PKI-Experte Hans-Joachim Knobloch (Secorvo) beschreibt nach seiner ausführlichen Untersuchung des Angriffs vom 28.07.2021 was dafür zu tun ist.

Dabei entdeckte er einige weitere beunruhigende Varianten. Denn Zertifikate können auch über den Network Device Enrollment Service (NDES) angefordert werden. Dabei kann es einem Angreifer je nach Konfiguration der PKI gelingen, ein Kerberos-Ticket zur Anmeldung am Domain-Controller mit administrativen Berechtigungen zu erschleichen. Hans-Joachim Knobloch listet in seinem Blog-Beitrag vom 30.07.2021 zahlreiche Maßnahmen, die vor dieser Attacke wirksam schützen.

Ersatz für Cookie-Banner?

In Kooperation mit den Sustainable Computing Labs der Wirtschaftsuniversität Wien möchte die NGO noyb die allgegenwärtigen Cookie-Banner durch Advanced Data Protection Control (ADPC) ersetzen. Die Idee veröffentlichte Max Schrems am 14.06.2021: Durch ein automatisches Browser-Signal soll der Nutzer eine Einwilligung erteilen oder verweigern, eine bereits erteilte Einwilligung widerrufen oder einer Verarbeitung aus einem berechtigten Interesse widersprechen können.

Dafür soll eine hersteller- und browserunabhängige standardisierte Schnittstelle eingeführt werden. Statt eines reinen Ja-Nein-Mechanismus' sollen Nutzer einerseits nach Art der Daten entscheiden und andererseits Entscheidungen für mehrere Webseiten treffen können. So soll auch ein „Opt In" möglich sein, das ein differenziertes Einwilligungsmanagement bietet. Dieser Ansatz sollte auch beim Einwilligungsmanagement nach § 26 TTDSG berücksichtigt werden (siehe SSN 6/2021). Für Firefox und Chromium-basierte Browser existieren bereits Prototypen.

Secorvo News

Septemberseminare

Endlich sind Präsenzseminare wieder ohne Bedenken möglich. Daher können wir Sie vom **20. bis 24.09.2021** wieder auf die berufsqualifizierende, angesehene T.I.S.P.-Zertifizierung vorbereiten. Nach Ihrer Anmeldung erhalten Sie vorab unser T.I.S.P.-Buch zugesandt (Amazon-Rating: 4,8).

Da wir während der Pandemie gelernt haben, dass Online-Formate sich besonders für eintägige Hands-On-Seminare eignen, bieten wir erneut am **15.09.2021** unser Live-Hacking-Lab online an. Und vom **28. bis 30.09.2021** stellen wir Ihnen mit IT Security Insights aktuelle Themen der IT-Sicherheit vor (als T.I.S.P.-Update anerkannt).

Alle Programme und die Möglichkeit zur Online-Anmeldung finden Sie auf unseren Webseiten.

Irren ist kryptografisch

Die Kryptoanalyse der ENIGMA ist eine der spannendsten Geschichten in der Kryptografie. Bis in die 70er Jahre wurde in der Öffentlichkeit – und nicht nur dort – angenommen, dass die wichtigste Verschlüsselungsmaschine des zweiten Weltkriegs nicht geknackt worden war. Ein Irrtum: Die ENIGMA wurde bereits in den 30er Jahren erfolgreich analysiert, und während des Krieges wurden in Bletchley Park (GB) Nachrichten deutscher U-Boote systematisch entschlüsselt.

Auf dem kommenden KA-IT-Si-Event am 30.09.2021 wird Johann Grathwohl (IT-Security-Architekt bei CONITAS) die Entwicklung und die historischen Hintergründe der ENIGMA vorstellen und ihre Funktionsweise erläutern. Anschließend wird er die Kryptoanalyse skizzieren und auf Schwachpunkte und Fehler im Design des Verschlüsselungsverfahrens eingehen und daraus einige wichtige Erkenntnisse für den Entwurfsprozess ableiten.

Wir freuen uns darauf, unsere KA-IT-Si-Events ab September wieder als Präsenzveranstaltungen durchführen und Ihnen unser „Buffet-Networking" zum persönlichen Austausch anbieten zu können. Um die Vorträge auch weiterhin so vielen Interessenten wie in den vergangenen Monaten zugänglich zu machen, werden wir auch eine Teilnahme per Livestream ermöglichen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2021	
05.-09.08.	DEF CON 29 (DEFCON, Las Vegas/US)
08.-10.08.	SOUPS 2021 (usenix, Vancouver/CAN)
11.-13.08.	30th USENIX Security Symposium (usenix, Vancouver/CAN)
16.-20.08.	Crypto 2021 (IACR, virtuell)
September 2021	
06.-10.09.	6th IEEE European Symposium on Security and Privacy (IEEE Computer Society, virtuell)
13.-16.09.	European Identity & Cloud Conference 2021 (KuppingerCole, München)
20.-24.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
27.09.-01.10.	Informatik 2021 (GI, Berlin)
28.-30.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
30.09.	Irren ist kryptografisch (KA-IT-Si, Karlsruhe/online)

Fundsache

Am 17.07.2021 hat der Landesbeauftragte für Datenschutz-und Informationsfreiheit in Baden-Württemberg eine Handreichung zur Durchführung von Online-Prüfungen veröffentlicht, nachdem er festgestellt hatte, dass bei zahlreichen Prüfungen von Hochschulen die räumliche und technische Privatsphäre von Studierenden verletzt worden war.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2021



Dialektik

Man mag den Marxismus für eine Irrung oder eine mindestens wirtschaftlich gescheiterte Ideologie halten. Eines der drei von Engels in etwas freier Umdeutung von Hegels Dialektik aufgestellten Grundgesetze ist jedoch zweifellos eine zutreffende Beschreibung eines immer wieder zu beobachtenden Phänomens: Des Umschlags von Quantität in Qualität.

So sorgen nicht einzelne Staubkörner für eine Verschmutzung (von Reinsträumen einmal abgesehen), sondern erst deren große Zahl. Sandkörner bilden Strände und Schneeflocken Skipisten – aber nur, wenn sehr viele davon an einer Stelle zusammenkommen. Der Punkt, an dem dabei die Quantität zu einer neuen Qualität wird, ist nicht exakt auszumachen und liegt vielleicht auch im Auge des Betrachters. Irgendwann aber gibt es keinen Zweifel mehr, dass sie zu Dreck, Strand oder Skipiste geworden sind.

Unter demselben Phänomen leidet der Datenschutz – schon immer, aber seit der Entdeckung der Digitalisierung immer offensichtlicher. Einzelne Verarbeitungen personenbezogener Daten bedrohen selten die freie Entfaltung. Wohl aber deren viele. So mag eine einzige Videokamera auf einem öffentlichen Platz eine erträgliche Freiheitsbeschränkung sein. Eine auf jedem öffentlichen Platz schon weniger – und die nahtlose Aufzeichnung öffentlicher Bereiche sicher nicht.

Das ist ein Kernproblem des Datenschutzes. Gegen eine einzelne Verarbeitung mag wenig einzuwenden sein, doch im Kontext vieler weiterer wird sie irgendwann Teil einer potentiellen Überwachungsinfrastruktur.

Was dem Datenschutz daher fehlt ist ein Limit, das das Umschlagen in Überwachung verhindert. Wäre z. B. die Größe der durch Videokameras zulässig überwachbaren Fläche begrenzt oder die Datenmenge, die Webseiten und Apps „nach Hause“ schicken dürfen, würden sehr bald sinnvolle Prioritäten gesetzt – und ließen sich viele Verarbeitungen entspannter ertragen.



Inhalt

Dialektik

Security News

Der Schein darf trügen

Self-Assessment

Druckereskalation

Better Hunting

Neue Mindeststandards des BSI

One Face fits most

Secorvo News

Seminare wieder möglich

Irren ist kryptografisch

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Der Schein darf trügen

Das Oberverwaltungsgericht Rheinland-Pfalz hat am 25.06.2021 entschieden, dass die DSGVO auf abgeschaltete Überwachungskameras nicht anwendbar ist. Die Aufsichtsbehörde hatte den Kläger aufgefordert, die Kamera zu beseitigen, dieser schaltete sie jedoch lediglich ab. Die Behörde stützte ihre Anordnung auf Art. 58 Abs. 2 lit. f) DSGVO. Nach Ansicht des Gerichts verarbeitet eine ausgeschaltete Kamera ebensowenig Daten wie eine Attrappe. Das ist sachlich richtig, denn wo keine Daten erhoben werden, findet auch keine Verarbeitung statt. In der Konsequenz bedeutet dies, dass auch kein Hinweis auf die nicht stattfindende Videoüberwachung erfolgen muss und damit auch keine Kennzeichnungspflicht besteht. Die Entscheidung reiht sich in weitere, die einen Unterlassungsanspruch in solchen Fällen ablehnen (z. B. OLG Frankfurt a. M., Beschluss vom 12.10.2017 – 3 U 195/16). Zwar bleibt für den Betroffenen das „Überwachungserlebnis" dasselbe, da er eine Verarbeitung annehmen muss – aber ohne Daten auch kein Datenschutz.

Self-Assessment

Besonders für kleinere und mittlere Unternehmen ist es oft aufwendig, sich Grundkenntnisse der IT-Sicherheit als Beratung einzukaufen oder gar ein eigenes Security-Team aufzubauen. Da können Self-Assessment-Werkzeuge helfen. Sie ersetzen zwar kein externes Audit, geben jedoch einen ersten Überblick über die aktuell wichtigsten Themenbereiche und Sensibilisierungsmaßnahmen.

Bekannte Tools sind z. B. der ExPress Informationssicherheits Check (EPIC) des BSI, das Cyber Resilience Review (CRR) der CISA, der Cyber Aware Action Plan des GCHQ, der Sec-O-Mat der TISiM, das Cybersecurity Self-Assessment for SMEs von Cyberwatching oder auch das Security and Risk Self-Assessment von Brennan IT. Eine zusätzliche wertvolle Ressource liefert das CIS mit den CIS Controls.

Als Einstieg in die Informationssicherheit ist ein solches Self-Assessment jedenfalls keine schlechte Wahl. Mit dem CSIRT Maturity Self-Assessment Tool der ENISA lassen sich sogar mögliche Optimierungen für ein bereits bestehendes IT-Sicherheitsmanagement finden.

Druckereskalation

Am 19.05.2021 wurde von HP eine Schwachstelle im Druckertreiber diverser HP LaserJet Drucker veröffentlicht. Die gemäß HP mit einem CVSS-Score von 8.8 bewertete Schwachstelle CVE-2021-3438 ermöglicht über einen Buffer Overflow die Gewinnung von Berechtigungen im System-Kontext. Das ist ein gravierender Bug, sowohl hinsichtlich der möglichen Auswirkungen als auch wegen dessen weiter Verbreitung. Angreifer können sich darüber dauerhaft in einem System mit hohen Privilegien festsetzen.

Über die vom Hersteller bereitgestellten Updates (die zügig eingespielt werden sollten) hinaus stellen sich gleich mehrere Fragen: Warum erfolgt die Ausgabe von Dateien an einen Drucker heute noch mit hohen Privilegien? Warum geht das nicht im Benutzerkontext? Und: Warum benötigt ein Druckertreiber eine 25 MB große Installationsdatei, mit Utilities sogar oft über 100 MB? Sind bei diesem Umfang und dieser Komplexität nicht übersehene Schwachstellen zu erwarten? Welche technologische Entwicklung rechtfertigt eine solche Treiberkomplexität? Nicht zuletzt: Wurden (und werden) die Treiber vom Hersteller überhaupt gründlich auf Schwachstellen untersucht? Nach Auskunft der Forscher, die die Schwachstelle entdeckten, bestand sie seit mindestens 16 Jahren.

Ganz ähnliches gilt für Grafik-Treiber, die heute oft einen Umfang von über 700 MB mitbringen. Gerade Drucker- und Grafiktreiber-Programmierer sollten sich professionell mit der Frage beschäftigen, wie die erforderlichen Funktionen kompakt und ohne Scheunentore bereitgestellt werden können. Helfen würde, wenn in Unternehmen und Behörden bei der Beschaffung von Hardware auch die Komplexität und Sicherheit der Treiber eine Rolle spielen würde (gemessen z. B. daran, wie viele Schwachstellen es bereits gab).

Better Hunting

Seit dem 02.08.2021 steht das forensische Werkzeug Autopsy in der neuen Version 4.19 zur freien Nutzung bereit. Sehr hilfreich ist das neue YARA-Ingest-Modul, das man mit eigenen Zusammenstellungen von Regeln für spezifische Fragestellungen (z. B. VBA-Macros in MS Office-Dokumenten) ablaufen lassen kann. Das Modul arbeitet problemlos mehrere tausend YARA-Regeln fehlerfrei ab, wenn man es z. B. zur Suche nach Schadsoftware auf eine Datenquelle anwendet.

Wesentlich beschleunigt wurde die Erstellung des Stichwort-Index, der nun nicht mehr versucht, eine Indexierung in mehreren Sprachen sowohl für unbekannte Dateiformate als auch für nicht belegten Speicherplatz eines Datenträgers (*unallocated space*) durchzuführen – für schnellere Triagen sehr hilfreich. Muss man als Incident Responder die „Nadel im Heuhaufen" suchen, kann die Suche zeitlich

abgetrennt werden, indem der gesamte unallocated space zuerst mit Autopsy in eine separate Datei extrahiert wird.

Auch die Autopsy-Fallakte wurde verbessert, sodass unterschiedliche Datenquellen jeweils genau einem System oder einem Fundort zugewiesen werden können. Damit sind z. B. ein Desktop-PC, ein Laptop, ein Smartphone oder ein USB-Gerät als einzelne Entitäten logisch gruppierbar. So können z. B. auch logische Extraktionen von unterschiedlichen Volumenschattenkopien einer Windows-Installation zugeordnet werden. Ergänzt wird die Fallakte durch die optionale Zuordnung einer Datenquelle zu einem definierten Nutzer.

Die Einarbeitung in dieses Werkzeug erfordert etwas Zeit. Versteht man aber die Logik, dann lassen sich viele Detailspuren finden. Durch unterstützende Plugins wurde zuletzt auch die forensische Unterstützung für QNX (Echtzeitbetriebssystem im Bereich Automotive) realisiert.

Neue Mindeststandards des BSI

Am 07.07.2021 hat das BSI zwei überarbeitete Mindeststandards zur Nutzung externer Cloud-Dienste und für Schnittstellenkontrollen veröffentlicht. Ein Cloud-Dienst, z. B. eine Datenablage oder eine Kollaborationsplattform, ist schnell eingekauft. Aber passt der Dienst wirklich zur Unternehmensstrategie, wurde an den Datenschutz gedacht und wie sehen die Exit-Optionen aus? Zu diesen Fragen formuliert der Standard in strukturierter Form von der Planung bis zur Beendigung Anforderungen, an die definitiv gedacht werden sollte. Im Rahmen der Überarbeitung wurden die Mitnutzung von Cloud-Diensten integriert und die Inhalte an den IT-Grundschutz-Baustein sowie den Kriterienkatalog Cloud Computing angepasst.

Über Schnittstellen kann es zu Schadsoftwarebefall oder unerwünschtem Abfluss von Daten kommen. Schnittstellen entstehen häufig „unkontrolliert“ mit einem neuen System oder einer Anwendung. Der Standard zeigt die wichtigsten Anforderungen im Lebenszyklus einer Schnittstelle und die zu ergreifenden Kontrollmaßnahmen.

Beide Standards gelten eigentlich nur für die Informationstechnik des Bundes, enthalten aber auch für andere Behörden und Unternehmen in kompakter Form wertvolle Hinweise. Sie können somit als Checklisten verstanden und genutzt werden. Systematisch und kostenlos – wenngleich die Umsetzung der Anforderungen (sinnvoll investierten) Aufwand verursacht.

One Face fits most

Am 01.08.2021 veröffentlichten israelische Forscher eine Studie mit dem Titel „Generating Master Faces for Dictionary Attacks with a Network-Assisted Latent Space Evolution“. Darin stellen sie vor, wie sie mit KI-Werkzeugen sprichwörtliche „Allerweltsgesichter“ erzeugen können, die beim Vergleich mit Einträgen einer Referenzdatenbank für Gesichtserkennung (Labeled Faces in the Wild – LFW) zahlreiche „False Positives“ lieferten. Einzelne der synthetisierten Gesichter wurden mit bis zu 20% der Referenzdatensätze positiv abgeglichen; mit nur neun speziell erzeugten Gesichtern gelang das bei 40% aller Referenzgesichter.

Die Untersuchung lässt erwarten, dass eine Authentifizierung mittels biometrischer Gesichtserkennung auch zukünftig keine große Verlässlichkeit bieten wird. Zweifel an der Zuverlässigkeit biometrischer Identifikation sind demnach geboten. Und die Erfahrung lehrt: Angriffe werden über die Zeit besser, nicht schlechter.

Secorvo News

Seminare wieder möglich

Noch gibt es freie Plätze bei unseren Herbst-Seminaren – T.I.S.P., T.P.S.S.E., Live-Hacking und PKI. Wir empfehlen eine baldige Anmeldung unter https://www.secorvo.de/seminare.

Irren ist kryptografisch

Die Kryptoanalyse der ENIGMA ist eine der spannendsten Geschichten in der Kryptografie. Bis in die 70er Jahre wurde in der Öffentlichkeit – und nicht nur dort – angenommen, dass die wichtigste Verschlüsselungsmaschine des zweiten Weltkriegs nicht geknackt worden war. Ein Irrtum: Die ENIGMA wurde bereits in den 30er Jahren erfolgreich analysiert, und während des Krieges wurden in Bletchley Park (GB) Nachrichten deutscher U-Boote systematisch entschlüsselt.

Auf dem kommenden KA-IT-Si-Event am 30.09. 2021 wird Johann Grathwohl (IT-Security-Architekt bei CONITAS) die Entwicklung und die historischen Hintergründe der ENIGMA vorstellen und ihre Funktionsweise erläutern. Anschließend wird er die Kryptoanalyse skizzieren und auf Schwachpunkte und Fehler im Design des Verschlüsselungsverfahrens eingehen und daraus einige wichtige Erkenntnisse für den Entwurfsprozess ableiten.

Wir freuen uns darauf, unsere KA-IT-Si-Events nun wieder als Präsenzveranstaltungen durchführen und Ihnen unser „Buffet-Networking“ zum persönlichen Austausch anbieten zu können. Um die Vorträge auch weiterhin so vielen Interessenten wie in den vergangenen Monaten zugänglich zu machen, werden wir auch eine Teilnahme per Livestream ermöglichen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2021	
06.-10.09.	6th IEEE European Symposium on Security and Privacy (IEEE Computer Society, virtuell)
13.-16.09.	European Identity & Cloud Conference 2021 (KuppingerCole, München)
20.-24.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
27.09.-01.10.	Informatik 2021 (GI, Berlin)
28.-30.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
30.09.	Irren ist kryptografisch (KA-IT-Si, Karlsruhe/online)
Oktober 2021	
04.-07.10.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
12.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
12.-14.10.	it-sa 2021 (NürnbergMesse GmbH, Nürnberg)
17.-21.10.	Eurocrypt 2021 (IACR, Zagreb/HRV)

Fundsache

Am 18.07.2021 hat Amnesty International Security Lab ein forensisches Mobile Verification Toolkit veröffentlicht, mit dem auf mobilen Geräten nach Spuren der Pegasus-Spyware gesucht werden kann. Die Python-Quellen und eine Anleitung finden sich auf Github.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

September/Oktober 2021



Aufgelöste Verantwortung

Schneller als gedacht sind Cloud-Dienste zum neuen Standard geworden. Doch unsere Vorstellung, dass es dabei im Wesentlichen auf die Wahl eines vertrauenswürdigen Anbieters ankäme, ist zu kurz gesprungen.

Denn tatsächlich bestehen viele Cloud-Lösungen selbst wieder aus zahlreichen Einzeldiensten, die über die Cloud eingebunden werden: Ticketsystem, E-Mail-Services, Zahlungssystem, Benutzersupport, Shopsystem, Chat, Telefonie, Adressdatenbank, Tracking, Videostreaming ... – warum sollte ein Anbieter das auch neu implementieren, wenn er es günstig hinzukaufen kann?

Das Ergebnis ist – zumindest aus der Perspektive eines Datenschützers – fatal. Die Auftragsverarbeitungsverträge der Lösungsanbieter lesen sich wie das Who-is-who einschlägiger Cloud-Dienstleister: seitenlange Tabellen mit Unterauftragnehmern. Und schaut man sich deren AV-Verträge an, finden sich dort weitere Listen. Viele Unterauftragnehmer haben ihren Sitz im nichteuropäischen Ausland; wenn nicht, dann nutzen sie selbst nichteuropäische Dienstleister. Dass alle Verträge in dieser Kette korrekt geschlossen und die dokumentierten Schutzmaßnahmen sowie die Listen der Unterauftragnehmer der Wirklichkeit entsprechen, ist wenig wahrscheinlich – und praktisch nicht mit vertretbarem Aufwand überprüfbar.

Die Idee der Auftragsverarbeitung wird damit ad absurdum geführt. Denn im zerstückelten „Klein-Klein“ atomarer Cloud-Dienste bleibt die Verantwortung auf der Strecke. Wie sollte der Anbieter, dessen Sub-Sub-Sub-Auftragsverarbeiter seine Tickets in den USA verarbeiten lässt, den datenschutzkonformen Umgang sicherstellen?

Das erinnert ein wenig an die Finanzkrise 2008. Damals wurden die Ausfallrisiken von Immobilienkrediten durch Zerstückelung und Verteilung auf Investitionspapiere marginalisiert. Bis sie sich durch das Platzen der Immobilienblase plötzlich wirkungsvoll manifestierten.



Inhalt

Aufgelöste Verantwortung

Security News

Augen überall

ISO-Leitlinie Löschkonzept

Bad Practice 1FA

Faxen unter der DSGVO

Transnationale Verhaltensregeln

Datentransfer-Folgenabschätzung

Willkommen 2FA

Secorvo News

Secorvo Seminare

Schwarzer Gürtel

Pilze und Sicherheitsstandards...

Krypto im Advent

Veranstaltungshinweise

secorvo
security consulting

Security News

Augen überall

Am 24.08.2021 berichtete das ZDF Magazin „frontal“, dass die von Tesla-Fahrzeugen regelmäßig in die Cloud des Herstellers hochgeladenen Daten auch die Bilddaten der am Auto verbauten acht hochauflösenden Kameras umfassen. Ob dafür der Hersteller (weil das Auto ohne die Übermittlung nicht vollumfänglich funktioniert) oder der Halter (da er der Übermittlung zugestimmt hat) die datenschutzrechtliche Verantwortung trägt, ist ungeklärt. Nach Auffassung der Aufsichtsbehörden sind Aufzeichnungen mit Dashcams nur in sehr engen Grenzen zulässig. Die niedersächsische Aufsichtsbehörde hält eine Speicherung nur bis maximal 30 Sekunden für rechtmäßig. Ähnliches gilt für die Video Doorbell von Ring, einer Amazon-Tochter, über die der SWR am 05.10.2021 berichtete. Über die mit Mikrofon ausgestattete Kamera können Hausbesitzer auf dem Mobilgerät verfolgen, was sich vor der heimischen Haustür so tut – und mit Besuchern Kontakt aufnehmen.

In beiden Fällen muss der Verantwortliche die Betroffenen nach Art. 12 ff. DSGVO über Art und Zweck der Verarbeitung informieren; dabei darf keine Erfassung des öffentlichen Raums erfolgen.

Die ggf. heimliche Tonübertragung der Video Doorbell kann zudem eine strafrechtlich relevante Verletzung der Vertraulichkeit des Wortes (§ 201 StGB) darstellen. Auch sind die Geräte vor einiger Zeit durch Schwachstellen aufgefallen.

Bis zu einer datenschutzkonformen Lösung muss man wohl empfehlen, um Teslas und Video Doorbells einen großen Bogen zu machen.

ISO-Leitlinie Löschkonzept

Als praxisbewährte Hilfestellung für die Entwicklung von Löschkonzepten wurde bis 2016 unter der Federführung von Secorvo und mit Unterstützung der Unternehmen Blancco, DATEV, Deutsche Bahn und Toll Collect die „Leitlinie Löschkonzept“ entwickelt und schließlich als DIN 66398 verabschiedet (SSN 4/2016). 2018 startete die DIN das Projekt ISO/IEC 27555 zur Überführung der Leitlinie in einen internationalen Standard (SSN 7/2018). Jetzt ist es so weit: Am 08.10.2021 wurde die ISO/IEC 27555:2021 (Information security, cybersecurity and privacy protection – Guidelines on personally identifiable information deletion) publiziert. Die Vorgehensweise entspricht der DIN 66398; im Detail gibt es einige wenige Unterschiede. Der Text wurde redaktionell überarbeitet und deutlich gekürzt. Die DIN 66398 wurde im Juni 2021 vom zuständigen Arbeitskreis bestätigt und wird zunächst beibehalten.

Bad Practice 1FA

Wie u. a. im SANS-Newsletter vom 30.08.2021 gemeldet, hat die amerikanische Cybersecurity & Infrastructure Security Agency (CISA) die Single-Factor-Authentifzierung auf die Liste der Bad Practices gesetzt. Aus unserer Sicht eine sinnvolle Ergänzung, nicht nur Best Practices sondern auch verbreitete „No Gos“ als Bad Practice zu „brandmarken“.

In internen Netzen und geschlossenen Umgebungen kann ein Kennwort als einziger Faktor ggf. noch angemessen sein. Bei über das Internet genutzten (Cloud-) Diensten ist das aufgrund der zahlreichen mit Kennworten verbundenen Gefährdungen wie Brute-Force-Angriffen, Phishing oder der Wiederverwendung von Kennworten nicht zu empfehlen.

One Time Token und Zertifikate haben sich in der Praxis bewährt. Wer darauf verzichtet, sollte sich darüber im Klaren sein, dass er bei einer Kompromittierung zu Recht eine Tasse mit Aufschrift „Das kannste schon so machen, aber dann isses halt …“ auf den Tisch gestellt bekommt. Auch die weiteren Anti-Empfehlungen der CISA Bad Practices lohnen einen genaueren Blick.

Willkommen 2FA

Viele Dienste bieten zur Verbesserung der Sicherheit zusätzlich eine Zwei-Faktor-Authentifizierung an. Ursprünglich waren dies TAN-Listen auf Papier. Mittlerweile werden die zusätzlichen Geheimnisse in Hardware-Token oder in Smartphone-Apps gespeichert wie die Authenticator-Apps von Google und Microsoft.

Privatanwendern wird nun für das Microsoft-Konto eine kennwortlose App-Authentifikation angeboten, die sie in den Sicherheitseinstellungen aktivieren können. Unternehmen und Bildungseinrichtungen steht diese Funktion bereits länger zur Verfügung. Statt der App kann z. B. auch ein FIDO2-Key verwendet werden. Angriffe auf gut zu merkende, aber zu einfache Passwörter sollen so der Vergangenheit angehören.

Prinzipiell kann das Verfahren als 2FA angesehen werden: Der Zugang erfordert den physischen Besitz des Smartphones, und beim iPhone ist die Authentikator-App zusätzlich durch einen Fingerabdruck gesichert. Damit das Entsperren des Smartphones dauerhaft nur dem Besitzer möglich ist, sind regelmäßige Sicherheitsupdates und eine komplexe PIN (oder gute Biometrie) essentiell. Damit zukünftig nicht jeder Dienst eine eigene Authentikator-App benötigt, bleibt zu hoffen, dass sich Standards wie FIDO2 durchsetzen.

Faxen unter der DSGVO

Nach der Bayrischen, der Niedersächsischen und der Bremischen Aufsichtsbehörde hat am 14.09.2021 auch der Hessische Datenschutzbeauftragte den Faxversand als unsicheres Übermittlungsverfahren eingestuft. Zwar verneint er die Zulässigkeit einer Fax-Übertragung personenbezogener oder auch besonders schutzbedürftiger Daten nicht generell, begrenzt sie jedoch auf dringliche Ausnahmefälle.

Der Vergleich der Aufsichtsbehörde mit dem E-Mail-Versand hinkt jedoch. Denn nach wie vor gilt (SSN 03/2021): Ein Fax ist genauso sicher wie ein Telefonat – beide nutzen heute TCP/IP-basierte Paketvermittlung. Und beide Übertragungen unterliegen dem Telekommunikationsgeheimnis, das die TK-Provider durch geeignete Schutzmaßnahmen sicherstellen müssen.

Die Technik der Faxübermittlung ist nicht unsicherer geworden. Die besonderen Gefahren beim Faxversand schützenswerter Daten liegen schon immer auf der „Benutzerebene", wie Zahlendreher bei der Fax-Nummer, Nutzung der Wahlwiederholungstaste oder ein Empfangsgerät, das Unberechtigten zugänglich ist. Daher ist die Empfehlung der Aufsichtsbehörde zutreffend, nach Möglichkeit alternative Übertragungstechniken zu wählen.

Transnationale Verhaltensregeln

Noch immer herrscht große Unsicherheit, wie die Anforderungen aus dem EuGH-Urteil Schrems II an internationale Datentransfers zu erfüllen sind. Ein Weg ist die Auswahl von Dienstleistern, die sich zur Einhaltung von der EU anerkannter transnationaler Verhaltensregeln verpflichten. Am 20.05.2021 wurden die Beschlussvorlagen zum EU Cloud Code of Conduct und zum Code of Conduct for Cloud Infrastructure Service Providers in der Version 2.11 als erster Transnational Code of Conduct vom Europäischen Datenschutzausschuss angenommen und damit deren DSGVO-Konformität bestätigt.

Datentransfer-Folgenabschätzung

Die am 04.06.2021 von der EU-Kommission verabschiedeten neuen Standardvertragsklauseln verlangen, dass im Hinblick auf internationale Datentransfers in Drittstaaten ohne anerkanntes angemessenes Datenschutzniveau sog. Transfer Impact Assessments (TIA) durchgeführt werden (Klauseln 14 a) - d)). Dabei ist eine mehrstufige Prüfung durchzuführen, die den besonderen Umständen der Datenübermittlung, also z. B. der Länge der Verarbeitungskette, den beabsichtigten Übertragungskanäle, den Kategorien und dem Format der übermittelten personenbezogenen Daten Rechnung tragen soll. Die relevanten Rechtsvorschriften des Bestimmungslandes müssen geprüft, die erforderlichen technischen und organisatorischen Schutzmaßnahmen (TOMs) müssen festgelegt werden.

Um hier eine Hilfestellung zu geben, hat die non-profit-Organisation iapp am 01.09.2021 ein Muster zur Durchführung eines solchen TIAs bereitgestellt, das für Übermittlungen in die USA hilfreich ist.

Secorvo News

Secorvo Seminare

Auf unserem letzten Seminar in diesem Jahr gibt es noch wenige freie Plätze: IT Security Insights, unser T.I.S.P.-Update (**30.11.–02.12.2021**). Natürlich freuen wir uns auch über Anmeldungen für unsere im kommenden Jahr geplanten Seminare. Eine Übersicht aller Termine und Seminarangebote finden Sie unter www.secorvo.de/seminare.

Schwarzer Gürtel

Unser Penetrationstester Enes Erdoğan hat jetzt ebenfalls den „schwarzen Gürtel" – seine OSCP-Zertifizierung. Herzlichen Glückwunsch!

Pilze und Sicherheitsstandards...

In den vergangenen Jahren ist die Zahl der Standards, Checklisten und Best Practices zur Informationssicherheit ständig gewachsen. Auf dem kommenden KA-IT-Si-Event am **18.11.2021** zeigt Ihnen Milan Burgdorf interessante Gebiete auf der Landkarte der Informationssicherheitsstandards und -frameworks. Dabei werden bekannte (ISO 2700x und IT-Grundschutz) und unbekannte Gegenden erkundet, damit Sie sich auf diesem unübersichtlichen Territorium besser zurecht finden. Wir freuen uns auf einen interessanten Abend mit Ihnen – diesmal wieder als Online-Event (zur Anmeldung).

Krypto im Advent

Mit unserem interaktiven Online-Adventskalender „Krypto im Advent" lernen Schülerinnen und Schüler (3.-9. Klasse) seit 2015 auf spielerische Weise Verschlüsselungstechniken kennen und können dabei attraktive Sachpreise gewinnen. Zusammen mit der PH Karlsruhe haben wir uns auch diesmal wieder spannende Kryptografie-Rätsel ausgedacht. Schulklassen und Profis können ebenfalls „miträtseln", letztere allerdings außer Konkurrenz. Anmeldungen sind ab dem 01.11.2021 auf Krypto-im-Advent.de möglich (Teilnahme kostenlos).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2021	
14.-19.11.	ACM CCS 2021 (ACM/SIGSAC, Seoul/KOR)
17.-19.11.	45. DAFTA (GDD, virtuell)
18.-19.11.	DeepSec 2021 (DeepSec, Wien/AT)
30.11.-02.12.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
Januar 2022	
24.-26.01.	Omnisecure 2022 (in TIME berlin, Berlin)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

November 2021



Keks-Transparente

Sie nerven. Kaum eine Webseite, die noch ohne Mausklick zu erreichen wäre: Zuerst muss man den „Cookie-Banner" hinter sich bringen. Schlimmer noch: Seltenst kann man das Tracking mit einem einzigen Klick ablehnen – erst auf einer weiteren Seite, oft nach längerem Scrollen und manchmal erst nach mühseligem Deaktivieren der (rechtswidrig) voreingestellten ungewünschten Datenerhebungen. Dabei versuchen Text, Hervorhebung und Farbe der „Knöpfe" den Besucher zu einem vorschnellen „Einverstanden" zu bewegen – „Nudging" heißt dieser neue Wettlauf zwischen Werbestrategen und genervten Seitenbesuchern.

Die gewählte Cookie-Einstellung wird gespeichert – in einem Cookie natürlich, das bei einer datensparsamen Browser-Konfiguration beim Schließen sorgsam von der Festplatte gelöscht wird. Und beim nächsten Seitenbesuch geht alles wieder von vorne los. Bleiben die Webseiten ohne Banner. Sie sind fast noch schlimmer, denn wer einen Tracker-Alarm in seinem Browser installiert hat, weiß, dass die meisten dieser Seiten einfach ohne Einwilligung tracken. So nagt unvermeidlich der Gedanke im Hinterkopf, dass man diese Seiten eigentlich sofort verlassen müsste.

Kein Wunder, dass viele Menschen ein Ziel für ihren Ärger suchen – und es in der DSGVO finden: einem weiteren Beispiel für ausufernde Brüsseler Regelungsbürokratie. Der britische Kultusminister Oliver Dowden dürfte vielen aus dem Herzen gesprochen haben, als er im August die „Abschaffung der endlosen Cookie-Hinweise" forderte.

Alles verständlich. Und dennoch Unsinn. Das ist, als würde man fordern, allen Autofahrern, die auf fremden Grundstücken parken wollen, das Fragen um Erlaubnis zu erlassen – weil so viele fragen.

Verursacher der Cookie-Banner ist nicht der Datenschutz. Sondern die hemmungslose Aufdringlichkeit, mit der Webseitenbetreiber unser Nutzerverhalten protokollieren und auswerten.



Inhalt

Keks-Transparente

Security News

Ja, ich will!

Ransomware: Never Ending Story

Ich sehe was, was Du nicht siehst

Videokonferenz-Mindeststandard

Kontextfreie MFA

Einmal keine Updates eingespielt…

Top Hardware-Schwachstellen

Secorvo News

Schwarze Gürtel

White Paper „Penetrationstests"

Seminare

Rätseln mit Lerneffekt

Veranstaltungshinweise

secorvo
security consulting

Security News

Ja, ich will!

Der Bayerische Beauftragte für Datenschutz hat am 01.09.2021 eine Orientierungshilfe zum Thema Einwilligung herausgebracht. Diese ist all denjenigen zur Lektüre zu empfehlen, die sich bei der Verarbeitung personenbezogener Daten auf Einwilligungen stützen. Besonders relevant ist dies bei der Gestaltung von Webseiten, die mehr als nur technisch notwendige Cookies verwenden. Unberücksichtigt bleibt darin leider das am 01.12.2021 in Kraft getretene TTDSG, in dem Einwilligungsmanagement und Einwilligungstreuhänder vorgesehen sind. Dazu sollte man sich zeitnah anderweitig informieren.

Ransomware: Never Ending Story

Am 08.11.2021 schaffte es wieder einmal ein Angriff mit Ransomware in die Tagespresse. Dass es sich bei dem Angriff auf den Media-Saturn-Konzern nicht um einen Einzelfall handelt, kann man live auf der Cyberbedrohung Echtzeitkarte von Kaspersky beobachten oder dem aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland des BSI entnehmen.

Neben einem angemessenen Schutz vor Ransomware und anderer Schadsoftware sollte es auch selbstverständlich sein, Vorkehrungen für die Schadensbegrenzung im Fall einer Infektion zu treffen: Verzicht auf unnötige administrative Berechtigungen, Virenschutz, Einschränkungen von Programmausführungen, Makrosicherheit und ein Backup nach der 3-2-1-Regel gehören dazu. Für dunkle Wintertage empfehlen wir die ausführliche Publikation des BSI zum Thema Ransomware mit sinnvollen weitergehenden Maßnahmen zur Lektüre.

Ich sehe was, was Du nicht siehst

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI) hat am 27.10.2021 Hinweise und eine Handreichung zur praktischen Nutzung von Videokonferenzsystemen veröffentlicht. Gemäß Pressemitteilung will der LfDI keine „detaillierten Hinweise zu allen möglichen Konfigurationen und Vertragsgestaltungen geben", sondern bei der Auswahl und Einrichtung des „richtigen" Systems unterstützen.

Leider gelingt dies der Handreichung nicht. Die einführenden Rahmenbedingungen und Empfehlungen sind möglicherweise für den einen oder anderen Nutzer hilfreich. Problematisch sind jedoch die Hinweise zu den verschiedenen Anbietern: Hier fehlt es an einer einheitlichen Darstellung und an der Bewertung des aktuellen Stands der datenschutzrelevanten Dokumente. Es wird erkennbar, dass keine neutrale Beurteilung stattgefunden hat. Daher sollte man zur Auswahl weitere Dokumente wie etwa den Mindeststandard des BSI zu Videokonferenzdiensten als Checkliste hinzuziehen (s. u.).

Videokonferenz-Mindeststandard

Am 07.10.2021 hat das BSI einen Mindeststandard für Videokonferenzdienste veröffentlicht. Obwohl die BSI-Mindeststandards unmittelbar nur für die Informationstechnik des Bundes gelten, enthalten sie häufig praxisorientierte Hinweise in kompakter Form, die auch für andere Behörden und Unternehmen hilfreich sind. Ohne auf bekannte Videokonferenzprodukte einzugehen, werden typische Sicherheits- und Funktionsanforderungen wie ein Rollenkonzept, Verschlüsselung, Dateiablagen, das Teilen von Bildschirminhalten oder Sicherheitsupdates vorgestellt. Zusätzlich wird darauf aufmerksam gemacht, nicht benötigte Funktionen abzuschalten und die Beschäftigten in die Verwendung und Moderation des Videokonferenz-Tools einzuweisen. Bei Einführung oder Betrieb eines Videokonferenzdienstes kann der Mindeststandard somit als Checkliste verwendet werden, um Informationssicherheitsanforderungen an einen Videokonferenzdienst systematisch umzusetzen.

Kontextfreie MFA

Dass auch eine Multi-Faktor-Authentifikation (MFA) ohne vernünftiges „User-Interface" schief gehen kann, illustrierte Roger Grimes am 20.10.2021 anhand einiger Beispiele. Darunter ist das eines Vice Präsidenten, der ein Login mehrfach mit einem zugesandten zweiten Faktor bestätigte, obwohl er sich nirgends anmelden wollte – und so Angreifer in die Firma ließ.

Solche Fehler darf man nicht allein dem Nutzer vorwerfen, denn oft fehlt bei der Zusendung des zweiten Faktors der Kontext. Einen Sicherheitsexperten wird eine kontextfreie MFA sicherlich Verdacht schöpfen lassen – einen an „kryptische" E-Mails von der IT gewöhnten Mitarbeiter aber vielleicht nicht. Verständlichkeit und Nachvollziehbarkeit sind für einen wirksamen Schutz unverzichtbar.

Einmal keine Updates eingespielt...

Im Tätigkeitsbericht der niedersächsischen Aufsichtsbehörde für 2020 wird von einem Bußgeld in Höhe von 65.000 Euro gegen einen Onlineshop-Betreiber berichtet, der seine Shop-Anwendung fünf Jahre lang nicht aktualisierte, obwohl der Softwarehersteller auf erhebliche Sicherheitslücken hingewiesen und eine neue Version bereitgestellt hatte. Wesentlich für die Aufsichtsbehörde war, dass nach Art. 24 Abs. 1 DSGVO Schutzmaßnahmen vom Verarbeiter überprüft und aktualisiert werden

müssen und dass die Verwendung aktueller, um Sicherheitslücken bereinigter Software für das Unternehmen nicht unverhältnismäßig gewesen wäre. Auch im Tätigkeitsbericht der baden-württembergischen Aufsichtsbehörde für 2020 findet sich ein Bericht über ein Bußgeld in Höhe von 1,2 Mio. Euro gegen eine Krankenkasse, die Maßnahmen zum Schutz der Daten von Gewinnspielteilnehmern nur unzureichend umgesetzt hatte.

Zur Handlungspflicht bei Kenntnis einer Schwachstelle gibt die Pressemitteilung der baden-württembergischen Aufsichtsbehörde Hinweise, was sie beispielsweise bei der Exchange-Lücke von den Betreibern erwartete.

Die Aufsichtsbehörden tolerieren eine nachlässige Umsetzung von technischen und organisatorischen Maßnahmen nicht, erwarten regelmäßige oder anlassbezogene Überprüfungen und insbesondere das zügige Einspielen von Sicherheitsupdates. Sofern personenbezogene Daten verarbeitet werden, ist Informationssicherheit nach Stand der Technik Pflicht.

Top Hardware-Schwachstellen

Die OWASP Top 10 sind mittlerweile jedem ein Begriff, wenn es um die verbreitetsten Schwachstellen in Web-Anwendungen geht. Dass Sicherheit jedoch gerade im Kontext von IoT auch weit mehr als klassische Web-Anwendungen umfasst, griff am 26.10.2021 die MITRE auf und veröffentlichte die 2021 CWE Most Important Hardware Weaknesses bestehend aus den zwölf bedeutendsten Schwachstellenklassen von Hardware. Dazu zählen beispielsweise schlechte kryptographische Implementierungen, unzureichender Schutz gegen Debugging oder fehlende Funktionen für Firmware-Updates.

Insgesamt haben sich die Common Weakness Enumeration (CWE) in den vergangenen Jahren immer weiter durchgesetzt und sind auch bei uns insbesondere im Pentesting zum Standard für die Kategorisierung von Schwachstellen geworden. So liefert die Datenbank nicht nur allgemeine Informationen zur Schwachstelle und Beispiele, sondern auch Gegenmaßnahmen und Referenzen zu Vorkommen der Schwachstelle in Form von CVEs. Für verschiedenste Anwendungsfälle bietet die Datenbank Mappings und Ansichten an, welche die Navigation signifikant erleichtern.

Secorvo News

Schwarze Gürtel

Im November haben Mitglieder des Secorvo-Teams drei weitere Zertifizierungen erhalten: Enes Erdoğan bestand die 24stündige Prüfung zum „Offensive Security Certified Professional“ (OSCP) und ist jetzt Träger des ‚schwarzen Gürtels‘ für Pentester. André Domnick erwarb in einer 48stündigen Prüfung den bereits dritten DAN und darf sich nun „Offensive Security Experienced Penetration Tester“ (OSEP) nennen. Und Milan Burgdorf erhielt die Zertifizierung zum ISO/IEC 27001-Auditor – die ‚Lizenz zum Prüfen‘. Herzlichen Glückwunsch!

White Paper „Penetrationstests”

Viele Unternehmen führen regelmäßig technische Sicherheitsprüfungen der IT-Infrastruktur in Form von externen Penetrationstests durch. Für solche Tests haben wir aus unserer langjährigen Erfahrung eine standardisierte Vorgehensweise entwickelt, die eine wiederholbare und modularisierte Durchführung erlaubt.

Am 11.11.2021 haben wir eine überarbeitete und erweiterte Version unseres White Papers „Penetrationstests“ veröffentlicht, in dem wir die Vorgehensweise von Secorvo vorstellen und konkrete Empfehlungen zur erfolgreichen Durchführung von Penetrationstests geben. Gerne finden wir auch für Sie die zu Ihrem Unternehmen passende Vorgehensweise.

Seminare

Mit sehr positiver Resonanz haben wir das Seminar „IT Security Insights“ erstmals online durchgeführt: praktische Übungen und aktuelle Themen der IT-Sicherheit als ‚Update‘ für IT-Sicherheitsbeauftragte und -Experten. Die nächste Gelegenheit zur Teilnahme, die hoffentlich wieder in Präsenz möglich sein wird, haben Sie vom **15. bis 17.03.2022**. Davor bieten wir Ihnen vom **07. bis 11.03.2022** die Möglichkeit, sich zum T.I.S.P. zu zertifizieren, unterstützt von unserem T.I.S.P.-Begleitbuch „Informationssicherheit und Datenschutz“. Weitere Termine, Programme und die Möglichkeit zur Anmeldung finden Sie unter secorvo.de/seminare.

Rätseln mit Lerneffekt

Es ist wieder so weit: Mit dem interaktiven Online-Adventskalender „Krypto im Advent“ lernen Schülerinnen und Schüler (3.-9. Klasse) vom 1. bis 24.12. auf spielerische Weise Verschlüsselungstechniken kennen und können dabei attraktive Sachpreise gewinnen. Die PH Karlsruhe und die KA-IT-Si haben sich für die siebte Auflage des Adventskalenders wieder spannende Kryptografie-Rätsel ausgedacht. Ein Einstieg ist auch nach dem 1.12. noch möglich. Auch Schulklassen und Profis dürfen miträtseln, letztere allerdings außer Konkurrenz (zur kostenfreien Registrierung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2022	
14.-16.01.	ShmooCon2022 (The Shmoo Group, Washington/US)
Februar 2022	
01.-02.02.	18. Deutscher IT-Sicherheitskongress (BSI, virtuell)
03.02.	KA-IT-Si-Event „Willkommen bei den Quanten“ (KA-IT-Si, hybrid)
03.-04.02.	29. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
März 2022	
07.-11.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
15.-17.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
23.03.	31. ID:SMART Workshop (Fraunhofer SIT, Darmstadt)
25.03.	Datenschutztag 2022 (COMPUTAS, Köln)
28.-31.03.	DFRWS EU 2022 (DFRWS, hybrid)
29.-31.03.	secIT 2022 (Heise Medien, Hannover)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2022



Rechtsstaatsprinzip

Vor fünf Jahren hat das BVerfG in seinem Urteil zum NPD-Verbot die Prinzipien der freiheitlich-demokratischen Grundordnung präzisiert – die Wesenseigenschaften unserer politischen Ordnung, die uns von einer Diktatur unterscheiden. Darunter: die „Rechtsbindung der öffentlichen Gewalt" nach Art. 20 Abs. 3 GG. Polizei, Verwaltung und Regierung müssen sich an geltende Gesetze halten.

Zugegeben: Gesetze gibt es viele in Deutschland, und manche davon mögen mit heißer Nadel gestrickt sein. Doch das entbindet kein Organ der Exekutive von der im Grundgesetz verankerten Pflicht, sich daran zu halten. Damit ist es allerdings gelegentlich nicht weit her.

§ 28a Abs. 4 des Infektionsschutzgesetzes in der Fassung vom 18.11.2020 regelt den Umgang mit Corona-bedingt erhobenen Kontaktdaten unmissverständlich: „Eine Weitergabe der übermittelten Daten durch die zuständigen Stellen nach Satz 3 oder eine Weiterverwendung durch diese zu anderen Zwecken als der Kontaktnachverfolgung ist ausgeschlossen."

Am 07.01.2022 meldete der SWR, dass die Mainzer Polizei für Ermittlungen in einem Unfall mit Todesfolge vom Gesundheitsamt die Kontaktdaten von 21 Gästen einer Mainzer Gaststätte angefordert und (unter Vortäuschung einer Infektion durch das Gesundheitsamt) erhalten hat – aufgrund einer „fehlerhaften Bewertung des Infektionsschutzgesetzes". Weitere Fälle seien nicht bekannt.

Inzwischen schon. In über 100 Fällen haben Staatsanwaltschaft und Polizei Kontaktlisten oder Kontaktdaten der Luca-App ausgewertet, wie das ZDF am 20.01.2022 berichtete. Soweit bekannt.

Offenbar gibt es Strafverfolger, die der Überzeugung sind, dass es in ihrer Entscheidungshoheit liegt, an welche Gesetze sie sich halten müssen – und an welche nicht. Genau diese Haltung ist es, die einen funktionierenden Rechtsstaat schleichend zu einem Unrechtsstaat mutieren lässt.



Inhalt

Rechtsstaatsprinzip

Security News

Videokonferenzen sind Telekommunikation

Aus für Google Analytics?

Ransomware-Prävention

MFA wird Standard

Koalitionsvorhaben

Orientierung im Einwilligungs-Dschungel

Datenschutz-Zertifizierungen

Gefragter Staat

Secorvo News

T.I.S.P. und IT Security Insights

Willkommen bei den Quanten

Veranstaltungshinweise

secorvo
security consulting

Security News

Videokonferenzen sind Telekommunikation

Mit Inkrafttreten der am 07.05.2021 verabschiedeten TKG-Novelle am 01.12.2021 fallen nun auch nummernunabhängige interpersonelle Telekommunikationsdienste (§ 3 Nr. 40 TKG) unter das TKG. Dahinter verbergen sich Messenger- und Videokonferenzdienste wie Teams oder Zoom. Statt der Datenschutzaufsichtsbehörden ist nun die Bundesnetzagentur zuständige Aufsichtsbehörde. Wichtige Folge: Für Telekommunikationsdienste müssen keine Auftragsverarbeitungsverträge nach Art. 28 DSGVO geschlossen werden, denn die Kommunikation fällt unter das Telekommunikationsgeheimnis des Art. 10 GG. Die Grundsätze des Datenschutzes bleiben gültig und sind nach wie vor zu beachten; dennoch wird der Einsatz in Unternehmen dadurch wesentlich erleichtert.

Aus für Google Analytics?

Vor dem Hintergrund der Schrems II-Entscheidung des EuGH vom 16.07.2020 (C-311/18), nach der es für eine Übermittlung personenbezogener Daten in die USA entweder einer Einwilligung der Betroffenen oder eines Vertrags nach den aktuellen Standardvertragsklauseln der EU-Kommission sowie „zusätzlicher effektiver Maßnahmen" zur Herstellung eines gleichwertigen Schutzniveaus bedarf, entschied die österreichische Datenschutzbehörde (DSB) am 22.12.2021, dass die Datenübermittlung eines Webseitenbetreibers an Google mittels Google Analytics nicht mit der DSGVO vereinbar und somit illegal ist. Nach Ansicht der DSB verhindern die zusätzlichen Maßnahmen einen Zugriff der US-Behörden auf die übermittelten Daten nicht.

Zwar wurde weder entschieden, ob eine Anonymisierung der IP-Adressen eine Vereinbarung entbehrlich macht, noch, ob eine Übermittlung an Google Irland zulässig wäre. Die DSB weist jedoch darauf hin, dass eine IP-Adresse nur ein Teil des „digitalen Fußabdrucks" eines Nutzers sei.

Die Entscheidung kann als Indiz für die künftige Position der deutschen Aufsichtsbehörden gelten, zumal die europäischen Datenschutzbehörden bei diesem Thema offenbar in einer Task-Force zusammenarbeiten. Solange Google keine tiefgreifenden Änderungen an Google Analytics vornimmt, ist Betreibern von Webseiten ein Wechsel zu europäischen Anbietern zu empfehlen.

Ransomware-Prävention

Am 30.11.2021 hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) ein anlassloses Prüfverfahren zur Ransomware-Prävention gestartet. Die Fragen der Aufsichtsbehörde zielen auf die in den geprüften Einrichtungen getroffenen Schutzmaßnahmen vor Ransomware-Angriffen. Der Fragebogen, die Handreichung und ein Informationsblatt des BayLDA ist auch für nicht betroffene Unternehmen eine gute Orientierung hinsichtlich der zu treffenden Mindestschutzmaßnahmen.

MFA wird Standard

Für Kunden von Salesforce wird ab dem 01.02.2022 die Multi-Faktor-Authentifizierung (MFA) zum Standard. Eine begrüßenswerte Maßnahme, gilt doch eine Kennwort-Authentifikation bei Cloud-Diensten als Schwachstelle. Zwar schützt eine MFA nicht vor allen Angriffen, aber eine solche Vorgabe (vgl. SSN 09+10/2021) verbessert die Sicherheit signifikant.

Bei der Wahl der Authenticator App sollte der Fokus auf Benutzerfreundlichkeit, Sicherheit und Datenschutzaspekten liegen. So sollte die App für mehrere Dienste nutzbar sein und die Authentifizierungsdaten ausreichend geschützt speichern.

Koalitionsvorhaben

Informationssicherheit und Datenschutz misst die neue Bundesregierung nach dem am 07.12.2021 unterzeichneten Koalitionsvertrag erhebliches Gewicht bei: Im Abschnitt „Digitale Bürgerrechte und IT-Sicherheit" werden ein „Recht auf Verschlüsselung" und ein „wirksames Schwachstellenmanagement" gefordert. Außerdem sollen Hersteller für Schäden durch fahrlässige IT-Sicherheitslücken in ihren Produkten haften. Staatliche Stellen sollen verpflichtet werden, „ihnen bekannte Sicherheitslücken beim BSI zu melden" und ihre IT-Systeme regelmäßig einer externen Prüfung zu unterziehen. Dem staatlichen Ankauf von Sicherheitslücken erteilt die Koalition eine klare Absage, und im Bundespolizeigesetz soll es keine Ermächtigung mehr zu Quellen-TKÜ und Onlinedurchsuchung geben.

Zum Datenschutz plant die Regierung einen weiteren Anlauf für ein Beschäftigtendatenschutzgesetz (inzwischen ein „running gag"), will in einem „ambitionierten Abkommen" mit den USA wieder datenschutzkonforme Datenübermittlungen auf europäischem Schutzniveau ermöglichen und die schon totgesagte E-Privacy-Verordnung wiederbeleben.

Orientierung im Einwilligungs-Dschungel

§ 25 des kürzlich in Kraft getretenen Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG) regelt die Anforderungen an Einwilligungen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK) hat daraufhin am 20.12.2021 eine

neue Version ihrer Orientierungshilfe für Anbieter:innen von Telemedien veröffentlicht. Darin weist sie ausdrücklich darauf hin, dass nicht nur Cookies, sondern alle Tracking-Technologien einwilligungsbedürftig sind. Wichtig ist auch die Unterscheidung zwischen der Einwilligung nach DSGVO und TTDSG, da es für letztere eben nicht auf den Personenbezug ankommt.

Hinsichtlich der Einwilligungsverwaltung für Cookies zeigt der aktuelle Beschluss des VG Wiesbaden vom 01.12.2021, dass die Aufklärung bei Aufruf einer Webseite transparent erfolgen und zu dem passen muss, was im Hintergrund abläuft. Werden Funktionen bspw. zur Anzeige von Informationen verwendet, die eine Verbindung mit Servern im Nicht-EU-Ausland herstellen, muss die Einwilligung hierfür vor deren Ausführung eingeholt werden.

Datenschutz-Zertifizierungen

Bis zum Inkrafttreten der DSGVO waren das Gütesiegel und das Audit des Unabhängigen Landeszentrums für Datenschutz in Schleswig Holstein (ULD) die bekanntesten Datenschutzzertifizierungen. Mit Art. 42 und 43 DSGVO wurden datenschutzspezifische Zertifizierungsverfahren und Datenschutzprüfzeichen zum Nachweis der DSGVO-Konformität bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingeführt.

Nach der in der DSGVO gewählten Formulierung können Datenschutz-Produkte, -Prozesse oder -Dienstleistungen zertifiziert werden, nicht jedoch Datenschutz-Managementsysteme, obwohl diese Systeme oft Grundlage für datenschutzgerechte Produkte sind. Der größte Bedarf an Zertifizierungen liegt sicherlich in der Zertifizierung von Auftragsverarbeitungen.

Als europaweit gemeinsame Grundlage für die Akkreditierung von Zertifizierungsstellen nach Art. 43 DSGVO hatte der Europäische Datenschutzausschuss im Dezember 2018 Leitlinien veröffentlicht. Daran anknüpfend haben die deutschen Datenschutzaufsichtsbehörden und die Deutsche Akkreditierungsstelle (DAkkS) einen Akkreditierungsprozess erarbeitet, der der DIN EN ISO/IEC 17065 und den ergänzenden Anforderungen der Datenschutzkonferenz folgt. Für in Deutschland tätige Zertifizierungsstellen wird die Akkreditierung durch die DAkkS zusammen mit der zuständigen Datenschutzaufsichtsbehörde erteilt.

Das von der DAkkS in einem Merkblatt veröffentlichte Musterzertifikat und die Ankündigungen verschiedener Datenschutzaufsichtsbehörden wie dem ULD lassen erwarten, dass es im Laufe des Jahres erste Datenschutz-Zertifizierungen geben wird.

Gefragter Staat

Beim Onlinekongress 2021 des Chaos Computer Club (CCC) stellte ReclaimYourFace das Ergebnis von 195 Anfragen zu Videoüberwachung im öffentlichen Raum vor, die sie über Fragdenstaat.de (auf Grundlage des Informationsfreiheitsgesetzes des Bundes und mehrerer Länder) an Polizeibehörden, Innenministerien und Datenschutzbehörden gesendet hatten. Nur auf 70 Anfragen erfolgte überhaupt eine Reaktion. 13 Angefragte lehnten eine Auskunft ab, 31 Anfragen wurden weiterverwiesen oder waren ergebnislos. Nur auf 26 Anfragen (13%) wurden Informationen herausgegeben, teilweise sehr ausführlich. In einigen Bundesländern wurden jedoch hohe Gebühren verlangt, zog sich der Vorgang über mehrere Monate hin oder kam erst auf Intervention von Datenschutzbeauftragten ins Rollen.

Kein besonders rühmliches Bild.

Secorvo News

T.I.S.P. und IT Security Insights

Wir hoffen, die nächsten Seminare wieder wie geplant in unseren Räumen in Karlsruhe durchführen zu können – das Zertifizierungsseminar T.I.S.P. (**07.–11.03.2022**) und das T.I.S.P.-Update-Seminar IT Security Insights (**15.–17.03.2022**) – und freuen uns auf Ihre Anmeldung.

Willkommen bei den Quanten

Der amerikanische Forscher Peter Shor schockte 1997 die Welt mit der Publikation eines Algorithmus', mit dem die Zerlegung sehr großer Zahlen in ihre Primfaktoren auf Quantencomputern in polynomieller Zeit gelingt – damit könnte man die wichtigsten der heute verwendeten asymmetrischen Kryptoverfahren brechen. Wie aber funktionieren Quantencomputer eigentlich? Warum lässt sich mit ihnen das „Faktorisierungsproblem" lösen? Sind auch symmetrische Verfahren wie der AES gefährdet? Bis wann müssen wir Ersatzverfahren verfügbar haben? Worauf sollten wir schon heute achten?

Um diese und weitere Fragen rund um Quantencomputer dreht sich das Expertengespräch von Professor Dr. Müller-Quade (KASTEL), Oliver Winzenried (WIBU-SYSTEMS) und Dirk Fox (Secorvo Security Consulting) auf dem Jahresstartevent der KA-IT-Si am **03.02.2022**. Die limitierten Präsenzplätze im jüngst eröffneten IT Security Club des „House of IT Security" der Karlsruher WIBU Systems sind bereits ausgebucht, aber Sie können das Expertengespräch per Livestream miterleben (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2022	
01.-02.02.	18. Deutscher IT-Sicherheitskongress (BSI, virtuell)
03.02.	KA-IT-Si-Event „Willkommen bei den Quanten“ (KA-IT-Si, hybrid)
02.-04.02.	29. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, virtuell)
März 2022	
07.-11.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
15.-17.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
23.03.	31. ID:SMART Workshop (Fraunhofer SIT, virtuell)
25.03.	Datenschutztag 2022 (COMPUTAS, Köln)
28.-31.03.	DFRWS EU 2022 (DFRWS, hybrid)
29.-31.03.	secIT 2022 (Heise Medien, Hannover)
April 2022	
05.-08.04.	GI Sicherheit 2022 (KIT, Karlsruhe)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-27.04.	Datenschutztage 2022 (FFD, hybrid)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Nicolas Blum, Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Nils Wiedemann

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2022



Zutatenverzeichnis

Ende des kommenden Jahres feiert die Regelung ihren 40. Geburtstag: Seit dem 26.12.1983 kennt das deutsche Lebensmittelrecht die Pflicht, jedem Produkt auf der Verpackung eine Zutatenliste in absteigender Reihenfolge der Zugabemenge beizufügen. Dank dieser Transparenz kennen Verbraucher seitdem die Bestandteile ihrer Nahrungsmittel und können somit Unverträglichkeiten vermeiden und die Qualität angebotener Lebensmittel einschätzen. Das ist sicherlich eine der wichtigsten Regelungen des Lebensmittelrechts, die zweifellos bereits viele Menschen mit schweren Allergien das Leben gerettet hat.

Leider sind wir in der Informationstechnik von einer solchen Offenheit weit entfernt. Dabei mixt inzwischen jeder Softwareentwickler unzählige Bibliotheken und Codefragmente beliebiger Provenienz in „seine" Programme – dank Cloud-Services, Open Source und offenen APIs mit steigender Tendenz. Kaum eine Entwicklungsumgebung, die ohne eigene Bibliotheksfunktionen daherkommt, kaum ein Softwareprodukt, das keinen Open Source-Code unter seiner Haube verbirgt. Letzteres unterliegt zwar klaren Offenlegungsregeln, die aber bei weitem nicht von jedem Hersteller beachtet werden.

Das Ergebnis dieser wachsenden Code-Mehrfachnutzung kann ein erheblicher Risikoanstieg sein: Wird ein Sicherheits-Bug in einer der verwendeten Bibliotheken oder Open-Source-Code-Basen bekannt, erfahren Nutzer davon nur, wenn der Hersteller sie warnt und Patches liefert. Das setzt allerdings voraus, dass der Hersteller die verwendeten Code-Teile sauber dokumentiert – und auch seine „Code-Zulieferer" dasselbe bei ihrem Programmcode tun.

Verlass ist darauf keineswegs: Wird ein Bug bekannt, geht die Suche los – und die Schwachstelle wird in einigen Anwendungen erst nach Wochen gefixt. Wäre der Hersteller zur Dokumentation seiner Code-Zutaten verpflichtet, könnte der Käufer das diesbezügliche Risiko schon vor dem Erwerb einschätzen.



Inhalt

Zutatenverzeichnis

Security News

TCF nicht DSGVO-konform

Nun auch Frankreich „ohne"

IT-GSK 2022 in XML

Patches erscheinen früher

US-Überwachungsrecht begutachtet

CDN und Datenschutz

Pfeift, gepfiffen, verpfiffen

Secorvo News

Verstärkung im Datenschutz

Secorvo Seminare

Lesen bildet II

Expertengespräch verpasst?

Geld oder Leben

Veranstaltungshinweise

secorvo
security consulting

Security News

TCF nicht DSGVO-konform

Die belgische Datenschutzbehörde (APD) hat am 02.02.2022 entschieden, dass das Transparency and Consent Framework (TCF) der IAB Europe gegen die DSGVO verstößt. Das TCF ordnet mittels eines sogenannten TC-Strings und eines Consent-Cookies das Verhalten des Nutzers dessen IP-Adresse zu und ermöglicht die Versteigerung zielgruppenspezifischer Werbeplätze. Nach Ansicht der ADP mangelt es dabei an einer Rechtsgrundlage, transparenten Informationen sowie ausreichenden technischen und organisatorischen Maßnahmen. IAB Europe sei zudem ihren Pflichten als Verantwortliche nicht nachgekommen. IAB will die Entscheidung rechtlich prüfen, zeigt sich aber optimistisch, dass die Verstöße behoben werden können. Sollte IAB nicht nachbessern, bleibt möglicherweise das RTB-Protokoll von Google als einzige technische Alternative.

Die Entscheidung gilt nach dem „one-stop-shop"-Prinzip für die gesamte Europäische Union und dürfte sich erheblich auf die digitale Werbewirtschaft auswirken.

Nun auch Frankreich „ohne"

Nach der österreichischen Datenschutzbehörde (siehe SSN 01/2022) untersagte am 10.02.2022 auch die französische Datenschutzbehörde CNIL Webseiten-Betreibern die Nutzung von Google Analytics. Zur Begründung führt die CNIL aus, dass die von Google getroffenen Maßnahmen nicht ausreichten, um das fehlende Schutzniveau in den USA auszugleichen und daher Art. 44 DSGVO verletzt sei. Betreibern empfiehlt sie, Dienste zu verwenden, die nur anonyme statistische Daten produzieren, um die sonst notwendige Einwilligung zu vermeiden. Zudem kündigte sie ein Evaluierungsprogramm an, mit dem festgestellt werden soll, welche Lösungen von der Einwilligungspflicht ausgenommen sind.

Da die für Google Europa zuständige Datenschutz-Aufsichtsbehörde in Irland nicht aktiv wird, treibt derzeit die Schrems-Initiative noyb mit Beschwerden alle anderen europäischen Aufsichtsbehörden in Sachen Google Analytics vor sich her. Eine Entscheidung der deutschen Datenschutzaufsicht ist wohl nur noch eine Frage der Zeit. Daher empfehlen wir dringend einen Wechsel zu europäischen Anbietern – oder eine effektive Anonymisierung.

IT-GSK 2022 in XML

Am 08.02.2022 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) das IT-Grundschutz-kompendium in der Version 2022 veröffentlicht. Wie jedes Jahr finden sich im neuen Kompendium redaktionelle und inhaltliche Änderungen sowie Ergänzungen, darunter vor allem neue Bausteine zur „Containerisierung" und Fernwartung. Eine wichtige Neuerung ist, dass das BSI das Kompendium nun nicht mehr nur in traditionellen „Lese-Formaten" wie PDF bereitstellt, sondern mit der Veröffentlichung als DocBook-XML-Version Anwendern die Möglichkeit gibt, recht einfach mit eigenen Tools den operativen Umgang mit den Bausteinen zu verbessern.

Patches erscheinen früher

Am 10.02.2022 wurden in Googles Project Zero Blog einige interessante Statistiken über die Behebung von gemeldeten Schwachstellen durch Herstellerpatches veröffentlicht. Während 2018 noch durchschnittlich 90 Tage von der Meldung bis zur Behebung einer Schwachstelle verstrichen, waren es 2021 im Schnitt nur noch 52 Tage. Diese deutlich beschleunigte Bereitstellung von Patches ist sehr zu begrüßen, sie hilft jedoch nur, wenn die Patches auch zügig eingespielt werden.

Wir empfehlen: Patchen Sie so schnell wie möglich – und sehen Sie Methoden zur Zurückführung auf einen stabilen Betriebszustand sowie Ersatzmaßnahmen vor, falls es zu Störungen kommt. Verzögerungen durch ausgiebige Tests der Patches sollte man nach Möglichkeit vermeiden – das Risiko eines Angriffs ist inzwischen größer als das eines durch einen Patch verursachten Ausfalls. Schließlich drohen bei verspätetem oder unterlassenem Patchen Datenschutz-Bußgelder (vgl. SSN 11/2021).

US-Überwachungsrecht begutachtet

Die Datenschutzkonferenz (DSK) hat am 25.01.2022 ein Gutachten von Stephen I. Vladeck zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse veröffentlicht. Das Gutachten zeigt detailliert die Anwendungsbereiche der einzelnen amerikanischen Gesetze und die theoretisch möglichen Rechtsbehelfe auf, was insbesondere für Transfer Impact Assessments (TIA) bei Datenübermittlungen in die USA relevant sein dürfte. Laut DSK sind wesentliche Befunde, dass die Anwendbarkeit der bereits im Schrems-II-Urteil behandelten Section 702 FISA sehr weit ist und dass die Aspekte Extraterritorialität und Rechtsschutzmöglichkeiten behandelt werden. Diese knappen Ausführungen der DSK werden dem Detailgrad des Gutachtens ebenso wenig gerecht, wie die teilweise verbesserungsbedürftige deutsche Übersetzung.

Die Datenschutz-Aufsichtsbehörden bewerten derzeit die Konsequenzen aus dem Gutachten. Eine ist zweifellos, dass bei Übermittlungen in die USA immer an ein TIA gedacht werden muss.

CDN und Datenschutz

Ein Content Delivery Network (CDN) hostet Kopien von Webseiten, um deren Laden zu beschleunigen. Der Nutzung stehen jedoch erhebliche datenschutzrechtliche Bedenken entgegen, da ein Hosting auf global verteilten Servern unweigerlich zur Problematik der Zulässigkeit einer Drittlandsübermittlung nach Art. 44 ff. DSGVO führt, wenn über das CDN personenbezogene Daten wie IP-Adressen übermittelt werden.

Insbesondere amerikanischen Anbietern fehlt in der Regel ein angemessenes Datenschutzniveau. So entschied am 01.12.2021 das VG Wiesbaden, dass ein Cookie-Dienst, der für das Abrufen eines Einwilligungsskripts auf das CDN einer US-Firma zurückgreift, wegen fehlender Einwilligung rechtswidrig sei. Eine Information in der Datenschutzerklärung genügt nicht.

Pfeift, gepfiffen, verpfiffen

Bis 17.12.2021 hätte die EU-Richtlinie 2019/1937, besser bekannt als „Whistleblower-Richtlinie", in deutsches Recht umgesetzt werden müssen. Dies ist bisher nicht erfolgt, und wann die neue Bundesregierung die Umsetzung angeht, ist nicht bekannt.

Die Regelungen betreffen Meldungen von Verstößen gegen ausgewählte Bestimmungen des EU-Rechts; sie richten sich sowohl an Unternehmen als auch an den öffentlichen Sektor. Bemerkenswert ist, dass eine von einem Hinweis betroffene Person im Vergleich zum Hinweisgeber eher dürftig geschützt wird. Zwar legt Art. 22 fest, dass deren Identität während der Untersuchung geschützt und selbstverständliche Rechte wie der Anspruch auf wirksame Rechtsbehelfe und ein faires Gerichtsverfahren gewährt werden sollen. Allerdings trägt die betroffene Person die Beweislast dafür, dass erteilte Hinweise falsch sind. Der Hinweisgeber soll bei Falschinformationen nur dann sanktioniert werden, wenn er von der Unrichtigkeit wusste. Immerhin weist Art. 16 Abs. 2 darauf hin, dass der Hinweisgeber gegenüber der betroffenen Person offengelegt werden muss, damit diese von ihren Verteidigungsrechten Gebrauch machen kann.

Secorvo News

Verstärkung im Datenschutz

Wir freuen uns über eine erneute Verstärkung unseres Datenschutz-Teams: Im Februar konnten wir den Volljuristen Christian Blaicher für das Secorvo-Team gewinnen. Herzlich willkommen!

Secorvo Seminare

Ab März finden unsere Präsenz-Seminare nach mehrmonatiger Pause endlich wieder statt. Freie Plätze gibt es noch auf unserem viertägigen PKI-Seminar (**25.–28.04.2022**). Wir freuen uns auf Ihre Teilnahme!

Lesen bildet II

Wir laden Sie herzlich zu unserem zweiten „Literarischen KA-IT-Si-Kabinett" am **10.03.2022** ein. An diesem Abend werden wir Ihnen weitere Werke der (Welt-)Literatur vorstellen, die sich mit dem Thema Datenschutz oder Datensicherheit beschäftigen und die Sicherheits- und Datenschutzexperten daher gelesen haben „müssen". Dabei freuen wir uns nicht nur auf Ihre Anmeldung, sondern auch über Ihre persönliche Rückmeldung: Welche weiteren Bücher gehören Ihrer Ansicht nach unbedingt auf diese „Liste"?

Expertengespräch verpasst?

Sie haben die Jahresauftaktveranstaltung „Willkommen bei den Quanten" der KA-IT-Si am 03.02.2022 verpasst oder möchten sich das Expertengespräch zur Bedrohung heutiger Kryptosysteme durch Quantencomputer noch einmal ansehen? Wir haben die Veranstaltung aufgezeichnet und auf unserem YouTube-Kanal veröffentlicht. Im Gespräch diskutieren Professor Dr. Müller-Quade (KASTEL), Oliver Winzenried (WIBU-SYSTEMS) und Dirk Fox (Secorvo Security Consulting) darüber, wie ernst die Bedrohung durch Quantencomputer genommen werden muss und was das für Hersteller und Anwender kryptografischer Systeme bedeutet.

Geld oder Leben

Wie erpressbar sind deutsche Unternehmen und Institutionen? Wer bei einem gezielten Hacker-Angriff seine gesamten Daten verliert und auf einen Schlag ohne IT-Dienste dasteht, wird geneigt sein, nahezu jeden Preis für die Wiederherstellung seiner Infrastruktur zu zahlen. Ein Unternehmen, das genau das nicht getan hat, ist das in Baden-Württemberg ansässige Familienunternehmen Pilz. Die Unternehmensleitung hat sich 2019 trotz eines Totalausfalls der gesamten IT dagegen entschieden, den Kriminellen Lösegeld zu zahlen – und ist durch eine harte Zeit gegangen.

Was Pilz aus diesem einschneidenden Erlebnis gelernt hat und anderen Unternehmen und Unternehmern mitgeben möchte, wird Herr Thomas Pilz, geschäftsführender Gesellschafter der Pilz GmbH & Co. KG, auf dem KA-IT-Si-Event am **07.04.2022** vorstellen. Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2022	
07.-11.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.03.	KA-IT-Si-Event „Lesen bildet II“ (KA-IT-Si, virtuell)
23.03.	31. ID:SMART Workshop (Fraunhofer SIT, virtuell)
24.-26.03.	ShmooCon 2022 (The Schmoo Group, Washington/US)
25.03.	Datenschutztag 2022 (COMPUTAS, Köln)
28.-31.03.	DFRWS EU 2022 (DFRWS, hybrid)
29.-31.03.	secIT 2022 (Heise Medien, Hannover)
April 2022	
05.-08.04.	GI Sicherheit 2022 (KIT, Karlsruhe)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-27.04.	Datenschutztage 2022 (FFD, hybrid)
Mai 2022	
03.-04.05.	Security Forum 2022 (Hagenberger Kreis, Hagenberg/AT)
05.05.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
09.-13.05.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.-13.05.	European Identity & Cloud Conference 2022 (KuppingerCole, Berlin/virtuell)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Nicolas Blum, Milan Burgdorf, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Nils Wiedemann

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

März 2022



Warnung

Am 15.03.2022 veröffentlichte das BSI eine Warnung vor dem Einsatz von Kaspersky-Virenschutzprodukten – und löste damit in den IT-Abteilungen vieler Unternehmen und Behörden hektische Betriebsamkeit aus.

Natürlich stimmt das Argument, dass die hohen lokalen Berechtigungen eines Virenschutzprodukts, das zudem regelmäßig große Datenmengen (Signaturdateien) nachlädt, sich für einen (nachrichtendienstlichen) IT-Angriff geradezu anbieten. Nur: Kein Geheimdienst der Welt, der einen solchen Angriff plant, würde damit wochenlang warten – vor „Cyberattacken" aus Russland hatte das BSI bereits im Februar gewarnt.

Die Empfehlung, Kaspersky-Produkte zu ersetzen, greift damit viel zu kurz. Wer solche Angriffe befürchtet, sollte sofort seine gesamte Infrastruktur analysieren – denn wenn sie geplant waren, muss man davon ausgehen, dass bereits Schadsoftware auf diesem Weg installiert wurde. Davon ist in der BSI-Warnung jedoch nichts zu lesen.

Auch ist unverständlich, warum sich die Warnung auf Kaspersky-Produkte beschränkt. Alle relevanten Geheimdienste der Welt bauen seit Jahr(zehnt)en Cybercrime-Abteilungen auf – und warten für ihre Attacken nicht auf einen begleitenden physischen Krieg. Neben Russland sind auch China, Israel und die USA sowohl technisch in der Lage als auch gesetzlich autorisiert, solche Angriffe in „Friedenszeiten" durchzuführen. Wer Kaspersky verbannt, darf auch keine Checkpoint-Firewalls, Huawei-Smartphones, Lenovo-Laptops, Intel-Prozessoren und Cisco-Router einsetzen – und sollte besser auf die Nutzung von Microsoft-Programmen, Apple-Apps und Google-Diensten verzichten.

Nicht möglich, sagen Sie? Richtig. Daher kommt es darauf an, bei der Angriffserkennung seine Hausaufgaben zu machen – damit man im Falle eines solchen Falles wenigstens zügig reagieren kann.



Inhalt

Warnung

Security News

Behördliche Unterstützung

Interessenskonflikte des DSB

Kali Linux 2022

Data-Act-Entwurf

#airtagged

Signatur als werbefreie Zone

Secorvo News

BSI Vorfall-Experte

Wer besitzt mein Smartphone?

Veranstaltungshinweise

secorvo
security consulting

Security News

Behördliche Unterstützung

Am 24.02.2022 veröffentlichte das BSI einen „Maßnahmenkatalog Ransomware“, in dem eine Vielzahl von ineinander greifenden Schutzmaßnahmen beschrieben wird. Das erste Kapitel enthält eine Checkliste mit konkreten Prüfpunkten zur Selbsteinschätzung und Beispiele, wie die Anforderungen des Maßnahmenkatalogs zu erfüllen sind.

Das ist wahrscheinlich hilfreich. Wie Behörden aber nicht nur Dokumente erzeugen, sondern auch konkrete Unterstützungsdienste erbringen können, zeigt die amerikanische Cybersecurity & Infrastructure Security Agency (CISA): Sie bietet Organisationen und Regierungseinrichtungen eine Reihe von kostenfreien Services zum Schutz vor Angriffen. So kann man über das Internet erreichbare Netzbereiche und Webanwendungen einer automatisierten Überprüfung auf typische Schwachstellen unterziehen lassen oder mit dem auf GitHub zum Download bereitgestellten Cyber Security Evaluation Toll (CSET) ein Ransomware Readiness (Self-) Assessment (RRA) durchführen (siehe SSN 7/2021). Diese Angebote ersetzen keinen Penetrationstest, sind aber eine einfache Maßnahme, um offensichtliche Mängel zu identifizieren und abzustellen – und damit ein wichtiger Beitrag zu einer wirkungsvollen Prävention.

Interessenskonflikte des DSB

Am 16.12.2021 verhängte die belgische Datenschutzbehörde aufgrund eines Interessenskonflikts des Datenschutzbeauftragten einer Bank ein Bußgeld von 75.000 €. Der interne Datenschutzbeauftragte war zugleich Leiter von drei Abteilungen, die das operative Risikomanagement, das Informationsrisikomanagement sowie eine Sonderermittlungsstelle umfassten. In seiner Funktion sei er nicht nur beratend oder überwachend tätig geworden, sondern habe aufgrund seiner Befugnisse über die Verarbeitung personenbezogener Daten entscheiden können. Nach Auffassung der belgischen Behörde darf ein Datenschutzbeauftragter keine Position innehaben, die Mittel und Zweck der Verarbeitung von personenbezogenen Daten festlegen kann.

Interessenskonflikte können durch eine sorgfältige Zuweisung von Aufgaben und vertragliche Regelungen vermieden werden. Sobald sich ein Datenschutzbeauftragter selbst überwachen müsste, sind Interessenskonflikte unvermeidbar. Die Entscheidung der belgischen Behörde ist daher nicht überraschend und sollte zum Anlass genommen werden, die sonstigen Aufgaben und Befugnisse des internen Datenschutzbeauftragten zu überprüfen.

Kali Linux 2022

Pünktlich zum Valentinstag kündigte Kali das neue Release „Kali Linux 2022.1“ an. Neben visuellen Änderungen wie einheitlichen BIOS/UEFI Boot-Menus und „professionelleren“ Shell-Prompts ziehen neue Tools in die offiziellen Repositories ein – eine umfangreiche Ergänzung zum bisherigen Toolset und eine Alternative zu gängigen Tools in den Bereichen OSINT, Port- und Schwachstellenscannern sowie Proxies. Zusätzlich wurde das „Kali Everything Image“ als optionaler Download eingeführt, ein Komplettpaket mit allen möglichen vorinstallierten Tools. Für bestimmte Situationen ist dieses Angebot sicherlich nützlich – auch die Hacking-Distribution BlackArch Linux bietet seit 2020 ein derartiges Komplettpaket an. Mit rund der Hälfte der Download-Größe (ca. 9.4 GB) ist das „Kali Everything Image“ eine zumindest platzsparende Alternative zum „Black Arch Full ISO“ (ca. 18 GB).

Data-Act-Entwurf

Die Europäische Kommission hat am 23.02.2022 einen Vorschlag zur Data-Act-Verordnung vorgelegt. Die Verordnung ist Teil einer groß angelegten Datenstrategie der Europäischen Union, die unter Wahrung von Datenschutzstandards und Verbraucherrechten die branchenübergreifende Nutzung von Daten fördern und die Vormachtstellung großer Konzerne zugunsten von KMUs und vor allem der Nutzer eindämmen soll.

Der Data Act ist bei der Verarbeitung personenbezogener Daten neben der DSGVO anwendbar, sodass Betroffene ihre Rechte aus beiden Verordnungen geltend machen können. Dabei sind die Rechte aus dem Data Act umfassender als die der DSGVO, da Daten nicht nur einmalig, sondern kontinuierlich in Echtzeit zur Verfügung gestellt werden sollen.

Die Zielsetzung des Entwurfs darf als gelungen, die Umsetzung muss aber als nicht ausreichend bewertet werden. Die Regelung des behördlichen Zugriffs ist schwammig und wird als rechtsstaatlich problematisch und als intensiver Eingriff in die Vertragsfreiheit sowie als eine Gefährdung der Wettbewerbsfähigkeit europäischer Unternehmen kritisiert. Auch wenn der Entwurf nachgebessert werden sollte, ist bereits jetzt erkennbar, dass die Auswirkungen der Verordnung auf die Wirtschaft in jedem Fall erheblich sein werden.

secorvo
security consulting

#airtagged

Seit dem 30.04.2021 verkauft Apple münzgroße Anhänger („AirTags"), die von Apple-Geräten im Umkreis von 10-50 m via Bluetooth und vom iPhone 11+ auf wenige cm genau geortet werden können. Das funktioniert über beliebige Distanzen weltweit: Entdeckt ein iPhone ein fremdes AirTag, schickt es die Geo-Koordinaten in die iCloud, wo sein Besitzer mit Apples „Find My"-App die Bewegung des AirTags auf einer Karte verfolgen kann. Die Idee ist bestechend: Einfach einen der rund 25 € teuren Anhänger am Hundehalsband, unter dem E-Bike-Sattel oder am Schlüsselbund befestigen, und Suchen ist Finden. Offenbar billigend in Kauf genommen hat Apple, dass sich damit auch fremde Habseligkeiten „markieren" lassen. So wurde z. B. am 15.12.2021 über AirTags berichtet, die an neuen Autos angebracht werden, um sie unbemerkt zu verfolgen – und einen guten Ort für einen Diebstahl abzupassen. Dass AirTags, in einer fremden Hand- oder Jackentasche versenkt, auch zu einem wertvollen Werkzeug für Stalker werden, ist inzwischen ebenfalls bekannt. Unterstützt wird der Missbrauch dadurch, dass die Identifikation des Eigners zu dessen Schutz technisch verhindert wird.

Zwar meldet sich ein AirTag mit einem Ton, wenn es acht bis 24 Stunden keinen Kontakt zum iPhone seines Besitzers hatte – aber das kann überhört oder mit einer einfachen Bohrung ausgeschaltet werden – auch werden inzwischen „Silent AirTags" mit deaktiviertem Lautsprecher angeboten. Die von Apple publizierte App zur Feststellung von längere Zeit in der Nähe befindlichen fremden AirTags warnt nach mehreren Stunden – befindet sich das „Opfer" aber mit Unterbrechungen in der Nähe des AirTags oder besitzt es kein iPhone, funktioniert der Alarm nicht. Offenbar fällt dieser Missbrauch sogar in eine „Strafbarkeitslücke", wie Lena Leffer und Michelle Weber in der DuD 3/2022 nachweisen.

Am 21.02.2022 veröffentlichte Fabian Bräunlein den Code für einen „Stealth AirTag Clone" auf Basis eines ESP32, der alle Schutzfunktionen des „Find My"-Protokolls von Apple umgeht. Und er macht klar, dass nicht die AirTags das eigentliche Problem sind – sondern die Tracking-Infrastruktur, die Apple mit dem „Find My"-Netzwerk schon vor Jahren etabliert hat.

Signatur als werbefreie Zone

Am 15.09.2021 befand das Kammergericht Berlin den Zusatz in der E-Mail-Signatur eines Unternehmens „[...] Organisiert, denkt mit, erledigt. Nutzen Sie www.[...].de" als unerlaubte Werbung im Sinne des § 7 UWG und gestand dem Kläger einen Unterlassungsanspruch gegen das Unternehmen zu. Der geringe Umfang dieses Zweizeilers und die Positionierung am Ende der Nachricht seien hier unerheblich: „Nach der Rechtsprechung des BGH" könne dieser kleine Zusatz auch nicht durch den vorangestellten, legitimen Inhalt der E-Mail gerechtfertigt werden. Auch diese sehr geringfügige Beeinträchtigung sei generalpräventiv zu untersagen, um ein Um-sich-Greifen solcher Werbung durch Nachahmung zu verhindern.

In welchem Maß und Format Hinweise auf das eigene Unternehmen in der E-Mail-Signatur überhaupt zulässig sind, dazu bietet das rechtskräftige Urteil leider keine Anhaltspunkte. Immerhin sprach das Gericht der Sache eine „grundsätzliche Bedeutung" zu, d. h. das Gericht sieht eine endgültige Klärung durch den Bundesgerichtshof für zumindest wünschenswert an. Bis dahin sollten E-Mail-Signaturen kritisch auf eine mögliche Werbewirkung überprüft werden.

Secorvo News

BSI Vorfall-Experte

Die „Einschläge kommen näher" – daher gewinnt die Vorbereitung auf einen Sicherheitsvorfall als Teil des Sicherheitsmanagements an Bedeutung. Seit dem vergangenen Jahr bietet das BSI eine Zertifizierung zum „Vorfall-Experten" an. Voraussetzung ist die Teilnahme an einer Aufbau-Schulung auf der Grundlage des Leitfadens des BSI zur Reaktion auf IT-Sicherheitsvorfälle.

Die dreitägige Aufbauschulung zum BSI Vorfall-Experten bietet Secorvo erstmals vom **17. bis 19.05.2022** an. Wir freuen uns auf Ihre Anmeldung – natürlich auch zum PKI-Seminar (**25.–28.04.2022**) oder dem Vorbereitungsseminar auf die T.I.S.P.-Zertifizierung (**09.–13.05.2022**).

Wer besitzt mein Smartphone?

Auch wenn wir uns kaum noch daran erinnern können, wie wir ohne sie klarkamen: Smartphones gibt es erst seit 15 Jahren. Genauso alt wie das Smartphone ist die Geschichte der Smartphone Hacks – von den ersten Jailbreaks über die Celebrity Nudes bis hin zu kommerzieller und staatlicher Spyware.

Anhand von Attack Trees und Live-Hacking-Demos zeigen Ihnen Armin Harbrecht und Maximilian Stauß (aramido) beim kommenden KA-IT-Si-Event am **19.05.2022**, wie Smartphones angegriffen werden. Dieses Verständnis ist Voraussetzung für effektive Schutzmaßnahmen. Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" – bei schönem Wetter auf der herrlichen Dachterrasse von aramido (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2022	
05.-08.04.	GI Sicherheit 2022 (KIT, Karlsruhe)
07.04.	„Geld oder Leben“ (KA-IT-Si, Karlsruhe)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-27.04.	Datenschutztage 2022 (FFD, hybrid)
Mai 2022	
03.-04.05.	Security Forum 2022 (Hagenberger Kreis, Hagenberg/AT)
05.05.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
09.-13.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.-13.05.	Blackhat Asia 2022 (Blackhat, hybrid)
10.-13.05.	European Identity & Cloud Conference 2022 (KuppingerCole, Berlin/virtuell)
10.-11.05.	BvD Verbandstage 2022 (BvD, Berlin)
16.-17.05.	23. Datenschutzkongress (EUROFORUM, Berlin)
16.-18.05.	Entwicklertag 2022 (VKSI, GI, ObjektForum, Karlsruhe)
17.-19.05.	BSI Vorfall-Experte – Aufbauschulung (Secorvo, Karlsruhe)
19.05.	„Wer besitzt mein Smartphone?“ (KA-IT-Si, Karlsruhe)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Nicolas Blum, Milan Burgdorf, Enes Erdoğan, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Nils Wiedemann

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2022



Cyber, Cyber, Cyberagentur

Mit der von der Bundesregierung 2020 gegründeten „Agentur für Innovation in der Cybersicherheit“ soll Deutschland „bei der Cybersicherheit im internationalen Vergleich die Führung, zumindest eine Spitzenposition übernehmen.“ Um das zu erreichen, soll sie Forschung und bahnbrechende Innovationen im Bereich der Cybersicherheit vorantreiben (Strategie 2022-2025). Bis 2023 stehen ihr dafür zunächst 280 Mio. € Steuergeld zur Verfügung. Wem hilft das? Seit 1991 gibt es das BSI mit inzwischen über 1.300 Mitarbeitern (Jahresetat 200 Mio. €), es forschen das Horst-Görtz-Institut für IT-Sicherheit in Bochum, das Helmholtz-Zentrum für Informationssicherheit in Saarbrücken, die KASTEL Security Research Labs am Karlsruher KIT und seit 2004 das Fraunhofer Institut für Sichere Informationstechnologie an der TU Darmstadt sowie die Lehrstühle für IT-Sicherheit an 50 deutschen Hochschulen und Universitäten und die Kompetenzzentren für IT-Sicherheit der 16 Bundesländer. An Institutionen und Agenturen mangelt es nun wirklich nicht.

Die Herausforderungen der Informationssicherheit liegen jedoch nicht in fehlenden Technologien, die auf zauberhafte Weise Sicherheit produzieren: Es mangelt an der Umsetzung bekannter Schutzmaßnahmen. Schließlich ist in der ISO 2700x, dem BSI IT-Grundschutz und vielen weiteren Standards ordentlich definiert, wie Unternehmen sich wirksam schützen können. Doch es fehlen nicht zuletzt Experten für die Umsetzung. Wie sinnvoll ist es, weitere Technologien am Ende der Fahnenstange zu erforschen, wenn die Stange selbst wackelig im Morast steckt? Wenn Hersteller mangels Produkthaftung Security Engineering und sichere Softwareentwicklung nicht ernst nehmen? Ein Auto braucht kein Radar zur Fußgängererkennung, wenn nicht mal die Bremsen zuverlässig funktionieren. Da könnte schon helfen, wenn Kinder bereits in der Grundschule lernen würden, besser nicht auf jeden Anhang zu klicken.



Inhalt

Cyber, Cyber, Cyberagentur

Security News

Cloud-Ausfallerscheinungen

Drum prüfe, wer prüfen lässt

Cookie-Banner

Bike Scamming

Neuer Auskunftsanspruch

Post-Corona-Aufräumarbeiten

NEO-Innovationspreis

Secorvo News

Der frühe Vogel ...

Wer besitzt mein Smartphone?

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Cloud-Ausfallerscheinungen

Den meisten Verantwortlichen, die Dienste und Anwendungen „in die Cloud“ auslagern, dürfte klar sein, dass man damit Risiken verlagert: Der Ausfall eigener Systeme wird weniger relevant, und eigene Maßnahmen zur Absicherung von Systemen und Räumlichkeiten können eingespart werden.

Im Gegenzug begibt man sich in eine Abhängigkeit: Bei Ausfall der Internetanbindung oder des Cloud-Anbieters selbst können die Dienste nicht genutzt werden. In den meisten Fällen wird man dieses Risiko tragen und in Kauf nehmen, dass ein Anbieter mal einzelne Stunden bis hin zu ein oder zwei Tagen nicht zur Verfügung steht.

Wie sieht es aber aus, wenn Dienste – wie am 05.04.2022 bei Atlassian – für bis zu zwei Wochen ausfallen? Welche Auswirkungen hat das auf die Geschäftsprozesse? Müssen Entwickler nach Hause geschickt werden, da sie ohne ihre Cloud-Werkzeuge keine Software entwickeln können? Gibt es zeitkritische Prozesse, die nicht mehr funktionieren, wenn ein Dienst länger nicht zur Verfügung steht? Werden möglicherweise Sicherheitsprobleme übersehen, wenn Alarmierungen aus der Cloud nicht mehr eingehen?

Gerade versteckte Abhängigkeiten in immer stärker miteinander verzahnten digitalen Prozessen werden bei einer oberflächlichen Risikobewertung leicht übersehen – je mehr Cloud-Dienste in Anspruch genommen werden, desto genauer und häufiger sollte die Risiko-Prüfung wiederholt werden. Zur Sicherheit sollte man außerdem „analoge“ Ersatzprozesse vorsehen, um größere Ausfall-Schäden zu verhindern.

Drum prüfe, wer prüfen lässt

Der von Google angebotene Dienst VirusTotal überprüft hochgeladene Dateien kostenlos mit etwa 70 verschiedenen Antiviren-Programmen. Doch nur wenige Nutzer dürften zuvor die Benutzerhinweise gelesen haben, in denen darauf hingewiesen wird, dass keine personenbezogenen Daten hochgeladen werden sollen.

Am 15.03.2022 warnte das BSI vor möglichen Datenabflüssen bei VirusTotal, wenn statt Datei-Hashwerten beispielsweise unternehmensinterne Dokumente oder E-Mails hochgeladen werden. Neben den unternehmenseigenen Vorgaben zu Datenschutz und Informationssicherheit sind bei der Nutzung das Geschäftsgeheimnisgesetz und die DSGVO zu beachten.

Das kann auch für Antiviren-Programme gelten, bei denen die Virenerkennung cloudbasiert erfolgt. Hat der Hersteller seinen Sitz außerhalb der EU, müssen die hohen rechtlichen Anforderungen an eine Übermittlung personenbezogener Daten in Drittstaaten (wie bspw. die USA) erfüllt sein.

Cookie-Banner

Auf heutigen Webseiten sind (nervtötende) Cookie-Banner allgegenwärtig. Wer keine Cookies möchte, dem wird die Ablehnung meist obendrein durch „Dark Pattern“-Techniken erschwert, mit denen Besucher durch entsprechende Gestaltung der Banner dazu bewegt werden sollen, gegen ihren Willen eine Einwilligung zu erteilen. Um dieser Entwicklung entgegenzuwirken hat das European Data Protection Board (EDBP) am 15.03.2022 Richtlinien zur korrekten Bannergestaltung beschlossen.

Zuvor hatte die französische Datenschutzaufsicht CNIL am 31.12.2021 wegen eines zu umständlichen Verfahrens zur Cookie-Ablehnung ein 150-Mio.-€-Bußgeld gegen Google verhängt. In dieselbe Kerbe schlägt jetzt auch die Hamburgische Datenschutzaufsicht. Am 05.04.2022 forderte Thomas Fuchs (HmbBfDI) für Cookie-Banner einen „Alles ablehnen“-Knopf: Eine wirksame Einwilligung läge nur dann vor, wenn Zustimmung und Ablehnung gleichermaßen schnell und einfach zugänglich seien.

Doch auch diese Forderung greift noch zu kurz. Denn tatsächlich sind Cookie-Banner eine absurde Degeneration der datenschutzrechtlichen Einwilligung. Stellen Sie sich vor, in Ihrem örtlichen Supermarkt lägen ab sofort mehrere Packungen Kekse in jedem Einkaufswagen, die Sie vor Einkaufsbeginn aus dem Wagen herausnehmen müssten, wenn Sie sie nicht kaufen wollen. Genauso zwingen Cookie-Banner Seitenbesucher den Aufwand einer aktiven Ablehnung auf – anstatt bei Ignorieren des Banners automatisch von einer nicht erteilten Einwilligung auszugehen. Tatsächlich ist zu wünschen, dass die Aufsichtsbehörden bei Cookie-Bannern noch eine deutlich härtere Gangart wählen.

Bike Scamming

Schon am 07.08.2021 hatte die New York Post über Scamming-Angriffe auf das Buchungsverfahren der in New York verbreiteten City Bikes berichtet, nachdem der Angriff kurz zuvor bei Reddit beschrieben worden war. Die Attacke ist geradezu trivial und kommt gänzlich ohne IT aus: Zum Freischalten des Mietrads muss der Nutzer den auf dem Rad aufgeklebten QR-Code mit der Buchungs-App einscannen. Klebt man den QR-Code eines Rads auf ein anderes, kann man „sein“ Rad durch einen anderen Kunden (auf dessen Kosten) freischalten lassen.

Dieser simple Scamming-Angriff funktioniert bei allen Sharing-Systemen, bei denen die Identifikation

des Fahrzeugs über einen aufgebrachten Code erfolgt – eine verbreitete Methode übrigens auch bei E-Scootern. Es lohnt also, sich vor Freischalten des Fahrzeugs davon zu überzeugen, dass der aufgebrachte Code nicht überklebt oder ausgetauscht wurde.

Der geschilderte Angriff ist ein eindrückliches Beispiel dafür, dass die Optimierung des Benutzerkomforts schnell auf Kosten der Sicherheit geht. Da lohnt es, sich gelegentlich Einsteins Bonmot in Erinnerung zu rufen: „Mache die Dinge so einfach wie möglich. Aber nicht einfacher."

Neuer Auskunftsanspruch

Das am 01.12.2021 in Kraft getretene Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) regelt in §§ 21 ff. verschiedene Auskunftsansprüche. Neu ist § 21 Abs. 2 TTDSG, der Betreiber von Social-Media-Plattformen verpflichtet, Betroffenen mitzuteilen, wer als Verursacher einer Persönlichkeitsverletzung in Betracht kommt. Der Anspruch ist auch gegen Anbieter von Telemedien durchsetzbar, die zwar keinen Sitz in Deutschland haben, aber ihre Dienste auch in Deutschland erbringen.

Allerdings begrenzte das Schleswig-Holsteinische Oberlandesgericht am 23.03.2022 die Auskunft auf Bestandsdaten; Nutzungsdaten sind nicht mitzuteilen. Da die Verletzung der Auskunftspflicht nicht strafbewehrt ist und ohne Nutzungsdaten kein Nachweis für die Täterschaft vorliegt, ist der Anspruch in der Praxis eher ein stumpfes Schwert. Um wenigstens mittelbar an die Nutzungsdaten zu gelangen, bleibt den Betroffenen daher auch weiterhin nur der Weg über eine Strafanzeige.

Post-Corona-Aufräumarbeiten

Während der Corona-Pandemie wurden an vielen Orten – in Restaurants, Schulen, Krankenhäusern, Pflegeheimen und bei den Gesundheitsämtern – personenbezogene Daten von Bürgern erhoben und gespeichert. Nach Ablauf der jeweiligen Löschfrist, spätestens aber mit dem Wegfall der Rechtsgrundlagen wie den Corona-Verordnungen und dem Infektionsschutzgesetz sind diese Daten zu löschen.

Der Baden-Württembergische Landesdatenschutzbeauftragte Dr. Stefan Brink hat die wichtigsten Verarbeitungen in seiner Pressemitteilung vom 08.04.2022 („Zurück zur Freiheit") aufgelistet. Darin weist er auch darauf hin, dass Arbeitgeber (bis auf die Heil- und Pflegebranche) alle erhobenen Daten über den Impfstatus der Mitarbeiter unverzüglich löschen müssen – und kündigt stichprobenartige Überprüfungen an.

NEO-Innovationspreis

Die TechnologieRegion Karlsruhe hat den diesjährigen Innovationspreis NEO2022 dem Thema „Cybersecurity" gewidmet. Für den mit 20.000 € dotierten Preis können sich Unternehmen bundesweit bis zum 19.05.2022 online bewerben. Die Preisverleihung wird am 21.10.2022 in Karlsruhe stattfinden.

Secorvo News

Der frühe Vogel …

… fängt den Wurm: Das gilt auch für die Buchung Ihrer Weiterbildung. Melden Sie sich bereits jetzt zum T.I.S.P.-Seminar im September an (**19.–23.09.2022**) und bereiten Sie sich mit dem T.I.S.P.-Buch von Secorvo, das wir Ihnen nach Ihrer Anmeldung zusenden, entspannt darauf vor.

Bereits zertifizierten T.I.S.P.-Absolventen und erfahrenen Sicherheitsexperten bieten wir das Seminar IT Security Insights mit ausgewählten vertieften Beiträgen zu aktuellen Themen der IT-Sicherheit (**27.–29.09.2022**).

Wer eine gründliche Einführung in Theorie und Praxis von Public Key Infrastrukturen sucht, sollte sich unser viertägiges PKI-Seminar (**04.–07.11.2022**) im Kalender vermerken. Und Ende November bietet sich die nächste Möglichkeit, sich zum BSI Vorfall-Experten ausbilden zu lassen (**29.11.–01.12.2022**).

Die ausführlichen Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Wer besitzt mein Smartphone?

Auch wenn wir uns kaum noch daran erinnern können, wie wir ohne sie klarkamen: Smartphones gibt es erst seit 15 Jahren. Genauso alt wie das Smartphone ist die Geschichte der Smartphone Hacks – von den ersten Jailbreaks über die Celebrity Nudes bis hin zu kommerzieller und staatlicher Spyware.

Anhand von Attack Trees und Live-Hacking-Demos zeigen Ihnen Armin Harbrecht und Maximilian Stauß (aramido) beim kommenden KA-IT-Si-Event am **19.05.2022** um 18 Uhr, wie Smartphones angegriffen werden. Dieses Verständnis ist Voraussetzung für effektive Schutzmaßnahmen.

Die Veranstaltung führen wir hybrid durch. Die Vor-Ort-Plätze bei aramido sind bereits ausgebucht, aber für eine Online-Teilnahme können Sie sich noch anmelden (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2022	
10.-13.05.	Blackhat Asia 2022 (Blackhat, hybrid)
10.-13.05.	European Identity & Cloud Conference 2022 (KuppingerCole, Berlin/virtuell)
10.-11.05.	BvD Verbandstage 2022 (BvD, Berlin)
16.-17.05.	23. Datenschutzkongress (EUROFORUM, Berlin)
16.-18.05.	Entwicklertag 2022 (VKSI, GI, ObjektForum, Karlsruhe)
19.05.	Wer besitzt mein Smartphone? (KA-IT-Si, Karlsruhe)
30.05.-03.06.	Eurocrypt 2022 (IACR, Trondheim/NOR)
Juni 2022	
06.-10.06.	7th IEEE European Symposium on Security and Privacy (IEEE Computer Society, Genua/I)
06.-08.06.	OWASP Global AppSec (OWASP Foundation, Dublin/IRL)
20.-21.06.	DuD 2022 (COMPUTAS, Berlin)

Fundsache

Am 31.03.2022 wurde Version 4.0 des PCI DSS Standards veröffentlicht. Der Standard legt umfangreiche technische und organisatorische Anforderungen an Zahlungssysteme und Dienstleistungen fest. Diese wurden konkretisiert und verschärft. Die Änderungen zur Vorgängerversion 3.2.1 sind ebenso wie der Standard selbst auf Englisch, Deutsch und Portugiesisch verfügbar. Einige neue Anforderungen müssen PCI-kompatible Anbieter bis spätestens 31.03.2025 umsetzen.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Milan Burgdorf, Stefan Gora (Editorial), Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Mai 2022



Behind the Scenes

Die meisten Internet-Nutzer werden wissen, dass Webseiten, die sie besuchen, ihre Seitenaufrufe tracken – nicht selten ohne rechtswirksame Einwilligung. Weniger Internet-Nutzer werden wissen, dass die auf der Seite angezeigte Werbung meist von Dritten eingespielt wird. Doch die wenigsten Internet-Nutzer wissen, dass und wie die Werbung auf sie persönlich zugeschnitten wird.

Tatsächlich versteigern die meisten Portalseiten die Werbeplätze erst beim Aufruf der Seite über „Real Time Bidding“ (RTB) innerhalb weniger Millisekunden. Dazu schickt ein Werbeplatz-Anbieter (oder dessen Broker) über das OpenRTB-Protokoll einen „Ad Request“ an einen RTB-Exchange-Server, der daraus einen „Bid Request“ erzeugt und per Broadcast an alle Werbetreibenden verteilt. Dieses Datenpaket enthält alle bekannten Angaben über das die Seite aufrufende Gerät (u. a. Hersteller und Modell, Betriebssystem, IP-Adresse, Hash der MAC-Adresse und aktuelle GPS-Koordinaten) und den Nutzer (User ID, Geschlecht, Geburtsjahr, Keyword-Liste der Interessen und GPS-Daten des „Heimatstandorts“).

Nach einer am 14.05.2022 veröffentlichten Studie des Irish Council for Civil Liberties (ICCL) werden allein von Google Bid Requests an über 4.500 Unternehmen in den USA und über 1.000 in Europa geschickt – bei jedem deutschen Surfer im Schnitt im Minutentakt. Jeder Empfänger kann darüber benutzerbezogene Surf- und (bei mobilen Devices) Bewegungsprofile erstellen – eine Quelle, die in den USA auch bereits Sicherheitsbehörden nutzen.

Jeder Entwickler weiß, dass Real-Time-Bidding auch ohne die Verteilung der Anfragen funktioniert – ein Schelm, wer Arges dabei denkt. Vielleicht sollten wir uns ab und zu Immanuel Kants 1785 in der „Grundlegung der Metaphysik der Sitten“ formulierten praktischen Imperativ in Erinnerung rufen: „Handle so, dass du die Menschheit, sowohl in deiner Person, als in der Person eines jeden andern, jederzeit zugleich als Zweck, niemals bloß als Mittel brauchest.“



Inhalt

Behind the Scenes

Security News

GPS-Tracking

25-jähriger Bug in cmd.exe

Videokonferenzen ohne AV-Vertrag

Datenschutz-Bußgeldbemessung

Klagerecht für Verbraucherschutzverbände

Cookie-Walls

ISO 27002 – neu und sortiert

Digital Services Act

Secorvo News

13. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

GPS-Tracking

In einem erst jetzt veröffentlichten Urteil vom 17.01.2022 hat das VG Wiesbaden Kriterien für den Einsatz von GPS-Tracking im Logistikbereich aufgestellt. Das klagende Unternehmen hatte Geo-Tracking in den Fahrzeugen verbaut, wodurch der Live-Standort der Fahrzeuge und der Benzinverbrauch feststellbar waren. Die Daten wurden mittels Fahrerkarte einzelnen Fahrern zugewiesen und 400 Tage in der Cloud gespeichert.

Begründet wurde das Tracking mit Effizienzsteigerung sowie Schutz vor Missbrauch und Diebstahl. Einwilligungen der betroffenen Arbeitnehmer lagen nicht vor, auch waren keine Maßnahmen ergriffen worden, um eine verdeckte Arbeitnehmerüberwachung zu verhindern. Das Gericht bestätigte die Einschätzung der zuständigen Aufsichtsbehörde: Eine Einwilligung der Arbeitnehmer sei als Rechtsgrundlage nicht ausreichend, da diese in der Regel von Arbeitnehmern nicht wirksam erteilt werden kann. In Betracht käme nur die Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) nach sorgfältiger Interessensabwägung. Ohne Prüfung, ob es keine weniger einschneidenden Mittel zur Zweckerfüllung gibt, sei das Tracking rechtswidrig.

25-jähriger Bug in cmd.exe

Na, wenn das kein Geburtstagsgeschenk ist: Auf full disclosure wurde am 10.05.2022 eine Denial-of-Service-Schwachstelle im 25 Jahre alten, noch aus Windows-NT-Zeiten stammenden Kommandozeilen-Interpreter cmd.exe gemeldet. Auch wenn die Auswirkung sich auf das „Abschießen" einer eigenen Instanz des Interpreters beschränkt und eine gezielte Ausnutzung oder Angriffe gegen andere Benutzer darüber nicht möglich sind, bleibt die Frage, wie ein so offensichtlicher Fehler so lange unbemerkt bleiben konnte.

Merke: Software reift nicht über die Jahre bei ruhiger Lagerung (wie Whisky oder guter Wein), sondern sollte (wie Champagner) regelmäßig gerüttelt (sprich: untersucht) werden. Auch jahrelang bewährte Software ist nicht automatisch fehlerfrei. Der Fall zeigt, wie wichtig Aktivitäten zur systematischen Untersuchung von Software sind, wie z. B. die der Open Source Security Foundation, sowie die regelmäßige Durchführung von Penetrationstests. Im konkreten Fall besteht kein weiterer Handlungsbedarf – die eigene Kommando-Zeile kann man auch ohne Crash schließen.

Videokonferenzen ohne AV-Vertrag

In der DuD 05/2022 diskutieren Friederike Schellhas-Mende, Nils Wiedemann und Nicolas Blum die Auswirkungen des am 01.12.2021 in Kraft getretenen TTDSG und des neuen TKG auf Videokonferenzsysteme. So wechselt nicht nur die datenschutzrechtliche Zuständigkeit zum BDfI, sondern führt die Einordnung als „nummernunabhängiger interpersoneller Telekommunikationsdienst" dazu, dass für Videokonferenzdienste i.d.R. kein Auftragsverarbeitungsvertrag zu schließen ist.

Datenschutz-Bußgeldbemessung

Am 12.05.2022 hat der Europäische Datenschutzausschuss (EDSA) Leitlinien für die einheitliche Sanktionierung von Bußgeldern bei Datenschutzverstößen veröffentlicht und damit die Leitlinien vom 03.10.2017 (WP 253) präzisiert. Die Datenschutzkonferenz der deutschen Aufsichtsbehörden (DSK) hatte bereits am 14.10.2019 ein abgestimmtes Verfahren veröffentlicht (SSN 10/2019), das nun mit der Veröffentlichung der EDSA-Leitlinien seine Gültigkeit verliert.

Das Konzept des EDSA unterscheidet sich wesentlich von dem der DSK. Zwar betont es ebenfalls, dass Bußgelder auf die spezifischen Bedingungen des Einzelfalls zugeschnitten sein müssen. Doch es bleibt deutlich abstrakter als das deutsche Konzept, das aus dem Jahresumsatz des Unternehmens einen „Grundwert" (Umsatz pro Tag) ermittelte und diesen abhängig von dem Schweregrad des Verstoßes mit einem Faktor belegte.

Ausgangspunkt des EDSA-Konzepts ist eine Bewertung der Art, Dauer und Schwere des Verstoßes, in die u. a. die Zahl der Betroffenen, der Zweck der Verarbeitung und die Größe des verursachten Schadens einfließen. Daraus wird ein „Startwert" als prozentualer Anteil des maximal möglichen Bußgelds abgeleitet. Aus dem Jahresumsatz des Unternehmens errechnet sich dann das minimal aufzuerlegende Bußgeld zu 0,2% (Kleinst-) bis 50% (Großunternehmen) des zuvor bestimmten Startwerts. Je nach Ernsthaftigkeit des Verstoßes und den Bedingungen des Einzelfalls, wie z. B. ergriffene Gegenmaßnahmen oder frühere Verstöße, wird von der zuständigen Aufsichtsbehörde dann das Bußgeld zwischen Minimal- und Startwert festgelegt.

Ob dieses Verfahren geeignet ist, die Höhe der verhängten Bußgelder europaweit zu vereinheitlichen und deren Bestimmung transparenter zu machen, darf bezweifelt werden: Als „Bußgeldrechner" eignet es sich noch weniger als das Konzept der DSA. Die Angemessenheit der europäischen Bußgelder wird also weiterhin vom Augenmaß der zuständigen Behörden (und ggf. der Gerichte) abhängen.

Klagerecht für Verbraucherschutzverbände

Am 28.04.2022 hat der EuGH Verbraucherschutzverbänden ein ähnliches Klagerecht eingeräumt wie schon bei Wettbewerbsfragen. Die Verbände dürfen demnach in Form von Verbandsklagen Unterlassungsklagen gegen Verletzungen des Schutzes personenbezogener Daten erheben. Damit erhalten auch diejenigen Verbraucherinnen und Verbraucher eine Stimme, die aus mangelnder Kenntnis ihrer Rechte nicht gegen Datenschutzverstöße vorgehen.

Cookie-Walls

Die französische CNIL hat am 16.05.2022 erste Empfehlungen für Cookie-Walls veröffentlicht. Cookie-Walls stellen Nutzer beim Aufruf einer Webseite vor die Wahl, entweder alle Cookies für Werbezwecke zu akzeptieren oder eine Gebühr für die werbefreie Nutzung zu zahlen. Zwar sei die Einwilligung freiwillig, jedoch müsse den Nutzern eine „echte und faire Alternative" angeboten werden, die sich an der Angemessenheit der Vergütung bemisst. Die CNIL gibt dafür keinen Schwellenwert an, sondern verlangt, dass diese begründbar ist und ermutigt zu einer transparenten Kostenfestsetzung.

Stimmt der Nutzer der kostenpflichtigen Alternative zu, dürfen nur für den Betrieb der Webseite erforderliche Cookies hinterlegt werden. Der Anbieter kann davon abweichen, wenn z. B. auf Webseiteninhalte von Dritten zugegriffen werden muss. Dafür wird wiederum eine Einwilligung benötigt. Umstritten ist, ob die CNIL als Datenschutzbehörde nicht ihre Kompetenzen überschreitet, indem sie sich zur Vergütung äußert. In ihren Leitlinien hatte die CNIL bereits 2019 Cookie-Walls als unzulässig bezeichnet, woraufhin ihr das oberste französische Verwaltungsgericht diesbezüglich die Zuständigkeit absprach. Die Datenschutzkonferenz (DSK) verweist in ihrer Orientierungshilfe für Anbieter von Telemedien vom 20.12.2021 hinsichtlich Cookie-Walls auf die Leitlinien zur Einwilligung der EDPB. Danach sind Cookie-Walls nur dann unzulässig, wenn sie keine echte Wahlmöglichkeit anbieten („is not presented with a genuine choice").

ISO 27002 – neu und sortiert

Im Februar 2022 wurde die dritte Überarbeitung der ISO 27002 veröffentlicht; eine neue Version der ISO 27001 ist wohl in Kürze zu erwarten. Die ISO 27001 legt die prüfbaren Anforderungen eines Informationssicherheitsmanagementsystems (ISMS) fest und listet im Annex A die Maßnahmen der ISO 27002 auf. Daher sollte die Anpassung des unternehmenseigenen ISMS an die überarbeiteten und neuen Maßnahmen frühzeitig eingeplant werden.

Neu sind elf der nunmehr 93 Maßnahmen; weitere wurden zusammengefasst oder um neue Inhalte wie Bezüge zum Datenschutz angereichert. Eine Hilfe ist die Einführung von Eigenschaften zu jeder Maßnahme. Darüber können Unternehmen die Maßnahmen nach fünf unterschiedlichen Kriterien sortieren: Art der Risikosteuerung, Informationssicherheitsziele, Cybersecurity-Methoden, Managementziele (wie in der ISO 27002:2013) oder Handlungsfelder nach der NIS-Richtlinie. Eine Übersicht der Änderungen und einen Vorschlag für den schrittweisen Umstieg von Version 2013 hat Milan Burgdorf in der DuD 05/2022 zusammengestellt.

Digital Services Act

Am 23.04.2022 haben sich Europäischer Rat und Parlament über den Digital Services Act (DSA) als Nachfolger der 20 Jahre alten E-Commerce-Richtlinie geeinigt. Dieser wird neben der DSGVO weitere Vorgaben für Online-Dienste wie Vermittlungsdienste, Hosting-Dienste und Online-Plattformen enthalten. So werden beispielsweise „Dark Patterns" und irreführende Benutzeroberflächen bei der Auswahl der Cookies verboten. Sensible Daten wie politische Ansichten, religiöse Überzeugungen und sexuelle Vorlieben dürfen in Zukunft nicht mehr für personalisierte Werbung verwendet werden. Auch dürfen über Minderjährige keine Daten mehr gesammelt und diesen auch keine personalisierte Werbung mehr angezeigt werden. Zudem schafft der DSA u. a. für Nutzer eine einfache Meldemöglichkeit, infolge derer die Online-Dienste illegale Inhalte wie Hassrede, Gewaltaufrufe oder Terrorpropaganda entfernen müssen.

Bußgelder bei Verstößen gegen den DSA fallen mit bis zu 6 % des weltweit erzielten Jahresumsatzes noch höher aus als bei der DSGVO. Betreiber von Online-Diensten müssen sich bald auf die Vorgaben des DSA einstellen, da die Verordnung nach einer nur dreimonatigen Übergangsfrist unmittelbar in allen EU-Staaten gelten wird.

Secorvo News

13. Tag der IT-Sicherheit

Wir freuen uns sehr, den 13. Karlsruher Tag der IT-Sicherheit am **14.07.2022** wieder als Präsenzveranstaltung durchführen zu können. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, dem Kompetenzzentrum für angewandte Sicherheitstechnologie am KIT (KASTEL) und dem CyberForum e.V. hat die Förderung des Erfahrungsaustauschs unter IT-Sicherheitsverantwortlichen (nicht nur) in der TechnologieRegion Karlsruhe zum Ziel. Das Programm und die Möglichkeit zur Anmeldung finden Sie unter www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2022	
06.-10.06.	7th IEEE European Symposium on Security and Privacy (IEEE, Genua/IT)
06.-08.06.	OWASP Global AppSec (OWASP Foundation, virtuell)
16.-17.06.	AREA41 Security Conference (DEFCON, Zürich/CH)
20.-21.06.	DuD 2022 (COMPUTAS, Berlin)
21.-23.06.	Omnisecure 2022 (in TIME, Berlin)
23.-24.06.	Annual Privacy Forum 2022 (ENISA, DG Connect Católica University of Portugal, Warschau/POL)
Juli 2022	
11.-15.07.	PETS 2022 (University of Minnesota, hybrid)
14.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
August 2022	
06.-11.08.	Blackhat USA 2022 (Blackhat, Las Vegas/US)
10.-12.08.	31st USENIX Security Symposium (usenix, Boston/US)
11.-14.08.	DEF CON 30 (DEFCON, Las Vegas/US)

Fundsache

Neben dem Bericht des BSI zur Lage der IT-Sicherheit sollte man auch einen Blick in das Bundeslagebild Cybercrime 2021 des BKA werfen: Sehr kompakt und übersichtlich wird darin über typische Angriffsziele und -methoden von Cyberkriminellen berichtet. Die erfassten Fälle nehmen zwar stetig zu, die aufgeklärten Fälle jedoch ebenfalls.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2022



Wer nicht hören will...

Dieser Grundsatz gilt fast überall, nur nicht für den Datenschutz im öffentlichen Bereich: Anlässlich des EuGH-Urteils vom 05.06.2018 hatte die Datenschutzkonferenz am 01.04. 2019 Anforderungen an den rechtskonformen Betrieb von Facebook-Fanpages aufgestellt. Zuletzt veröffentlichten die Datenschutzaufsichtsbehörden hierzu am 18.03.2022 ein Kurzgutachten und forderten im selben Atemzug Ministerien und weitere öffentliche Stellen auf, für datenschutzkonforme Zustände zu sorgen, sprich: die Nutzung von Facebook-Fanpages einzustellen. Passiert ist seitdem: nichts. Und es ist fraglich, ob sich daran etwas ändert. Denn anders als Unternehmen und Bürger müssen Behörden Vorgaben der Aufsichtsbehörden faktisch nicht umsetzen. Juristisch ausgedrückt: § 20 Abs. 7 BDSG entzieht den Aufsichtsbehörden die Befugnis zur Anordnung der sofortigen Vollziehung nach § 80 Abs. 2 Nr. 4 VwGO ausdrücklich, und § 43 Abs. 3 BDSG schließt die Verhängung von Bußgeldern gegen öffentliche Stellen aus. Behörden sind, wie Meldungen aus den Aufsichtsbehörden zeigen, auch nicht gewillt, sich freiwillig zu unterwerfen.

Angesichts der Vorbildfunktion der öffentlichen Hand schwant einem nichts Gutes: Hier werden Ignoranz und Respektlosigkeit gegenüber hoheitlichem Handeln zum Schutz der Privatsphäre rechtlich gebilligt. Ein Staat, der seinen Behörden einen Freibrief bei datenschutzwidrigem Verhalten einräumt, verletzt nicht nur das Rechtsstaatsprinzip der Gesetzmäßigkeit der Verwaltung (Art. 20 GG), sondern setzt auch seine Autorität aufs Spiel, wenn er von Bürgern, Schulen und Unternehmen verlangt, wichtige Arbeitsmittel wie z. B. Teams oder Microsoft 365 durch Open-Source-Lösungen zu ersetzen und damit die eigene Arbeitsfähigkeit zu gefährden. Der Verweis auf den Klageweg ist da ein stumpfes Schwert – ein Griff in die Haushaltskasse der Behörde (auch mal in sechsstelliger Höhe, wie es in anderen EU-Ländern Gang und Gäbe ist) dürfte da schon wirkungsvoller sein, auch wenn das Bußgeld nur von der rechten in die linke Tasche wandert.



Inhalt

Wer nicht hören will...

Security News

Don't Stop Top 10

Cloud Computing Threats

Drittstaatenübermittlung

Schmerzensgeld für Google Fonts

Zoom in der Schule

Tracking durch ID-Provider

Erhalte das freie Internet

Secorvo News

Spätsommerbildung

13. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Don't Stop Top 10

Regelmäßig veröffentlichen Hersteller, Fachportale oder Behörden die fünf, sieben oder zehn häufigsten Risiken oder gefährlichsten Schwachstellen, wahlweise in IT-, Informations- oder Cybersicherheit. So auch am 17.05.2022 die CISA mit zehn Handlungsfeldern bezüglich schwacher Sicherheitsmaßnahmen und typischer Angriffswege auf IT-Systeme. Andere Zusammenstellungen wie die CWE Top 25 Most Dangerous Software Weaknesses oder die OWASP Top 10 listen verbreitete Schwachstellen in der Software-Entwicklung.

Solche Rankings unterstützen eine schnelle Risiko-Priorisierung der jeweiligen Bedrohungen und nennen teilweise, wie die CISA-Liste, Maßnahmen zur Abschwächung oder Abhilfe. Sie richten den Blick allerdings nur auf ausgewählte verbreitete Risiken und ersetzen daher keine umfassende Risikoanalyse, wie sie ein Informationssicherheitsmanagementsystem (ISMS) fordert. Ihren vollen Nutzen entfalten sie auch erst im Kontext eines ISMS (bspw. nach ISO 27001 oder BSI IT-Grundschutz), das sicherstellt, dass die Umsetzung der Maßnahmen zur Reduktion der ermittelten Risiken regelmäßig und systematisch überprüft werden.

Cloud Computing Threats

Die Cloud Security Alliance (CSA) veröffentlichte am 06.06.2022 die elf Top Threats to Cloud Computing. Dazu waren zuvor über 700 Experten befragt worden. In der Auflistung finden sich zahlreiche Bekannte wie „Insufficient Identity" oder „Insecure Interfaces and APIs". Dennoch ist der Bericht lesenswert, denn er beschreibt die einzelnen Bedrohungen im Detail und vergleicht die Ergebnisse mit denen des Berichts aus dem Jahr 2019. So kann er helfen, die eigenen Risikoabschätzungen und Maßnahmenlisten für Cloud-Dienste zu überprüfen.

Drittstaatenübermittlung

Anlässlich des Beginns des fünften Geltungsjahrs der Datenschutzgrundverordnung (DSGVO) forderte der IT-Verband Bitkom am 25.05.2022, dass sich der „Datenschutz an realen Gefahren orientieren" müsse, nicht an „theoretischen Risiken", wie beispielsweise bei der Frage der Zulässigkeit des Einsatzes von Videokonferenzsystemen von US-Unternehmen in deutschen Schulen.

Dabei kommt es bei der Feststellung der Zulässigkeit einer Übermittlung von personenbezogenen Daten in Drittstaaten (Art. 44 ff. DSGVO) auf das Risiko gar nicht an. Entscheidend ist einzig, ob „das betreffende Drittland [...] ein angemessenes Schutzniveau" für die personenbezogenen Daten bietet. Dies hat Auswirkungen auf die Bewertung von Rechtsakten der Drittstaaten, die die Rechte (insbesondere ausländischer) Betroffener beschränken, wie der CLOUD-Act der USA. Und der EuGH stellte 2020 im Schrems II-Urteil klar, dass personenbezogene Daten nur dann in ein Drittland übermittelt werden dürfen, wenn das vom Anbieter garantierte Schutzniveau dem in der Union garantierten gleichwertig ist.

Das stellt viele Unternehmen bei der Nutzung von Cloud-Diensten vor Herausforderungen, denn die Verantwortung für die in ihrem Auftrag durch Dritte verarbeiteten Daten und die Pflicht zur Einholung von Einwilligungen liegt bei ihnen – auch dann, wenn ein Unter-Unter-Unterauftragnehmer eines Dienstleisters die Daten in ein Drittland übermittelt.

Schmerzensgeld für Google Fonts

Am 20.01.2022 sprach das Landgericht München I einem Kläger 100 € Schmerzensgeld zu, da auf einer von diesem besuchten Webseite Google Fonts eingebunden waren und damit seine IP-Adresse ohne Einwilligung an Google-Server übermittelt worden war. Da half auch nicht, dass Google (nach eigenen Angaben) die IP-Adresse nicht speichert.

Mit Verweis auf dieses Urteil wird derzeit versucht, Schadensersatzansprüche in Höhe von 100 € bei Webseitenbetreibern geltend zu machen, die Google Fonts in ähnlicher Weise nutzen – leicht feststellbar mit einem Browser-Plugin zur Tracking-Analyse. Das kann lukrativ sein, denn Google Fonts wurden bereits mehr als 63 Billionen Mal abgerufen.

Wir empfehlen, die Einbindung von Google Fonts zu überprüfen und gegebenenfalls zu korrigieren. Gleiches gilt für die Einbindung anderer Dienste von Anbietern in Drittstaaten wie Karten, Videos oder Social Media Share Buttons: Auch hier wird die IP-Adresse an den Anbieter übermittelt, was nur mit expliziter Einwilligung des Besuchers in die Übermittlung an und die Datenverarbeitung in dem jeweiligen Drittstaat zulässig ist.

Zoom in der Schule

Der hessische Beauftragte für Datenschutz und Informationsfreiheit teilte am 21.06.2022 mit, dass nun der Einsatz von Zoom für Lehrveranstaltungen nach dem „Hessischen Modell" erlaubt sei. Das setzt voraus, dass ein von Zoom unabhängiger Auftragsverarbeiter mit Servern und Sitz in der EU beauftragt wird und die Inhalte Ende-zu-Ende verschlüsselt werden. Ein Abfluss von personenbezogenen Daten in die USA wird durch diese Maßnahmen verhindert.

Tracking durch ID-Provider

Am 14.01.2020 hatte Google angekündigt, die Unterstützung von Third-Party-Cookies im Chrome-Browser im Jahr 2022 auslaufen zu lassen, und Apple hatte bereits am 26.04.2021 mit iOS 14.5 das Tracking durch Apps als Voreinstellung deaktiviert. Diese Entwicklung bedeutet keineswegs das Ende des Tracking (da Google und Apple über ausreichend selbst erhobene Verhaltensdaten verfügen) – wohl aber das Ende der Datenbasis heutiger Werbenetzwerke (siehe Editorial SSN 5/2022).

Die suchen bereits fieberhaft nach Alternativen, um auch zukünftig Verhaltensdaten zu gewinnen – idealerweise mit Bezug zu möglichst invarianten IDs wie der Mobilfunknummer oder der E-Mail-Adresse von Seitenbesuchern und App-Nutzern. Was liegt da näher, als die Nutzer-Identifikation gleich mit dem Login zu koppeln? Google, Apple und Facebook machen es seit Jahren vor: Sie bieten Login-Schnittstellen an, die Webseitenanbieter einbinden können, um sich damit die Implementierung einer eigenen Nutzerverwaltung zu sparen. Zahlreiche weiterer Identitätsanbieter erblicken gerade das Licht der Welt: Sie verschenken den Dienst und verdienen an den gehashten ID-Daten (wie bspw. Zoetap), die sie an zahlende Werbeanbieter und -broker weiterleiten.

Ohne Einwilligung der Betroffenen ist die Nutzung von ID-Anbietern, die (pseudonymisierte) Daten an Dritte weitergeben, allerdings genauso rechtswidrig wie die Nutzung der ID-Services von Google & Co.

Erhalte das freie Internet

Mit diesem Claim begrüßt TrustPid – ein von Vodafone und der Deutschen Telekom entwickelter ID-Service, der als deutsche Alternative zum Cookie-Tracking gedacht ist – seine Seitenbesucher. Willigt der Nutzer ein, wird aus der Mobilfunknummer und der IP-Adresse des Besuchers eine TrustPid-ID abgeleitet. Alle auf diese bezogenen Tracking-Informationen einer Seite, die TrustPid nutzt, werden dann an den TrustPid-Server übermittelt.

Die vom Nutzer erteilte Einwilligung lässt sich (anders als bei Cookies, die man beim Schließen des Browsers löschen lassen kann) allerdings nicht so leicht widerrufen. Der Weg ist umständlich und intransparent: Ein Widerruf ist nur aus dem Mobilfunknetz im Datenschutzportal von TrustPid oder (gegebenenfalls) auf der die Daten erhebenden Webseite möglich.

TrustPid befindet sich derzeit im Technik-Test beim Axel-Springer-Verlag und kommt beispielsweise auf bild.de zum Einsatz. Dort erfolgt der Widerruf über separate Einwilligungsverwaltungen: „Widerruf Nutzerkennungen“ (TrustPid) und „Widerruf Tracking“ (Cookies). Die Provider behalten sich vor, dass die Löschung der TrustPid-Daten bis zu 90 Tage dauern kann. Ein Widerruf ist damit deutlich umständlicher als die Einwilligung und zudem sowohl in TrustPid als auch auf bild.de für Nutzer kaum erkennbar, da er lediglich in der Datenschutzerklärung, nicht aber auf der „Cookie-Wall“ Erwähnung findet (obwohl in letzterer die Einwilligung eingeholt wird).

Die deutschen Aufsichtsbehörden haben noch keine abschließende Bewertung zu TrustPid abgegeben. Für die Verwendung einer ähnlichen Technik hatte Verizon in den USA am 07.03.2016 einen Bußgeldbescheid der Federal Communication Commission über 1,35 Millionen US-Dollar erhalten.

Secorvo News

Spätsommerbildung

Wer schon vor dem Sommerurlaub wissen möchte, was sie oder er anschließend lernen wird, sollte sich unseren Frühbucherrabatt sichern: z. B. für das T.I.S.P.-Seminar (19.-23.09.2022) mit anschließender Möglichkeit zur Zertifizierung oder das Seminar IT Security Insights (27.-29.09.2022). Wir freuen uns auf Ihre Anmeldung und Ihren Besuch in Karlsruhe!

13. Tag der IT-Sicherheit

Wir freuen uns sehr, Sie zum diesjährigen Karlsruher Tag der IT-Sicherheit am **14.07.2022** in den Saal Baden der IHK Karlsruhe einladen zu können. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, dem Kompetenzzentrum für angewandte Sicherheitstechnologie am KIT (KASTEL) und dem CyberForum e.V. will den Erfahrungsaustausch unter IT-Sicherheitsverantwortlichen (nicht nur) in der TechnologieRegion Karlsruhe fördern.

Es erwarten Sie spannende Fachvorträge zu den Themen Digitale Souveränität, Sicherheit und Erklärbarkeit von KI, Quantencomputer und Cybersicherheit sowie sicheres Betriebssystem durch Asset-, Lifecycle- und Patch-Management – und ein intensives Buffet-Networking.

Das Programm und die Möglichkeit zur Anmeldung finden Sie hier.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2022	
11.-15.07.	PETS 2022 (University of Minnesota, Sydney/AUS)
11.-14.07.	DFRWS USA 2022 (DFRWS, virtuell)
14.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
August 2022	
06.-11.08.	Blackhat USA 2022 (Blackhat, Las Vegas/US)
07.-09.08.	SOUPS 2022 (usenix, Boston/US)
10.-12.08.	31st USENIX Security Symposium (usenix, Boston/US)
11.-14.08.	DEF CON 30 (DEFCON, Las Vegas/US)
13.-18.08.	Crypto 2022 (IACR, Santa Barbara/US)
September 2022	
19.-23.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
26.-30.09.	Informatik 2022 (GI, Hamburg)

Fundsache

Der beste Schutz gegen Cyberattacken sind sensibilisierte Mitarbeitende. Das ist das Zwischenergebnis einer Datenschutzprüfung zur Ransomware-Prävention des Bayerischen Landesamts für Datenschutz (BayLDA). Für Unternehmen werden Ransomware-Angriffe und wirksame Gegenmaßnahmen in einem Infoblatt und einer Handreichung checklistenartig erklärt.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende (Editorial), Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2022



Moderne Abhängigkeiten

Lange schon sind die Produktlebenszyklen bei IT-Produkten – verglichen mit anderen Branchen – recht kurz. Das gilt besonders für Software. Solange die Produkte in Organisationen oder bei Privatpersonen betrieben wurden, erwuchs daraus selten ein Problem: Man nutzte ein Programm so lange, bis ein nicht behebbarer Fehler oder fehlende Features eine Migration erzwangen.

Inzwischen sind immer mehr Organisationen und Menschen von IT-Diensten abhängig, die sie nicht mehr selbst kontrollieren, wie bspw. Cloud-Dienste, Steuersysteme in Fahrzeugen oder auch Lösungen, die bedeutsam für die Gesundheit von Menschen sind.

Die Abgabe von Kontrolle und der Einsatz von fremdbetreuten Diensten sind verlockend, weil sie einige unmittelbare Vorteile bieten: Zeitersparnis und die Kompensation von fehlendem Know-How. Und häufig betreiben Anbieter die Lösungen zudem effizienter und professioneller als ihre Kunden das selbst könnten.

Manchmal geht aber auch etwas schief. So gibt es zahlreiche Beispiele für Störungen – u. a. bei Amazon, Microsoft, Google, Facebook und Atlassian. Auch werden Dienste eingestellt, siehe die umfangreiche Killed by Google-Liste. Und was passiert, wenn darunter ein kritischer Dienst ist? Das ist keine hypothetische Frage: Wegen wirtschaftlicher Schwierigkeiten stellte 2020 ein Unternehmen aus dem Medizinbereich seinen Support für ein Retina-Implantat ein. Bei ca. 350 Betroffenen, die temporär wieder sehen konnten, bleibt nun im Falle eines Defekts Medizinschrott ohne Funktion im Körper.

Daher ist es ratsam, sich nicht blind in die Cloud zu stürzen, sondern nüchtern mögliche Risiken zu betrachten und sich über kompensierende Maßnahmen Gedanken zu machen. Eine Hilfestellung können dabei Anleitungen sein wie der Grundschutzbaustein Cloud-Nutzung oder der Kriterienkatalog Cloud Computing C5 des BSI.



Inhalt

Moderne Abhängigkeiten

Security News

Dünne Luft für Google Analytics

Post-Quantum-Kryptoverfahren

Cloud Encryption

Rechtswidrige Wächter-Modi

Ampeln zur Klassifizierung

Big Brother Deutsche Bahn

Leaky Forms

Secorvo News

Wenn nicht jetzt – wann dann?

Hokus Pokus Fidibus

Veranstaltungshinweise

Fundsache

Security News

Dünne Luft für Google Analytics

Die am 17.08.2020 publizierten 101 Beschwerden der noyb zu EU-US-Datentransfers wirken weiter: Nach der österreichischen dsb (SSN 1/2022) und der französischen CNIL (SSN 2/2022) hat nun auch die italienische Datenschutzbehörde GPDP entschieden, dass die Verwendung von Google Analytics gegen die DSGVO verstößt.

Eine Risikobewertung, die annimmt, dass US-Behörden wahrscheinlich nicht nach den Daten fragen, lehnt sie ab. Vielmehr müssen Unternehmen garantieren, dass das Grundrecht auf informationelle Selbstbestimmung weiterbesteht, wenn die Daten den Europäischen Wirtschaftsraum verlassen. Gekürzte IP-Adressen sind für die GPDP personenbezogene Daten; die Kürzung sei keine ausreichende Anonymisierung. Angesichts dieser Entwicklung sollten Analytics-Kunden ihr Tracking zügig auf datenschutzkonforme Alternativen umstellen.

Post-Quantum-Kryptoverfahren

Quantencomputer bedrohen die Sicherheit aller heute eingesetzten asymmetrischen Kryptoverfahren, denn mit dem von Peter Shor 1994 entwickelten Quanten-Algorithmus ist eine effiziente Faktorisierung großer Zahlen und Berechnung diskreter Logarithmen möglich. Damit wären RSA und DSA gebrochen.

Zwar benötigen solche Quantencomputer mehr als 2000 Qubits – heutige erreichen gerade einmal 127 (IBM, 2021). Aber es ist nur eine Frage der Zeit, bis es so weit ist. Um rechtzeitig gut untersuchte neue Verfahren zu etablieren, schrieb das NIST daher 2016 einen Wettbewerb für Post-Quantum-Algorithmen aus. Aus ursprünglich 69 Vorschlägen wählte das NIST am 05.07.2022 einen Kandidaten für Verschlüsselung und Key Exchange (CRYSTALS-KYBER) und drei für digitale Signaturen (CRYSTALS-Dilithium, FALCON und SPHINCS+) zur Standardisierung aus, die 2024 abgeschlossen werden soll. Vier weitere Verfahren nahm das NIST in die vierte Evaluationsrunde auf (vollständiger Bericht). Kurz darauf wurde eines davon, SIKE, am 30.07.2022 von Forschern der Universität Leuven gebrochen.

Nach 45 Jahren mit sicheren asymmetrischen Verfahren bricht nun eine Phase der Unruhe an – mit bisher noch ungewissem Ausgang.

Cloud Encryption

Der stärkste Vorbehalt gegen die Nutzung von Cloud-Diensten ist die Zugriffsmöglichkeit des Anbieters auf die verarbeiteten Daten – die in einigen Drittstaaten auch Nachrichtendiensten einen Datenzugang eröffnet. Davor schützt auch keine Datenverschlüsselung – denn während der Verarbeitung liegen die Daten und der Entschlüsselungsschlüssel offen im Arbeitsspeicher (RAM) des Servers. Abhilfe soll das am 19.07.2022 von Corey Sanders im Microsoft-Blog vorgestellte „Azure Confidential Computing“ schaffen. Dabei kommen spezielle Eigenschaften neuerer Prozessoren von AMD und Intel zum Einsatz (SME/SEV bzw. SGX): die Verschlüsselung aller vom Prozessor als Cache genutzten RAM-Bereiche. Damit liegen auch in einem Memory Dump Daten, Passwörter oder Schlüssel, die der Prozessor genutzt hat, nur verschlüsselt vor.

Sofern die Passwörter und Schlüssel für diese RAM-Verschlüsselung selbst in einem zugriffsgesicherten Bereich (Hardware Security Module, HSM) gehalten werden und die Verfahren keine Hintertür für behördlichen Zugriff haben, könnte eine solche Lösung den „zusätzlichen Garantien“ entsprechen, die der EuGH im Schrems-II-Urteil bei Verarbeitungen in datenschutzrechtlich unsicheren Drittstaaten fordert (SSN 10/2020).

Rechtswidrige Wächter-Modi

Am 19.07.2022 hat der Verbraucherzentrale Bundesverband (vzbv) bekanntgegeben, dass er Tesla wegen des (in den SSN 9+10/2021 vorgestellten) „Wächter-Modus“ im Model 3 verklagen wird. Dabei filmt das geparkte Fahrzeug mit den eingebauten Kameras die Umgebung; auf die Livebilder kann mit der Tesla Mobile App zugegriffen werden. Bei nahenden Passanten wird der Warnzustand aktiviert, in dem die Videobilder zusätzlich im Fahrzeug gespeichert werden.

Nach Ansicht des vzbv ist eine datenschutzkonforme Nutzung im öffentlichen Raum nicht möglich und die Datenverarbeitung damit unzulässig. Grundsätzlich bedürfe es dafür entweder einer Einwilligung der Passanten (praktisch nicht umsetzbar) oder eines überwiegenden Interesses des Fahrzeughalters oder -fahrers (bei anlassloser Überwachung nicht begründbar).

Auch bei dem anderen in den SSN 9+10/2021 vorgestellten „Wächter-Modus“ regt sich Widerstand: Am 13.07.2022 erklärte US-Senator Ed Markey nach einer Befragung von Amazon Ring das von über 2.100 US-Strafverfolgungsbehörden genutzte Angebot, direkten Zugriff auf die Geräte von Ring-Nutzern zu erhalten, für rechtswidrig. Zudem habe Amazon 2022 in elf Fällen Bildmaterial ohne Einwilligung der betroffenen Ring-Nutzer weitergegeben.

Nutzer solcher Wächter-Lösungen sollten sich nicht darauf verlassen, dass der Hersteller für die Einhal-

tung der datenschutzrechtlichen Anforderungen sorgt. Bußgeldbewehrt ist der rechtswidrige Betrieb – und verantwortlich der Betreiber. Das gilt nach der DSGVO auch für Privatpersonen.

Ampeln zur Klassifizierung

Die Forderung nach Informationsklassifizierung und angemessener Kennzeichnung sind seit jeher Bestandteil der Anforderungen der ISO 27002, wie schon des Vorgängers BS 7799-2. Bei der Umsetzung kann der Standard „Traffic Light Protocol (TLP)“ helfen, dessen Version 2.0 das Forum of Incident Response and Security Teams (FIRST) am 05.08.2022 veröffentlichte. Darin hat sich die CERT-Community auf eine einheitliche Nomenklatur für Vertraulichkeitsklassen geeinigt. Die Verwendung einheitlicher Bezeichnungen kann für die Kommunikation zwischen Organisationen hilfreich sein – z. B. indem Organisationen die FIRST-TLP adaptieren, ähnlich wie das BSI am 12.05.2022.

Big Brother Deutsche Bahn

Am 11.04.2022 veröffentlichten der Blogger Mike Kuketz und Peter Hense das vernichtende Ergebnis ihrer datenschutzrechtlichen Untersuchung der DB Navigator-App. So hält die Bahn 10 Dienstleister, darunter Adobe Analytics und Optimizely, für erforderliche Adressaten sämtlicher Daten, die im Rahmen einer Ticketbuchung erfasst werden.

Eine rechtliche Grundlage gebe es dafür nicht, denn um diese Verarbeitung zu vermeiden müssten Reisende ihr Ticket entweder am Automaten oder im Reisezentrum erwerben. Für den kurzfristigen Ticketkauf gebe es keine Alternative zur App, da Schaffner keine Tickets mehr im Zug verkaufen. Am 20.07.2022 teilte Kuketz mit, dass er jetzt gemeinsam mit digitalcourage die Bahn verklage, da die DB Navigator App erfasste Daten auch dann noch sendet, wenn in den Einstellungen „Nur erforderliche Cookies verwenden“ ausgewählt wurde. Die Klage kann man auf der Seite von digitalcourage unterstützen.

Leaky Forms

Auf dem diesjährigen 31. Usenix Security Forum (10.-12.08.2022) stellten vier Forscher aus Leuven, Nijmegen und Lausanne die Ergebnisse ihrer Mitte 2021 durchgeführten umfangreichen Studie zum rechtswidrigen Tracking von Daten in Web-Formularen vor. Dazu hatten sie mit eigens entwickelten Crawlern auf den 100.000 meistbesuchten europäischen und amerikanischen Webseiten je rund 50.000 Formularseiten identifiziert, auf denen E-Mail-Adressen abgefragt wurde. Trugen die Crawler dort eine Adresse ein, so wurde sie von 1.850 europäischen (3,7%) und 2.950 amerikanischen (5,9%) Servern ohne Einwilligung des Nutzers – d. h. vor der Betätigung des „Senden“-Knopfes – an den Tracker übertragen. Eine solche Übermittlung ist rechtswidrig – und kann obendrein Daten umfassen, deren Übermittlung gar nicht beabsichtigt war, wenn beispielsweise der „Autofill“-Mechanismus des Browsers verwendet wird. Ihre Datenbasis und die verwendete Software zur Identifikation der rechtswidrigen Tracker haben die Autoren auf Github veröffentlicht.

Secorvo News

Wenn nicht jetzt – wann dann?

1.700 Experten haben es schon – das T.I.S.P.-Zertifikat. Regelmäßig treffen sie sich zum Erfahrungsaustausch auf dem T.I.S.P.-Community-Meeting.

Falls Sie noch nicht dazu gehören: Vom **19.09. bis 23.09.2022** bieten wir Ihnen mit unserem T.I.S.P.-Seminar die nächste Gelegenheit, sich auf die Prüfung vorzubereiten. Mit Ihrer Anmeldung zum Seminar erhalten Sie vorab unser T.I.S.P.-Begleitbuch „Informationssicherheit und Datenschutz“. Wir freuen uns auf Sie!

Alle weiteren Seminarthemen und Termine unter https://www.secorvo.de/seminare.

Hokus Pokus Fidibus

Wie geht das – Entwicklung und Produktion von Hardware-Security-Modulen in Deutschland? Welche Herausforderungen sind damit verbunden – und wie werden die von einem der wenigen deutschen Hersteller von IT-Security Hardware gemeistert, der WIBU-SYSTEMS aus Karlsruhe? Das grenzt manchmal schon an Zauberei …

Erfahren Sie bei unserem kommenden KA-IT-Si-Event am **15.09.2022** aus erster Hand, welche Hürden bei der Entwicklung, den Multiplattform-Tests, der Beschaffung und der sicheren Produktion von Security Controllern „Made-in-Germany“ zu bewältigen sind. Wir erhalten die seltene Gelegenheit, die Fertigung zu besichtigen und Einblick in die automatisierten Prozesse des Downloads finaler Firmware, der Schlüsselerzeugung und optional individueller Schlüsselspeicherung für kundenspezifische Produkte zu bekommen. Die Spezialisten von WIBU-SYSTEMS und der Vorstand Oliver Winzenried stehen Ihnen dabei Rede und Antwort.

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ – diesmal mit einem phänomenalen Blick auf den Schwarzwald (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2022	
19.-23.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
26.-30.09.	Informatik 2022 (GI, Hamburg)
27.-29.09.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
Oktober 2022	
04.-06.10.	heise devSec 2022 (dpunkt verlag, heise, Karlsruhe)
17.-19.10.	IDACON 2022 (WEKA-Akademie, München)
24.-26.10.	ISSE 2022 (IEEE, Wien/A)
25.-27.10.	it-sa 2022 (NürnbergMesse GmbH, Nürnberg)
November 2022	
07.-11.11.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
07.-11.11.	ACM CCS 2022 (ACM/SIGSAC, Los Angeles/US)
09.-10.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)

Fundsache

TeleTrusT hat am 22.06.2022 einen Podcast zum "Stand der Technik in der IT-Sicherheit" veröffentlicht. Darin stellen Tomasz Lawicki (Leiter AK Stand der Technik) und Karsten U. Bartels (TeleTrusT Vorstand) die Methode zur Entwicklung der Handreichung "Stand der Technik", rechtliche Positionen und weitere Aspekte vor. Hörenswert.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian (Editorial), Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2022



Deep Fake

Die technischen Möglichkeiten, Bilder, Videos und Sprache zu verfälschen, sind inzwischen gleichermaßen bekannt wie verbreitet. Mit ihrer Hilfe lassen sich biometrische Authentifikationsverfahren austricksen und „fake news“ erzeugen. Doch ist der Aufwand für praktisch nicht nachweisbare Fälschungen noch immer so hoch, dass sie zum Glück bisher isolierte Einzelerscheinungen sind – und bei ihrem Erscheinen schnell Zweifel an der Echtheit laut werden.

Ganz anders ist das bei Verfahren, die derzeit fast unbemerkt Einzug in unsere Lebenswirklichkeit halten: die KI-gesteuerte Erzeugung von Texten. Eine solche KI-Anwendung, die am 08.09.2020 durch einen Artikel des Guardian Furore machte, ist GPT-3 – eine KI der Firma OpenAI. Gefüttert wird sie mit Inhalten aus dem Internet und erzeugt zu einem vorgegebenen Thema kurze Notizen bis hin zu ganzen Büchern, die sogar an ausgewählte Schreibstile angepasst werden können. Sie sind stilistisch so elegant, dass sie mühelos als menschliche Werke durchgehen.

Die Wahrheit eines Sachverhalts kann GPT-3 allerdings nicht prüfen und ist daher auf eine Bewertung der Plausibilität angewiesen. Was aber könnte plausibler sein als eine sehr oft wiederholte Behauptung? GPT-3-Texte wiederholen also vor allem Verbreitetes – und verstärken damit selbst deren Plausibilität.

Wenn nun (was sicher bereits passiert) immer mehr Texte von solchen Automaten erzeugt werden, werden Plagiate, insbesondere bei wissenschaftlichen Arbeiten, zukünftig wohl kaum noch zu identifizieren sein. Vor allem aber werden Widerlegungen, die es heute schon schwer haben (wie z. B. der Mythos vom hohen Eisengehalt von Spinat), schon bald nicht mehr wahrgenommen werden – und Ähnliches könnte für neue Erkenntnisse gelten, denn die haben ja gerade die Eigenschaft, selten publiziert worden zu sein. KI-Fakes werden die Welt oberflächlicher machen. Und uns dümmer.



Inhalt

Deep Fake

Security News

Video-Fake-Ident

Pimp my Tesla

Kein Konzernprivileg

Viele Daten sind besonders

Jagd auf Cookie-Banner

Verhältnismäßig

Secorvo News

T.I.S.P. und IT Security Insights

Hokus Pokus Fidibus

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Video-Fake-Ident

Der Chaos Computer Club meldete am 10.08.2022, dass es ihm gelungen sei, mehrere videobasierte Online-Identifizierungsverfahren zu täuschen. Schon am Vortag hatte die Gematik den Vorgang zum Anlass genommen, die Nutzung von VideoIdent bis auf Weiteres zu untersagen.

Nach dem Untersuchungsbericht von Martin Tschirsich bedurfte es für die Angriffe keiner kostenintensiven Hard- oder Software. Es genügte, vor der Kamera ein manipuliertes Video abzuspielen, in dem das Passfoto auf dem Ausweis ersetzt worden war. Die Manipulationen wurden von keiner der sieben getesteten Lösungen erkannt. Zwar nennt der Bericht keine Hersteller, es ist aber zu befürchten, dass die Angriffe bei den weitaus meisten Video-Ident-Lösungen funktionieren.

Ursache ist, dass viele optische Sicherheitsmerkmale des Personalausweises am übertragenen Bild nicht geprüft werden können. Ein Hologramm ist beispielsweise nur zweidimensional zu sehen, und dem übertragenen Bild kann man nicht trauen, da das Equipment unter der Kontrolle eines Angreifers betrieben werden kann. Somit können das Video-Bild der Person oder die auf dem Ausweis angezeigten Daten „on the fly" verändert werden. Das bietet bestenfalls für einfache Anwendungen ein angemessenes Sicherheitsniveau.

Unverständlich ist, warum die eID-Funktion des vor 12 Jahren eingeführten „neuen Personalausweises" nicht selbstverständlich für derartige Anwendungen genutzt wird, obwohl die Zertifikatsinfrastruktur von den Bürgern mit der Personalausweisgebühr bereits teuer bezahlt wurde.

Pimp my Tesla

Die Anzahl von Kameras auf und an den Straßen Deutschlands hat sich, Tesla sei Dank (SSN 07/2022), in den letzten Jahren vervielfacht. Jetzt sind an einem Erprobungsfahrzeug montierte Kameras VW zum Verhängnis geworden: Der Landesbeauftragte für den Datenschutz Niedersachsens verhängte am 26.07.2022 ein Bußgeld in Höhe von 1,1 Mio. €, da die Kameras nicht gekennzeichnet waren.

Wird das Verkehrsgeschehen um das Fahrzeug herum aufgezeichnet, unterliegen auch Kameras an und in Fahrzeugen der Kennzeichnungspflicht nach Art. 13 DSGVO. Das gilt auch für Rückfahrkameras, Kameras von Einparkassistenten und teilautonomen Fahrzeugen. Eine interessante Vorstellung, dass Tesla-Fahrer zukünftig ihre acht Außenkameras einzeln kennzeichnen müssen – inklusive Angabe der für die Verarbeitung verantwortlichen Stelle…

Kein Konzernprivileg

Für einen Gehaltsvergleich übermittelte ein Unternehmen Arbeitsvertrag, Name, Einstellungsdatum, Gehalt und weitere Angaben zu einer Mitarbeiterin an eine Tochtergesellschaft. Eine Einwilligung der Mitarbeiterin wurde nicht eingeholt und ihr Widerspruch nicht beachtet. Ein teurer Fehler, denn die DSGVO kennt kein Konzernprivileg: Das LG Bochum widersprach nicht nur dem geltend gemachten überwiegenden Interesse des Unternehmens, sondern bezweifelte auch die Erforderlichkeit der Übermittlung, da die Vergleichswerte auch mit pseudonymisierten Daten hätten erstellt werden können.

Mit dem Ziel einer abschreckenden Wirkung sprach das LG Bochum der Mitarbeiterin 8.000 € Schadensersatz für den durch die rechtswidrige Verarbeitung erlittenen immateriellen Schaden zu; das OLG Hamm reduzierte diesen auf 4.000 €.

Ob ein Schadensersatz überhaupt eine abschreckende, d. h. sanktionierende Wirkung haben oder vielmehr nur zum Schadensausgleich dienen darf, ist Gegenstand von Vorlagefragen des AG München vom 03.03.2022 an den EuGH.

Viele Daten sind besonders

Am 01.08.2022 hat der Europäische Gerichtshof entschieden, dass die Definition der besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO weit auszulegen ist.

Anlass war die Beurteilung des litauischen Gesetzes zur Korruptionsbekämpfung über den Ausgleich öffentlicher und privater Interessen im öffentlichen Dienst. Danach müssen bestimmte Personen eine Erklärung über private Interessen abgeben – mit Angabe sowohl des eigenen als auch des Namens des Ehepartners. Laut EuGH lässt sich daraus mittels „gedanklicher Kombination oder Ableitung" ohne Weiteres auf die sexuelle Orientierung von Ehepaaren schließen. Demnach liegt eine Verarbeitung besonderer Kategorien personenbezogener Daten bereits dann vor, wenn diese Daten „geeignet sind, die sexuelle Orientierung einer natürlichen Person indirekt zu offenbaren." Deren Verarbeitung ist grundsätzlich untersagt und nur in Ausnahmefällen zulässig.

Die Argumentation des EuGH ist in zahlreichen weiteren Fällen anwendbar, da personenbezogene Daten häufig erlauben, indirekt Rückschlüsse auf besondere Kategorien personenbezogener Daten zu ziehen, wie z. B. die Bestellung koscheren Essens im Flugzeug oder der Schlüsseleintrag auf dem Führerschein (Brille, Hörgerät oder Prothese).

Wegen des hohen Schutzniveaus dieser Daten können von der weiten Interpretation des EuGH zahlreiche Datenverarbeitungen betroffen sein, bei denen die Verantwortlichen bisher davon ausgehen, lediglich „normale“ personenbezogene Daten zu verarbeiten. Das kann bedeuten, dass eine Datenschutz-Folgenabschätzung durchgeführt und ergänzende Maßnahmen zum Schutz dieser Daten ergriffen werden müssen.

Jagd auf Cookie-Banner

Die Initiative „My Privacy is None of Your Business“ (noyb) hat am 09.08.2022 angekündigt, erneut tausende Webseiten zu scannen, die Consent Management Platforms (CMP) wie OneTrust, TrustArc, Cookiebot, Usercentrics oder Quantcast verwenden.

Bereits am 31.05.2021 (SSN 6/2021) hatte noyb an 560 Unternehmen, die auf ihren Webseiten das CMP „OneTrust“ einsetzen, einen Beschwerdeentwurf samt Schritt-für-Schritt Anleitung zur rechtskonformen Anpassung ihrer Cookie-Banner versandt und eine 60-tägige Schonfrist zur Nachbesserung gewährt. 24 % aller angemahnten Verstöße wurden innerhalb dieser 60 Tage behoben, die meisten Unternehmen kamen der Aufforderung jedoch nicht oder nicht vollständig nach. Daraufhin reichte noyb 226 Beschwerden bei 18 Aufsichtsbehörden ein. Daraufhin wurden 42 % der verbleibenden Verstöße innerhalb von 30 Tagen korrigiert.

Webseitenbetreiber, die ihre Cookie-Banner auf Rechtskonformität prüfen möchten, finden u. a. beim Landesbeauftragten für Datenschutz und Informationssicherheit Baden-Württemberg hilfreiche Hinweise und Beispiele.

Verhältnismäßig

Die Frage der Erforderlichkeit einer Ende-zu-Ende-Verschlüsselung wird auch zwischen den Aufsichtsbehörden für den Datenschutz kontrovers diskutiert. Am 15.07.2022 hat nun das VG Frankfurt in der Frage, wann eine Ende-zu-Ende-Verschlüsselung elektronischer Kommunikation notwendig ist und wann eine Transportverschlüsselung ausreicht, einen Beschluss gefasst.

Sollen personenbezogene Daten übermittelt werden, müssen gemäß Art. 32 DSGVO und Erwägungsgrund 83 zur Gewährleistung von Sicherheit und Vertraulichkeit der Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die (je nach Fall ggf. unterschiedliche) Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geprüft werden.

Das VG Frankfurt hat nun den Stand der Technik als das ausschlaggebende Kriterium für die Anforderungen an die angemessene Verschlüsselung gesetzt und entschieden, dass auch eine Transportverschlüsselung ausreichend sein kann, wenn es keine strengeren gesetzlichen Vorgaben gibt und die Sensibilität der verarbeiteten Daten dies zulässt. Damit geht es weiter als die bereits differenzierende Orientierungshilfe des AK Technik zu „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ vom 13.03.2020.

Secorvo News

T.I.S.P. und IT Security Insights

In der Woche **19.–23.09.2022** bieten wir Ihnen mit dem T.I.S.P.-Seminar die nächste Gelegenheit zur Zertifizierung Ihrer Kenntnisse in der IT-Sicherheit.

In der darauffolgenden Woche können Sie Ihre Kenntnisse in aktuellen Themen der Informationssicherheit und des Datenschutzes auf dem Seminar IT Security Insights auffrischen (**27.–29.09.2022**). Wir freuen uns auf Ihre Anmeldung!

Hokus Pokus Fidibus

Wie geht das – Entwicklung und Produktion von Hardware-Security-Modulen in Deutschland? Welche Herausforderungen sind damit verbunden – und wie werden die von einem der wenigen deutschen Hersteller von IT-Security Hardware gemeistert, der WIBU-SYSTEMS aus Karlsruhe? Das grenzt manchmal schon an Zauberei …

Erfahren Sie bei unserem kommenden KA-IT-Si-Event am **15.09.2022** aus erster Hand, welche Hürden bei der Entwicklung, den Multiplattform-Tests, der Beschaffung und der sicheren Produktion von Security Controllern „Made-in-Germany“ zu bewältigen sind.

Wir erhalten die seltene Gelegenheit, die Fertigung zu besichtigen und Einblick in die automatisierten Prozesse des Downloads finaler Firmware, der Schlüsselerzeugung und optional individueller Schlüsselspeicherung für kundenspezifische Produkte zu bekommen. Die Spezialisten von WIBU-SYSTEMS und der Vorstand Oliver Winzenried stehen Ihnen dabei Rede und Antwort.

Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ mit einem phänomenalen Blick auf den Schwarzwald (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2022	
19.-23.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
26.-30.09.	Informatik 2022 (GI, Hamburg)
27.-29.09.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
Oktober 2022	
04.-06.10.	heise devSec 2022 (dpunkt verlag, heise, Karlsruhe)
17.-19.10.	IDACON 2022 (WEKA-Akademie, München)
24.-26.10.	ISSE 2022 (IEEE, Wien/A)
25.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
25.-27.10.	it-sa 2022 (NürnbergMesse GmbH, Nürnberg)
November 2022	
07.-11.11.	ACM CCS 2022 (ACM/SIGSAC, Los Angeles/US)
09.-10.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)

Fundsache

Der Beirat Digitaler Verbraucherschutz des BSI hat Empfehlungen zur Kommunikation über Passwörter veröffentlicht. Danach sollen Unternehmen ihre Online-Dienste mit 2FA-Authentizierung absichern und Nutzern verständliche Passwort-Regeln vermitteln; Nutzer wiederum sollen angehalten werden, Passwörter in Passwort-Managern zu speichern und nicht mehrfach zu verwenden.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2022



Androide Gegner

Noch sind sie nicht die Regel, aber vereinzelt dürften sie bereits vorkommen: mit künstlicher Intelligenz optimierte Angreifer.

Das wachsende Angebot Cloud-basierter – also schnell und kostengünstig skalierbarer – KI-Systeme bietet immer mehr leistungsfähige Möglichkeiten, Angriffe auf IT-Systeme mit maschinellem Lernen zu verbessern.

Dass Angreifer die Suche nach bekannten Schwachstellen mit Crawlern automatisieren, ist lange bekannt. Auch die mühsame manuelle Suche nach Schwächen in der Eingabe-Validierung von Web-Anwendungen wird seit vielen Jahren mit Fuzzy-Systemen maschinell unterstützt.

Doch inzwischen könnten KI-Systeme auch gänzlich neue Schwachstellen identifizieren – vorausgesetzt, man würde sie mit geeigneten Samples „füttern". Ist der Source Code (wie z. B. bei Open-Source-Lösungen) zugänglich, funktioniert das zumindest im Labor.

Aber auch herkömmliche Angriffsmethoden lassen sich mit KI-Systemen perfektionieren. So können „Textgenerierungs-KIs" bereits heute beispielsweise an den Stil eines bestimmten Absenders adaptierte E-Mails formulieren, die von dessen eigenen nicht zu unterscheiden sind (siehe SSN 8/2022). Ein ideales Hilfsmittel für Spear-Phishing-E-Mails – und eine perfekte Methode, um CEO-Fraud zu optimieren. Schlimmer noch: Mit Stimm-Samples eines CEO trainiert kann ein KI-gesteuerter Sprachgenerator (siehe SSN 10/2020) einen täuschend echten Anruf des CEO vorspielen, sodass selbst engste Mitarbeiter die Falle nicht erkennen. Ganz ähnlichen Angriffen sehen sich heute biometrische Authentifikationsverfahren ausgesetzt. KI-Systeme können Bilder, Videos oder auch Fingerabdrücke erzeugen, die sich von echten nicht unterscheiden lassen.

Auch wenn KI-Systeme den Turing-Test noch nicht bestehen – in der Hand von Angreifern sind sie bereits ein gefährlicher Gegner.



Inhalt

Heimlicher Gegner

Security News

Bug-Bounty-Marketing

Nmap-Jubiläum

Missbräuchliche Abmahnungen

Déjà-vu

Falsch verstandene Transparenz

Secorvo News

Teamverstärkung

T.I.S.P. und BSI Vorfall-Experte

Gotcha.

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Bug-Bounty-Marketing

Finden Forscher Schwachstellen in Software-Produkten, so erfolgt oft eine „responsible disclosure", sprich: eine Vorab-Benachrichtigung des Herstellers, die diesem Zeit einräumt, die Schwachstelle vor der Veröffentlichung zu beheben. Nach Ablauf dieser Karenzzeit werden Ursache und Auswirkungen der Schwachstelle meist als CVE (Common Vulnerabilities and Exposures) veröffentlicht. Um Nutzer der Software vor der Schwachstelle zu warnen, erfolgt die Veröffentlichung auch dann, wenn der betroffene Hersteller nicht reagiert hat. Inzwischen wird die Suche nach Schwachstellen von einigen Unternehmen durch Bug-Bounty-Programme gefördert: Wer eine Schwachstelle meldet, erhält eine kleine oder auch etwas größere Prämie. Das ist erstmal alles nicht neu (siehe SSN 12/2019).

Findet man zu einem Produkt wenige oder sogar keine CVEs, so kann das bedeuten, dass sich noch niemand die Mühe gemacht, es zu untersuchen. Bei verbreiteten Produkten ist es aber wahrscheinlicher, dass keine (oder nur wenige) Schwachstellen gefunden werden konnten – und das spricht für die Qualität des Produkts.

Wie die Forscher von modzero am 22.08.2022 veröffentlichten, gibt es allerdings noch eine dritte Möglichkeit: Jemand hat das Produkt untersucht, Schwachstellen festgestellt, sie dem Hersteller gemeldet, eine Prämie erhalten – sich aber über die Bestimmungen des Bug-Bounty-Programms verpflichtet, keine CVE zu veröffentlichen. Das Fehlen von CVEs sagt daher inzwischen leider wenig über die Sicherheit eines Produktes aus – Bug-Bounty-Programme als irreführendes Marketing…

Nmap-Jubiläum

Unglaublich, aber wahr: Nmap, der wohl bekannteste Netzwerk-Portscanner („Network Mapper"), wird 25 Jahre alt. Damit ist Nmap eines der (wenn nicht das) am längsten fortlaufend gepflegte Werkzeug für IT-Sicherheitsfachkräfte, Netzwerker und Administratoren. Die Entwicklung vom einfachen Portscanner über die Erkennung von Diensten und Betriebssystemen bis zur Bedienung über eine grafische Oberfläche – die Liste der Erweiterungen im Changelog ist lang. Nach wie vor kann man performant komplette Netzbereiche durchforsten und so bekannte und ggf. auch nicht zuzuordnende IT-Systeme und Netzwerk-Dienste finden.

Mit Nmap gelingt das genauso zuverlässig (und kostenlos) auch in der OT (Operational Technology) – zur Identifikation von im Netz erreichbaren Systemen muss man auch heute keine komplexen und kostspieligen Werkzeuge beschaffen. Wer wissen will, welche Systeme und Dienste in den eigenen Netzen – seien es Leittechnik oder Bürokommunikation, die DMZ oder der „Blick" vom Internet auf das eigene Netz – dem empfehlen wir der Einsatz von Nmap. Wir gratulieren, Fyodor!

Missbräuchliche Abmahnungen

Seit August erfasst eine Abmahnwelle Unternehmen und Privatpersonen in Österreich und Deutschland, die auf ihren Webseiten bei Google gehostete Fonts eingebunden haben. Darin werden – mit Bezug auf das Urteil des LG München (siehe SSN 6/2022) – Schadensersatzforderungen in Höhe von 100-200 € nach Art. 82 DSGVO geltend gemacht.

Tatsächlich sind die Schadensersatzansprüche in den meisten Fällen unbegründet, da der Anspruchsteller zur Ermittlung des Einsatzes von Google Fonts einen WebCrawler nutzt und die Abmahnungen automatisiert verschickt. Der Anspruchsteller war demnach nie persönlich auf den Webseiten, womit der Tatbestand des Art. 82 Abs. 1 DSGVO nicht erfüllt ist, da er nicht als natürliche Person betroffen war; die Schadensersatzforderung selbst erfolgt rechtsmissbräuchlich. In Österreich erstatteten daher Anwälte von Betroffenen Anzeige wegen gewerbsmäßigen Betrugs.

Der Fall zeigt, dass man beim Erhalt von Abmahnungen nicht vorschnell einen geforderten Schadensersatz direkt begleichen sollte. Wir empfehlen in einem solchen Fall Ruhe zu bewahren, zunächst die Begründetheit des Anspruchs genau zu prüfen und ihn gegebenenfalls zurückzuweisen.

Davon unbenommen sollte man allerdings auf der eigenen Webseite verwendete Google Fonts tatsächlich nicht einbinden, sondern auf dem eigenen Server hosten – Anleitungen dafür und hilfreiche Tools finden sich zahlreich im Internet.

Déjà-vu

Am 12.09.2022 stellte Martin Rost auf der Sommerakademie des ULD Schleswig-Holstein Neuerungen beim Standard Datenschutzmodell (SDM) sowie die Ergebnisse einer Umfrage zur Nutzung des SDM vor. Die wichtigste (und begrüßenswerte) Neuerung: Im Baustein 41 wurde eine aus dem IT-Grundschutz stammende Soll-Ist-Prüfung aufgenommen. Die in der Umfrage geäußerten Erfahrungen der Nutzer des SDM decken sich allerdings mit unseren Praxiserfahrungen: Es ist sehr aufwändig, die beschriebenen Maßnahmen zu prüfen und umzusetzen.

Das klingt nach einem déjà-vu. Im Jahr 2018 hatte das Bundesamt für Sicherheit in der Informations-

technik (BSI) aus denselben Gründen nach 15 Jahren die umfänglichen Maßnahmenvorschriften im IT-Grundschutz-Katalog auf Anforderungen an die Informationssicherheit in Form des IT-Grundschutz-Kompendiums umgestellt. Das BSI hatte (endlich) erkannt, dass Betreiber von Managementsystemen die operative (und unternehmerische) Freiheit benötigen, risikobezogen über Maßnahmen und deren Umsetzung zu entscheiden.

Im CON.2-Baustein des IT-Grundschutz-Kompendiums referenziert das BSI auf das SDM, aber es hat wohl geahnt, dass man Unternehmen besser nicht zur Umsetzung zwingt. Ein weiser Schritt, denn es gibt auch andere, kostengünstigere Wege, ein wirksames Datenschutz-Managementsystem (DSMS) aufzubauen, als alle Gewährleistungsziele mit Maßnahmenbergen zu erschlagen. Die Vorgehensweise nach dem SDM ist grundsätzlich gut, allerdings sollten die Bausteine wie beim „neuen" Grundschutz praxistauglicher gestaltet werden.

Falsch verstandene Transparenz

Seit dem 01.08.2022 sind die Inhalte des „Gemeinsamen Registerportals der Länder" kostenfrei abrufbar. Das ist das Ergebnis der unmittelbaren Anwendung der „Digitalisierungsrichtlinie" der EU (Richtlinie 2019/1151) vom 20.06.2019 durch das Gesetz zur Umsetzung der Digitalisierungsrichtlinie (DiRUG). Dem Inkrafttreten folgte ein „Aufschrei", weil nun über das Registerportal auch Dokumente eingesehen werden können, die zuvor nicht ohne weiteres zugänglich waren – wie die Privatadressen von Unternehmern, Geschäftsführern und Aufsichtsräten oder deren gescannte Unterschriften. Frei verfügbare Daten, die geradezu zum Missbrauch einladen.

Ziel der Digitalisierungsrichtlinie ist es, digitale Unternehmensgründungen zu vereinfachen und durch Transparenz Missbrauch und Betrug vorzubeugen. Klare Vorgabe des Gesetzgebers ist es, dass dabei die Grundsätze des Datenschutzes nach der DSGVO zu berücksichtigen sind. Bei der deutschen Umsetzung ist das zumindest teilweise schiefgegangen, da die beteiligten Registergerichte offensichtlich keine Interessenabwägung zwischen den schutzwürdigen Interessen der Unternehmer und der Sicherstellung von Vertrauenswürdigkeit durch Transparenz vorgenommen haben.

Fein raus sind lediglich Unternehmen, die ihre Dokumente vor dem 01.01.2007 eingereicht haben – die liegen nicht digital vor und sind daher auch nicht online abrufbar. Es ist zu hoffen, dass die Regelung einer Überprüfung unterzogen wird.

Secorvo News

Teamverstärkung

Seit dem 01.09.2022 verstärkt uns Oliver Oettinger in den Sicherheitsthemen Public Key-Infrastrukturen und Forensik. Herzlich willkommen im Secorvo-Team!

T.I.S.P. und BSI Vorfall-Experte

In der Woche **14.–18.11.2022** bieten wir Ihnen mit dem T.I.S.P.-Seminar die letzte Gelegenheit in diesem Jahr zur Zertifizierung Ihrer Kenntnisse in der IT-Sicherheit. Nach Eingang Ihrer Anmeldung erhalten Sie das von Secorvo verfasste Begleitbuch zum T.I.S.P. zur Vorbereitung auf das Seminar und die anschließende Prüfung. Wir empfehlen eine baldige Anmeldung.

Unser letztes Seminarangebot in diesem Jahr ist die Vorbereitung auf die Zertifizierung zum BSI Vorfall-Experten nach dem Curriculum des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der Kalenderwoche 48 (**29.11.–01.12.2022**). Wir freuen uns auf Ihre Anmeldung!

Die Seminar-Programme und weitere Informationen zu unseren Seminaren finden Sie auf unserer Webseite unter https://www.secorvo.de/seminare.

Gotcha.

Das Nachverfolgen oder das Erstellen von Profilen zu Besuchern von Webseiten mittels Cookies ist bekannt und bekommt öffentliche Aufmerksamkeit – bei E-Mails haben Tracking und Profiling hingegen bisher kaum Aufmerksamkeit erfahren, obwohl diese bei Newslettern und deren Inhalten regelmäßig angewendet werden.

Auf dem kommenden Online-Event der KA-IT-Si am 03.11.2022 stellen Milan Burgdorf und Christian Blaicher (Secorvo) exemplarisch die technischen Möglichkeiten und Umsetzungen für Tracking und Profiling in E-Mails vor und beleuchten die rechtlichen Rahmenbedingungen für deren Verwendung. Wir freuen uns auf Ihre Teilnahme.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Oktober 2022	
04.-06.10.	heise devSec 2022 (dpunkt verlag, heise, Karlsruhe)
17.-19.10.	IDACON 2022 (WEKA-Akademie, München)
24.-26.10.	ISSE 2022 (IEEE, Wien/A)
25.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
25.-27.10.	it-sa 2022 (NürnbergMesse GmbH, Nürnberg)
November 2022	
07.-11.11.	ACM CCS 2022 (ACM/SIGSAC, Los Angeles/US)
09.-10.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
14.-18.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
29.11.-01.12.	BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe)
Dezember 2022	
05.-08.12.	Black Hat Europe 2022 (Blackhat, London/UK)

Fundsache

Die Landesdatenschutzbeauftragte für den Datenschutz Niedersachsen hat im August 2022 FAQ zur Auftragsverarbeitung nach Art. 28 DSGVO veröffentlicht, die auf 15 Seiten lebensnahe Antworten zu Fragen rund um AV-Verträge geben.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2022



SPoTs

Viele Desaster haben ihren Ursprung in einem „Single Point of Failure“ (SPoF) – einem Glied in einer wichtigen Prozesskette, dessen Ausfall nicht kompensiert werden kann und den Prozess zum Stillstand (oder, schlimmer noch, zum Kippen oder Aufschwingen) bringt. So gab es auf der Titanic, als nach der Kollision mit einem Eisberg sechs statt maximal vier geschottete Bereiche voll Wasser liefen, nicht genügend Rettungsboote, um alle Passagiere aufzunehmen. Und in Tschernobyl löste eine Stromabschaltung im Rahmen eines Sicherheitstests die Katastrophe aus.

Besonders bei der Digitalisierung ist ein SpoF schnell übersehen: Analoge Fall-Back-Lösungen, auf die man sich bei der Prozesseinführung noch verlassen konnte, verschwinden unvermittelt, ohne dass ihre Rolle im Prozess bedacht wird. Oder ein SPoF wird „sehenden Auges“ in Kauf genommen, weil die Alternativlösung teuer ist oder ein Ausfall unwahrscheinlich erscheint – und schon steht die Gasversorgung auf der Kippe.

Eine ähnliche Rolle spielen „Single Points of Trust“ (SPoT) in IT-Infrastrukturen. Sie werden besonders leicht übersehen, weil ihre Bedeutung meist nur Experten verständlich und selbst diesen nicht immer präsent ist. So hängt die Sicherheit einer Verschlüsselungslösung beispielsweise am Zufallszahlengenerator oder die des Unternehmensnetzwerks am Zugang zum Domain-Controller. Angreifer und Nachrichtendienste lieben SPoTs, denn sie erlauben fokussierte Angriffe mit großer Wirkung und eher geringem Entdeckungsrisiko.

Die SPoTs des Internet sind die Root-Zertifikate in Browsern und Betriebssystemen. Wer darüber verfügt, kann vertrauenswürdige Software, Webseiten und E-Mails erzeugen. Nach einer Untersuchung der Washington Post vom 08.11.2022 könnte das amerikanischen Nachrichtendiensten über einen Spyware-Spezialisten unter dem Decknamen TrustCor gelungen sein. Mehr als 10.000 Zertifikate sind betroffen. Nicht zum ersten Mal.



Inhalt

SPoTs

Security News

ITSIG 2.0-Umsetzung

Safe Harbor III

Grundschutz-Renovierung

Unvollstreckbar

AV mit US-Konzerntöchtern

BCM-Standard

Cookie-Nervenschoner

Cybersecurity Skills

Secorvo News

Secorvo Seminare

Lernen wird überbewertet

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

ITSIG 2.0-Umsetzung

Für Unternehmen, die zur kritischen Infrastruktur zählen, dürfte die am 29.09.2022 vom BSI veröffentlichte finale Version der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung von großer Bedeutung sein. Darin konkretisiert das BSI die Umsetzung der Anforderungen aus § 8a BSI Absatz 1a. Vor dem Hintergrund, dass das ITSIG 2.0 bereits im Mai 2021 verabschiedet wurde und die Anforderungen daher bis Mai 2023 umgesetzt werden müssen, kommt die Veröffentlichung überraschend spät – umso mehr, als die Orientierungshilfe sehr umfangreiche Detailanforderungen stellt.

Safe Harbor III

Die am 07.10.2022 von US-Präsident Biden unterzeichnete Executive Order soll das neue transatlantische Data Privacy Framework vorbereiten. Die Verordnung sieht ein Datenschutzüberprüfungsgericht vor und führt den Verhältnismäßigkeits- und Notwendigkeitsgrundsatz für den Zugriff auf Daten durch US-Geheimdienste ein. Damit wollen die USA die Anforderungen aus dem Schrems-II-Urteil des EuGH (siehe SSN 8/2020) umsetzen.

Doch es gibt bereits Kritik. So ist zum einen eine Executive Order kein Gesetz, sondern lediglich eine interne Anweisung an US-Bundesbehörden. Zum anderen ist das zu gründende „Gericht" lediglich eine beim Director of National Intelligence angesiedelte Verwaltungsstelle zur Entgegennahme und Prüfung von Beschwerden. Der LfDI Baden-Württemberg, Dr. Stefan Brink, hat am 26.10.2022 erhebliche Zweifel geäußert, dass damit den Anforderungen des EuGH entsprochen wird.

Auch Max Schrems hat bereits am 07.10.2022 eine detaillierte Prüfung angekündigt. Nun muss die EU-Kommission entscheiden, ob sie auf dieser Basis einen neuen Angemessenheitsbeschluss erlassen kann. Eines ist jedenfalls sicher: Sollte es zu einer Anerkennung der EU kommen, ist ein weiteres EuGH-Urteil unausweichlich.

Grundschutz-Renovierung

Wegen der kontinuierlichen Weiterentwicklung des IT-Grundschutzes müssen zertifizierte Organisationen neue Bausteine im Blick behalten. Dazu pflegt das BSI eine Liste der Final-Draft-Versionen der Bausteine, die überarbeitet oder neu im IT-Grundschutz-Kompendium erscheinen werden, ggf. ergänzt um ein Änderungsdokument. Kürzlich wurden in der Liste 11 Bausteine als Final Draft publiziert, die 2023 in das Kompendium aufgenommen werden sollen. Die beiden prominentesten sind wohl SYS.1.1 Allgemeiner Server und SYS.1.2.3 Windows Server. Hier stechen vor allem die Hinweise auf die Modellierung vom Baustein SYS.1.1 und die Veröffentlichung eines Bausteins für Windows Server unabhängig von einem konkreten Release ins Auge.

Unvollstreckbar

Am 20.10.2022 hat die französische CNIL, wie zuvor bereits die italienische, die griechische und die britische Datenschutzaufsichtsbehörde, gegen das US-Unternehmen Clearview AI ein Bußgeld in Höhe von 20 Mio. € verhängt. Clearview AI durchsucht das Internet nach öffentlich verfügbaren Fotografien von Gesichtern, erfasst diese und bietet u. a. Strafverfolgungsbehörden Zugriff auf diese Datenbank an, um Personen mit Gesichtserkennungsverfahren zu identifizieren (siehe SSN 1/2020). Dagegen haben Einzelpersonen sowie Privacy International Einspruch erhoben.

Zuvor hatten die Aufsichtsbehörden in Absprache unabhängig voneinander Clearview AI aufgefordert, auf ihrem Staatsgebiet die Erhebung und Nutzung von Daten von Personen ohne Rechtsgrundlage einzustellen und die Ausübung der Betroffenenrechte sicherzustellen. Clearview AI reagierte nicht oder verwies darauf, dass es keiner Geschäftstätigkeit innerhalb der EU nachgehe.

Da Clearview AI nicht über einen europäischen Repräsentanten oder eine europäische Niederlassung verfügt, können die verhängten Bußgelder und Bescheide nicht vollstreckt werden. Das neue Data Privacy Framework mit den USA sollte daher auch die Durchsetzung europäischer Sanktionen regeln.

AV mit US-Konzerntöchtern

Am 07.09.2022 hob das Oberlandesgericht (OLG) Karlsruhe eine Entscheidung der Vergabekammer Baden-Württemberg auf, die den Einsatz von Infrastrukturdiensten europäischer Tochterunternehmen von US-Cloud-Anbietern als grundsätzlich datenschutzwidrig eingestuft hatte.

Ganz so einfach ist es demnach nicht: Allein aus der Tatsache, dass ein Dienstanbieter die europäische Tochter eines US-Konzerns ist, darf nicht geschlossen werden, dass das Unternehmen sein Leistungsversprechen nicht erfüllen kann. Die Konzernbindung führt nicht zwangsläufig zu rechts- und vertragswidrigen Weisungen der Konzernmutter, und es darf auch nicht unterstellt werden, dass die Geschäftsführung solche Weisungen ohne weiteres umsetzen wird. Wenn die europäische Gesellschaft vertraglich zusichert, dass sie die Daten

nur innerhalb der EU verarbeitet, darf man darauf vertrauen.

BCM-Standard

Am 26.09.2022 machte das BSI den zweiten Community Draft des Standards BSI 200-4 Business Continuity Management zugänglich. Anders als in der ersten Entwurfsversion richtet sich der Standard nicht mehr an einem Stufenmodell aus, sondern ist nach den einzelnen Prozessschritten strukturiert. Für die Umsetzung von Business oder IT-Service Continuity ist der Standard auch im derzeitigen Entwurfsstadium bereits eine hilfreiche Leitlinie.

Cookie-Nervenschoner

Die Verbraucherzentrale Bayern hat am 11.10.2022 den „Nervenschoner" vorgestellt, ein Browser-Plugin für Firefox und Chrome, das Cookie-Banner auf Webseiten blockiert. Da der EuGH für das Setzen von Cookies eine Einwilligung des Webseitenbesuchers fordert, kann bei einem blockierten und ausgeblendeten Cookie-Banner keine Einwilligung erteilt werden – was einem Click auf „Alles Ablehnen" entspricht. Der „Nervenschoner" basiert auf dem bekannten Browser-Plugin uBlock Origin und blockiert neben dem Einwilligungsbanner auch die zugehörigen Tracker. Er ist genau wie uBlock Origin Open Source Software.

Neben dem „Nervenschoner" gibt es ähnliche Tools, auch für andere Browser (wie beispielsweise Hush für Safari auf macOS und iOS), für die der „Nervenschoner" bisher nicht verfügbar ist.

Cybersecurity Skills

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) veröffentlichte am 19.09.2022 das European Cybersecurity Skills Framework (ECSF). Es soll ein gemeinsames Verständnis der Rollen, Kompetenzen, Fähigkeiten und Kenntnisse schaffen, die zur Gewährleistung von Cybersecurity in Unternehmen zusammenwirken sollten. Neben dem Chief Information Security Officer (CISO) beschreibt das ECSF elf weitere Rollen wie den Cyber Incident Responder, den Cybersecurity Educator oder den Digital Forensics Investigator.

Ergänzend zum ECSF stellte die ENISA ein 50seitiges Benutzerhandbuch online, in dem der Aufbau einer Cybersecurity-Organisationsstruktur u. a. anhand von sieben Use Cases veranschaulicht wird.

Für kleine und mittelständische Unternehmen dürfte das Konzept wie ein „overkill" wirken – ist es doch schon herausfordernd genug, die Rolle des CISO kompetent zu besetzen. Es zeigt allerdings auch, dass der für einen wirksamen Schutz vor Cyberangriffen erforderliche Aufwand nicht unterschätzt werden sollte.

Secorvo News

Seminarangebote

Unser letztes T.I.S.P.-Seminar in diesem Jahr (**14.–18.11.2022**) ist ausgebucht. Für Schnellentschiedene: Die nächsten Gelegenheiten für eine T.I.S.P.-Qualifizierung bieten wir am **27.–31.03.2023** und **19.–23.06.2023**, jeweils optional mit anschließender Prüfung. Und zur Vorbereitung legen wir Ihnen unser T.I.S.P.-Begleitbuch ans Herz, das wir Ihnen nach Ihrer Anmeldung zusenden.

Eine letzte Chance für eine Weiterbildung in diesem Jahr bieten wir Ihnen mit unserem neuen dreitägigen Seminar BSI Vorfall-Experte (**29.11.–01.12.2022**) – einige wenige Plätze haben wir noch frei.

Die vollständigen Programme und den Link zur Online-Anmeldung finden Sie auf unserer Webseite.

Lernen wird überbewertet

Vor rund einem Jahr sorgte die Schwachstelle log4j für erhebliche Aufregung. Der Auslöser wurde mittlerweile beseitigt, und viele der betroffenen Softwareprodukte von den Herstellern gepatcht.

Doch die tiefere Ursache des Problems besteht weiterhin. Denn die Schwachstelle war gar kein Fehler, sondern eine gewünschte Funktionalität, die über viele Jahre in der Bibliothek enthalten war. Das eigentliche Problem bestand vielmehr darin, dass eine komplexe und leistungsfähige Bibliothek für sehr einfache Aufgaben eingesetzt und an der Schnittstelle nutzergenerierte Inhalte ohne Input-Validierung übergeben wurden. Verursacher war also nicht log4j, sondern die Tatsache, dass die Bibliothek verwendet wurde, ohne zuvor zu prüfen, ob die Funktionalität überhaupt gebraucht wird.

Security-by-Design geht anders, wie Johann Grathwohl (CONITAS) auf dem kommenden **KA-IT-Si-Event am 08.12.2022** in seinem (Online-) Vortrag zeigen wird. Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2022	
07.-11.11.	ACM CCS 2022 (ACM/SIGSAC, Los Angeles/US)
09.-10.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
14.-18.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
29.11.-01.12.	BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe)
Dezember 2022	
05.-08.12.	Black Hat Europe 2022 (Blackhat, London/UK)
08.12.	KA-IT-Si-Event „Lernen wird überbewertet“ (KA-IT-Si, online)
Januar 2023	
20.-22.01.	ShmooCon 2023 (The Shmoo Group, Washington/US)

Fundsache

Auf iPhones und iPads dürfen Verschlusssachen der Kategorie VS-NfD „Nur für den Dienstgebrauch“ verarbeitet werden. Das hat das BSI am 05.10.2022 bestätigt. Voraussetzungen sind die Umsetzung von Vorgaben an das Nutzerverhalten, VPN-Anbindung und Mobile Device Management.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

November 2022



Festgebissen

Was die Animosität ausgelöst hat, wird sich kaum mehr feststellen lassen. Sicher ist: Die deutschen Aufsichtsbehörden haben sich auf Microsoft eingeschossen, wie die aktuelle Entscheidung der Datenschutzkonferenz (DSK) zu MS 365 vom 24.11.2022 belegt. Wie berechtigt die Kritik auch einmal gewesen sein mag: Sie bewirkte schon vor 20 Jahren einen Strategiewechsel bei Microsoft. Nicht nur, dass Microsoft sich bereits 2007 (!) beim ULD mit dem „Update Service 6.0“ und „WSUS 2.0“ für ein Datenschutz-Gütesiegel qualifizierte. Microsoft war auch der erste amerikanische Software-Riese, der 2014 mit auf das EU-Recht abgestimmten Verträgen für Office 365 auf Servern in Irland warb – lange bevor Cisco, Amazon oder Google auch nur das Problem verstanden hatten. Secorvo war seitdem bei vielen Unternehmen an der Abstimmung von MS 365-Verträgen gutachterlich oder mit einer DSFA beteiligt, und ich erinnere mich gut an meine eigene Überraschung über die hohe Qualität und Transparenz der Unterlagen von Microsoft. Seitdem hat Microsoft wiederholt nachgelegt, z. B. mit der Reaktion auf das Schrems-II-Urteil (New steps to defend your data und Initiative Tech fit 4 Europe) oder der Ankündigung einer „EU Data Boundary“ für die MS-Cloud am 06.05.2021. Auch zum CLOUD Act hat Microsoft Position bezogen und bemüht sich um möglichste Transparenz, z. B. durch Veröffentlichung aller Law Enforcement Requests.

Man mag argwöhnen, dass das substanzloses Marketing-Geklapper ist. Aber ist das plausibel? Anders als die US-Internet-Giganten lebt Microsoft nicht von Nutzerdaten. Im Gegenteil: Ein einziger begründeter Verdacht, dass Microsoft trotz seiner Zusicherungen Kundendaten missbraucht, würde den gesamten europäischen Markt zusammenbrechen lassen. Dem Datenschutz wäre mehr gedient, wenn die DSK sich endlich die erklärten Feinde des Datenschutzes vornehmen würde, anstatt das erkennbare Bemühen Microsofts mit fadenscheinigen Einwänden zu entmutigen.



Inhalt

Festgebissen

Security News

Abgelaufen

Abgesichert

Abgemeldet

Abgemahnt

Abgelehnt

Abgestraft

Secorvo News

E-Mail-Tracking

Seminarprogramm 2023

Lernen wird überbewertet

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Abgelaufen

Eine Möglichkeit, die Übermittlung personenbezogener Daten in Drittländer (also Ländern außerhalb des europäischen Wirtschaftsraums) ohne ein anerkannt gleichwertiges Datenschutzniveau rechtskonform zu gestalten ist der Abschluss eines Vertrags nach den von der EU Kommission vorgegebenen Standardvertragsklauseln. Die „alten" Standardvertragsklauseln aus dem Jahr 2001 wurden als Folge des Schrems-II-Urteil des EuGH mit Durchführungsbeschluss 2021/914 vom 04.06.2021 abgelöst (siehe SSN 6/2021). Bis zum 27.12.2022 müssen alle bestehenden Verträge auf die neuen Standardvertragsklauseln für internationalen Datentransfer umgestellt werden. Altverträge werden nach dem zweiten Weihnachtstag automatisch unwirksam – und damit die betroffene Datenübermittlung rechtswidrig.

Abgesichert

Die wachsende Bedeutung des Schutzes von Software Supply Chains wurde erst kürzlich durch die Veröffentlichung des Enduring Security Frameworks der NSA vom 24.08.2022 deutlich. Dabei spielen Code-Signaturen zum Schutz der Authentizität und Integrität von Software eine zentrale Rolle. Doch bis vor kurzem galten für Code-Signing noch Bedingungen, die denen der „Prä-LetsEncrypt-Ära" für Web-Zertifikate entsprachen: kompliziert, aufwändig, teuer. Besonders Open-Source-Entwickler scheuten den Aufwand zur Schlüsselverwaltung und Beschaffung von Zertifikaten. Das könnte sich nun ändern: Das am 17.11.2022 von Newman, Meyers und Torres-Arias veröffentlichte Open-Source-Projekt „Sigstore" – inspiriert durch Let's Encrypt – könnte die Hürden für Code-Signaturen deutlich senken. Dahinter steckt eine Sammlung von Werkzeugen, mit deren Hilfe Code(fragmente) extrem einfach signiert und zur Prüfung in Transparency Logs veröffentlicht werden können. Unter der etwas irreführenden Bezeichnung „keyless signing" arbeitet Sigstore mit Einmalschlüsseln, für die nach einer Bestätigung der Identität des Entwicklers über OpenID-Connect ein kurzlebiges Zertifikat ausgestellt wird. Mit diesem kann ein Codefragment signiert, im Log veröffentlicht und von jedermann auf Gültigkeit überprüft werden. Sigstore übernimmt das Schlüsselmanagement für den Entwickler. Dieser muss sich lediglich um den Schutz seiner OpenID kümmern.

Abgemeldet

Der Messenger-Dienst WhatsApp bedient sich bekanntlich (SSN 4/2016) am Adressbuch des Smartphones und lädt auch die Namen und Telefonnummern von Personen hoch, die weder bei WhatsApp noch bei Instagram oder Facebook ein Benutzerkonto haben. Zu diesen Personen erstellt Meta ein sogenanntes Schattenprofil.

Bisher waren die Möglichkeiten begrenzt, das zu verhindern. Verwehrt man WhatsApp den Adressbuchzugriff, wird bei jeder Nachricht nur noch die Telefonnummer des Absenders angezeigt – eine erhebliche Komforteinbuße.

Zwar steht Betroffenen nach der DSGVO ein Recht auf Löschung zu, jedoch werden die Daten nach einer Löschung beim nächsten Adressbuchabgleich erneut an Meta übermittelt. Und der Versand von Unterlassungserklärungen an alle eigenen Telefonbuchkontakte ist keine besonders freundschaftserhaltende Option.

Am 31.10.2022 berichtete Shona Ghosh bei Businessinsider, dass Meta offenbar seit Mai 2022 „Nicht-Kunden" eine Möglichkeit bietet, im globalen Meta-Adressbuch nach der eigenen Telefonnummer oder E-Mail-Adresse zu suchen – und sie auf Wunsch löschen und in eine „Blacklist" aufnehmen zu lassen. Der Link ist in den „Informationen für Personen, die keine Meta-Produkte nutzen" versteckt – im Absatz „Klicke hier, wenn du eine Frage zu den Rechten hast, die dir möglicherweise zustehen." Irreführender geht es kaum.

Abgemahnt

Die systematischen und automatisierten Abmahnungen von Webseitenbetreibern wegen der Einbindung von Google Fonts (SSN 8/2022) reißen nicht ab. Neuerdings enthalten einige Abmahnschreiben neben Schmerzensgeldanspruch und Gebührenrechnung auch noch ein Auskunftsersuchen.

Zwar sind Zweifel angebracht, dass die Erheblichkeitsschwelle für die Geltendmachung eines Schadensersatzanspruchs überschritten ist (vgl. OLG Frankfurt/Main, Urteil v. 30.06.2022, 16 U 229/20). Einem Auskunftsersuchen hingegen ist unabhängig davon nachzukommen. Allerdings muss der Betroffene dafür seine Identität nachweisen. Stellt sich jedoch heraus, dass die Berufung auf die Betroffenenrechte missbräuchlich erfolgt, besteht auch keine Auskunftspflicht.

Abgelehnt

Am 24.11.2022 veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Zusammenfassung des Berichts zum datenschutzkonformen Einsatz von Microsoft 365 und stellt fest, „dass der Nachweis von Verantwortlichen, Microsoft 365 da-

tenschutzrechtskonform zu betreiben, (...) nicht geführt werden kann." Kernpunkt der Kritik ist weiterhin die Datenverarbeitung von Microsoft für legitime Geschäftszwecke und die angebliche Unmöglichkeit, der Rechenschaftspflicht als Auftragsverarbeiter beim Einsatz von Microsoft 365 wegen intransparenter Datenverarbeitungen durch Microsoft nachzukommen.

Hier verliert die DSK völlig aus dem Blick, welche Anforderungen vernünftigerweise an eine Auftragsverarbeitung zu stellen sind. Dass ein Unternehmen zur Erfüllung der Rechenschaftspflicht seines Auftraggebers sämtliche Datenverarbeitungen und damit auch gegebenenfalls Geschäftsgeheimnisse offenlegen soll, ist nicht nachvollziehbar. Unberücksichtigt bleibt auch, dass Microsoft eine bestimmte Menge an Diagnose- und Telemetriedaten verarbeiten muss, um die angebotenen Dienste überhaupt vertragsgemäß erbringen zu können. Warum die DSK zudem nicht die angekündigten Neuerungen in Sachen EU Data Boundary abgewartet hat, ist nicht zu verstehen.

Microsoft hat in einer Stellungnahme bereits auf die Verlautbarung reagiert und die Kritik (erwartungsgemäß) zurückgewiesen. Für Verantwortliche aus dem öffentlichen Sektor bringt das DSK-Papier viel Arbeit mit sich, wenn sie Microsoft 365 dennoch datenschutzkonform einsetzen möchten – möglich bleibt das jedoch, aller Kritik zum Trotze.

Abgestraft

Im Jahr 2018 hatten 40 (!) US-amerikanische Bundesstaaten Google wegen der heimlichen Sammlung von Standortdaten verklagt. Auslöser war ein Bericht von Keith Collins vom 21.11.2017, in dem er aufdeckte, dass Android seit Anfang 2017 auch bei abgeschalteten Location Services und sogar ohne eingelegte SIM-Karte Standortinformationen in Gestalt der Cell ID der Mobilfunkzellen in Reichweite sammelt und an Google übermittelt, sobald das Smartphone wieder online ist.

Nach vier Jahren wurde Google nun am 14.11.2022 zur Zahlung einer Geldstrafe von 391,5 Mio. US$ verurteilt – ein historisches Urteil, nicht nur wegen der Höhe der Strafe, sondern weil es zeigt, dass sich auch in den USA langsam eine Sensibilität für die Schutzwürdigkeit der Privatsphäre entwickelt.

Secorvo News

E-Mail-Tracking

Das Nachverfolgen (Tracking) von Webseitenbesuchen und die Erstellung von Besucherprofilen stehen schon lange im Fokus des Datenschutzes und müssen von Anbietern via Cookie-Banner transparent gemacht werden. Tracking und Profiling bei E-Mails sind hingegen bisher der Aufmerksamkeit von Aufsichtsbehörden entgangen – obwohl sie bei E-Mail-Newslettern inzwischen üblich sind. Meist erfolgt das heimlich – und verstößt somit gegen geltendes Datenschutzrecht.

Am 03.11.2022 gaben Christian Blaicher und Milan Burgdorf beim KA-IT-Si-Event „Gotcha. E-Mail-Tracking und -Profiling" einige vertiefte technische und rechtliche Einblicke in das Thema. Dabei ging es einerseits darum, wie Unternehmen E-Mail Tracking und Profiling innerhalb der Grenzen der DSGVO und des TTDSG rechtskonform gestalten können. Andererseits wurde erläutert, wie sich Empfänger solcher E-Mails sowohl rechtlich als auch technisch davor schützen können. Die Referenten haben das Wichtigste in einem Handout zusammengefasst.

Sollten Sie den Vortrag verpasst haben: Christian Blaicher wird zu dem Thema auf der DFN-Konferenz „Sicherheit in vernetzten Systemen" am 09.02.2023 um 14 Uhr in Hamburg vortragen.

Seminarprogramm 2023

Seit Ende November ist der Secorvo-Seminarkalender 2023 online – just in time für Ihre frühzeitige Weiterbildungsplanung im kommenden Jahr.

Lernen wird überbewertet

Vor rund einem Jahr sorgte die Schwachstelle log4j für erhebliche Aufregung. Der Auslöser ist mittlerweile beseitigt, und viele der betroffenen Softwareprodukte wurden von den Herstellern gepatcht. Doch die tiefere Ursache des Problems besteht weiterhin. Denn die Schwachstelle war gar kein Fehler, sondern eine gewünschte Funktionalität, die über viele Jahre in der Bibliothek enthalten war.

Das eigentliche Problem bestand darin, dass eine komplexe und leistungsfähige Bibliothek für sehr einfache Aufgaben eingesetzt und an der Schnittstelle nutzergenerierte Inhalte ohne Input-Validierung übergeben wurden. Verursacher war also nicht log4j, sondern die Tatsache, dass die Bibliothek verwendet wurde, ohne zuvor zu prüfen, ob die Funktionalität überhaupt gebraucht wird.

Security-by-Design geht anders, wie Johann Grathwohl (CONITAS) auf dem kommenden KA-IT-Si-Event am **08.12.2022** in seinem Vortrag „Log4j und was wir (nicht) daraus gelernt haben" zeigen wird. Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Dezember 2022	
05.-08.12.	Black Hat Europe 2022 (Blackhat, London/UK)
08.12.	Lernen wird überbewertet (KA-IT-Si, virtuell)
Januar 2023	
20.-22.01.	ShmooCon 2023 (The Shmoo Group, Washington/US)
Februar 2023	
08.-10.02.	30. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
13.-16.02.	OWASP 2023 Global AppSec (OWASP Foundation, Dublin/IRL)
März 2023	
14.-16.03.	secIT 2023 (Heise Medien, Hannover)
21.-22.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
27.-31.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Am 11.11.2022 veröffentlichte die ENISA die TOP 10 aufkommenden Cybersicherheitsbedrohungen bis 2030. Neben aktuell diskutierten Bedrohungen wie gefährdeten Lieferketten oder Desinformationskampagnen werden darin auch der Missbrauch intelligenter Geräte oder künstlicher Intelligenz und Lösungen für die erwarteten Herausforderungen in der Cybersicherheit beschrieben.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Dezember 2022



Runder Kopf

Der Kopf ist rund, damit das Denken die Richtung wechseln kann.
Francis Picabia

Verfolgt man, welche Standpunkte in jüngster Zeit zum Thema Datenschutz eingenommen werden, lassen sich nur zwei Positionen finden: Die derjenigen, die jegliche Risiken für die Betroffenen vermeiden, und die derjenigen, die den Datenschutz am liebsten ganz abschaffen möchten.

So fordert Alena Buyx, Vorsitzende des deutschen Ethikrats, am 08.12.2022 im Interview mit der Süddeutschen Zeitung, nicht über Risiken von Daten zu sprechen, sondern über deren Nutzen. Zu viel Datenschutz gefährde Patienten. Liest man hingegen beispielsweise die FAQ zu MS365 des LfDI Rheinland-Pfalz, so scheint nach Auffassung der Aufsichtsbehörden eine Verarbeitung nur noch zulässig zu sein, wenn keinerlei Risiken für den Betroffenen verbleiben.

Beide Positionen gehen am Kern der DSGVO vorbei. Denn dort geht es in erster Linie um den Umgang mit möglichen Risiken: So dürfen personenbezogene Daten im lebenswichtigen Interesse der Betroffenen immer verarbeitet werden (Art. 6 Abs. 1 d)), während sich in anderen Fällen die Zulässigkeit einer Verarbeitung nach der Frage richtet, welche konkreten Risiken es gibt, wie wahrscheinlich deren Eintritt ist und welche Maßnahmen dagegen ergriffen werden (können). Schließlich soll nach dem Grundsatz „Privacy by Design" der Datenschutz schon bei der Konzeption und Entwicklung innovativer Lösungen mitberücksichtigt werden.

Auch die datenschutzrechtlich Verantwortlichen sind Grundrechtsträger und verfolgen berechtigte Interessen. Die sind abzuwägen gegen die schutzwürdigen Interessen der Betroffenen. Das gelingt nur mit einem unverstellten Blick auf die tatsächlichen Risiken und die Umstände des Einzelfalls. Das ist mühsamer als ein pauschales „so nicht" – wird aber zu besseren Entscheidungen führen.



Inhalt

Runder Kopf

Security News

Spy Kit

Domain-Trickserei

Threema-Verschlüsselung

Bußgeld-Krimi

Garantien von Microsoft

Mit Daten bezahlen

Secorvo News

Seminare

Veranstaltungshinweise

secorvo
security consulting

Security News

Spy Kit

Die Firma Pushwoosh vertreibt Software Development Kits (SDK) zur Auswertung von Nutzeraktivitäten in Apps (Tracking, Profiling), die Entwickler in ihre Programme integrieren können. Nach der Webseite des Herstellers nutzen bereits über 80.000 Firmen ein Pushwoosh-SDK.

Am 14.11.2022 wurde das vorgeblich in den USA ansässige Unternehmen nach Reuters-Recherchen in Novosibirsk verortet: Es hat 40 Mitarbeiter und einen Jahresumsatz von (umgerechnet) 2,4 Mio. €. „Mailand oder Madrid, Hauptsache Italien!" möchte man da fast sagen… Am selben Tag veröffentlichte Internet Safety Labs eine Liste einiger tausend Apps, die vorgeblich Pushwoosh-Code verwenden – darunter auch Training-Apps der US Army. Offenbar hatte man angenommen, das Unternehmen käme aus Washington D.C.

Tatsächlich bietet die Webseite von Pushwoosh Anlass für Skepsis: Eine Firmenanschrift sucht man dort vergeblich. Wer fremde Software in seine „Supply Chain" integriert, sollte daher schon genau hinsehen – vor allem, wenn der Code Nutzerdaten auf externe Server überträgt.

Domain-Trickserei

Schon immer konnte man den Kartendienst Google Maps sowohl über maps.google.com als auch über google.com/maps erreichen. Wie Rutger Roffel am 02.12.2022 auffiel, ersetzt Google jedoch neuerdings die URL maps.google.com beim Aufruf durch google.com/maps. Kleiner Schritt – große Wirkung:

Bisher waren alle Dienste von Google (wie news.google.com oder mail.google.com) durch eine eigene Sub-Domain logisch von der Top-Level-Domain google.com getrennt – mit der Folge, dass Browser-Freigaben nur für den jeweils aktiven Dienst gelten. Diese Trennung hat Google nun bei Maps aufgehoben und den Kartendienst damit zu einem Teil der Top-Level-Domain google.com gemacht. Gibt ein Nutzer für den Kartendienst die Übermittlung seines Standorts durch den Browser frei, gilt diese Freigabe für die gesamte Domain google.com – der Standort wird also auch bei der Google-Suche übermittelt. Ein Schelm, wer…

Datenschutzrechtlich ist das ein Verstoß gegen das Transparenzgebot (Art. 12 DSGVO), denn Google täuscht Nutzerinnen und Nutzern vor, dass sich die Standortfreigabe lediglich auf Maps bezieht. Da sich Google bei der Verarbeitung zudem auf „berechtigtes Interesse" beruft, wird der Standort auch dann verarbeitet, wenn im Consent-Banner „alles" abgelehnt wird. Die Zustimmung zur Standort-Übermittlung durch den Browser ist jedoch keine rechtskonforme Datenschutz-Einwilligung.

Immerhin: Firefox-User sind nicht betroffen, da Firefox ausschließlich temporäre Standortfreigaben erteilt.

Threema-Verschlüsselung

Am 09.01.2023 veröffentlichten Forscher der ETH Zürich eine kryptografische Analyse der Threema-Verschlüsselung. Darin beschreiben sie sieben Angriffsmöglichkeiten auf das Protokoll des verbreiteten Messengers. Laut Threema ist das im Dezember 2022 eingeführte neue Protokoll Ibex für die dargestellten Angriffe nicht anfällig; soweit bekannt wurde auch keiner der beschriebenen Angriffe in der Praxis eingesetzt.

Doch der Fall ist ein Paradebeispiel für mehrere Lektionen, die bei der Entwicklung kryptografischer Protokolle beachtet werden sollten. So war nicht eine fehlerhafte Implementierung kryptografischer Verfahren das Problem, sondern deren Zusammenstellung zu miteinander verwobenen Protokollen. Zusätzlich zum bekannten Mantra „don´t roll your own crypto" lautet die generelle Empfehlung der ETH-Forscher, wann immer möglich auf bekannte und bewährte Protokolle wie beispielsweise TLS zurückzugreifen – spätestens seit dem Desaster des WEP-Protokolls (SSN 3/2002) sollte das eigentlich das „übliche Vorgehen" sein.

Auch Schneier´s Law haben die Threema-Entwickler missachtet: Danach kann ein kryptografisches Protokoll (genau wie ein kryptografischer Algorithmus) nur durch unabhängige Analysen seine Sicherheit unter Beweis stellen. Für die Einordnung solcher Sicherheitsanalysen muss zudem definiert sein, gegen welche Angriffsmodelle das Protokoll schützen soll; erst daraus können Sicherheitsaussagen abgeleitet werden. Die Definition von Standard-Angriffsmodellen, gegen die ein kryptografisches Protokoll für einen Messenger schützen soll, wäre daher für Entwickler und Sicherheitsexperten hilfreich.

Um Protokoll-Analysen zu erleichtern ist der derzeitigen Darstellung des Threema-Protokolls eine höhere Detailtiefe zu wünschen – vergleichbar der der Dokumentation des Signal Protokolls.

Bußgeld-Krimi

Seit dem 20.08.2018 hatte sich die für ihre laxe Haltung in Datenschutzfragen bekannte irische Datenschutzaufsichtsbehörde (DPC) mit offensichtlichen Datenschutzverstößen von Meta beschäftigt – nicht auf eigene Initiative, sondern ausgelöst

durch eine Beschwerde der von Max Schrems gegründeten Non-Profit-Organisation NOYB bei der belgischen Datenschutzaufsicht vom 25.05.2018.

Um die strengen datenschutzrechtlichen Anforderungen an eine Einwilligung zu umgehen hat Meta die Verarbeitung von Nutzerdaten für personalisierte Werbung als Klausel in die AGB von Facebook und Instagram aufgenommen, da diese für die Bereitstellung der Dienste erforderlich sei. Ein Umgehen der Einwilligung durch die Aufnahme in einen Vertrag ist jedoch durch das Kopplungsverbot (Art. 6 Abs. 4 DSGVO) untersagt. Der Verstoß hat zusätzliches Gewicht durch die Monopolstellung von Meta.

Gegen den vorläufigen Entscheidungsentwurf der DPC legten neun europäische Aufsichtsbehörden Beschwerde ein, sodass eine Streitbeilegung nach Art. 65 durch die europäische Datenschutzaufsicht (EDPB) erforderlich wurde. Derweil verhängte die DPC am 15.03.2022 ein 17 Mio. €-Bußgeld gegen Facebook und am 28.11.2022 ein 265 Mio. €-Bußgeld gegen Instragram. Wenige Tage später veröffentlichte der EDPB am 05.12.2022 die verbindlichen Anordnungen zu Facebook und zu Instagram, in denen Meta die Praxis untersagt und von der DPC die Verhängung eines höheren Bußgelds verlangt wird. Die reagierte am 31.12.2022 mit einem weiteren Bußgeldbescheid über 390 Mio. €. Darin ist allerdings die Abschöpfung der von Meta mit den unrechtmäßig verarbeiteten Daten erwirtschafteten (Milliarden-) Gewinne nicht enthalten – das letzte Wort ist also wohl noch nicht gesprochen.

Vor diesem Hintergrund wirkt die Stellungnahme von Meta gegenüber der DPA geradezu hämisch: „Wir glauben zutiefst, dass unser Ansatz die EU-Datenschutzverordnung respektiert […].“

Garantien von Microsoft

Am 15.12.2022 hat Microsoft bekannt gegeben, dass das lange angekündigte EU Data Boundary für Microsoft 365 (SSN 11/2022) zum 01.01.2023 in Betrieb geht. Automatisch kommt man aber nicht in den Genuss der Vorteile dieser Regelung: Nur wer das Data Protection Addendum auf die Fassung vom 01.01.2023 aktualisiert, kann sicher sein, dass seine Daten in dem von Microsoft beschriebenen Rahmen innerhalb der EU gespeichert und verarbeitet werden. Die Verantwortung dafür liegt beim Kunden. Das Angebot richtet sich nicht nur an Kunden mit Volumenlizenzvertrag, sondern an alle, die mit Microsoft Vereinbarungen im Zusammenhang mit deren Cloud-Produkten und –Dienstleistungen abgeschlossen haben.

Mit Daten bezahlen

Am 29.11.2022 hat die Datenschutzkonferenz (DSK) einen Beschluss zu den „Auswirkungen der neuen Verbrauchervorschriften über digitale Produkte im BGB auf das Datenschutzrecht“ veröffentlicht – dem „Bezahlen mit Daten“, das durch die Änderung des § 312 BGB zur Umsetzung der EU-Richtlinie zu digitalen Inhalten und Dienstleistungen nun zulässig ist. Die DSK beschränkt sich allerdings darauf festzustellen, dass die neuen Regelungen nur auf Verträge über digitale Produkte anwendbar sind, und nicht, wenn Betroffene lediglich ihre Einwilligung bei Consent Bannern erteilen. Bei Consent Walls wird man hingegen davon ausgehen dürfen, dass es zu einem Vertragsabschluss kommt.

Die Frage nach dem angemessenen Preis, wenn sich Betroffene dafür entscheiden, statt mit Geld mit ihren Daten zu bezahlen, wird auch von der DSK nicht beantwortet.

Secorvo News

Seminare

Ins Jahr 2023 startet unser Seminarbereich mit dem Seminar BSI Vorfall-Experte. Vom **07.03.** bis **09.03.2023** haben Sie die Möglichkeit, sich bei uns auf die Zertifizierung zum BSI-Experten nach dem Curriculum des Bundesamts für Sicherheit in der Informationstechnik (BSI) vorzubereiten.

Im Seminar IT Security Insights – T.I.S.P. Update vom **21.03.** bis **22.03.2023** können Sie Ihren Wissenstand rund um die Themen Informationssicherheit und Datenschutz auffrischen. Kurz vor Ostern (**27.03.–31.03.2023**) bieten wir Ihnen mit dem T.I.S.P.-Seminar die Möglichkeit, Ihre IT-Security-Kenntnisse nicht nur zu vertiefen, sondern auch zertifizieren zu lassen – zur Vorbereitung erhalten Sie nach Ihrer Anmeldung unser T.I.S.P.-Buch „Informationssicherheit und Datenschutz“ (erschienen im dpunkt-Verlag).

Die Seminarprogramme und weitere Informationen zu unseren Seminaren finden Sie auf unserer Website. Wir freuen uns auf Ihre Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2023	
20.-22.01.	ShmooCon 2023 (The Shmoo Group, Washington/US)
Februar 2023	
08.-10.02.	30. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
13.-16.02.	OWASP 2023 Global AppSec (OWASP Foundation, Dublin/IRL)
März 2023	
07.-09.03.	BSI Vorfall-Experte (Secorvo, Karlsruhe)
14.-16.03.	secIT 2023 (Heise Medien, Hannover)
21.-22.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
21.-24.03.	DFRWS EU 2023 (DFRWS, hybrid)
27.-31.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
April 2023	
23.-27.04.	Eurocrypt 2023 (IACR, Lyon/FR)
24.-27.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-27.04.	Datenschutztage 2023 (WEKA, virtuell)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Stefan Gora, Kai Jendrian, Oliver Oettinger, Friederike Schellhas-Mende (Editorial), Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2023



Datenparadies Irland

Gegen die europäischen Niederlassungen mehrerer Meta-Unternehmen hatte Max Schrems' Initiative noyb wegen Umgehung der Einwilligungspflicht bei personalisierter Werbung sowie mangelnder Transparenz bei verschiedenen europäischen Aufsichtsbehörden mehrere Datenschutz-Beschwerden eingereicht – pünktlich zum Inkrafttreten der DSGVO am 25.05.2018.

Angelockt von niedrigen Steuern haben viele amerikanische „Big Tech"-Konzerne wie Microsoft, Meta, Google oder Apple ihre europäische Hauptniederlassung in Irland. In Datenschutzfragen ist damit die irische Datenschutzbehörde DPC zuständig.

Jahrelang verschleppte die DPC die Entscheidungen über die Beschwerden. Zunächst hatte die DPC sogar versucht, eine Leitlinie des Europäischen Datenschutzausschusses (EDSA) zu beeinflussen, um die Umgehung der Einwilligung durch Meta zu legitimieren. In einem ersten Entscheidungsentwurf vom 06.10.2021 ging die DPC nur auf die Transparenzverstöße ein, ließ das Vertragsmodell unberücksichtigt und empfahl ein Bußgeld von 28 bis 36 Mio. €. Nach Einsprüchen mehrerer europäischer Aufsichtsbehörden hob der EDSA am 05.12.2022 die vorläufigen Bußgeldbescheide der DPC gegen Facebook über 17 Mio. € (15.03.2022) und Instagram über 265 Mio. € (28.11.2022) auf und erhöhte die Bußgelder von Facebook, Instagram und WhatsApp auf insgesamt 390 Mio. € (SSN 12/2022).

Keine europäische Aufsichtsbehörde stellte sich dabei auf die Seite der DPC. Die Ankündigung der DPC, gegen den verbindlichen Beschluss des EDSA vorzugehen, spricht Bände. Dabei ist die DPC trotz eines Jahresbudgets von 19 Mio. € die Aufsichtsbehörde Europas mit den mit Abstand meisten unerledigten Fällen: Von 164 Beschwerden mit europaweiter Bedeutung wurden erst vier erledigt, wie ein Bericht des Irish Council for Civil Liberties vom 13.04.2022 aufzeigt. Die Geduld des EDSA ist nun hoffentlich zu Ende.



Inhalt

Datenparadies Irland

Security News

Detailfrage

iCloud-Verschlüsselung

NIS2

Verbannt

Teure Wahlkampfhilfe

IT-Grundschutz-Kompendium

Cookie-Chaos

Secorvo News

Secorvo auf der DFN-Konferenz

Seminare

Phish me, if you can

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Detailfrage

Mit seinem Urteil vom 12.01.2023 hat der EuGH auf ein Vorabentscheidungsersuchen des Obersten Gerichtshofs Österreichs eine wichtige Auslegung des Art. 15 Abs. 1 lit. c DSGVO (Datenschutz-Auskunftsersuchen) geklärt: Danach muss der Verantwortliche (im vorliegenden Fall die Österreichische Post AG) die Identität der (Daten-) Empfänger so konkret wie möglich benennen, um dem Transparenzgrundsatz zu genügen und dem Betroffenen eine weitere Rechtsausübung überhaupt erst zu ermöglichen. Ist dem Verantwortlichen dies (noch) nicht möglich, darf er sich darauf beschränken die Kategorien der betreffenden Empfänger mitzuteilen.

Eine Auskunft kann verweigert werden, wenn ein Antrag offenkundig unbegründet oder exzessiv ist; das muss der Verantwortliche jedoch nachweisen.

iCloud-Verschlüsselung

Apple hat am 23.01.2023 auch in Deutschland die Möglichkeit freigeschaltet, unter iOS 16.2 und macOS 13.1 den erweiterten Datenschutz zu aktivieren. Damit lassen sich fast alle Daten in der iCloud Ende-zu-Ende verschlüsseln. Die Funktion muss vom Nutzer ausgewählt werden.

Die US-Bundespolizei FBI kritisiert die Ende-zu-Ende Verschlüsselung; im Rahmen von Ermittlungen bekommt sie nun nur noch eingeschränkten Zugriff auf die Daten in der iCloud. Gemäß Apples jüngstem Transparenzbericht von 2021 wurden in fast 4000 Fällen iCloud-Daten an Behörden herausgegeben – darunter auch iCloud Backups.

iCloud Mail, Kalender und Kontakte sowie zahlreiche Metadaten wie Dateinamen, Checksummen und Safari-Lesezeichen werden allerdings weiterhin nicht Ende-zu-Ende verschlüsselt. Die Lösung hat daher noch Luft nach oben.

NIS2

Am 14.12.2022 wurde die so genannte NIS2-Richtlinie über „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union“ (EU 2022/2555) im EU-Amtsblatt veröffentlicht. Ziel der Richtlinie ist ein einheitlicheres Niveau der IT-Sicherheit kritischer Infrastrukturen innerhalb der EU. Sie muss bis Oktober 2024 in nationales Recht umgesetzt werden. In Deutschland ist vieles bereits im IT-Sicherheitsgesetz 2.0 geregelt (siehe SSN 5/2021).

Die Richtlinie gilt für Unternehmen in kritischen Infrastrukturen mit mindestens 50 Mitarbeitern und 10 Mio. € Umsatz. Teile der digitalen Infrastruktur und der öffentlichen Verwaltung sollen unabhängig von der Größe reguliert werden. Die Unternehmen müssen „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen“ nach dem „Stand der Technik“ ergreifen, die sie nach einer „systemischen Analyse“ festlegen. Zuständig für die Umsetzung der Maßnahmen ist die Geschäftsführung. Die getroffenen Maßnahmen sind systematisch mit Hilfe eines implementierten Risikomanagementsystems zu dokumentieren.

Bei Verstößen können Bußgelder verhängt werden, deren Höhe an die der DSGVO angelehnt wurde: bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes bei wesentlichen und 7 Mio. € bzw. 1,4 % des Jahresumsatzes bei wichtigen Einrichtungen. Das kann teuer werden, da im schlimmsten Fall auch noch ein Bußgeld wegen Verstoßes gegen die DSGVO hinzukommen kann.

Verbannt

Am 25.11.2022 machte die US-Regierung ernst: In einer aktualisierten Auslegung des Secure Equipment Act vom 11.11.2021 (H.R.3919) verbot sie die Zulassung von chinesischen Telekommunikations- und Videoüberwachungseinrichtungen, da sie eine Gefahr für die nationale Sicherheit darstellten. Damit dürfen Komponenten von Huawai, ZTE und anderen chinesischen Herstellern zukünftig nicht mehr in Mobilfunkeinrichtungen oder Routern verbaut werden; auch Smartphones könnten betroffen sein.

Zwar gilt auch diese Regelung nicht ohne Ausnahmen und spielten sicher auch wirtschaftliche Interessen bei der Entscheidung eine Rolle. Doch macht sie deutlich, dass die USA die Gefahr einer technischen „Unterwanderung“ der IT-Infrastrukturen ernst nimmt. Anders als die Bundesregierung, die von einer entsprechenden Regelung in § 9b IT-Sicherheitsgesetz bisher keinen Gebrauch macht.

Teure Wahlkampfhilfe

Am 22.12.2022 stimmte Meta einem Vergleich zu: Der Konzern zahlt 725 Mio. US$ an Betroffene für die rechtswidrige Weitergabe der Daten von 87 Mio. Facebook-Nutzern an Cambridge Analytica. Das Unternehmen hatte die Daten 2016 im Wahlkampf von Donald Trump und für die britische Brexit-Kampagne genutzt. Nach Bekanntwerden des Skandals musste Cambridge Analytica am 02.05.2018 Insolvenz anmelden (siehe SSN 4+5/2018). Im Juli 2019 hatte Facebook bereits ein Bußgeld der US-Verbraucherschutzbehörde in Höhe von 5 Mrd. US$ akzeptiert. 660 € pro Datensatz – ein teurer Spaß für die Aktionäre. Auch in diesem Sinne kann sich Datenschutz auszahlen.

secorvo
security consulting

IT-Grundschutz-Kompendium

Am 01.02.2023 hat das BSI die Edition 2023 des IT-Grundschutz-Kompendiums vorgestellt. In der aktuellen Version finden sich 10 neue Bausteine, darunter ein Baustein zum allgemeinen IT-Betrieb, dem nun versionsunabhängigen Baustein „Windows Server“ sowie die vollständige Überarbeitung der Bausteine zur Nutzung und dem Anbieten von Outsourcing. Bei 21 Bausteinen gab es Änderungen, die das BSI in einem eigenen Dokument zusammengefasst hat. Das Kompendium steht in den Formaten PDF und XML zur Verfügung.

Für alle Unternehmen und Einrichtungen, die sich nach IT-Grundschutz zertifizieren lassen, sind ab dem 01.02.2023 die Versionen 2022 und 2023 verbindlich. Aber auch für alle anderen Unternehmen bietet das Kompendium gute Anregungen für die Implementierung von Maßnahmen der Informationssicherheit.

Cookie-Chaos

Cookie-Banner sind ein Ärgernis für Webseitenbesucher, Datenschützer und Webseitenbetreiber – wenn auch aus jeweils anderen Gründen. Zwar sind die gesetzlichen Anforderungen klar: Wer personenbezogene Daten ohne Vertrag oder andere gesetzliche Grundlage verarbeiten möchte (hier: Tracking von Webseitenbesuchern) benötigt eine Einwilligung der Betroffenen.

Wie aber ist eine solche Einwilligung auf einer Webseite rechtskonform zu gestalten? Da gehen die Auffassungen schon seit vielen Jahren (siehe z. B. SSN 2/2015) erheblich auseinander. Am 14.03.2022 hatte sich das European Data Protection Board (EDPB) auf eine Richtlinie zu „Dark Patterns“ geeinigt (SSN 4/2022), mit denen Seitenanbieter versuchen, Besucher zur Zustimmung zu verleiten.

Das ist aber nur ein Teil des Problems. Angesichts der Schwemme der Beschwerden über vorgeblich rechtswidrige Cookie-Banner haben die Datenschutz-Aufsichtsbehörden daher eine „Taskforce Cookie Banner“ eingerichtet, die am 17.01.2022 ihren Bericht vorgelegt hat. Er enthält zahlreiche bereits durch einschlägige Urteile bestätigte Klarstellungen (wie die Forderung, dass ein Tracking erst nach der expliziten Zustimmung erfolgen, die Zustimmung nicht vorausgewählt sein und optionale Cookies nicht als „erforderlich“ deklariert werden dürfen), bleibt aber beispielsweise hinsichtlich der Gestaltung eines „alles Ablehnen“-Knopfs unscharf. Wer Cookies und Tracking wirksam verhindern möchte, bleibt daher bis auf weiteres auf Browser-Plugins wie Privacy Badger der EFF (SSN 12/2017) oder uBlock Origin angewiesen (SSN 10/2022).

Secorvo News

Secorvo auf der DFN-Konferenz

Auf der diesjährigen 30. DFN-Konferenz Sicherheit in vernetzten Systemen (08.-10.02.2023) referierten unsere Datenschutzexperten Friederike Schellhas-Mende und Christian Blaicher zu „E-Mail-Tracking und -Profiling“, und der Krypto-Experte Hans-Joachim Knobloch beschrieb den „Kampf gegen Goldene Zertifikate“ und wie man sich vor Angriffen über die ‚Certifried'-Schwachstelle schützen kann. Die Beiträge erschienen im Konferenzband.

Seminare

Das Seminar BSI Vorfall-Experte vom **07.03.** bis **09.03.2023** bietet Ihnen eine Vorbereitung nach dem Curriculum des Bundesamts für Sicherheit in der Informationstechnik (BSI) auf die Zertifizierung zum BSI-Experten.

Das Seminar IT Security Insights – T.I.S.P. Update vom **21.03.** bis **22.03.2023** frischt Ihren Wissensstand rund um die Themen Informationssicherheit und Datenschutz auf. Und kurz vor Ostern (**27.03.–31.03.2023**) bieten wir Ihnen mit dem T.I.S.P.-Seminar die Möglichkeit, Ihre IT-Security-Kenntnisse nicht nur zu vertiefen, sondern auch zertifizieren zu lassen – zur Vorbereitung erhalten Sie nach Ihrer Anmeldung unser T.I.S.P.-Buch „Informationssicherheit und Datenschutz“ (erschienen im dpunkt-Verlag).

Die Seminarprogramme und weitere Informationen zu unseren Seminaren finden Sie auf unserer Website. Wir freuen uns auf Ihre Anmeldung.

Phish me, if you can

Ein weltweit agierendes Kollektiv anarchischer Hacker hat sich, getrieben von anarchistischen Freiheitsidealen zum Ziel gesetzt, die vorherrschenden Gesellschaftsstrukturen zu destabilisieren und in totales Chaos zu stürzen. Ihr erstes Ziel ist die Energiewirtschaft.

Beim Jahreseröffnungsevent der KA-IT-Si am **16.03.2023** berichtet Jan Tomasch, Information Security Awareness Manager der EnBW, in seinem Vortrag „Security Awareness Kampagne mit Gamification“, wie die Mitarbeitenden der EnBW als Cyber-Interventionsteam ihre Verteidigungslinie aufbauen, um den Hackern das Handwerk zu legen.

Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2023	
13.-16.02.	OWASP 2023 Global AppSec (OWASP Foundation, Dublin/IRL)
März 2023	
07.-09.03.	BSI Vorfall-Experte (Secorvo, Karlsruhe)
14.-16.03.	secIT 2023 (Heise Medien, Hannover)
16.03.	Phish me, if you can (KA-IT-Si, Karlsruhe)
21.-22.03.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
21.-24.03.	DFRWS EU 2023 (DFRWS, hybrid)
27.-31.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
April 2023	
23.-27.04.	Eurocrypt 2023 (IACR, Lyon/FR)
24.-27.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-27.04.	Datenschutztage 2023 (WEKA, virtuell)
25.-26.04.	Security Forum 2023 (Hagenberger Kreis, Hagenberg/AT)

Fundsache

Die DSK hat am 24.11.2022 Version 3.0 des Standard-Datenschutzmodells beschlossen. Diese Methode zur Datenschutzberatung und -prüfung erleichtert die Umsetzung der rechtlichen Anforderungen der DSGVO in konkrete technische und organisatorische Maßnahmen.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher (Editorial), Stefan Gora, Kai Jendrian, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2023



Leichen im Keller

Jede App, die personenbezogene Daten verarbeitet, muss diese Verarbeitung in einer Datenschutzerklärung erläutern. Nur so ist eine „faire und transparente" Verarbeitung der Daten – wie von der DSGVO gefordert – möglich, da für einen Nutzer beispielsweise nicht offensichtlich ist, ob eine App die Verarbeitung lokal durchführt oder einen Cloud-Dienst in Anspruch nimmt.

Geht die Verarbeitung über den eigentlichen Anwendungszweck der App hinaus, weil der Anbieter zusätzliche Daten für eigene (bspw. Marketing-) Zwecke erhebt, wie zur Bildung von Nutzerprofilen, oder gar Daten an Dritte (beispielsweise verbundene Unternehmen) weitergibt, ist eine Einwilligung der Betroffenen erforderlich – und die ist nur rechtswirksam, wenn sie *informiert* erfolgt. Eine am 23.02.2023 veröffentlichte Forschungsstudie der Mozilla Foundation zeigt, dass zahlreiche Unternehmen hier „Leichen im Keller" haben: Von den 40 Apps mit den höchsten Download-Zahlen des Google Play Store stimmten bei fast 80% die Angaben in der Datenschutzerklärung nicht mit den Angaben der Entwickler in Googles Data Safety Form überein, die im Google Play Store angezeigt werden. Bei 40% der Apps waren die Abweichungen gravierend – so weisen beispielsweise weder TikTok noch Twitter ihre Datenweitergaben an Werbeplattformen aus. Eine auf solchen unvollständigen Informationen beruhende Einwilligung in die Verarbeitung ist damit unwirksam – und die Verarbeitung der Daten somit rechtswidrig.

Die Zahlen sind erschreckend, denn die Studie untersuchte nur die Abweichung der Datenschutzerklärung von den Angaben der Entwickler im Play Store – welche Daten von den Apps (und den dahinter liegenden Plattformen) *tatsächlich* verarbeitet und an Dritte weitergegeben werden, wurde nicht untersucht. Nach einer Langzeitstudie von ARD und ZDF verbrachten die Deutschen 2021 rund 3,4 h pro Tag mit dem Smartphone. Die dabei anfallenden Daten liefern ein Verhaltensprofil aller Deutschen.



Inhalt

Leichen im Keller

Security News

Tesla reagiert

Vorgaben für S/MIME-Zertifikate

It's not a bug

Leitlinien gegen Irreführung

Spyware auf Diensthandys

E-Mail-Tracking & Profiling

Secorvo News

Was sind „Goldene Zertifikate"?

Secorvo Seminare

Phish me, if you can

Veranstaltungshinweise

secorvo
security consulting

Security News

Tesla reagiert

Am 22.02.2023 veröffentlichte die niederländische Datenschutz-Aufsichtsbehörde (DPA) ihr Untersuchungsergebnis des „Wächter-Modus“ in Tesla-Fahrzeugen. Danach hat Tesla erfreulicherweise auf die vielfach geäußerte Kritik (siehe SSN 07/2022 und SSN 08/2022) reagiert: Möchte der Fahrzeuginhaber den „Wächter-Modus“ nutzen, muss er ihn nun zunächst aktivieren. Die Aufnahmen werden nur noch für die Dauer von zehn Minuten und ausschließlich im Fahrzeug gespeichert; so wird eine Dauerüberwachung der Fahrzeugumgebung vermieden. Zudem filmen die Kameras nur, wenn das Fahrzeug berührt wird. Eine Anzeige im Fahrzeug und die Innenbeleuchtung signalisieren Betroffenen, dass Videoaufnahmen stattfinden. Die DPA hat deshalb von der Verhängung eines Bußgelds gegen Tesla abgesehen und weist darauf hin, dass der Fahrzeughalter datenschutzrechtlich für die Videoaufnahmen verantwortlich ist. Grundsätzlich gelten für in Fahrzeugen verbaute Kameras die gleichen Regelungen wie für jede andere Kamera.

Vorgaben für S/MIME-Zertifikate

Trust Center, die Zertifikate anbieten, die von Browsern akzeptiert werden sollen, müssen sich an die Vorgaben des 2005 gegründeten CA/Browser-Forums (CAB) halten. Am 01.01.2023 veröffentlichte das CAB nun die von einer Arbeitsgruppe über gut zwei Jahre entwickelten Mindestanforderungen an S/MIME-Zertifikate. 84 Seiten füllen die Vorgaben, die am 01.09.2023 in Kraft treten. Danach müssen Zertifikatsaussteller die Identität des Antragstellers bei Personenzertifikaten genauer prüfen und diese Prüfung dokumentieren. Die Kriterien für die Auditierung der PKI werden noch diskutiert und zu einem späteren Zeitpunkt veröffentlicht.

Die Identitätsprüfung ist bei S/MIME-Zertifikaten zweifellos ein (sicherheits)kritischer Punkt – das Vertrauen in Personenzertifikate dürfte daher durch die neuen Vorgaben steigen. Allerdings könnten auch die bestehenden Registrierungsprozesse in Unternehmen, die öffentliche S/MIME-Zertifikate beziehen, von den Vorgaben betroffen sein – schlimmstenfalls ist beim nächsten Zertifikatswechsel die Registrierung zu wiederholen.

It’s not a bug

Am 08.02.2023 wurde eine kontrovers diskutierte Schwachstelle im verbreiteten Passwort-Manager KeePass behoben. Konkret ging es um eine für Automatisierungsprozesse eingebaute Funktion, mit der die Passwort-Datenbank nach dem Entsperren durch den Anwender unverschlüsselt exportiert werden kann. Das (vermeintliche) Problem: Kann ein Angreifer die Konfigurationsdatei von KeePass ändern, dann kann er diese Funktionalität ohne Wissen des Benutzers aktivieren und darüber die Passwörter auslesen.

Der Fall lässt Parallelen zur Schwachstelle Log4Shell erkennen, bei der eine Funktion, die die meisten Anwender nicht erwarteten, letztlich zu einem Sicherheitsproblem führte. Auch wenn bei KeePass die Auswirkungen deutlich geringer sind: Eine automatisierte Exportfunktion werden hier nur die wenigsten Anwender erwartet haben.

Doch ein Angreifer mit Schreibzugriff auf die Konfigurationsdatei von KeePass kann weitaus mächtigere Angriffe durchführen. Das erläutert KeePass selbst schon seit einigen Jahren auf der eigenen Website. Mit den Worten der KeePass-Entwickler: „KeePass cannot magically run securely in an insecure environment.“

Die neue Version 2.53.1 verlangt nun grundsätzlich bei einem Datenbankexport die erneute Eingabe des Master-Passworts.

Leitlinien gegen Irreführung

Nach elfmonatiger öffentlicher Kommentierungsphase veröffentlichte der Europäische Datenschutzausschuss (EDSA) am 14.02.2023 seine Leitlinien zu irreführenden und DSGVO-widrigen Design-Elementen auf Social-Media-Plattformen als Version 2.0. In dem 74-seitigen Dokument werden zahlreiche Irreführungen beschrieben, mit denen Plattformbetreiber versuchen, Benutzer zu verleiten, gegen besseres Wissen ihre Zustimmung zu Tracking und anderen Datenerhebungen zu erteilen. Die verschiedenen Methoden werden in sechs Kategorien strukturiert und anhand 61 konkreter Beispiele veranschaulicht. Einige der beschriebenen irreführenden Design-Elemente finden sich auch auf anderen Plattformen.

Es ist zu erwarten, dass die im Dokument beschriebenen Methoden von den Datenschutz-Aufsichtsbehörden zukünftig bei der Prüfung von Portalen auf Datenschutzverstöße herangezogen werden.

Spyware auf Diensthandys

Nach mehreren Warnungen und dem Verbot der Installation und Nutzung von TikTok, der Videoplattform des chinesischen Bytedance-Konzerns, auf Dienst-Handys der amerikanischen Bundesbehörden haben nun die EU-Kommission (am 28.02.2023) und das EU-Parlament (am 01.03.2023) die

Installation und Nutzung des Dienstes auf Dienst-Handys untersagt.

Tatsächlich sind Apps mit großer Verbreitung perfekte Einfallstore für Spionage-Software: Die Geräte sind „always on“, kennen den Aufenthaltsort und die Kontaktdaten des Benutzers sowie sein Nutzungsverhalten und können, wenn der Benutzer es zulässt, auf Mikrofon und Kameras zugreifen. Zusätzliche Funktionen lassen sich (bei Bedarf sogar „zielgruppenspezifisch“) in Updates unterbringen, an deren ständigen Download sich Smartphone-Nutzer bereits gewöhnt haben. Zwar verhindern Schutzmechanismen der Betriebssysteme, dass eine App auf beliebige Daten und Sensoren zugreift; die erteilten Berechtigungen genügen aber meist, um ein Smartphone in ein Überwachungsgerät zu verwandeln.

Solche Angriffe sind für einen Nutzer bestenfalls an einer kürzeren Laufzeit des Geräts oder erhöhtem Internet-Traffic zu erkennen. Zwar kann man sie temporär außer Gefecht setzen, indem man den GPS-Sensor deaktiviert und die Internet-Verbindung kappt – damit deaktiviert man allerdings auch (fast) alle anderen Anwendungen auf dem Gerät.

Da viele Anbieter nicht einmal die von ihnen verarbeiteten Daten korrekt offenlegen (siehe Editorial), bleibt derzeit nur der Rückgriff auf Apps wie Gardion, die den Netzwerkverkehr des Smartphones nach Vorgaben filtern. Denen muss man allerdings vertrauen.

E-Mail-Tracking & Profiling

In ihrem Vortrag auf der 30. DFN-Konferenz am 09.02.2023 gingen Friederike Schellhas-Mende und Christian Blaicher auf die rechtskonforme Gestaltung von E-Mail-Tracking und Profiling ein. Denn nicht nur im Browser und in Apps wird das Nutzerverhalten analysiert, sondern zunehmend auch über Newsletter. Aber auch hier gelten UWG, DSGVO und TTDSG.

Damit bedürfen Newsletter mit Werbung nicht nur einer Einwilligung nach § 7 Abs. 2 Nr. 2 UWG. Protokollieren sie das Nutzerverhalten, benötigen sie außerdem eine Einwilligung nach § 25 TTDSG. Wenn zudem Benutzerprofile erstellt werden, ist obendrein eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO erforderlich. Eine Volltextveröffentlichung finden Sie auf der Secorvo-Webseite.

Da das Tracking in E-Mail-Newslettern gerne US-amerikanischen Tools (wie klaviyo und Mailchimp) überlassen wird, sollte man sich in einem solchen Fall angesichts der derzeitigen Abmahnungen besonders um eine rechtskonforme Gestaltung kümmern.

Secorvo News

Was sind „Goldene Zertifikate“?

Auf der Heise-Konferenz secIT in Hannover führten Hans-Joachim Knobloch und Oliver Oettinger am 14.03.2023 auf einem eintägigen Workshop in die Grundlagen der zertifikatsbasierten Anmeldung am Active Directory und Angriffe mit „Goldenen Zertifikaten“ ein. Einen verdichteten Überblick zum Thema gab Hans-Joachim Knobloch am 15.03.2023 in seiner Keynote.

Secorvo Seminare

Tanken Sie fünf Tage geballtes Wissen und lassen Sie sich anschließend als Experte für IT-Sicherheit zertifizieren: In unserem T.I.S.P. Seminar vom **27.** bis **31.03.2023** haben wir noch letzte freie Plätze.

Von den Grundlagen bis zur Planung Ihrer eigenen PKI: Alle wichtigen Aspekte von Public Key Infrastrukturen lernen Sie im PKI-Seminar vom **24.** bis **27.04.2023** kennen. In Workshops setzen Sie die Erkenntnisse aus den Vorträgen direkt um.

Von Praktikern für Praktiker: Mit unserem 3-Tages-Seminar „BSI Vorfall-Experte – Aufbauschulung“ vom **09.** bis **11.05.2023** sind Sie bestens gerüstet für die Zertifizierung zum Vorfall-Experten gemäß BSI-Curriculum.

Wir freuen uns auf Ihre Anmeldung.

Phish me, if you can

Ein weltweit agierendes Kollektiv anarchischer Hacker, getrieben von anarchistischen Freiheitsidealen, hat sich zum Ziel gesetzt, die vorherrschenden Gesellschaftsstrukturen zu destabilisieren und in totales Chaos zu stürzen. Ihr erstes Ziel: die Energiewirtschaft.

Beim Jahreseröffnungsevent der KA-IT-Si am **16.03.2023** berichtet Jan Tomasch, Information Security Awareness Manager der EnBW, in seinem Vortrag „Security Awareness Kampagne mit Gamification“, wie die Mitarbeitenden der EnBW als Cyber-Interventionsteam ihre Verteidigungslinie aufbauen, um den Hackern das Handwerk zu legen.

Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Net(t)-working“. Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen – und empfehlen eine zügige Anmeldung, da die Teilnehmerzahl auf 150 beschränkt ist.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2023	
14.-16.03.	secIT 2023 (Heise Medien, Hannover)
16.03.	KA-IT-Si Event Phish me, if you can (KA-IT-Si, Karlsruhe)
21.-24.03.	DFRWS EU 2023 (DFRWS, hybrid)
27.-31.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
April 2023	
23.-27.04.	Eurocrypt 2023 (IACR, Lyon/FR)
24.-27.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-27.04.	Datenschutztage 2023 (WEKA, virtuell)
25.-26.04.	Security Forum 2023 (Hagenberger Kreis, Hagenberg/AT)
Mai 2023	
09.-10.05.	BvD Verbandstag 2023 (BvD, Berlin)
09.-11.05.	BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe)
09.-12.05.	Blackhat Asia 2023 (Blackhat, Singapur/ASE)
09.-12.05.	European Identity and Cloud Conference 2023 (KuppingerCole, Berlin, hybrid)
10.-11.05.	19. Deutscher IT-Sicherheitskongress (BSI, virtuell)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Stefan Gora, Kai Jendrian, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2023



Von Bäumen und Wäldern

Es gab eine Zeit in der IT-Sicherheit, da galten einfache, klare Regeln. So erforderte eine gute Authentifikation ‚Wissen' und ‚Besitz' und wurden Daten, die von außen durch die Firewall gelangten, grundsätzlich als ‚potentiell gefährlichen Inhalts' eingestuft.

Das war einmal. Nicht, dass diese Prinzipien in Frage stünden. Wohl aber kippt immer öfter die praktische Umsetzung. Drei Beispiele: Für den bequemen Zugriff vom Mobilgerät auf E-Mails oder die Unternehmens-Cloud verlässt man sich zunehmend auf die Authentifikation des Nutzers am Gerät – die nicht selten auf schwachen Wischcodes oder leicht zu täuschenden Fingerabdruck-Scannern beruht. „Moderne" Zahlungssysteme lassen sich gänzlich ohne Transaktions-Authentifikation nutzen – um keine Kunden an andere Anbieter zu verlieren, geht das inzwischen sogar mit der EC-Karte (bis 50 € und fünfmal in Folge) und über Apple oder Google Pay. Und damit wir unseren Terminkalender nicht mehr pflegen müssen, werden per E-Mail zugesandte Einladungen ungefragt von Outlook eingetragen.

Der Preis, den wir für diese Bequemlichkeiten zahlen, ist hoch. So werden schwache Authentifikationen durch immer ausgefeiltere Datenerhebungen und Profilbildungen kompensiert (entsprechen Höhe und Empfänger der Zahlung den Gewohnheiten? kommt sie von demselben Endgerät – und aus dem richtigen Land?) – mit den unvermeidlichen Begleiterscheinungen gelegentlicher Sperrungen durch „false positives" und einer Verhaltensanalyse, die selbst George Orwells Vorstellungsvermögen überstiegen hätte. Zugleich eröffnet die dadurch anwachsende Komplexität der IT immer wieder unerwartete Angriffsflächen – vom „Denial of Service" auf das Konto bis zur Outlook-Attacke via Termineinladung (siehe „Termin-Hack").

Dagegen helfen würde mehr Einfachheit: ein „Stopp" bei vermeidbarer Komplexität, sodass neben den Bäumen der Wald wieder in den Blick käme. Aber das wäre wahrscheinlich – kompliziert.



Inhalt

Von Bäumen und Wäldern

Security News

Termin-Hack

Produkthaftung für Software

Don't roll your own crypto

TrustPid freigegeben

90-Tage-Zertifikate

Kontrolle ist besser

Secorvo News

Secorvo Seminare

AD = Anno Domini?

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Termin-Hack

Am 14.03.2023 hat Microsoft eine kritische Lücke (CVE-2023-23397) in allen Outlook-Versionen gepatched, über die ein Angreifer mit einer präparierten E-Mail ohne Zutun des Empfängers den NetNTLMv2-Hash des Nutzers abgreifen konnte. Die Schwachstelle existiert offenbar schon eine Weile – und wurde nachweislich schon seit April 2022 ausgenutzt. Am 20.03.2023 wurde ein Proof of Concept auf Github veröffentlicht. Man sollte übrigens Microsofts Empfehlung folgen und den Port TCP 445/SMB (ausgehend) an der Firewall sperren – die Lücke ist offenbar noch ausnutzbar.

Die Details der Schwachstelle sind delikat. Wer einen Outlook-Kalendereintrag erzeugt, kann diesem Termin eine selbst gewählte Sound-Datei für den Erinnerungsalarm zuordnen. Wird der Termin an einen (externen) Teilnehmer geschickt, öffnet dessen Outlook zum Zeitpunkt des Alarms diese Sound-Datei. Verlinkt der Angreifer hier auf einen externen Server, dann versucht der Outlook-Client des Empfängers, sich mit dessen Credentials dort anzumelden…

Die Schwachstelle ist das Ergebnis einer Software-Entwicklungsstrategie, die automatisiertes „Eindringen" in eine fremde Infrastruktur zur Regel macht: Outlook trägt jede Terminänderung ohne Freigabe des Empfängers beim Eintreffen der E-Mail automatisch in dessen Kalender ein. Verwunderlich ist daher nicht die Schwachstelle, sondern die Tatsache, dass Spammer und Phisher diesen Mechanismus nicht schon längst nutzen – denn was macht ein Empfänger wohl mit einem Link in einem Termin, den er nicht zuordnen kann?

Produkthaftung für Software

Die National Cybersecurity Strategy der US-Regierung vom 01.03.2023 listet auf 35 Seiten, strukturiert in fünf „Säulen" (Schutz kritischer Infrastrukturen, Bekämpfung von Angreifern, Stärkung der Widerstandskräfte des Marktes, Investitionen in Widerstandsfähigkeit und Internationale Zusammenarbeit), zahlreiche Maßnahmen und Vorgaben zum Schutz digitaler Infrastrukturen. (Allein die kompakte Darstellung ist beispielgebend – die Cybersicherheitsstrategie der Bundesregierung vom 08.09.2021 benötigte 142 Seiten, davon allein vier für das Inhaltsverzeichnis.) Folgenreich könnte die Zuweisung der Verantwortlichkeit von Software-Unternehmen für Sicherheitsmängel sein: "*Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers.*" Daraus lässt sich eine Haftung bei Pflichtverletzungen ableiten: Wer gegen Best Practices verstößt oder typische Fehler wiederholt, muss für daraus entstehende Schäden gerade stehen.

In Deutschland hält sich bisher die Auffassung, dass Software – juristisch – kein Produkt ist: Der Käufer erwirbt lediglich ein Nutzungsrecht. Ein Schritt zu mehr Herstellerverantwortung war die Einführung einer Aktualisierungspflicht zum 01.01.2022 (in § 475b und § 327f BGB). Mit dem EU Cyber Resilience Act vom 15.09.2022 will die EU-Kommission nun die Anforderungen an die Sicherheit von Software und den Umgang mit Schwachstellen stärker regulieren. Im Entwurf der neuen Produkthaftungsrichtlinie gilt Software als Produkt. Damit unterläge Software der Produkthaftung – eine gute Nachricht für Unternehmen, die sich schon heute um Software-Sicherheit kümmern.

Die Forderungen an die Hersteller im Anhang des Richtlinienentwurfs sind äußerst konkret: „*Products with digital elements shall be delivered without any known exploitable vulnerabilities, (…) with a secure by default configuration, (…) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data').*"

Don't roll your own crypto

Die Implementierung von Krypto-Algorithmen ist fehleranfällig (SSN 12/2022). So darf beispielsweise die Zufallszahl, die der ECDSA für die Signatur einer Nachricht benötigt, nicht erneut verwendet werden. Daher wird diese Zahl auch „Nonce" (= number used only once) genannt. Eine am 06.03.2023 veröffentlichte Untersuchung von Kudelski Security zeigt eine weitere Angriffsmöglichkeit: Wird für ECDSA ein schlechter Pseudozufallszahlengenerator verwendet, dessen Ausgabewerte in einem polynomiellen (oder sogar linearen) Zusammenhang stehen, kann unter speziellen, aber plausiblen Umständen der private Schlüssel rekonstruiert werden. Als die Autoren ihr Verfahren an den Signaturen in der Bitcoin Blockchain ausprobierten, konnten sie den privaten Schlüssel von 762 Wallets (im Wert von rund 9,4 Mio. US$) rekonstruieren – dank fehlerhafter ECDSA-Implementierungen, die Nonces wiederverwenden. Daher sollte – wo immer möglich – auf Standard-Krpyto-Bibliotheken und -Protokolle zurückgegriffen werden.

TrustPid freigegeben

Mit TrustPid sollen Mobilgeräte-Nutzer zukünftig nicht mehr durch Cookies oder Browser Fingerprinting, sondern durch ihre Internet-Provider getrackt werden (SSN 06/2022). Die Einwilligung der Nutzer

wird über die Webseite verwaltet. Nach erfolgreicher Durchführung des Machbarkeitstests soll TrustPID nun europaweit eingesetzt werden; dafür hat die EU-Kommission am 10.02.2023 die wettbewerbsrechtliche Freigabe erteilt. Als technische Plattform für digitale Werbung in Europa haben die europäischen Mobilfunkanbieter Orange, Telefónica, Vodafone und Telekom ein Gemeinschaftsunternehmen mit Sitz in Belgien gegründet.

Trotz seiner Unzuständigkeit hat sich Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, zu TrustPid geäußert: Zwar erfolge der Einsatz auf der Grundlage einer Einwilligung der Nutzer, dennoch sei die besondere Vertrauensstellung, die Telekommunikationsanbietern zukommt, „nur schwer mit einem Tracking ihrer Nutzerinnen und Nutzer vereinbar". Außerdem müssten potenzielle Gefahren wie die Zusammenführung von pseudonymen Kennungen mit Login-Daten bei Webdiensten, die eine Re-Identifikation und die Verknüpfung von Tracking-Daten ermöglichen, verhindert werden. Fazit: Besser deaktivieren.

90-Tage-Zertifikate

Am 03.03.2023 hat das Chromium-Projekt von Google erneut eine drastische Verringerung der Gültigkeiten von Browser-Zertifikaten vorgeschlagen (und angekündigt, dies ggf. direkt im Chrome-Root-Programm zu verankern): Root-Zertifikate sollen maximal sieben, CA-Zertifikate bis zu drei Jahre und öffentliche TLS-Sever-Zertifikate nur noch 90 Tage gültig sein (bei Let's Encrypt ist das schon lange Praxis). Mit diesem Schritt sollen CAs dazu gebracht werden, etwa alle fünf Jahre ihre Infrastruktur auf den aktuellen Stand der Technik zu bringen – und die Server-Betreiber, automatisierte Protokolle wie ACME zur Zertifikatsaktualisierung zu verwenden. Sollte sich der Vorschlag durchsetzen, wäre das der Anfang vom Ende des Geschäftsmodells der kommerziellen Zertifikatsanbieter. Zugleich könnte er die Entwicklung von ACME-Clients für Plattformen jenseits der verbreiteten Betriebssysteme und Webserver (wie Hypervisor, Appliances oder IoT-Schnittstellen) beschleunigen – und so die überfällige Automatisierung der Zertifikatsaktualisierung zum Standard machen.

Kontrolle ist besser

Für großes Erstaunen, nicht nur bei der Landesbeauftragten für den Datenschutz Niedersachsen, Barbara Thiel, hat die Entscheidung des VG Hannover vom 09.02.2023 zur ununterbrochenen Überwachung von Mitarbeitern mit Handscannern bei Amazon gesorgt (10 A 6199/20). Obwohl beim EuGH (Rechtssache C-34/21) gerade die Frage der DSGVO-Konformität des § 26 BDSG zur Entscheidung ansteht, ist das VG Hannover überzeugt, dass das berechtigte Interesse des Unternehmens hier die Interessen der Arbeitnehmer überwiegt. Die von Amazon geltend gemachten Zwecke zur Steuerung der Logistik und der Mitarbeiterqualifizierung sowie zur Schaffung objektiver Bewertungsgrundlagen für Feedbackgespräche seien (ge)wichtiger als der permanente Überwachungsdruck auf die Arbeitnehmer. Diese wüssten um die Überwachung und müssten angesichts der großen Anzahl offener Stellen auch keine Angst vor Arbeitsplatzverlust haben, wenn sie sich dieser Überwachung nicht aussetzen wollten. Zwar seien einige Punkte wie etwa die Speicherdauer grenzwertig, aber letztlich könne man sich der Argumentation von Amazon anschließen.

Unternehmen, die Überwachungsmaßnahmen planen, sollten ihre Motivation plausibel darlegen und dokumentieren – und sich in Niedersachen ansiedeln. Allerdings prüft die LfDI Niedersachsen gerade den Gang in die nächste Instanz.

Secorvo News

Secorvo Seminare

Machen Sie den ersten Schritt zum BSI Vorfall-Experten mit unserem Seminar „BSI Vorfall-Experte – Aufbauschulung" vom **09. bis 11.05.2023.** Oder krönen Sie Ihre Qualifikation mit dem T.I.S.P.-Zertifikat: Beim vorbereitenden T.I.S.P.-Seminar vom **19. bis 23.06.2023** sind noch Plätze frei.

Das Seminarprogramm und weitere Informationen finden Sie auf unserer Website. Wir freuen uns auf Ihre Anmeldung.

AD = Anno Domini?

Wie realistisch ist es für Angreifer, mit frei verfügbaren und öffentlichen Informationen Domain-Administrator auf einem fremden System zu werden? Beim KA-IT-Si-Event am **04.05.2023** in der *Church* (CyberForum e.V.) zeigen die Ethical Hacker von aramido in ihrem Vortrag „In 30 min. zum Domain-Admin" anhand von realen Bedrohungen, wie ein Angreifer auf interne Systeme zugreifen und anschließend die gesamte Infrastruktur übernehmen kann, indem er Domain-Admin-Privilegien erlangt. Dabei wird auch auf mögliche Abwehrmaßnahmen und Best Practices für die IT-Sicherheit eingegangen.

Anschließend gibt es natürlich wieder den fachlichen und persönlichen Austausch beim „Buffet-Networking". Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2023	
23.-27.04.	Eurocrypt 2023 (IACR, Lyon/FR)
25.-27.04.	Datenschutztage 2023 (WEKA, virtuell)
25.-26.04.	Security Forum 2023 (Hagenberger Kreis, Hagenberg/AT)
Mai 2023	
04.05.	KA-IT-Si-Event: "AD = Anno Domini?" (KA-IT-Si, Karlsruhe)
09.-10.05.	BvD Verbandstag 2023 (BvD, Berlin)
09.-11.05.	BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe)
09.-12.05.	Blackhat Asia 2023 (Blackhat, Singapur/ASE)
09.-12.05.	European Identity and Cloud Conference 2023 (KuppingerCole, hybrid)
10.-14.05.	ISSE 2023 (IEEE, Timisoara/ROU)
10.-11.05.	19. Deutscher IT-Sicherheitskongress (BSI, virtuell)
22.-24.05.	Omnisecure 2023 (in TIME berlin, Berlin)
23.-24.05.	24. Datenschutzkongress (EUROFORUM, Berlin)
23.-24.05.	IMF 2023 (Fraunhofer-Institut IAO, München)

Fundsache

Am 23.03.2023 hat das BSI eine neue Technische Richtlinie (TR 03145-5) mit Anforderungen an den sicheren Betrieb von Public Key Infrastrukturen für technische Sicherheitseinrichtungen veröffentlicht (26 Seiten).



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2023



Lernen durch Schmerzen

In jüngster Zeit mussten sich Gerichte vermehrt mit Schadensersatzklagen im Zusammenhang mit Datenschutzverstößen befassen. Immer wieder war dabei die Frage zu beantworten: Reicht es für einen Schmerzensgeldanspruch, dass sich ein Datenschutz-Risiko verwirklicht hat? Und falls ja, welches Schmerzensgeld ist angemessen?

Gemäß Art. 82 Abs. 1 DSGVO lässt sich die erste Frage schnell mit „Ja“ beantworten: Haftung und Verantwortung sind Wesenselemente des europäischen Datenschutzrechts. Allerdings messen die Gerichte mit zweierlei Maß: Bei Daten-Scraping (also dem Abgreifen personenbezogener Daten, die bspw. über ein Social-Media-Profil zugänglich sind) wird ein Schadensersatzanspruch in der Regel abgelehnt (so z.B. vom LG Gießen am 03.11.2022), selbst wenn die Betroffenen dabei ein „schlechtes Gefühl“ beschleicht. Anders sieht es bei einem „richtigen“ Datenschutzvorfall aus: Dann besteht ein Anspruch unabhängig davon, ob die Betroffenen durch das verwirklichte Risiko tatsächlich einen Schaden erlitten haben oder nicht – es reiche aus, dass die Betroffenen ein wenig Bauchgrummeln verspüren (so das OLG Hamm am 20.01.2023). Denn wenn nur genügend Betroffene ihre Ansprüche geltend machen würden, sei das in der Summe für den Verantwortlichen schmerzhaft, und Abschreckung müsse schließlich sein.

Übersehen wird dabei allerdings, dass für einen Schadensersatzanspruch auch ein materieller oder immaterieller Schaden entstanden sein muss – ein „Strafschmerzensgeld“ ist dem deutschen Recht nicht bekannt. Und das aus gutem Grund: Für die Sanktionierung von Datenschutzvorfällen und -verstößen sind die Datenschutz-Aufsichtsbehörden zuständig – und sollen das auch bleiben. Der Spagat zwischen einem wirksamen Grundrechtsschutz und der vorsätzlichen missbräuchlichen Ausnutzung lässt sich nur durch eine einheitliche Rechtsprechung bewältigen.



Inhalt

Lernen durch Schmerzen

Security News

Grundschutz in der Cloud

Bauchschmerzen

Software Security Game

Jahr des DSB

Mut zum Besseren

Der Preis ist heiß

Patchpolizei Exchange

Datenschutzmanagement

Gesetzgeber gefordert

Secorvo News

Seminare

Wo ist meine schwache Stelle?

Tag der IT-Sicherheit

Veranstaltungshinweise

secorvo
security consulting

Security News

Grundschutz in der Cloud

Am 03.04.2023 hat Microsoft drei Leitfäden zur Umsetzung von IT-Grundschutz bei der Nutzung der Cloud-Lösungen Azure, Office 365 und Dynamics 365 veröffentlicht. In den Workbooks wird zu den Anforderungen aus dem Baustein OPS.2.2 des Grundschutz-Kompendiums zur Cloud-Nutzung erläutert, welche Microsoft-Funktionen und Konfigurationen deren Umsetzung unterstützen. Die Workbooks enthalten Referenzen auf weiterführende Microsoft-Informationen, und in einem weiteren Kapitel wird ausgeführt, was zur Erfüllung des „Mindeststandards des BSI zur Nutzung externer Cloud-Dienste“ (NCD.2) zu tun ist.

Angesichts der zahlreichen von Microsoft zur Verfügung gestellten Funktionen und Optionen sind die Leitfäden eine wertvolle Hilfestellung für alle am IT-Grundschutz ausgerichteten IT-Infrastrukturen, die die Microsoft-Cloud nutzen. Der Bericht der europäischen Datenschutz-Aufsichtsbehörde (edpb) vom 17.01.2023 über die Prüfung der Nutzung von Cloud-Diensten im öffentlichen Bereich dürfte Microsoft motiviert haben, die Nutzer bei der Umsetzung der technischen und organisatorischen Schutzmaßnahmen besser zu unterstützen.

Bauchschmerzen

Das OLG Hamm entschied am 20.01.2023, dass für einen Schadensersatzanspruch ein „schlechtes Gefühl“ der von einer Datenpanne betroffenen Person ausreicht. Nur wenn der Verantwortliche beweisen kann, dass er in keinerlei Hinsicht für die Panne verantwortlich ist, ist seine Haftung nach Art. 82 Abs. 3 DSGVO ausgeschlossen. Dafür müssen sämtliche notwendigen technischen und organisatorischen Maßnahmen ergriffen, umgesetzt und ausreichend dokumentiert sein.

Dies gilt übrigens auch für die Frage, ob eine nicht umfänglich erteilte Auskunft einen Schadensersatzanspruch auslösen kann (siehe Urteile des LAG Niedersachsen und des LArbG Nürnberg). Wer nicht zwischen den Mahlsteinen der Justiz zerrieben werden will, erteilt die Auskunft so, wie es Art. 12 DSGVO vorsieht. Dafür unerlässlich ist ein Datenschutzmanagement mit etablierten und dokumentierten Regelungen und Prozessen.

Software Security Game

Am 21.03.2023 hat GitHub als Teil seiner Ausbildungsangebote ein Spiel veröffentlicht, mit dem sich die Kenntnisse zur Sicherheit von Software trainieren lassen. Dieses Secure Code Game richtet sich an Entwickler, die Schwachstellen in Software besser erkennen und vermeiden wollen. Der Fokus liegt auf der Programmiersprache Python, doch sind die vermittelten Konzepte größtenteils sprachunabhängig. Das Spiel kann lokal geclont oder in GitHub Codespaces genutzt werden.

Jahr des DSB

Der Europäische Datenschutzausschuss (EDSA) hat am 15.03.2023 für das Jahr 2023 eine koordinierte Prüfung der Situation der Datenschutzbeauftragten (DSB) angekündigt. Geprüft werden soll, ob die DSB gemäß den Vorgaben der Art. 37-39 DSGVO organisatorisch eingebunden und mit ausreichenden Ressourcen ausgestattet sind. Dazu werden zunächst Fragebögen an die DSB verschickt (deren Auswertung später zur Verfügung gestellt werden soll), ggf. gefolgt von förmlichen Untersuchungen der nationalen Aufsichtsbehörden.

Mut zum Besseren

„Das Bessere ist der Feind des Guten“ wusste schon Voltaire. Hätte es damals schon IT gegeben, wären ihm allerdings Zweifel gekommen – denn da hält man gerne an Bewährtem fest, solange z. B. Kryptoverfahren nicht komplett gebrochen sind. Das war schon bei der Hashfunktion SHA-1 so, bis das CA/Browser-Forum 15 Jahre später den Einsatz des Nachfolgers SHA-2 erzwang.

Für die Linux-Festplattenverschlüsselung LUKS hat der Linux-Entwickler Matthew Garrett am 17.04.2023 empfohlen, von älteren Versionen mit der Schlüsselableitung per PBKDF2 (Ursprung 1993) auf das vor 9 Jahren eingeführte LUKS2 mit Argon2id zu wechseln. Zwar muss man dem dieser Empfehlung zu Grunde liegenden Gerücht über einen erfolgreichen Angriff auf PBKDF2 mit Skepsis begegnen. Aber Argon2 wurde gegen Angriffstypen gehärtet, die beim Design von PBKDF2 noch gar nicht „auf dem Schirm“ waren. Daher sollte man den Mut zum Besseren haben – der Wechsel wird sicherlich weniger schmerzen als vielleicht befürchtet.

Der Preis ist heiß

Neben den klassischen Cookie-Bannern gibt es – insbesondere auf Webseiten mit „redaktionellen Inhalten“ – Cookie-Walls, bei denen die Nutzer entscheiden müssen, ob sie mit Daten (Zustimmung zu Tracking und Werbung) oder mit Geld bezahlen wollen (Pur-Abo). Die DSK hat am 22.03.2023 entschieden, dass solche Abo-Modelle zulässig sind, wenn beide Varianten (Tracking und Geldzahlung) gleichwertig sind. Dafür müssen „die Angebote zumindest dem Grunde nach die gleiche Leistung umfassen“. Leider klärt die DSK nicht, welches Entgelt angemessen ist und verweist nur auf die Marktüblichkeit. Das ist bedauerlich, da ein unan-

gemessenes Entgelt die Freiwilligkeit der Einwilligung in Frage stellen kann.

Patchpolizei Exchange

Im Exchange-Team-Blog kündigte Microsoft am 23.03.2023 an, dass Exchange-Server in der Cloud zukünftig sukzessive keine Nachrichten mehr von ungepatchten on-premise-Exchange-Servern annehmen werden. Betreiber verwundbarer Exchange-Server sollen erst informiert, dann der Empfang gedrosselt und, sofern innerhalb von 90 Tagen keine Abhilfe geschaffen wird, die Verbindung abgebrochen werden. Betroffene E-Mail-Absender werden darüber informiert.

Keine Frage: Für die „Internet-Hygiene“ und die Sicherheit der Allgemeinheit ist es eine gute Sache, wenn Patch-Muffel unter Druck gesetzt werden. Aber maßt sich Microsoft hier nicht eine bestenfalls hoheitliche Aufgabe an? Und was passiert mit nicht gepatchten Postfix-Mailservern? Oder veralteten Webservern? Sollte in solchen Fällen zukünftig auch ein E-Mail-Empfang als erzieherische Maßnahme verweigert werden? Aber bei wem liegt die Verantwortung, wenn einem Nutzer, der den Patch-Stand des Servers seines Providers nicht beeinflussen kann, durch die Nichtzustellung einer Nachricht ein Schaden entsteht? Zwar wird man Microsoft nicht vorwerfen können, dass dabei Nachrichten unterdrückt werden, um einem Dritten einen Nachteil zuzufügen (§ 274 Abs. 1 StGB). Allerdings könnten die verweigerten E-Mails einwandfrei sein, nur eben der versendende „Gammel“-Server nicht: In diesem Fall läge nicht zwingend eine Bedrohung für Exchange-Online vor. Daher empfehlen wir eine genauere Betrachtung der insbesondere rechtlichen Implikationen einer solchen Zwangsmaßnahme.

Datenschutzmanagement

Ein Verarbeitungsverzeichnis muss regelmäßig gepflegt werden; darauf weist der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) in einer Kurzinformation vom 01.04.2023 hin.

Die Umsetzungstipps sind nicht nur für öffentliche Stellen wertvoll. Dennoch greift diese Sicht zu kurz: Nicht nur das Verzeichnis der Verarbeitungstätigkeiten, sondern alle wesentlichen Datenschutz-Dokumente sollten regelmäßig, mindestens jährlich auf Vollständigkeit, Aktualität, Eignung und Korrektheit überprüft werden. Dazu sind, wie beim Informationssicherheitsmanagement, die notwendigen Abläufe (Prozesse) festzulegen und umzusetzen. Genau das sind Wesenselemente eines Datenschutzmanagementsystems – es wird Zeit, dass die Aufsichtsbehörden diese Gesamtsicht in den Blick nehmen.

Gesetzgeber gefordert

Mit seinem Urteil vom 30.03.2023 hat der Europäische Gerichtshof (EuGH) festgestellt, dass die Regelung in § 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes den Anforderungen der DSGVO nicht genügt. Damit dürfen diese und gleichlautende Regelungen zum Beschäftigtendatenschutz (also auch § 26 BDSG) nicht mehr angewendet werden. Wer seine Datenverarbeitungen auf diese Rechtsgrundlage stützt, sollte schnellstmöglich nach einer Alternative suchen. Die Rechtmäßigkeit der Verarbeitung richtet sich nunmehr ganz allgemein nach Art. 6 Abs. 1 DSGVO, solange die Gesetzgeber des Bundes und der Länder nicht durch entsprechende (neue) Regelungen dafür sorgen, dass ein Beschäftigtendatenschutz in Deutschland endlich vernünftig eingeführt und umgesetzt wird (was die DSK schon seit Längerem fordert).

Secorvo News

Seminare

Bereiten Sie sich mit unserem T.I.S.P.-Seminar vom **19. bis 23.06.2023** auf Ihre Zertifizierung vor: In 18 Lernmodulen vertiefen Sie Ihr Wissen in Informationssicherheit und Datenschutz. Bei Buchung bis zum 14.05.2023 profitieren Sie von unserem Frühbucherrabatt. Wir empfehlen eine schnelle Anmeldung – es sind nicht mehr viele Plätze frei.

Wo ist meine schwache Stelle?

Schwachstellen sind die Kletterhaken der Angreifer – wer Software entwickelt, muss sie meiden wie der Teufel das Weihwasser. Wie man mit Hilfe von Vulnerability Management Systemen Schwachstellen sucht und bewertet, wird das Thema des nächsten KA-IT-Si-Events am **22.06.2023** um 18 Uhr in den wunderbaren Räumen der WIBU-Systems (IT Security Club) sein. Wir freuen uns auf Ihre Anmeldung!

Tag der IT-Sicherheit

Nach zwei ausgefallenen (2020, 2022) und einer reinen Online-Veranstaltung (2021) wird der 13. Tag der IT-Sicherheit in diesem Jahr endlich wieder im bewährten Format in der IHK Karlsruhe stattfinden. Zusammen mit KASTEL, dem CyberForum und der IHK laden wir sie herzlich ein, am **20.07.2023** ab 14 Uhr mit Experten, IT-Sicherheits- und Datenschutzbeauftragten über aktuelle Herausforderungen wie Quantencomputer, KI und Patch-Management zu diskutieren. Auch hier empfehlen wir eine frühe Anmeldung – die Zahl der Plätze ist begrenzt (und die Nachfrage groß).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2023	
04.05.	KA-IT-Si-Event: "AD = Anno Domini?" (KA-IT-Si, Karlsruhe)
09.-10.05.	BvD Verbandstag 2023 (BvD, Berlin)
09.-12.05.	Blackhat Asia 2023 (Blackhat, Singapur/ASE)
09.-12.05.	European Identity and Cloud Conference 2023 (KuppingerCole, hybrid)
10.-14.05.	ISSE 2023 (IEEE, Timisoara/ROU)
10.-11.05.	19. Deutscher IT-Sicherheitskongress (BSI, virtuell)
22.-24.05.	Omnisecure 2023 (in TIME berlin, Berlin)
23.-24.05.	24. Datenschutzkongress (EUROFORUM, Berlin)
23.-24.05.	IMF 2023 (Fraunhofer-Institut IAO, München)
Juni 2023	
01.-02.06.	Annual Privacy Forum 2023 (ENISA et al., Lyon/FR)
12.-13.06.	DuD 2023 (COMPUTAS, Berlin)
14.-15.06.	Entwicklertag 2023 (VKSI, GI, ObjektForum, Karlsruhe)
19.-23.06.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
21.-22.06.	31. ID:SMART Workshop (Fraunhofer SIT, Darmstadt)
22.06.	Wo, bitte, ist meine schwache Stelle? (KA-IT-Si, Karlsruhe)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende (Editorial), Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Mai 2023



Tröpfchen

Ohne Einwilligung, gesetzliche Grundlage oder einen Vertrag ist die Verarbeitung personenbezogener Daten verboten. Das gilt auch für Daten, die nach Vertragsende oder Ablauf einer Aufbewahrungspflicht noch in Systemen schlummern.

Diese Daten sind der Kern des (Datenschutz-) Problems. Sie erlauben eine Rekonstruktion vieler unserer Lebensbereiche: Reisen (Flug- und Bahnkarten, GPS-Daten), Nutzung (Apps, Browser, Online-Shops) und Kommunikation (Telefonie, E-Mail, Messenger). Inzwischen protokollieren auch Geräte (Autos, Saugroboter, Sportuhren, ...) unser Leben. Wer diese Daten kennt, kennt die Menschen: ihre Kaufentscheidungen, ihr Sozialverhalten und ihre Freizeitbeschäftigungen, ihre Gesundheit, ihr Fahrverhalten und ihre Vorlieben. Und damit wachsen auch die Begehrlichkeiten – sowohl kommerzielle als auch staatliche.

Welche Größenordnungen letztere schon heute annehmen zeigt eine Antwort der Bundesregierung auf eine Anfrage im Bundestag vom 27.04.2023 zu Fluggastdatenabfragen: 424 Mio. Datensätze von 121 Mio. Passagieren wurden von den Fluggesellschaften 2022 an das Bundeskriminalamt (BKA) geliefert. Damit wurden rund 19.800 zur Fahndung ausgeschriebene Passagiere identifiziert und es kam zu knapp 1.400 Festnahmen – 0,001% der von den BKA-Abfragen betroffenen Personen. In 99,999% der Fälle wurden vom BKA also Daten von Unschuldigen erhoben und verarbeitet. Klammern wir die Kosten für den Aufbau (54 Mio. €) und den Betrieb (14,5 Mio. €, also 10.500 € je Festnahme) des Fluggastdatensystems einmal aus: Kann man das noch „verhältnismäßig“ nennen?

Dabei hat das BKA die Auto- und Scooterverleiher noch gar nicht entdeckt. Viele speichern bislang praktisch unkontrolliert GPS-Daten – meist ohne Löschfristen. Erst am 28.03.2023 hatte die französische Aufsichtsbehörde CNIL ein Bußgeld gegen Cityscoot verhängt (125.000 €). Ein Tröpfchen auf einem glühenden Stein.



Inhalt

Tröpfchen

Security News

Eine Kopie ist (k)eine Kopie

Recovery Attack

Vertrauenskett(ch)en

Top Secret

Kausalitätsprinzip

Geburtstagswünsche

Secorvo News

Secorvo Seminare

Wo, bitte, ist meine schwache Stelle?

Back to normal

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Eine Kopie ist (k)eine Kopie

Am 04.05.2023 stellte der EuGH zum datenschutzrechtlichen Auskunftsanspruch nach Art. 15 DSGVO klar, dass es nicht ausreicht, den Betroffenen Auskunft in Form allgemeiner Beschreibungen der Daten bzw. Datenkategorien zu geben. Das Recht auf Kopie bedeutet, dass „der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten" zu übermitteln ist. Ist dies nicht möglich, müssen die verarbeiteten Daten so zur Verfügung gestellt werden, dass „der betroffenen Person die wirksame Ausübung der ihr durch diese Verordnung verliehenen Rechte" ermöglicht, dabei aber auch die Rechte und Freiheiten anderer berücksichtigt werden. Damit werden insbesondere Geschäftsgeheimnisse und die Rechte Dritter geschützt. Dem Anspruch auf eine originalgetreue Kopie dürfen die Verantwortlichen also nicht uneingeschränkt nachkommen, sondern müssen eine Abwägung mit Rechten und berechtigten Interessen Dritter vornehmen.

Recovery Attack

Zusätzliche Sicherheitsmechanismen können auch zusätzliche Risiken bergen, wie Apples Recovery Key beweist. Der bereits 2014 eingeführte Mechanismus schützt die Apple-ID: Hat man das Kennwort zu seiner Apple-ID vergessen oder wurde es bei einem Angriffsversuch gesperrt, kann es mit einem vorher erzeugten, 28-stelligen zufälligen Recovery Key zurückgesetzt werden. Den Key sollte man außerhalb des Geräts speichern oder ausgedruckt in einen Tresor legen. Seit iOS 14 (2020) unterstützt Apple nach Aktivierung des Recovery Keys kein anderes Rücksetzungsverfahren mehr. Damit kann der Mechanismus nach hinten losgehen: Gewinnt ein Angreifer kurzzeitig physischen Zugriff auf das iPhone, kann er einen Recovery Key wählen oder einen bestehenden durch einen neuen ersetzen. Damit kann sich der Angreifer später jederzeit Zugriff auf die Apple-ID und damit das iCloud-Backup aller zugehörigen Geräte verschaffen – und den Geräteinhaber „aussperren".

Vertrauenskett(ch)en

Wer eine Vertrauenskette aufbaut, steht vor dem gleichen Dilemma wie Baron Münchhausen, der sich samt Pferd am eigenen Zopf aus dem Sumpf zog – im echten Leben gelingt das nur mit einer standfesten Verankerung. In der angelsächsischen Version der Legende zieht der Protagonist sich an den eigenen Stiefelriemen heraus – er „boot strap"-t.

Ist im Betriebssystem Secure-Boot aktiviert, prüft es, ob die UEFI-Firmware des Computers korrekte Daten zur Integritätsprüfung übergibt. Wie UEFI die herleitet, ist eine andere Frage. Um den Vertrauensanker dazu möglichst stabil zu gestalten, bietet Intel (in teureren CPUs) das Boot-Guard Verfahren an, dessen Details leider nicht offengelegt sind. Die Grundzüge sind wie folgt: Ein Computerhersteller kann über „Fuses" den Hashwert eines eigenen Public-Keys in die verbaute CPU brennen. Mit dessen Hilfe prüft der Microcode in der CPU die Integrität des ersten UEFI-Codeblocks, noch ehe ein Befehl aus der Firmware des Computers aufgerufen wird.

Dumm nur, wenn, wie Anfang Mai MSI und zuvor schon Lenovo passiert, der Private-Key dazu entschlüpft. Noch schlimmer, wenn der Mechanismus gar nicht aktiviert ist und eine UEFI-Malware den eigenen Key in die CPU-Fuses brennen könnte, um sich auch dort schon einzunisten – und somit Firmware-Updates zum Entfernen der UEFI-Malware selbst dem Hersteller nur noch durch Austausch der CPU möglich wären.

Insgesamt fehlt es der Secure-Boot-Vertrauenskette an Transparenz und Aufsicht. Im Web-PKI-Ökosystem ist – trotz Verbesserungspotenzials auch dort – die Vertrauenskette um Größenordnungen besser etabliert. Das CA/Browser-Forum ist die Steuerungsinstanz, die Requirements transparent veröffentlicht und ein recht striktes Aufsichts-Regime mit jährlichen Audits, Certificate Transparency usw. etabliert hat. Secure-Boot sollte da bald nachziehen, damit dessen Vertrauenskette nicht dauerhaft auf tönernen Füßen steht – und dessen Nutzer sich in falscher Sicherheit wähnen, wenn Secure-Boot aktiviert ist.

Top Secret

Am 24.11.2022 veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Stellungnahme zum datenschutzkonformen Einsatz von Microsoft 365 (SSN 11/2022) und stellte dabei Anforderungen an den Auftragsverarbeiter, die sich so nicht in der DSGVO wiederfinden. Daraufhin hat Microsoft zum 01.01.2023 das EU Data Boundary eingeführt (SSN 12/2022), wonach personenbezogene Daten im beschriebenen Rahmen innerhalb der EU gespeichert und verarbeitet werden sollen. An der Position der DSK hat sich jedoch nichts geändert.

Mittlerweile haben die Länder ein Rechtsgutachten zum Datenschutz konformen Einsatz von MS 365 anfertigen lassen. Ein Antrag von Frag den Staat auf Überlassung des Gutachtens wurde am 14.02.2023 abgelehnt. Begründung: Die Herausgabe dürfe nicht dazu führen, dass sich Dritte durch darin enthaltene Informationen wirtschaftliche Vorteile zu

Lasten öffentlicher Haushalte verschaffen (§ 14 Nr. 7 Landestransparenzgesetz Rheinland-Pfalz). Darüber hinaus würde eine Herausgabe das Verfahren zum Einkauf cloudbasierter Software und deren Vertragsmodalitäten – und damit die Verhandlungsposition gegenüber Microsoft – *„erheblich beeinträchtigen“* (§ 6 lit. b IFG NRW). Eine Anfrage von golem wurde ebenfalls abgelehnt.

Dabei liegt doch ein datenschutzkonformer Einsatz von Microsoft 365 mit geeigneten technischen und organisatorischen Mahnahmen im Interesse aller Beteiligten. Da fragt man sich doch, wie ein offenes und transparentes Vorgehen die Verhandlungsposition der Länder wohl schwächen könnte...

Kausalitätsprinzip

Am 04.05.2023 hat der EuGH die Voraussetzungen für das Vorliegen eines immateriellen Schadens nach Art. 82 DSGVO konkretisiert. Demnach setzt der Schadensersatzanspruch für immaterielle Schäden nicht voraus, dass der Schaden eine gewisse Erheblichkeit erreichen muss. Auch führt ein bloßer Verstoß gegen die Regelungen der DSGVO nicht automatisch zu einem Schadensersatzanspruch. Vielmehr bedarf es (1) eines Verstoßes gegen die DSGVO, (2) eines materiellen oder immateriellen Schadens, der aus diesem Verstoß resultiert, und (3) eines Kausalzusammenhangs zwischen Schaden und Verstoß. Dies entspricht dem deutschen Schuldrecht, welches ebenfalls einen kausalen Schaden als Voraussetzung für den Schadensersatz verlangt (§ 280 Abs. 1 BGB).

Zwar steigt durch das Urteil des EuGH das Risiko für Unternehmen auf Schadensersatzansprüche durch Betroffene, allerdings wird sich in der Praxis der Nachweis eines immateriellen Schaden schwierig gestalten.

Geburtstagswünsche

Mit Inkrafttreten der DSGVO am 25.05.2018 wurde innerhalb des Europäischen Wirtschaftsraums ein „einheitliches Datenschutzrecht“ geschaffen und das Recht auf informationelle Selbstbestimmung der Betroffenen gestärkt.

Allerdings mangelt es noch immer an einer konsequenten Durchsetzung und Kontrolle durch die Aufsichtsbehörden. Zwar erhielten die deutschen Aufsichtsbehörden im letzten Jahr ein Gesamtbudget von ca. 114 Millionen Euro, das deutlich über dem Budget anderer Mitgliedstaaten liegt. Doch verursacht der Föderalismus unterschiedliche Interpretationen und Durchsetzungsansätze bei den 17 deutschen Aufsichtsbehörden (inklusive der Sonderzuständigkeiten für Medien und Kirchen). Beschwerden konnten im letzten Jahr nicht zufriedenstellend bearbeitet werden. So kam es entweder nur zu geringen oder gar keinen Bußgeldern. Viele Beschwerden wurden insbesondere durch die Schaffung einer „Erheblichkeitsschwelle“ abgewiesen. Auch mangelt es an Transparenz, da – anders als in anderen Mitgliedstaaten – die Entscheidungen der Aufsichtsbehörden nicht konsequent veröffentlicht werden. Der Fokus liegt auf Informations- und Beratungstätigkeit und nicht auf konkreten Entscheidungen, wie sie beispielsweise zum Einsatz von Microsoft 365 überfällig wären.

Auch bei anderen europäischen Aufsichtsbehörden wird ein Großteil der Beschwerden nicht bearbeitet. Darüber hinaus zeigt der Bericht der ICCL deutlich, dass die irische Aufsichtsbehörde noch immer die Rolle eines Verhinderers bei der Durchsetzung des Datenschutzes gegen große IT-Unternehmen spielt. So wurden in der Vergangenheit rund 88 % der Entscheidungen der irischen Datenschutzbehörde durch den Europäischen Datenschutzausschuss außer Kraft gesetzt. Zum Geburtstag wünschen wir der DSGVO klarere Entscheidungen, einheitlichere Auslegungen des Datenschutzrechts und in der Höhe abgestimmte Bußgelder.

Secorvo News

Secorvo Seminare

Auf unserem Spätsommer-T.I.S.P.-Seminar vom **18. bis 22.09.2023** sind noch Plätze frei. Wir freuen uns auf Ihre Anmeldung.

Wo, bitte, ist meine schwache Stelle?

Schwachstellen sind die Kletterhaken der Angreifer – wer Software entwickelt, muss sie meiden wie der Teufel das Weihwasser. Wie man mit Hilfe von Vulnerability Management Systemen Schwachstellen sucht und bewertet, erfahren Sie am **22.06.2023** um **18 Uhr** auf dem kommenden Event der KA-IT-Si von den Experten der WIBU-Systems. Genießen Sie beim anschließenden „Buffet-Networking“ den Sommer auf der Dachterrasse. Schnell anmelden – die Zahl der Plätze ist begrenzt.

Back to normal

Endlich wieder im bewährten Format: Der 13. Tag der IT-Sicherheit findet am **20.07.2023** ab **14 Uhr** im Saal Baden der IHK Karlsruhe statt.

Es erwarten Sie Fachvorträge u. a. zur Bedrohung durch Quantencomputer, den Herausforderungen durch KI und zum Patchmanagement – sowie ein intensives Buffet-Networking. Hier geht's zu Programm und Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2023	
12.-13.06.	DuD 2023 (COMPUTAS, Berlin)
14.-15.06.	Entwicklertag 2023 (VKSI, GI, ObjektForum, Karlsruhe)
19.-23.06.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
22.06.	Wo, bitte, ist meine schwache Stelle? (KA-IT-Si, Karlsruhe)
Juli 2023	
03.-07.07.	8th IEEE European Symposium on Security and Privacy (IEEE, Delft/NL)
09.-12.07.	DFRWS USA 2023 (DFRWS, hybrid)
10.-15.07.	PETS 2023 (Université de Lausanne, hybrid)>
20.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, CyberForum, KASTEL Karlsruhe)

Fundsache

Die aktualisierte Handreichung zum "Stand der Technik" des TeleTrusT vom 09.05.2023 führt technische und organisatorische Maßnahmen auf, die gemäß definiertem Bewertungsschema von Unternehmen und Institutionen umgesetzt werden sollten. Die Handreichung wird kontinuierlich weiterentwickelt, ergänzt und stellt in kompakter Form die jeweilige Maßnahme vor und welche Schutzziele sie unterstützt. Aus unserer Sicht absolut lesenswert.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2023



Die IT frisst ihre Kinder

Es war wohl der IBM PC, der vor über 40 Jahren den Siegeszug der Informationstechnik auslöste. Das Versprechen: Computer machen unser Leben leichter. Und tatsächlich: Wer zuvor Schreibmaschine und Stift für die Korrespondenz benutzt hatte, konnte seinen Durchsatz mit Tastatur und E-Mail leicht verzehnfachen.

Als rund 20 Jahre später Internet-Portale Bankgeschäfte, Einkäufe, Musikgenuss, Videoverleih und Behördengänge von zuhause ermöglichten, steigerte auch das unsere Lebensqualität. Die Ersetzung des transportresistenten PC durch Laptops und Smartphones, auf denen Kommunikation, Portale, Unterhaltung und Nachrichten per Fingertipp verfügbar sind, krönte diese Entwicklung und festigte die Überzeugung, dass IT unser Leben verbessert. Doch stimmt das noch?

Selbst wenn man verödende Innenstädte, erhöhtes Verkehrsaufkommen durch individuelle Warentransporte, die Verlagerung von „Tippdiensten" (Stichwort Grundsteuer) auf die Bevölkerung und den Energieverbrauch von IT-Geräten (inzwischen fast 30% des Strombedarfs) als unvermeidliche Nebeneffekte hinnimmt, macht uns die Digitalisierung zunehmend das Leben schwer. Wer sich durch eine Telefon-Hotline „durchgeklickt", seine Steuererklärung mit digitalen Rechnungen gemacht, einen Smartphone-Modellwechsel durchgezogen, versucht hat, an einer Kasse mit leerem Handy-Akku zu bezahlen oder sich gerade wieder beim Online-Banking per Transaktion neu authentifizieren muss, obwohl er erst am Vortag eine Überweisung getätigt hat, kann davon ein Lied singen.

Dabei ist ein großer Teil der Komplexität hausgemacht. Das gilt nicht zuletzt für Schutzmechanismen – in sehr vielen Fällen sind Authentifikationen überflüssig, in anderen Fällen ließen sie sich durch Nutzung der 2021 eingeführten eID-Funktion des Personalausweises vereinfachen. Und: Im Biergarten kann man nach wie vor sicher und anonym mit Bargeld bezahlen. Solange man noch einen Geldautomaten findet.



Inhalt

Die IT frisst ihre Kinder

Security News

Cloud Supply Chain Security

Harmonie

Verpfiffen

Don´t roll your own crypto

Brute-Force-Biometrie-Attacke

Trau keinem Trust-Center

Secorvo News

Herzlich willkommen

Seminare nach der Sommerpause

13. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Cloud Supply Chain Security

Ein Satz wie „Der Angriff erfolgte ausschließlich auf den Dienstleister" (Kommentar der Barmer Ersatzkasse vom 17.06.2023 nach einem Hackerangriff auf den Dienstleister des Bonussystems) ist für Kunden keine Beruhigung. Vor allem: Ein Unternehmen wird die Verantwortung für die Datenverarbeitung durch die Verlagerung in die Cloud nicht los – häufig aber den Überblick.

Am 01.06.2023 veröffentlichte TeleTrusT einen Leitfaden zum Thema Cloud Supply Chain Security, der kompakt zusammenfasst, worauf es beim Einsatz von Cloud-Lösungen in der Supply Chain ankommt. Durch Maßnahmen wie „SBOM" (*Software Bill of Materials*) erfahren Auftraggeber, welche konkreten Frameworks und Software-Komponenten in den gebuchten Cloud-Diensten zum Einsatz kommen. Damit kann für die genutzten Cloud-Dienste im Incident Handling ein temporäres Abschalten bei der Identifikation ungepatchter Software-Komponenten vorgesehen werden.

Harmonie

Am 24.05.2023 hat der europäische Datenschutzausschuss (EDPB) die fast 50-seitigen Richtlinien zur einheitlichen Bemessung von Bußgeldern bei Verstößen gegen die DSGVO nach einjähriger öffentlicher Kommentierungsmöglichkeit (SSN 5/2022) verabschiedet. Das Vorgehen umfasst fünf Schritte von der Identifizierung bis zur finalen Bewertung. Besonders relevant für die Bußgeldhöhe ist die Festlegung des Ausgangspunktes. Dazu werden die Schwere (bezogen auf den Einzelfall), die Art und die Dauer des Verstoßes sowie die maximale Bußgeldhöhe herangezogen, die vom Umsatz des Unternehmens bestimmt wird. Erscheint der Verstoß schwerer als gleichartige Verstöße, soll das Bußgeld höher ausfallen. Bewertet wird auch das Verhalten des Verantwortlichen in Vergangenheit und Gegenwart; je nachdem erhöht oder vermindert sich das Bußgeld.

Die Richtlinien schaffen durch viele Beispielfälle mehr Transparenz bei der Bemessung von Bußgeldern. Sie liefern allerdings keine mathematische Formel, nach der Verantwortliche das Bußgeld berechnen könnten. Der Ermessenspielraum der einzelnen Aufsichtsbehörden bleibt trotz aller Vereinheitlichung erhalten – und das ist auch gut so.

Don´t roll your own crypto

Sichere Verschlüsselung ist schwierig umzusetzen. Schwachstellen können über fehlerhaft entworfene Protokolle (SSN 12/2022) oder auch schwache Komponenten, wie beispielsweise Zufallszahlen-generatoren (SSN 03/2023) entstehen.

Am 13.06.2023 veröffentlichten Forscher der Universität des Negev in Israel einen Seitenkanalangriff, der in der Lage ist, einen geheimen Schlüssel von einem Smartphone oder aus einer Smartcard auszulesen. Dafür wurde eine Variante der „Poweranalysis" verwendet, bei der der Stromverbrauch des Prozessors während einer Krypto-Operation zeitlich hoch aufgelöst aufgezeichnet und daraus der geheime Schlüssel abgeleitet wird.

Die Besonderheit bei dem neuen Angriff: Der Stromverbrauch des Prozessors wurde aus dem Flackern der Power-LED des Smartcard-Lesers bestimmt. Dafür war keine spezielle Kamera nötig: Der Angriff wurden mit einem handelsüblichen iPhone 13 durchgeführt. Das Geheimnis: Beim technisch bedingten „Rolling-Shutter" wird das Bild zeilenweise ausgelesen – die Zeilen des Bildes entstehen daher nicht zeitgleich. Füllt das Licht der Power-LED das gesamte Bild, so liefert jede Zeile eines Bildes Informationen über einen anderen Zeitpunkt. Wird durch den „Rolling-Shutter" das einzelne Bild beispielsweise in 1000 Schritten ausgelesen, so kann aus einem Video mit 60 Bildern pro Sekunde eine Messreihe mit 60.000 Messpunkten pro Sekunde abgeleitet werden. Diese Auflösung ist für eine „Poweranalysis" ausreichend. Allerdings benötigt der Angriff gut eine Stunde Videomaterial mit kontinuierlichen Krypto-Operationen, was einen realen Angriff mit dieser Methode stark erschwert. Der Angriff zeigt aber wieder einmal, dass (wie McGraw und Vega schon vor über 20 Jahren aufzeigten) bei der Implementierung von Kryptoverfahren viel schief gehen kann – auch an unerwarteten Stellen.

Verpfiffen

Der deutsche Gesetzgeber hat mit Verspätung zum 31.05.2023 das deutsche Hinweisgeberschutzgesetz beschlossen. Es tritt am 02.07.2023 in Kraft und beinhaltet für Unternehmen ab 50 Mitarbeitern die Pflicht, eine interne Meldestelle einzurichten. Unternehmen ab 250 Mitarbeiter müssen die Meldestelle mit Inkrafttreten errichtet haben; für kleinere Unternehmen gilt eine Umsetzungsfrist bis zum 17.12.2023.

In ihrer Orientierungshilfe zu Whistleblowing-Hotlines vom 14.11.2018 haben die Datenschutzaufsichtsbehörden darauf hingewiesen, dass die Meldungen von Hinweisgebern auch für die durch den Hinweis belasteten Personen ein hohes Risiko für deren Rechte und Freiheiten darstellen. Deshalb verlangen sie zu Recht die Durchführung einer

Datenschutz-Folgenabschätzung vor der Einführung von technischen Systemen zur Umsetzung der Meldestellenpflicht. Auch müssen die Mitarbeiter über etwaige Datenverarbeitungen informiert werden.

Wer dies vermeiden möchte, kann die Meldestelle bei einer Anwaltskanzlei einrichten – das spart nicht nur die Kosten für ein hoffentlich selten eingesetztes System, sondern auch dessen Pflege und Wartung.

Brute-Force-Biometrie-Attacke

Am 18.05.2023 veröffentlichten zwei chinesische Forscher einen BrutePrint getauften neuen Angriff auf die Fingerabdruck-Erkennung diverser Smartphone-Modelle. Anders als die meisten derartigen Angriffe versucht BrutePrint jedoch nicht, den Fingerabdruck zu fälschen: Die Forscher hängen nach Öffnen des Gehäuses ein eigenes Gerät in die SPI-Bus-Verbindung vom Fingerabdrucksensor zum Smartphone – ähnlich einem Hardware-Keylogger, der in die Tastaturleitung eingeschleift wird. Darüber kann der Angreifer übertragene Fingerabdruck-Samples mitlesen oder als Man-in-the-Middle eigene einspielen und durchprobieren. Daher auch der Name des Angriffs: *Brute*-Force-Finger-*Print*. Unter den getesteten Smartphones waren nur die (noch mit Touch-ID ausgestatteten) iPhones weitgehend resistent gegen den Angriff, da Apple als einziger Hersteller die SPI-Bus-Verbindung kryptographisch sichert.

Zwar haben alle Geräte einen Fehlbedienungszähler, der nach mehreren falschen Fingerpints eine Pause erzwingen soll, um Angreifer auszubremsen. Aber sogar bei iPhones war es möglich, den Vorgang über den SPI-Bus abzubrechen, bevor der Fehlbedienungszähler erhöht wird. Bei vielen Geräten war außerdem während der erzwungenen Pause zwar keine Anmeldung möglich, aber eingespielte Fingerabrücke wurden dennoch weiterhin ungebremst geprüft. Ein Lehrbeispiel dafür, wie man biometrische Sensoren nicht integrieren sollte.

Trau keinem Trust-Center

Zur einfachen Beantragung und automatisierten Erneuerung von TLS-Serverzertifikaten wird das ACME-Protokoll (zu Recht) immer populärer. Dabei verbindet sich ein ACME-Client (wie Certbot oder acme.sh) mit dem Trust-Center, das die Zertifikate ausstellt. Allerdings sollte sich das Vertrauen in das Trust-Center nur auf die ausgestellten Zertifikate und Sperrinformation beziehen, wie der am 08.06.2023 bekannt gewordene Vorfall bei einem chinesischen Trust-Center zeigt: Der Betreiber hatte eine unbekannte Remote-Code-Injection-Schwachstelle in acme.sh ausgenutzt, um während des Zertifikats-Enrollments zusätzliche Kommandos auf dem beantragenden Server auszuführen.

Zwar wurde schon am 09.06.2023 eine korrigierte Version von acme.sh veröffentlicht, aber da amce.sh manchmal auch in die Firmware von Appliances, Firewalls o. ä. integriert ist, kann es eine Weile dauern, bis nur noch gefixte Versionen im Einsatz sind. Eine Vorsichtsmaßnahme wäre, auf betroffenen Appliances ACME temporär zu deaktivieren und in den sauren Apfel des manuellen Enrollments zu beißen. Dann muss sich auch der Betreiber der chinesischen CA etwas Neues ausdenken…

Secorvo News

Aus dem Secorvo-Team

Mit Jochen Schlichting hat seit Juni ein weiteres Mitglied unseres Beratungsteams als „ISO/IEC 27001:2022 Lead Auditor“ die Lizenz zum Prüfen. Und seit Anfang Juli unterstützt uns unser neuer Kollege Paul Blenderman mit seiner über 20-jährigen Erfahrung mit IT-Sicherheit in Produktionsumgebungen. Willkommen im Secorvo-Team!

Seminare nach der Sommerpause

Bevor Sie Ihre Urlaubskoffer packen, werfen Sie doch noch einen Blick in unser Seminarangebot für das 2. Halbjahr. Wir starten mit unserem T.I.S.P.-Seminar vom **18. bis 22.09.2023** in den Herbst – noch gibt es freie Plätze.

Das Seminar IT-Security-Insights (**26.–27.09.2023**) aktualisiert Ihren Wissenstand zur Informationssicherheit. Wer sich mit Public-Key Infrastrukturen auskennen möchte, ist bei unserem PKI-Seminar (**09.–12.10.2023**) genau richtig. Und mit der Teilnahme am BSI-Seminar (**17.–19.10.2023**) bereiten Sie sich auf die Zertifizierung zum BSI-Vorfall-Experten vor. Wir freuen uns auf Ihre Anmeldung.

13. Tag der IT-Sicherheit

Endlich wieder im bewährten Format: Der 13. Tag der IT-Sicherheit findet am **20.07.2023 ab 14 Uhr** im Saal Baden der IHK Karlsruhe statt. Es erwarten Sie Fachvorträge zur Bedrohung durch Quantencomputer, den Herausforderungen durch die gestiegene Leistungsfähigkeit von KIs und zum Patchmanagement – sowie ein intensives Buffet-Networking. Hier geht's zum vollständigen Programm und zur Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2023	
10.-15.07.	PETS 2023 (Université de Lausanne, Lausanne/CH)
20.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, CyberForum, KASTEL, Karlsruhe)
August 2023	
05.-10.08.	Blackhat USA 2023 (Blackhat, Las Vegas/US)
06.-08.08.	SOUPS 2023 (usenix, Anaheim/US)
09.-11.08.	32nd USENIX Security Symposium (usenix, Anaheim/US)
10.-13.08.	DEF CON 31 (DEFCON, Las Vegas/US)
19.-24.08.	Crypto 2023 (Santa Barbara/US)
September 2023	
11.-13.09.	heise devSec 2023 (dpunt.verlag, heise, Karlsruhe)
18.-22.09.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-27.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
27.-29.09.	Informatik 2023 (GI, Hamburg)

Fundsache

Das Bayerische Landesamt für Datenschutzaufsicht hat sich der vom EDSA angekündigten Prüfaktion zu Stellung und Aufgaben von Datenschutzbeauftragten angeschlossen. Die Fragen zur Prüfung kann man u. a. bei IITR Datenschutz GmbH herunterladen.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2023



Die Quanten kommen

Im Jahr 1994 schockierte Peter Shor die Krypto-Community mit der Publikation eines Algorithmus', mit dem die Faktorisierung ganzer Zahlen und die Bestimmung diskreter Logarithmen auf einem Quantencomputer mit einen Aufwand von O(log n) möglich ist – also in polynomieller Zeit. Damit erschütterte er die Grundlagen der modernen (asymmetrischen) Kryptographie, kurz: den Kern aller heutigen Schutzmechanismen in vernetzten IT-Systemen. Seitdem beten die Kryptologen, dass Quantencomputer in der erforderlichen Größe (10-100 Mio. QBits für 2048-bit-Schlüssel) so schnell nicht kommen – und suchen derweil fieberhaft alternative, gegen Quantencomputer resistente Algorithmen. Die 2016 vom US-amerikanischen NIST gestartete Standardisierungs-Initiative für Post-Quantum Public Key-Algorithmen hat inzwischen schon zahlreiche gebrochene Verfahren aussortiert – mit anderen mathematischen Problemen, die sich für asymmetrische Verfahren eignen könnten, kennen wir uns eben bei weitem nicht so gut aus wie mit der Faktorisierung ganzer Zahlen und dem diskreten Logarithmus.

Sollten die Kryptologen das Wettrennen gegen die Milliardeninvestitionen in Quantencomputer nicht gewinnen, werden wir wohl in archaische IT-Verhältnisse zurückfallen, denn ohne asymmetrische Kryptografie lassen sich Cloud-Computing, Internet-Banking oder Online-Shops praktisch nicht absichern.

Vielleicht haben die Kryptologen noch etwas Zeit. Denn Quantencomputer heutiger Konstruktion sind nicht so einfach herzustellen: Sie müssen bis nahe an den absoluten Nullpunkt gekühlt werden und verbrauchen daher gigantische Energiemengen. Auch die Bereitstellung einer großen Zahl an QBits ist bisher nicht einfach – und da kann man mit größeren Schlüssellängen ein wenig gegensteuern.

Irgendwann aber wird es solche Quantencomputer geben. Ich habe gewettet, dass das noch mindestens 30 Jahre dauert. Mit mehr als einer Kiste Bier wollte ich dabei allerdings nicht ins Risiko gehen.



Inhalt

Die Quanten kommen

Security News

Dritter Anlauf

Blindgänger aus Crypto War

Signierte Malware-Kernel-Treiber

BSI Standard 200-4 – Finale Version

Mobilfunk-Bewegungsdaten

Im Überwachungsstaat

Secorvo News

Überarbeitetes T.I.S.P.-Curriculum

Secorvo Seminare

Authenticate. Generate. Repeat.

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Dritter Anlauf

Nach dem Scheitern von Safe Harbour und Privacy Shield verabschiedete die Europäische Kommission am 10.07.2023 mit dem Data Privacy Framework (DPF) den dritten Angemessenheitsbeschluss für die USA. Personenbezogene Daten dürfen damit wieder ohne zusätzliche Maßnahmen in die USA übertragen werden, sofern die Empfänger DPF-zertifiziert sind. Das U.S. Department of Commerce pflegt die öffentliche Liste aller zertifizierten Organisationen – die sich blitzschnell mit rund 2.500 Einträgen füllte, da das DPF eine reine Selbst-Zertifizierung ist.

Gemäß den Urteilen Schrems I und Schrems II des EuGH ist die US-Überwachung nach FISA 702 und EO 12.333 nicht verhältnismäßig und damit rechtswidrig. In der EO 14.086 (einer leicht angepassten Version der EO 12.333) wurde eine Verhältnismäßigkeitsprüfung ergänzt, die aber faktisch wenig Relevanz haben dürfte: Beschwerden können an den Civil Liberties Protection Officer (CLPO) gerichtet werden, der die Beschwerde jedoch nur prüfen und interne Weisungen erteilen kann. Das Ergebnis der Prüfung kann von einem Data Protection Review Court überprüft werden. Dem Betroffenen wird jedoch nicht mitgeteilt, ob er tatsächlich von einer Überwachungsmaßnahme betroffen war und welche Wirkung seine (anerkannte) Beschwerde hatte.

Nachdem der EUGH bereits die ersten beiden Angemessenheitsbeschlüsse für nichtig erklärt und Max Schrems angekündigt hat, auch den aktuellen Beschluss gerichtlich prüfen zu lassen, sollte man besser nicht auf eine lange Lebenszeit des DLP wetten.

Blindgänger aus Crypto War

Unter dem Namen TETRA:BURST hat die niederländische IT-Sicherheitsfirma Midnight Blue am 24.07.2023 fünf Schwachstellen veröffentlicht, die sie im Auftrag der NLnet-Stiftung mit Hilfe eines Motorola-Fahrzeugfunkgeräts im TETRA-Standard gefunden hat. Dieser 1995 entwickelte ETSI-Standard wird in über 120 Ländern in den Funknetzen von Polizei und Feuerwehr genutzt.

Die meisten Verwundbarkeiten hängen direkt oder indirekt mit der verwendeten proprietären, geheim gehaltenen 80-bit-Stromchiffre zusammen, für die kein öffentliches Peer Review erfolgte. Aufgrund der damaligen Exportbeschränkungen wurde (wie auch bspw. bei Lotus Notes) sogar eine Schwachstelle eingebaut: Damals entwickelte Export-Geräte verwenden effektiv nur 32 Bit lange Schlüssel, die die Forscher mit einem Laptop in wenigen Minuten knacken konnten. Die Details der Schwachstellen (CVE-2022-24400 bis -24404) sollen am 09.08.2023 publiziert werden.

Eine von der ETSI angekündigte Überarbeitung des Standards und die Updates der Hersteller werden die kompromittierten Kryptoverfahren jedoch kaum komplett ersetzen, da die (ungepatchte) Gebrauchsdauer von einmal beschafften Funkgeräten weit über der eines Durchschnitts-PCs oder Smartphones liegt.

Signierte Malware-Kernel-Treiber

Sophos X-Ops publizierte am 11.07.2023 zeitgleich mit einem Microsoft Advisory (ADV230001), dass sie über 100 mit Malware versetzte Windows-Kernel-Treiber entdeckt haben, die bis April 2021 zurückreichen und von Microsoft und anderen Code-Signing-Autoritäten digital signiert worden waren.

Die entdeckten Treiber waren entweder Varianten bekannter Windows-Rootkits oder „Protection Disabler", die Schutzmechanismen des Betriebssystems deaktivieren. Microsoft hat die Treiber in ihre Sperrliste aufgenommen und Sophos hat die Hashwerte und weitere Details zu den betroffenen Treibern in Github publiziert.

BSI Standard 200-4 – Finale Version

Seit dem 14.06.2023 ist der BSI Standard 200-4 „Business Continuity Management" 1.0 verfügbar, der den BSI Standard 100-4 „Notfallmanagement" abgelöst hat. Dies markiert das Ende eines sehr intensiven Peer-Reviewprozesses von Community Drafts (CD 1.0 01/2021, CD 2.0 09/2022) bis zum international gültigen Standard ISO/IEC 22301:2019 „Security and resilience – Business continuity management systems – Requirements".

Der 200-4 geht inhaltlich deutlich über den ISO/IEC 22301 hinaus und bietet eine Mischung aus Anforderungen, Umsetzungsvorschlägen und selbsterklärenden Texten. Sehr praktisch ist der Anforderungskatalog zum Standard 200-4 in Excel, der ein detailliertes Mapping auf die Anforderungen des ISO-Standards enthält, deren Erfüllung so nach Implementierung eines BCM-Systems (BCMS) nach 200-4 leichter nachgewiesen werden kann.

Da bereits der Vorgängerstandard 100-4 im Umfeld von MaRisk und KRITIS als Anforderungskatalog genutzt wurde, ist davon auszugehen, dass auch der 200-4 eine größere Rolle in der Finanzbranche spielen wird. Dabei eignet er sich für jedes Unternehmen, dass ein BCMS in deutscher Sprache aufbauen möchte.

Besonders wertvoll sind die sehr umfangreichen und ziemlich ausgereiften Hilfsmittel zum 200-4

wie Vorlagen und ein Kennzahlensystem. Einziger Wermutstropfen: Die thematische Struktur folgt nicht genau dem zertifizierbaren ISO 22301:2019.

Mobilfunk-Bewegungsdaten

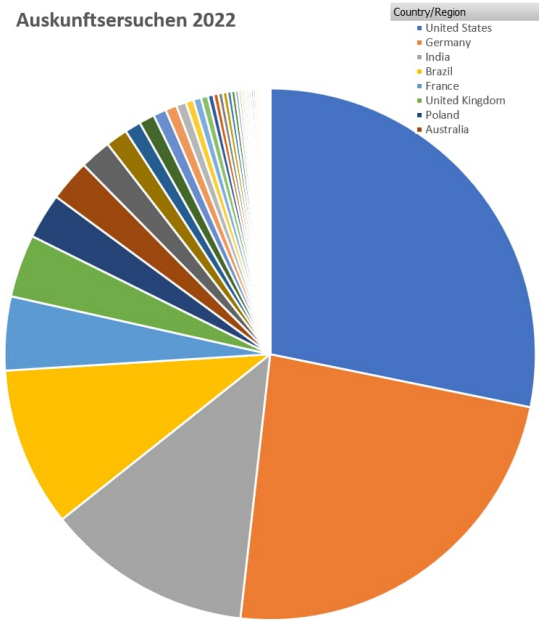
Die Mobilfunknetzbetreiber in Deutschland sammeln, analysieren und verkaufen die Bewegungen ihrer Kunden in anonymisierter Form zu Marketingzwecken an Drittunternehmen. Das ist nicht neu – wir berichteten darüber schon vor fast 15 Jahren (SSN 12/2008).

Durch das Schrumpfen der durchschnittlichen Größe einer Funkzelle in LTE-Netzen werden diese Daten immer genauer – in Städten geben sie ein ziemlich präzises Bewegungsprofil eines Mobilfunkteilnehmers, aus dem sich Wohnort, Arbeitsplatz, Einkaufsverhalten und Freizeitaktivitäten ablesen lassen.

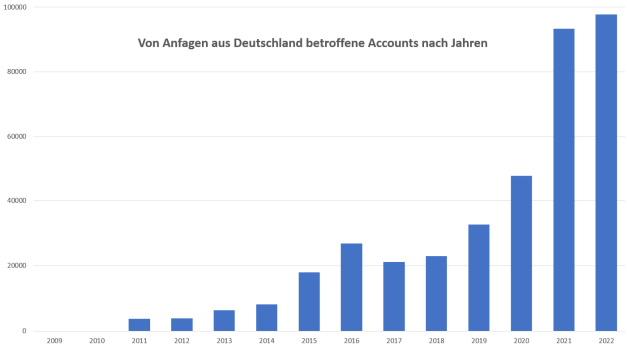
Zwar wirbt Telefónica mit einem dreistufigen Anonymisierungsverfahren; konkrete Informationen über dessen Funktionsweise möchten aber weder sie noch andere Netzbetreiber wie die Telekom herausgeben. Immerhin: Man kann der Verarbeitung der Bewegungsdaten widersprechen. Als Kunde von Telefónica (O2, Blau, Fonic, Simyo u. w.) muss man dafür eine (kostenlose) SMS mit dem Text „Abmelden" an die Nummer 66866 senden. Telekom-Kunden (Congstar, Klarmobil u. w.) können über ein Opt-Out-Portal widersprechen.

Im Überwachungsstaat

Seit 2009 dokumentiert Google in seinem Transparenzbericht die weltweiten Auskunftsanfragen von behördlichen Stellen. Sieht man sich die Statistiken ein wenig genauer an, kommt man zu ernüchternden Einsichten: Es sind keineswegs die „Schurkenstaaten", die Google mit Anfragen überhäufen: Auf die USA folgt mit weitem Abstand vor allen anderen 91 Ländern – Deutschland.



Auch steigt die Zahl der von deutschen Anfragen insgesamt betroffenen Accounts seit vielen Jahren. Willkommen im Überwachungsstaat.



Secorvo News

Überarbeitetes T.I.S.P.-Curriculum

Seit dem 01.07.2023 gilt für den TeleTrusT Information Security Professional ein umfangreich überarbeitetes Curriculum. Alle Inhalte wurden von den Anbietern auf den Prüfstand gestellt, aktualisiert, ergänzt oder gekürzt. Hinzu kamen zwei neue Module zu „Virtualisierung" und „Cloud-Security". Damit wurden die Inhalte des T.I.S.P.-Seminars zum dritten Mal an aktuelle Entwicklungen der Informationssicherheit angepasst.

In einem Beitrag in der iX 9/2023 stellt Stefan Gora das neue Curriculum des T.I.S.P. ausführlich vor.

Secorvo Seminare

Noch keine Weiterbildung in diesem Jahr besucht? Dann werfen Sie doch mal einen Blick auf unsere Fachseminare im Herbst – Infos und Anmeldung unter https://www.secorvo.de/seminare.

Authenticate. Generate. Repeat.

Das nächste KA-IT-Si-Event am **14.09.2023** (18 Uhr) in der IHK Karlsruhe widmet sich dem Einsatz von PKIs in der Industrie.

Tamás Horváth von Nexus wird einen Überblick über IoT-typische Bedrohungen und die entsprechenden Sicherheitsziele geben. Gemeinsam mit der Firma STIHL wird er am Beispiel des internetfähigen Mähroboters iMow zeigen, wie die Provisionierung digitaler Identitäten mit Hilfe einer autonomen Factory CA gelingt.

Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum intensiven Buffet-Networking. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2023	
10.-13.08.	DEF CON 31 (DEFCON, Las Vegas/US)
19.-24.08.	Crypto 2023 (Santa Barbara/US)
September 2023	
11.-13.09.	heise devSec 2023 (dpunt.verlag, heise, Karlsruhe)
14.09.	Authenticate. Generate. Repeat. (KA-IT-Si, Karlsruhe)
18.-22.09.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-27.09.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
28.09.	IT-Sicherheitsrechtstag 2023 (Swiss Cyber Storm Association, Bern/CH)
Oktober 2023	
9.-12.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
10.-12.10.	it-sa 2023 (NürnbergMesse GmbH), Nürnberg
17.-19.10.	BSI Vorfall-Experte – Aufbauschulung (Secorvo, Karlsruhe)

Fundsache

Eine gute Hilfestellung bei der Prüfung von Auftragsverarbeitungsverträgen bietet die Checkliste des „Datenschutz-Gurus“ Rechtsanwalt Stephan Hansen-Oest.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2023



Wayback Machine

Sie erinnern sich zweifellos: Es war ein Monat weltbewegender Ereignisse. Bundesverteidigungsminister Rudolf Scharping wurde von Gerhard Schröder entlassen, die Bahn eröffnete die Schnellstrasse Frankfurt-Köln und MCI WorldCom geriet in die Insolvenz. Michael Schuhmacher wurde zum fünften Mal (und vorzeitig) Formel-1-Weltmeister, Serena Williams gewann Wimbledon vor ihrer Schwester und die deutsche Fußballnationalmannschaft musste im Finale der Weltmeisterschaft Brasilien den Vortritt lassen. Chang Sang wurde erste weibliche Premierministerin in Südkorea und George Bush errichtete als Reaktion auf die Terroranschläge von 9/11 ein Ministerium für „Homeland Security".

Sie ahnen es: Es geht um den Juli 2002, den Monat, in dem die erste Ausgabe der Secorvo Security News das Licht der Welt erblickte. Seitdem schlägt sie Monat für Monat eine „Schneise in die Informationsflut", wie wir es uns in der Erstausgabe vor 21 Jahren vorgenommen haben. Inzwischen sind exakt 250 Ausgaben erschienen – mit einem Umfang von je vier Seiten, einem Editorial, relevanten Nachrichten zu IT-Security und Datenschutz aus dem vorausgegangenen Monat und aktuellen Terminhinweisen.

1000 Seiten „SSN" sind so zusammengekommen, die wir Ihnen zur Feier dieses Jubiläums in einem „Großen Buch der Security News" zum Download zusammengefasst haben. Eine (gar nicht so kurze) Geschichte der IT-Sicherheit, gespickt mit zahlreichen Déjà-vus. Da mischt sich das eine oder andere Schmunzeln in die Erinnerung – aber auch die ernüchternde Einsicht, wie häufig Fehler wiederholt werden und wie selten aus der Geschichte gelernt wird.

Wir freuen uns auf viele weitere Ausgaben der Security News, in denen wir die weitere Entwicklung der IT-Sicherheit und des Datenschutzes begleiten werden. Und über ein Feedback von Ihnen – und natürlich Ihre begeisterte Weiterempfehlung.



Inhalt

Wayback Machine

Security News

Verlorener Generalschlüssel

Gefährliche Altlasten

Backdoor Browserweiterung

Excel Disclosure

Verschlüsselte Backups

NIST CSF 2.0

Der DSA kommt

Secorvo News

Secorvo Seminare

Authenticate. Generate. Repeat.

Veranstaltungshinweise

secorvo
security consulting

Security News

Verlorener Generalschlüssel

Den am 11.07.2023 von Microsoft veröffentlichten Angriff auf Office-365-Instanzen von mindestens 25 Unternehmen durch eine chinesische Hackergruppe hatte nicht Microsoft, sondern eine amerikanische Bundesbehörde entdeckt. Seit dem 15.05.2023 besaßen die Hacker einen gültigen Signierschlüssel für Authentifikationstoken der Azure-Cloud – einen Generalschlüssel, den Microsoft offenbar nicht in einer geschützten Hardware, sondern auf einem Rechner gespeichert hatte. Bei einem Systemabsturz war er bereits im April 2021 (!) im Snapshot eines Crash-Dumps gelandet – der in das „Debugging Environment" verschoben worden war. Dort konnten die Hacker über den Account eines Mitarbeiters eindringen und den Crash Dump analysieren – so die Ergebnisse der am 06.09.2023 veröffentlichten Untersuchung von Microsoft.

Die – teilweise pikanten – technischen Details des Angriffs hat Hans-Joachim Knobloch (Secorvo) analysiert und in der iX 9/2023 beschrieben.

Wir lernen daraus: Bei Azure ist es keinesfalls selbstverständlich, dass die Generalschlüssel in Hardware Security Modules liegen – bei PKIs ist das normalerweise der Standard. Generalschlüssel, die nicht mehr benötigt werden, werden bei Microsoft auch nicht unverzüglich gesperrt; stattdessen können sie in Crash Dumps auftauchen. Und auf die haben Angreifer Zugriff, die sich anscheinend ungestört im Entwicklernetz von Microsoft tummeln.

Zum Glück ist Cloud Computing sicher.

Gefährliche Altlasten

Mehrere englischsprachige Cybersecurity Agencies haben am 03.08.2023 ein gemeinsames Cybersecurity Advisory (2022 Top Routinely Exploited Vulnerabilities) veröffentlicht, in dem sie vor im Jahr 2022 besonders häufig von Angreifern genutzten Schwachstellen warnen. Allein von den 12 kritischsten CVEs stammen eines aus dem Juni 2019 und sechs weitere aus dem Jahr 2021. Offenbar ist noch immer bei zahlreichen Behörden und Unternehmen ein systematisches Patch-Management keine Selbstverständlichkeit.

Backdoor Browserweiterung

Ein wichtiger Schritt zur Verringerung des Angriffsrisikos war vor einigen Jahren, Windows-Benutzern die lokalen Administrationsrechte zu entziehen, damit sie nicht mehr alles installieren können, was im Internet glänzt. Daher bieten inzwischen Softwarehersteller (und Angreifer) vermehrt Installationen im Benutzerkontext an.

Das betrifft auch Chrome- und Edge-Extensions sowie Firefox-Add-ons. Zwar verhindert Firefox seit Jahren die Ausführung von bekannt problematischen Erweiterungen – die Sperrliste hat bereits eine beachtliche Länge. Und Google kündigte am 16.08.2023 an, Chrome-Anwender zumindest vor solchen Erweiterungen zu warnen. Entfernen oder wenigstens abschalten müssen die Nutzer sie allerdings selbst. Vor allem aber kann man bei allen drei Browsern per Policy festlegen, welche Erweiterungen Anwender installieren dürfen. Das zentrale Management von zulässigen Erweiterungen ist inzwischen ebenso zu empfehlen wie der noch immer wichtige Entzug der lokalen Administrationsrechte.

Excel Disclosure

Täglich tauschen Organisationen untereinander Millionen Excel-Dateien aus. Doch das Dateiformat ist tückisch: So können ausgeblendete oder schlicht übersehene Kommentare, Spalten, Zeilen oder ganze Arbeitsblätter enthalten sein: Die Berechnung im Angebot könnte die Marge, ein Kommentar im Vertragstext den vorhandenen Spielraum verraten. Das BSI widmete diesem Problem im Februar 2020 sogar einen eigenen Grundschutz-Baustein. Besonders heikel wird es, wenn Excel- (oder andere Office-) Dateien veröffentlicht werden. Diese Aufgabe sollte man daher geschulten Mitarbeitern übertragen.

Bei der Polizei von Nordirland scheint das noch nicht angekommen zu sein: Am 08.08.2023 beantwortete eine Nachwuchskraft eine Anfrage nach dem Informationsfreiheitsgesetz mit einer Datei, die außer den angefragten Daten auch Nachname und Initialen, Position, Rang, Standort und Abteilung sämtlicher Mitarbeiter enthielt. Brisante Daten in einem Land, in dem vor allem katholische Polizisten um ihre Sicherheit bangen müssen. Die Datei war zwar nur drei Stunden abrufbar, hat aber in dieser Zeit den Weg in die Welt gefunden. Nun verfolgt die irische Polizei Einzelpersonen, die im Besitz einer Kopie der Datei sind – ein eher aussichtsloses Unterfangen.

Vor solchen unerwünschten Preisgaben bewahren geeignete DLP-Verfahren und -Systeme, oder die Verwendung des weniger verfänglichen PDF-Formats.

Verschlüsselte Backups

Der kleine dänische Webhoster CloudNordic wurde am 18.08.2023 Opfer eines Ransomware-Angriffs, bei dem auch die Backups verschlüsselt wurden. Daraufhin erklärte man den Kunden auf einer provisorischen Homepage: *Leider hat es sich als unmöglich erwiesen, weitere Daten wiederherzustellen, und die meisten unserer Kunden haben alle Daten bei uns verloren.* Es folgt noch der Hinweis, der Kunde könne, sofern er kein eigenes lokales Backup habe, seine Webseiteninhalte möglicherweise der Wayback Machine entnehmen.

Dort findet man übrigens auch die Version der CloudNordic-Webseite vom Juni 2023, auf der der Hoster erklärt, alle Grundsätze der ISO 27001 zu befolgen und sich auf eine Zertifizierung vorzubereiten. Angeblich waren auch Maßnahmen ergriffen worden, die verhinderten, dass Angreifer von der Produktionsumgebung auf Management- oder Backupsysteme zugreifen konnten – wegen eines Umzugs waren sie jedoch vorübergehend deaktiviert worden. Eine Gelegenheit, auf die die Angreifer offenbar gewartet haben.

Und die Moral? Glauben Sie nicht blind den Sicherheitsversprechen Ihrer Dienstleister – denn auch Profis können mal schwächeln. Ein eigenes Backup ist daher eine gute Idee: Better safe than sorry.

NIST CSF 2.0

Am 08.08.2023 hat das NIST das Cybersecurity Framework (CSF) 2.0 als Initial Public Draft veröffentlicht. Zur Diskussion stehen neue Versionen des Frameworks selbst sowie des Framework Cores. Wie in der Vorversion 1.1 beschäftigt sich das erste Dokument mit der Anwendung, das zweite beschreibt Anforderungen mit Umsetzungsbeispielen.

In der neuen Version wurden die Bezüge des CSF zu anderen NIST-Standards mit ihren eigenen Sichten auf die Informationssicherheit in das Cybersecurity and Privacy Reference Tool ausgelagert. Zudem wird der Anwendungsbereich von Unternehmen der kritischen Infrastrukturen auf alle Unternehmen ausgeweitet. Bei den Anforderungen finden sich – ähnlich wie in der neuen Version der ISO 27002 – einige Reorganisationen und Umstrukturierungen.

Die vielleicht wichtigste Neuerung ist, dass mit „Governance" eine alle Phasen des Entwicklungszyklus umfassende Schicht mit eigenen Anforderungen hinzugekommen ist.

Der DSA kommt

Ab dem 17.02.2024 müssen Anbieter digitaler Dienste den Anforderungen des Digital Services Act (DSA) genügen (SSN 05/2022). Dazu zählen, dass illegale Inhalte unverzüglich zu löschen und Nudging und Dark Pattern verboten sind. Auch die Nutzung von Werbeprofilen, die auf besonderen Kategorien personenbezogener Daten (wie der sexuellen Orientierung, politischen Überzeugung oder der ethnischen Herkunft) beruhen, ist unzulässig. Zum Erhalt des Prinzips der freien Rede darf kein allgemeines Content Monitoring betrieben werden. Am 25.04.2023 hatte die EU-Kommission 19 sehr große Plattformen und Suchmaschinen (sog. VLOPs) festgelegt, die die Regelungen bereits seit Ende August erfüllen müssen.

Verstöße gegen Bestimmungen des DSA haben empfindliche Bußgelder zur Folge – sie können bis zu 6% des weltweiten Jahresumsatzes betragen. Die EU hat am 25.04.2032 eine „Questions & Answers"-Seite zum DSA bereitgestellt, die die Umstellung unterstützen soll.

Secorvo News

Secorvo Seminare

Im Oktober starten unsere Seminare in die goldene Herbstsaison. Mit der Teilnahme am Seminar „BSI-Vorfall-Experte – Aufbauschulung" vom **17.-19.10.2023** erfüllen Sie eine wesentliche Voraussetzung für die entsprechende BSI-Zertifizierung zum Vorfall-Experten. Oder Sie sichern sich noch einen der wenigen freien Plätze im letzten T.I.S.P.-Seminar des Jahres vom **13.–17.11.2023**: Krönen Sie Ihre Kenntnisse in der Informationssicherheit mit einem anerkannten Zertifikat und werden Sie Teil der engagierten „T.I.S.P.-Community".

Das inhaltlich gründlich überarbeitete und didaktisch neu konzipierte T.P.S.S.E.-Seminar startet **vom 27. bis 30.11.2023** in die erste Runde. Für Software-Entwickler definitiv ein „Must-have" – gelebte Informationssicherheit. Profitieren Sie vom Frühbucherrabatt. Wir freuen uns auf Ihre Anmeldung!

Authenticate. Generate. Repeat.

Das nächste KA-IT-Si-Event widmet sich dem Einsatz von PKIs in der Industrie. Tamás Horváth von Nexus wird einen Überblick über IoT-typische Bedrohungen und die entsprechenden Sicherheitsziele geben. Gemeinsam mit der Firma STIHL wird er am Beispiel des internetfähigen Mähroboters iMow zeigen, wie die Provisionierung digitaler Identitäten mit Hilfe einer autonomen Factory CA gelingt. Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum intensiven Buffet-Networking.

Wir freuen uns auf Sie am **14.09.2023** um 18 Uhr in den Räumen der IHK Karlsruhe (Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2023	
11.-13.09.	heise devSec 2023 (dpunkt.verlag, heise, Karlsruhe)
14.09.	Authenticate. Generate. Repeat. (KA-IT-Si, Karlsruhe)
27.-29.09.	Informatik 2023 (GI, Hamburg)
28.09.	IT-Sicherheitsrechtstag 2023 (Swiss Cyber Storm Association, Bern/CH)
Oktober 2023	
10.-12.10.	it-sa 2023 (NürnbergMesse GmbH, Nürnberg)
12.10.	Ransomware as a Service (KA-IT-Si, Karlsruhe)
17.-19.10.	BSI Vorfall-Experte – Aufbauschulung (Secorvo, Karlsruhe)
24.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
November 2023	
07.-09.11.	IDACON 2023 (WEKA-Akademie, München)
08.-09.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
13.-17.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
26.-30.11.	ACM CCS 2023 (ACM/SIGSAC, Copenhagen/DNK)
27.-30.11.	T.P.S.S.E. (TeleTrusT Professional for Secure Software Engineering) (Secorvo, Karlsruhe)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blendermann, Robert Eitel, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2023



Morgengrauen

Seit dem Inkrafttreten der Datenschutz-Grundverordnung hat sich die Spannung zwischen Grundrechtschützern und (nicht allein staatlichen) Kontrollinteressen spürbar verschärft. Während einerseits engagierte Datenschützer wie Max Schrems von vielen klaren EuGH-Entscheidungen zu Gunsten des Persönlichkeitsschutzes Recht bekamen, fielen zugleich immer mehr Lebensbereiche der raumgreifenden digitalen Erfassung unseres Verhaltens zum Opfer: Kameras und GPS-Sensoren in Fahrzeugen, Nutzungsprofile in Cloud-Apps und Präferenzanalysen von Musik- und Video-Streaming-Diensten liefern inzwischen nicht nur ein lückenloses Bild unserer Tagesabläufe, sondern können sogar – meist auf der rechtlichen Grundlage von einmal erteilten und längst vergessenen Einwilligungen – unser zukünftiges Verhalten zuverlässig vorhersagen (siehe z. B. Churn Prediction).

Die wegweisenden EuGH-Entscheidungen zu Datentransfers, Tracking, Schadenersatzansprüchen und anderen wichtigen Datenschutz-Fragen kommen allerdings häufig spät und scheinen immer wieder der Realität hinterherzuhinken, während die Digitalisierung unseres Lebens sich ungebremst auszubreiten scheint. Aber manchmal kommt es eben doch anders als man denkt – und das gibt immer wieder Anlass zu Hoffnung. Denn Grundsatzentscheidungen hoher Gerichte können im Handstreich nicht nur ganze Klassen von Datenverarbeitungen für rechtswidrig erklären, sondern auch elementare Begehrlichkeiten und Haltungen. Daher ist das Urteil des Bundesverwaltungsgerichts vom 07.09.2023, mit dem die Vorratsdatenspeicherung endgültig für unzulässig erklärt wurde, in seiner Bedeutung kaum zu überschätzen. Das Signal ist eindeutig: Die Nutzung und Speicherung personenbezogener Daten für andere als die eigentlichen Zwecke der Erhebung ist unzulässig – und ist der Zweck erfüllt, sind die Daten zu löschen. Das gilt für Strafverfolgungsbehörden genauso wie für Unternehmen.



Inhalt

Morgengrauen

Security News

Gefährliche Zeitkorrekturen

Passwörter in der Cloud

Dreimal Pieps und der Zug steht

Quod licet Iovi...

Wenn aus Apps Trojaner werden

Recht sicher, nicht rechtssicher

Secorvo News

Silbernes Jubiläum

Secorvo Seminare

RaaS – Ransomware as a Service

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Gefährliche Zeitkorrekturen

2016 erweiterte Microsoft den Windows Time Service um die fragwürdige Fähigkeit, die korrekte Uhrzeit aus dafür nicht gedachten Feldern im TLS-Handshake auszulesen und eine abweichende Systemuhrzeit rigoros daran anzugleichen. Gedacht, um Probleme auf kleinen Endgeräten ohne batteriegestützte Hardwareuhr zu lösen, wurde das Feature jedoch so implementiert, dass es auch auf Servern greift. Und da sorgt es immer wieder für dramatische Probleme, wenn es etwa das Datum um 55 Tage in die Zukunft verlegt.

Microsoft verlässt sich für die Implementierung darauf, dass im Handshake die Unix-Zeit verwendet wird. Das steht aber schon seit 2013 in Frage und ist bspw. in OpenSSL deaktiviert. Dennoch hält Microsoft bis heute an dem Feature fest, hat aber immerhin dokumentiert, wie man es abschalten kann. Nicht nur wir, sondern auch einer von Microsofts Escalation Engineers empfiehlt, das auf Domain Controllern sowie auf allen Servern zu tun.

Passwörter in der Cloud

Passwortmanager helfen nicht nur, sich zahlreiche unterschiedliche Passörter zu merken, sondern auch, schlechte und bereits verwendete zu vermeiden. Cloudbasierte Lösungen wie 1Password oder LastPass sind derzeit weit verbreitet. Im November 2022 gelang es Hackern, Passwort-Datenbanken bei LastPass von den Cloudservern abzuziehen. Am 22.12.2022 gestand LastPass ein, den Schlüssel für einzelne Datenbanken mit viel zu wenig PBKDF2-Interationen aus dem Master-Passwort berechnet zu haben. Und am 28.08.2023 wurde bekannt, dass ein paar der Datenbanken mit Brute-Force-Angriffen entschlüsselt werden konnten. Den Einfluss der PBKDF2-Iterationen erläuterte daraufhin Wladimir Palant in seinem Blog: Sehr alte Datenbanken mit nur einer Iteration können in etwa 17 Stunden entschlüsselt werden; erst bei 100.000 Iterationen steigt der Aufwand auf rund 100.000 GPU-Jahre.

Softwareentwicklern, die nicht in dieselbe Falle tappen wollen, empfehlen wir die Teilnahme an einem T.P.S.S.E.-Seminar...

Dreimal Pieps und der Zug steht

Am 11.01.2008 berichtete The Telegraph, wie ein Jugendlicher im polnischen Łódź mit einer TV-Fernbedienung U-Bahn-Weichen umgestellt und so mindestens eine Entgleisung verursacht hatte (SSN 01/2008). Sicherer ist die Technik auch 15 Jahre später nicht: Am 26.08.2023 meldete die BBC, dass (mutmaßlich mit Russland verbundene) Hacker bei etwa zwanzig polnischen Zügen eine Notbremsung ausgelöst hatten, indem sie per Funk drei kurze Signaltöne sandten. Erst im kommenden Jahr soll die unsichere analoge UKW-Funktechnik in Polen durch GSM-R ersetzt werden.

Ein Beispiel für Risiken, die aus der oft sehr langen Betriebszeit solcher analogen Systeme erwachsen – vermutlich findet sich ähnlich archaische Technik auch noch anderswo auf der Welt in sicherheitsrelevanten Umgebungen.

Quod licet Iovi...

Inzwischen gibt es zahlreiche gesetzliche Regelungen und Rechtsprechung zur optischen und inhaltlichen Gestaltung von Cookie-Bannern (siehe zuletzt SSN 8/2023). Probleme mit der rechtskonformen Anpassung der Banner sowie dem Einwilligungsmanagement hat jedoch offenbar die öffentliche Verwaltung: Hier stolpert man immer wieder über unzulässige Lösungen. Ursache dafür mag sein, dass öffentliche Stellen im Unterschied zu Unternehmen bei Datenschutzverstößen keine Bußgelder fürchten müssen (SSN 6/2022). Unzulässiges Tracking und rechtswidrige Cookie-Banner sind aber ein rechtswidriger Grundrechtseingriff und daher inakzeptabel.

Um diesem Missstand einen Riegel vorzuschieben, richten wir gerade einen „Banner-Pranger“ ein. Dort sollen ausgewählt schöne Beispiele wie die Cookie-Banner der Regierungspräsidien Baden-Württemberg, der baden-württembergischen Gerichte oder der rekordverdächtige Abwahl-Banner des Guinness Buchs der Rekorde öffentlich gemacht werden. Wir freuen uns auf Ihre Einreichungen und Vorschläge (redaktion-security-news@secorvo.de)!

Wenn aus Apps Trojaner werden

Hin und wieder werden SmartPhone-Apps mit guter Reputation von ihren Entwicklern an Dritte verkauft, die die Anwendung um Funktionen ergänzen, die nicht im Interesse der Nutzer sind. So berichtete ESET Research am 23.05.2023, dass die Android-App iRecorder vermutlich schon im August 2022 über ein Update zu einem Spionagetrojaner erweitert wurde. Ähnliches passierte kürzlich auch einer Mac-Anwendung: Die eigentlich überflüssig gewordene App NightOwl, die noch auf vielen Macs installiert ist, wurde vom Käufer über ein automatisches Update einem Botnet hinzugefügt. Sofern die Zusatzfunktion weitere Berechtigungen benötigt, werden die immerhin über das Betriebssystem zur Freigabe angefragt. Ein solches Pop-Up-Fenster nach einem Update sollte daher alarmieren und nicht zur reflexartigen Freigabe verleiten.

Recht sicher, nicht rechtssicher

Mit dem am 10.07.2023 veröffentlichten EU-US Data Privacy Framework (DPF) hat die EU-Kommission einen neuen Angemessenheitsbeschluss gefasst. Die Datenschutzkonferenz der deutschen Aufsichtsbehörden (DSK) hat nun Anwendungshinweise zum DPF veröffentlicht, in denen sie die wesentlichen Hintergründe und Inhalte erläutert, u. a. die neu geschaffenen Rechtsschutzmöglichkeiten für betroffene Personen sowie die Schaffung von geeigneten Garantien, sofern der Auftragsverarbeiter nicht DPF-zertifiziert ist.

Vom Votum der DSK weicht der Thüringer LfDI mit einer eigenen Stellungnahme ab: Er hat insbesondere bei zertifizierten Unternehmen Bedenken, da diese lediglich eine Selbstzertifizierung durchführen, die ausschließlich im Beschwerdefall geprüft werden werde. Auch bestünde weiterhin die Gefahr einer rechtswidrigen Datenverarbeitung durch US-Behörden bei Strafverfolgung und in Fällen der „nationalen Sicherheit". Zudem schließt er sich den von Max Schrems geäußerten Kritikpunkten an.

Trotz der Anerkennung durch die EU-Kommission sollten Übermittlungen personenbezogener Daten in die USA auch weiterhin sehr zurückhaltend erfolgen, denn wir teilen die Einschätzung des Thüringer LfDI, dass „die Wahrscheinlichkeit, dass der Europäische Gerichtshof den Adäquanzbeschluss aufheben wird, (...) recht hoch" ist. Anfang September reichte der französische Parlamentarier Philippe Latombe als Privatperson Klage beim EuGH ein, und Max Schrems hat angekündigt, vor nationalen Gerichten gegen Unternehmen zu klagen, die sich bei der Übermittlung von personenbezogenen Daten in die USA auf das DPF berufen.

Secorvo News

Silbernes Jubiläum

Vor 25 Jahren, am 01.09.1998, erblickte Secorvo das Licht der Welt – und zählt damit zu den ältesten IT-Security-Dienstleistern in Deutschland.

Mit weit über 2.000 erfolgreichen Projekten für fast 1.000 deutsche und internationale Unternehmen, rund 450 Fachveröffentlichungen und vielen hundert Fachveranstaltungen mit insgesamt rund 35.000 Teilnehmern sowie 1.000 Seiten „Secorvo Security News" blicken wir ein wenig stolz auf dieses Vierteljahrhundert zurück – und freuen uns, in dieser Zeit wirksam zu Informationssicherheit und Datenschutz in Deutschland beigetragen zu haben.

Wir danken unseren Kunden für das in uns gesetzte Vertrauen und allen ehemaligen und derzeitigen Mitarbeiterinnen und Mitarbeitern für ihren engagierten und kompetenten Einsatz – und freuen uns auf ein weiteres Vierteljahrhundert, in dem wir diese Welt noch ein kleines Stück besser machen.

Secorvo Seminare

Sichern Sie sich noch einen der letzten freien Plätze auf unserem T.I.S.P.-Seminar vom **13.–17.11. 2023.** Profitieren Sie vom Wissenstransfer in über 20 Modulen des aktuellen Curriculums und lassen Sie sich im Anschluss zertifizieren. Die **vierte Auflage** unseres T.I.S.P.-Begleitbuchs wird Anfang 2024 erhältlich sein.

Wer Software-Entwicklung sicher gestalten will, dem bieten wir mit unserem neu konzipierten T.P.S.S.E.-Seminar **vom 27. bis 30.11.2023** jede Menge Inhalte mit Praxisbezug und interaktiven Workshops – und im Anschluss auch hier die Möglichkeit, sich zertifizieren zu lassen.

Planen Sie schon Ihre Weiterbildung für nächstes Jahr? Dann werfen Sie doch einen Blick in unseren Seminarkalender 2024. Wir freuen uns auf Ihre Anmeldung!



RaaS – Ransomware as a Service

Was McDonald's mit Ransomware gemeinsam hat und wie mit dem Geschäftsmodell „Ransomware-as-a-Service" auch technisch weniger versierte Akteure mit leistungsstarken Angriffstools zu erfolgreichen Cyberkriminellen werden können, stellt Martin Dukek vom Kompetenzzentrum IT-Sicherheit beim nächsten KA-IT-Si-Event im House of Living Labs (FZI) vor.

Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum intensiven Buffet-Networking. Wir freuen uns auf Sie am **12.10.2023** um 18 Uhr! (Zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Oktober 2023	
10.-12.10.	it-sa 2023 (NürnbergMesse GmbH, Nürnberg)
12.10.	RaaS – Ransomware as a Service (KA-IT-Si, Karlsruhe)
24.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
November 2023	
7.-8.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
7.-9.11.	IDACON 2023 (WEKA-Akademie, München)
13.-17.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-30.11.	ACM CCS 2023 (ACM/SIGSAC, Kopenhagen/DK)
27.-30.11.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Fundsache

Durch das EuGH-Urteil vom 30.03.2023 steht § 26 BDSG auf tönernen Füßen. Die FAQs des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg zeigen alternative Rechtsgrundlagen zur Verarbeitung von Beschäftigtendaten.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Robert Eitel, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2023



Herrschaftswissen

Der Philosoph *Max Scheler* (1874-1928) definierte in seiner Anthropologie Herrschaftswissen als das Wissen, das der Stabilisierung einer Herrschaft und deren Machtbestrebungen dient.

Im Kern ist darunter jeder Wissensvorsprung zu verstehen, der in diesem Sinne vorteilhaft für den Wissenden ist. Jede Herrschaft ist bestrebt, sich mit solchen exklusiven Wissensvorsprüngen zu stabilisieren – je prekärer die Legitimation, je geringer der Rückhalt bei den Beherrschten und je größer die äußere Bedrohung, desto stärker dieses Bestreben. Spionage, nach außen und nach innen, ist daher die logische Folge jeder Herrschaft – vor allem einer prekären.

Da Herrschaftswissen in der Hand der Herrschenden eine mächtige Waffe sein kann, versuchen Demokratien, Herrschaftswissen überall dort zu begrenzen, wo es der Exekutive Macht über den eigentlichen Souverän – das Volk – gibt. Aus dieser Perspektive lässt sich Datenschutz verstehen als eine systematische Begrenzung des Herrschaftswissens über Menschen: Die Forderung einer Rechtsgrundlage für die Verarbeitung, die strikte Zweckbindung und strenge Löschfristen sollen verhindern, dass solches Herrschaftswissen überhaupt erst entsteht.

Auch im sozialen Miteinander soll Datenschutz die Allokation von Herrschaftswissen zumindest erschweren, denn ein Airtag, der einem Stalker den Aufenthaltsort seines Opfers verrät, ist ein ähnlich starkes Machtinstrument wie eine Spionage-Drohne oder ein versteckter GPS-Sender. Daher sollte dem Verbot der anlasslosen Vorratsdatenspeicherung (BVerwG 6 C 6.22/7.22) nun auch bald ein Verbot der Nutzung von Informationstechnik zur heimlichen Feststellung des aktuellen Aufenthaltsorts von Personen folgen.

Auf kurze Löschfristen sollte man auch bei jeder App achten, die personenbezogene Daten speichert. In die falschen Hände geraten können auch sie – und damit zu Herrschaftswissen mutieren.



Inhalt

Herrschaftswissen

Security News

Konfigurationsfehler

Schwachstellenschwemme

Secure by Design – Joint Effort

Meinungsmache

Auskunftsrecht

HSM-Restrisiko

Website Evidence Collector

Secorvo News

Secorvo Seminare

Passe partout

Veranstaltungshinweise

secorvo
security consulting

Security News

Konfigurationsfehler

Am 05.10.2023 stellten CISA und NSA eine gemeinsame Übersicht der Top Ten Cybersecurity Misconfigurations. Einige der aufgelisteten Konfigurationsfehler scheinen auf den ersten Blick ein alter Hut zu sein: In der Praxis ermöglichen aber offensichtlich eben diese alten Hüte immer wieder Einbrüche in IT-Infrastrukturen. Das Dokument enthält detaillierte Ursachenanalysen und Gegenmaßnahmen für die identifizierten Top Ten. Dabei wird immer wieder auf die hilfreichen Werkzeuge Mitre ATT&CK und Mitre D3FEND verwiesen.

Die Hartnäckigkeit der Schwachstellenmuster im Betrieb ähnelt der der Weaknesses in der Software-Entwicklung. Vielleicht sollten sie ähnlich exponiert und populär kommuniziert werden, wie es Mitre mit den CWE vormacht.

Schwachstellenschwemme

Die National Vulnerability Database des NIST weist für Oktober 2023 erneut über 2000 neu veröffentlichte Schwachstellen aus. Mindestens zehn dieser Verwundbarkeiten werden bereits aktiv ausgenutzt. Betroffen sind u. a. der Netscaler (Citrix) und Confluence (Atlassian). Besonders kritisch ist die mit dem Maximalscore 10.0 bewertete Cisco-IOS-XE-Lücke, da die Admin-Schnittstelle von Tausenden von Switches und Routern über das Internet erreichbar ist (siehe NET.3.1.A4, BSI-Grundschutz) und die Geräte daher ein leichtes Opfer sind. Dabei wären viele Lücken vermeidbar, etwa beim Cisco Emergency Responder, der mit einem Standard-Admin-Passwort ausgeliefert wurde.

Secure by Design – Joint Effort

Am 25.10.2023 hat die US-amerikanische CISA vor dem Hintergrund einer nicht nachlassenden Anzahl von Security-Schwachstellen in Produkten nachdrücklich auf die Handreichung Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software hingewiesen. Darin haben viele internationale Sicherheitsbehörden grundlegende Bausteine für sichere Software-Produkte übersichtlich zusammengestellt. Die Hinweise wurden im April 2023 vom BSI vorgestellt.

Wir empfehlen nachdrücklich, die darin vorgestellten Prinzipien ernst zu nehmen – auch vor dem Hintergrund der Anforderungen, die voraussichtlich mit dem Cyber-Resilience-Act an die Sicherheit von Software gestellt werden.

Das Thema Secure by Design Software ist auch ein Baustein im T.P.S.S.E.-Seminar, das sich umfassend mit Sicherheit in der Software-Entwicklung beschäftigt – die Bekämpfung von Schwachstellen also von der Wurzel aus angeht.

Meinungsmache

Am 04.09.2023 veröffentlichte die Mozilla Foundation eine „Studie", nach der moderne Autos ein „Datenschutz-Albtraum" seien. Mehrere Medien zitierten die Veröffentlichung, darunter der heise-Newsticker. Befasst man sich jedoch eingehender mit dem Text (vulgo: liest man ihn…), kommt man schnell zu dem Ergebnis, dass von einer systematischen Analyse keine Rede sein kann – die „Forschungsergebnisse" sind Resultat einer Durchsicht der Datenschutzerklärungen von 25 Herstellern und einer offenbar vorurteilsbeladenen und kompetenzbefreiten Sicht der Autoren. Zitat: „Automarken stellen mit Ihren persönlichen Daten oft alles Erdenkliche an, was noch irgendwie im rechtlichen Rahmen zulässig ist." Oder: „Am meisten Sorgen macht uns, dass wir nicht einmal wissen, ob überhaupt eine der geprüften Marken alle persönlichen, im Auto gespeicherten Daten verschlüsselt." Die anhängenden Vitae der Autoren lassen ebenfalls kein Expertenwissen im Datenschutz erkennen – die Autoren sehen sich selbst als „investigative Storyteller".

Undifferenzierte und inkompetente Positionspapiere dieser Art stiften mehr Schaden als Nutzen, machen sie es doch leicht, die Kritik als Scharlatanerie abzutun. Denn in einigen Punkten ist fundierte Kritik durchaus berechtigt – und tatsächlich sollten die Datenschutzerklärungen vieler Hersteller durchaus aussagekräftiger sein.

Auskunftsrecht

Das Recht eines jeden Menschen auf Auskunft über Verarbeitungen seiner personenbezogenen Daten ist in Art. 8 der EU-Grundrechtscharta verankert. In der Folge wurde 2013 das Recht auf Einsichtnahme in die eigene Patientenakte als § 630g ins Bürgerliche Gesetzbuch aufgenommen. Seitdem wurde allerdings immer wieder über die Frage gestritten, ob ein Patient die Kosten des Kopierens der Akte tragen muss.

Am 26.10.2023 hat nun der EuGH diese Frage abschließend höchstrichterlich beantwortet – mit einem klaren „Nein". Die Kosten der (ersten) Kopie einer Patientenakte sind vom Arzt bzw. der Klinik zu tragen (C-307/22). Das ist ein Sieg der Transparenz – der aber auch zu einer erheblichen Belastung medizinischer Einrichtungen werden kann, wenn viele Patienten eine Kopie anfordern.

Die Entscheidung des EuGH könnte daher die Digitalisierung im Gesundheitswesen beschleunigen, denn eine elektronische Gesundheitsakte würde nicht nur die Archivierung, sondern auch die Beauskunftung erheblich vereinfachen.

HSM-Restrisiko

Es ist immer eine gute Idee, wichtige Schlüssel in einem Hardware Security Modul (HSM) zu halten – beispielsweise solche, mit denen Zertifikate oder Authentication-Token signiert werden. Das alleine garantiert aber noch keine vollständige Sicherheit. Zu berücksichtigen ist auch, wer über die Schlüssel im HSM verfügen darf: Bei mindestens einem (verbreiteten) HSM-Modell darf das jeder Benutzer auf dem Windows-Server, an den das HSM angeschlossen ist.

Hans-Joachim Knobloch (Secorvo) erläutert diesen Schwachpunkt in seinem Blog-Artikel vom 06.10. 2023 und zeigt, wie man sich darüber ein Goldenes Zertifikat von einer Microsoft-CA erschleichen könnte – falls der CA-Server nicht so gehärtet ist, dass sich nur berechtigte Administratoren anmelden können. In der Tradition der einschlägigen Angriffsvektoren ESC1 bis ESC11 hat er diesen „ESC12“ getauft.

Website Evidence Collector

Bereits am 22.10.2019 wurde der Website Evidence Collector des Europäischen Datenschutzbeauftragten von der International Conference of Data Protection and Privacy Commissioners (ICDPPC) mit dem Global Privacy and Data Protection Award für Innovation ausgezeichnet. Das Tool für die automatische Überprüfung der Erhebung und des Schutzes personenbezogener Daten auf Websites kann Belege für die Verarbeitung personenbezogener Daten (wie Cookies) oder Anfragen an Dritte erzeugen.

Es lädt ohne weitere Benutzerinteraktion nacheinander alle im Besuch einer URL enthaltenen Webseiten. Dabei werden unter anderem Screenshots der Seiten angefertigt und Listen der http-Links, der besuchten Webseiten, der im lokalen HTML5-Speicher gehaltenen Informationen, aller Cookies, des http-Verkehrs sowie alle über Web Sockets ausgetauschten Nachrichten erzeugt.

Das unter der EU Public Licence (EUPL 1.2) veröffentlichte Tool ist auf GitHub für Linux, macOS und Windows zum Herunterladen verfügbar. Es ermöglicht eine schnelle und einfache Prüfung von Webseiten: Bleibt zu hoffen, dass es nicht für automatisierte Abmahnwellen missbraucht wird.

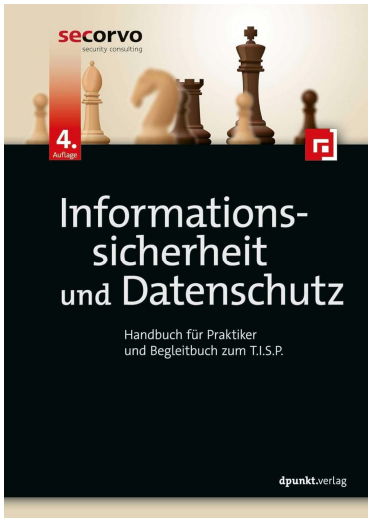
Secorvo News

Secorvo Seminare

Last but not least: Mit unserem neu konzipierten T.P.S.S.E.-Seminar beschließen wir vom **27. bis 30.11.2023** das Seminarjahr 2023: Vier Tage interaktive Workshops und jede Menge Inhalte mit Praxisbezug rund um die sichere Software-Entwicklung.

Die nächste Chance für Ihre T.I.S.P.-Zertifizierung bieten wir Ihnen auf unserem T.I.S.P.-Seminar vom **11. bis 15.03.2024**: Wissenstransfer aus über 20 Modulen des jüngst aktualisierten Curriculums. Dazu erscheint Anfang 2024 die **vierte Auflage** unseres T.I.S.P.-Begleitbuchs im dpunkt-Verlag.

Bevor wir Sie in die Adventszeit entlassen, werfen Sie doch noch einen Blick in unseren Seminarkalender 2024. Wir freuen uns auf Ihre Anmeldung!



Passe partout

Je mehr kryptografische Zertifikate als Authentifikationsmechanismus genutzt werden, desto kritischer sind Konfigurations- oder Implementierungsfehler, die es Angreifern ermöglichen, gefälschte Zertifikate als „Dietrich“ zu benutzen. Das hat erst kürzlich der Diebstahl eines „Generalschlüssels“ zur Microsoft Cloud gezeigt (siehe SSN 8/2023).

Beim Jahresabschlussevent 2023 der KA-IT-Si am **23.11.2023** werden Hans-Joachim Knobloch und Oliver Oettinger (Secorvo) aktuelle Angriffe auf das Active Directory mit solchen „Goldenen Zertifikaten“ demonstrieren und zeigen, wie man sich davor schützen kann. Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum Networking am Buffet.

Wir freuen uns auf Sie im Haus der Wirtschaft der IHK Karlsruhe – und empfehlen (wie immer) eine schnelle Anmeldung...

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2023	
23.11.	Passe partout (KA-IT-Si, Karlsruhe)
26.-30.11.	ACM CCS 2023 (ACM/SIGSAC, Kopenhagen/DK)
27.-30.11.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Dezember 2023	
04.-07.12.	Black Hat Europe 2023 (Blackhat, London/UK)
Januar 2024	
12.-14.01.	ShmooCon 2024 (The Shmoo Group, Washington/US)
22.-24.01.	Omnisecure 2024 (in TIME berlin, Berlin)
30.-31.01.	31. DFN Konferenz (DFN-CERT, Hamburg)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

November/Dezember 2023



Lernen durch Schmerzen

Also doch. Bei der Publikation der Untersuchungsergebnisse, wie Microsoft mindestens ein Entra-ID-Signierschlüssel abhanden kommen konnte, sprach das Unternehmen am 06.09.2023 noch von einer Aneinanderreihung unglücklicher, aber verzeihlicher Fehler. Die Ankündigung des stellvertretenden Vorstandsvorsitzenden Brad Smith vom 02.11.2023 klingt da schon ganz anders: Die Cyberangriffe der letzten Monate hätten Microsoft von der Notwendigkeit einer Reaktion überzeugt - der Secure Future Initiative. Es ist die Rede von einer firmenweiten Anstrengung, bei der auch KI zum Einsatz kommen soll. Das vom Marketing zunächst kleingeredete Ereignis hat das Unternehmen intern wohl doch erschüttert.

Vor allem will sich Microsoft nun um eine ordentliche Aufbewahrung von privaten Schlüsseln kümmern: Der Einsatz von Hardware Security Modules (HSMs) wird explizit erwähnt – damit bestätigt Microsoft die Vermutung von u. a. unserem PKI-Experten Hans-Joachim Knobloch (SSN 8/2023), dass die Schlüssel bisher nicht in HSMs gespeichert wurden.

Die Verlautbarung erinnert an Bill Gates' denkwürdiges Memo vom 15.01.2002, in dem er – aus ähnlichem Anlass – die Trustworthy Computing Initiative ankündigte, die bis heute bei Microsoft umgesetzt wird. Dass das von Gates beschriebene hehre Ziel allerdings in den seither vergangenen Jahr(zehnt)en noch nicht erreicht wurde, wissen wir alle nur zu gut.

Zwar macht Microsoft tatsächlich in der Cloud vieles besser als die meisten IT-Abteilungen in ihren Rechenzentren. Aber auch Microsoft kocht nur mit Wasser. Und wenn einem so großen Cloud-Anbieter Fehler unterlaufen, sind in der Regel auch die Auswirkungen erheblich größer.

By the way: Falls Sie eine eigene PKI betreiben und Ihre Root Keys bisher nicht in HSMs speichern, sollten Sie das besser ändern.



Inhalt

Microsoft ist lernfähig

Security News

Quantencomputing

Besorgniserregend

CVSS runderneuert

Zögern kostet

Umstrittenes Provisorium

Arbeitgeberhaftung

Fast täglich grüßt das Murmeltier

Angst als Schaden

KI plaudert Geheimnisse aus

Better safe than sorry?

Hoffnungslos, aber nicht ernst

Secorvo News

Weiterbildung 2024

Veranstaltungshinweise

secorvo
security consulting

Security News

Quantencomputing

Am 13.11.2023 hat das BSI die schon im August fertiggestellte Version 2.0 der erstmals im Mai 2018 verfassten Studie zum Entwicklungsstand der Quantencomputer veröffentlicht. Auf 217 Seiten bietet sie nicht nur eine hervorragende Übersicht über die aktuellen Fortschritte sondern enthält auch 42 (!) Seiten Literaturreferenzen. Die 14-seitige deutsche Zusammenfassung wurde als separates Dokument publiziert.

Nach dem derzeitigen Stand der Technik erscheint die Faktorisierung eines 2048-bit-RSA-Schlüssels mit 20 Mio. physikalischen QBits in acht Stunden möglich. Davon sind Quantencomputer derzeit weit entfernt: IBMs „Osprey" vom 14.11.2022 hat 433 QBits. Allerdings könnte bereits in zehn Jahren ein ausreichender Quantencomputer verfügbar sein, sofern es gelingt, die Algorithmen zur Korrektur der Quantenfehler deutlich zu verbessern und damit die erforderlichen physikalischen QBits zu reduzieren.

Besorgniserregend

Am 02.11.2023 hat das BSI den Bericht zur Lage der IT-Sicherheit 2023 veröffentlicht. Wem die Lektüre aller 96 Seiten zu zeitintensiv ist, dem sei zumindest das Fazit ans Herz gelegt. Die Bewertung *„Schwachstellen bei Software auf besorgniserregendem Niveau"* belegt die Publikation durch den Verweis auf die 2701 neuen Schwachstellen, die allein im Oktober 2023 veröffentlicht wurden. Das Wiki-Tool Confluence (on premise) war sogar mit zwei Schwachstellen mit maximaler Bewertung (10.0) vertreten (CVE-2023-22515 und CVE-2023-22518).

CVSS runderneuert

Das Common Vulnerability Scoring System (CVSS) ist ein De-facto-Standard zur Bewertung von Produktschwachstellen. Am 01.11.2023 löste die Version CVSS v4.0 des Forums of Incident Response and Security Teams (FIRST) die acht Jahre alte Grundlage CVSS 3 ab. Die neue Fassung legt besonderen Wert darauf, Basis-Bewertungen (Base Metrics) von erweiterten Bewertungen zu trennen und auszuweisen. Der CVSS-Calculator und die FAQ geben Hinweise darauf, wie die Bewertungen zustande kommen; hilfreiche Werkzeuge beim Umgang mit CVEs sind auch CVEDetails und OpenCVE.

Zögern kostet

Laut Arbeitsgericht Duisburg sind Auskunftsersuchen nach Art. 15 DSGVO grundsätzlich unverzüglich, also „ohne schuldhaftes Zögern" zu erteilen. Die Monatsfrist (Art. 12 DSGVO) sei lediglich eine Maximalfrist, die nicht routinemäßig ausgeschöpft werden dürfe, da der Grundsatz sonst leerlaufen würde. Bei unkomplizierten Anfragen, bei denen keine Daten im Unternehmen vorliegen, sei eine Woche als Frist ausreichend. Betroffene würden aufgrund eines temporären Kontrollverlusts einen immateriellen Nachteil erleiden, da sie bis zur Auskunft die Verarbeitung der eigenen Daten nicht prüfen und ggfs. weitere Rechte ausüben könnten. Dem Kläger wurden 750 € Schadenersatz zugesprochen.

Unternehmen sollten daher effiziente Prozesse für die Bearbeitung von Auskunftsersuchen vorsehen – und dabei die EuGH-Rechtsprechung (SSN 5/2023) berücksichtigen, nach der alle personenbezogenen Daten eines Verarbeitungsvorgangs zu beauskunften sind.

Umstrittenes Provisorium

Am 16.11.2023 hat das EU-Parlament die vorläufige Vereinbarung zur Reform der EiDAS-Verordnung veröffentlicht – und damit einen Sturm der Entrüstung ausgelöst. Kritisiert wird insbesondere Art. 45 des Entwurfs, der nach Ansicht einer Vielzahl von Wissenschaftlern und anderen Experten Privatsphäre und Sicherheit der EU-Bürger bei der Nutzung von Webbrowsern in Frage stellt. Kommt es so, wie im Entwurf vorgesehen, dann könnten staatliche Behörden selbst Zertifikate erstellen und damit beliebige Webseiten authentisch erscheinen lassen. In einem offenen Brief fordern über 550 Wissenschaftler, dass durch eine Klarstellung der Trilog-Partner die Regelung entsprechend geändert wird.

Bereits in früheren Entwürfen waren Regelungen zu den kritisierten Qualified Website Authentication Certificates (QWACs) enthalten. Der Kompromissvorschlag des EU-Parlaments berücksichtigte die Kritik, konnte sich aber offenbar in den Trilog-Verhandlungen nicht durchsetzen.

Arbeitgeberhaftung

Der Deutsche Wohnen SE war am 05.11.2019 wegen eines Verstoßes gegen die Löschpflichten der DSGVO ein Bußgeld in Höhe von 14,5 Mio. € auferlegt worden (SSN 11/2019). Nachdem zunächst das LG Berlin den Bußgeldbescheid als unwirksam angesehen hatte (SSN 03/2021), legte die Staatsanwaltschaft Berlin Rechtsmittel ein. Das Kammergericht Berlin legte daraufhin dem EuGH die Frage vor, ob eine juristische Person für von Mitarbeitern begangene DSGVO-Verstöße belangt werden kann. Der EuGH hat am 05.12.2023 entschieden, dass der Arbeitgeber auch für vorsätzlich oder fahrlässig begangene Verstöße von Mitarbeitern haftet.

secorvo
security consulting

Fast täglich grüßt das Murmeltier

Inzwischen mehren sich die dringenden verbindlichen Entscheidungen des Europäischen Datenschutzausschuss (EDPB) an die Irische Aufsichtsbehörde DPC (siehe SSN 12/2022 und das Editorial in den SSN 1/2023). Dieses Mal hat die Norwegische Aufsichtsbehörde einen entsprechenden Antrag auf Untersagung der Verarbeitung personenbezogener Benutzerdaten für Verhaltenswerbung im gesamten Europäischen Wirtschaftsraum (EWR) gestellt, da die DPC von sich aus nicht tätig geworden war.

Am 01.11.2023 veröffentlichte der EDPB die am 27.10.2023 angenommene Entscheidung: Meta ist es nunmehr untersagt, verhaltensbezogene Werbung zu verwenden. Die DPC muss innerhalb von zwei Wochen Maßnahmen zur Umsetzung dieser Entscheidung treffen. Die angestrebten effektiveren Regeln zur Durchsetzung der DSGVO bei grenzüberschreitenden Sachverhalten sind ganz offensichtlich dringend erforderlich – auch Studien zum Trotz, die Irland als Vorbild des Datenschutzes in der EU feiern.

Angst als Schaden

Am 26.09.2023 wollte der BGH vom EuGH wissen, ob es für einen immateriellen Schaden ausreichend ist, dass ein DSGVO-Verstoß Ärger, Unmut, Unzufriedenheit, Sorge oder Angst auslöst. Nun hat der EuGH am 14.12.2023 geurteilt, dass es ausreicht, dass eine betroffene Person bei einem Verstoß gegen die DSGVO eine missbräuchliche Verwendung ihrer Daten befürchtet. Art. 82 Abs. 1 DSGVO sei hier (sehr) weit auszulegen. Die Befürchtung muss allerdings im Einzelfall begründet sein.

KI plaudert Geheimnisse aus

Einen kuriosen Angriff, um aus Chatbots Trainingsdaten zu extrahieren, publizierten Forscher am 28.11.2023: Fordert man Chatbots auf, ein Wort endlos oft zu wiederholen, beginnen sie nach einigen Wiederholungen plötzlich damit, Trainingsdaten zu reproduzieren. Ursache für dieses Verhalten ist das Training der Sprachmodelle: Um zu signalisieren, wann ein Dokument in den Trainingsdaten endet, werden Trennsignale eingebaut. Nach dem Training wird der Chatbot einem „Alignment“ unterzogen; dabei wird der Nutzereingabe eine unsichtbare Systemeingabe vorangestellt. Durch die Wiederholung des Trennsignals „lernt“ das Sprachmodell so jedoch, häufige Wiederholungen mit einem Kontextwechsel gleichzusetzen und fängt daher an, unkontrolliert Text auszugeben, der auch Trainingsdaten enthält. Problematisch ist das, wenn mit vertraulichen Daten trainiert wurde.

Better safe than sorry?

Am 05.10.2023 berichtete Bitkom Research, dass der europäische Datenschutz nach einer Umfrage unter 500 deutschen Unternehmen von 69 % als Nachteil im internationalen Wettbewerb und von 56 % als Innovationsbremse gesehen werde. Zu einem ähnlichen Ergebnis kommt die Befragung Global Security Research (fastly) vom November 2023 unter 200 IT-Entscheidern aus Österreich, Deutschland und der Schweiz: Für 55% der Befragten beeinträchtige die IT-Sicherheitsstrategie ihre Innovativität.

Hoffnungslos, aber nicht ernst

Den zweiten „Geburtstag“ von Log4Shell am 10.12.2023 nahm Veracode zum Anlass, die aktuelle Bedrohungslage zu dieser berüchtigten Schwachstelle zu recherchieren – mit erschreckenden Ergebnissen: Insgesamt nutzen noch 38% aller untersuchten Anwendungen eine anfällige Version der Bibliothek, 32% nutzen eine, deren End-of-Life auf August 2015 datiert. Dass nicht nur in diesem Punkt dringend Handlungsbedarf für den Schutz der Software Supply Chain besteht, zeigt die Veracode-Studie State of Software Security vom 05.01.2023: Über 74% der von Veracode im vorangegangenen Jahr untersuchten Anwendungen hatten mindestens eine Schwachstelle, über 56% eine aus den Top 25 CVE. Da wirkt der grundsätzlich korrekte Appell mehrerer Sicherheitsbehörden vom 06.12.2023, auf speichersichere Programmiersprachen zu wechseln, leider realitätsfern. Wer das Problem bei der Wurzel packen möchte, dem empfehlen wir das Seminar T.P.S.S.E. zur sicheren Softwareentwicklung.

Secorvo News

Weiterbildung 2024

In das neue Jahr starten wir mit unserem „Flaggschiff“-Seminar, dem TeleTrusT Information Security Professional (T.I.S.P.) vom **11. bis 15.03.2024**, zu dem Sie nach Eingang Ihrer Anmeldung unser Begleitbuch „Informationssicherheit und Datenschutz“ erhalten.

Im April folgen die Aufbauschulung zum BSI Vorfall-Experten (**09.–11.04.2024**), das Seminar PKI – Grundlagen, Vertiefung, Realisierung (**15.–18.04.2024**) und die Schulung zum TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) (**22.–25.04.2024**).

Unser vollständiges Seminarprogramm und alle Termine 2024 finden Sie auf unseren Webseiten. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2024	
12.-14.01.	Shmoocon 2024 (The Shmoo Group, Washington/US)
22.-24.01.	Omnisecure 2024 (in TIME berlin, Berlin)
30.-31.01.	31. DFN Konferenz Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
Februar 2024	
22.02.	KA-IT-Si-Jahresauftaktevent: „HackGPT“ (KA-IT-Si, Karlsruhe)
März 2024	
05.-07.03.	secIT 2024 (Heise Medien, Hannover)
11.-15.03.	TeleTrusT Information Security Professional (T.I.S.P.) (Secorvo, Karlsruhe)
19.-22.03.	DFRWS EU 2024 (DFRWS, Zaragoza/ES)
April 2024	
09.-11.04.	BSI Vorfall-Experte – Aufbauschulung (Secorvo, Karlsruhe)
15.-18.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.04.	Blackhat Asia 2024 (Blackhat, Singapur/SG)
22.-25.04.	TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) (Secorvo, Karlsruhe)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Paul Blenderman (Editorial), Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2024



Checks & Balances

Datenschutz ist schon immer ein kontroverses Thema. Zwar hört man die Gleichsetzung der 80er Jahre „Datenschutz = Täterschutz“ und das naiv-plakative „Ich habe nichts zu verbergen“ („Dann geben Sie mir doch bitte Zugriff auf Ihr E-Mail-Konto“) nur noch selten. Doch jüngst häufen sich Äußerungen, die ihn als Verhinderung jeder modernen Datenverarbeitung schmähen.

Eine beunruhigende Entwicklung. Denn angesichts der um sich greifenden Digitalisierung gibt es kein wichtigeres Grundrecht. Darüber wachen in Deutschland mehrere Aufsichtsbehörden. Für Bundesbehörden und Unternehmen, die bundesweit Post- und Telekommunikations¬dienste erbringen, ist der Bundesdatenschutzbeauftragte zuständig: eine unabhängige Kontrollinstanz, die auf Vorschlag der Bundesregierung vom Bundestag gewählt wird.

Jede funktionierende unabhängige Kontrolle ist unbequem, auch für demokratische Regierungen. Wie unbequem die des Bundesdatenschutzbeauftragten Ulrich Kelber ist, kann man in seinen Tätigkeitsberichten nachlesen. Im jüngsten Bericht kennt die Ampel, mit der er die Umsetzung seiner Empfehlungen aus dem Vorjahr bewertet, nur eine Farbe: rot. Aber er wirkt: Die Liste der konkreten Beanstandungen und Verwarnungen an Bundesbehörden umfasst knapp drei Seiten – im Vorjahr war die Liste noch zehn Seiten lang.

Die Amtszeit von Ulrich Kelber endete am 07.01.2024. Trotz seiner unbestrittenen rechtlichen und technischen Kompetenz und seiner unaufgeregten Art will die Bundesregierung sie nicht verlängern. Über die Nachfolge wird gerade politisch geschachert. Das ist bedenklich, denn funktionierende Kontrolle ist der Seismograf einer Demokratie. Regierungen, die einem wirksamen Grundrechtsschutz nicht die gebührende Achtung entgegenbringen, demontieren nicht nur ihre eigene Legitimität, sondern schaden der gesamten demokratischen Ordnung.

(Eine Langfassung dieses Editorials erschien in der iX 1/2024.)



Inhalt

Checks & Balances

Security News

Falschmeldung

Mitarbeitertracking

Post-Quantum-Debatten

Identische Public Keys

Datenschutz-Werkzeugkästen

Ersatz immaterieller Schäden

Secorvo News

Teamzuwachs

Secorvo Seminare

HackGPT

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Falschmeldung

Noch am 16.10.2023 hat die U.S. Börsenaufsicht SEC ihre X-Follower gewarnt: „Seien Sie vorsichtig bei dem, was Sie im Internet lesen. Die beste Quelle für Informationen über die SEC ist die SEC selbst." Und bereits im Dezember 2022 hatte sie Anklage gegen acht Social-Media-Influencer erhoben – wegen Aktienmanipulation über Discord und Twitter im Wert von 100 Mio. Dollar.

Nun musste die SEC am 09.01.2024 einräumen, dass ihr eigenes X-Konto mit 750.000 Followern kompromittiert und eine gefälschte Erklärung, dass künftig Bitcoin-Fonds zugelassen würden, den Bitcoin-Kurs kurzfristig hatte steigen lassen. Dabei stellte sich heraus, dass die SEC ihr X-Konto nicht mit einem zweiten Faktor gesichert hatte: Das Passwort ließ sich per SMS zurücksetzen, sodass der Account via SIM-Swap kompromitiert werden konnte. Lesson Learned: IT-Sicherheitsverantwortliche sollten auch die Social-Media-Konten ihrer PR-Abteilung im Blick behalten.

Mitarbeitertracking

Die französische Datenschutzaufsichtsbehörde CNIL hat am 27.12.2023 gegen Amazon France Logistique wegen exzessiven Monitorings des Beschäftigtenverhaltens eine Geldstrafe von 32 Mio. € verhängt. Sie beanstandete, dass Amazon bei den Mitarbeitern erhebt, wenn die Dauer des Abscannens unter 1,25 Sekunden liegt, Unterbrechungen länger als eine und Pausen über 10 Minuten dauern, und diese Daten über 31 Tage speichert. Zudem wurden Zeitarbeiter bis April 2020 nicht korrekt über die Erhebung informiert.

Die Niedersächsische Datenschutzbeauftragte hatte Amazon diese Praxis im Logistikzentrum in Winsen bereits am 28.10.2020 untersagt; die Entscheidung wurde jedoch vom Verwaltungsgericht Hannover am 09.02.2023 aufgehoben. Das seit April laufende Berufungsverfahren ist noch nicht abgeschlossen.

Durch das Fehlen präziser Regelungen zum Beschäftigtendatenschutz dürften solche Fragen weiterhin über Jahre die Gerichte beschäftigen: So wurde das Datenschutzkontrollverfahren in Niedersachsen bereits am 27.11.2017 eingeleitet.

Post-Quantum-Debatten

Das BSI empfiehlt seit Oktober 2021, quantensichere Public-Key-Algorithmen zunächst mit klassischen zu kombinieren, da erstere noch nicht gut erforscht seien – sie könnten daher anfällig für Implementierungsfehler oder Seitenkanalangriffe sein. Die am 07.01.2024 von Daniel J. Bernstein veröffentlichte KyberSlash-Schwachstelle in Implementierungen von Crystals Kyber zeigt, dass es für die Vorsicht des BSI und von Krypto-Experten wie Bernstein gute Gründe gibt.

Die NSA hingegen lehnt hybride Lösungen wegen der damit verbundenen Komplexität ab. Dabei wurde deren Praktikabilität bereits mehrfach demonstriert, z. B. mit OpenSSH 9.0 vom 08.04.2022. Bernstein vermutet daher, die NSA könnte Einfluss auf die Auswahl des NIST genommen haben, insbesondere bei Kyber-512: Dessen Sicherheitsanalysen wiesen große Unsicherheitsintervalle auf und seien teils fehlerhaft.

Sicher ist: Die jüngsten Angriffe auf PQC-Algorithmen wie SIKE (siehe SSN 7/2022) oder Kyber wecken Zweifel an deren Einsatzreife.

Identische Public Keys

Auf dem 37. Jahreskongress des Chaos Computer Club vom 27. bis 30.12.2023 präsentierten Christoph Saat Johann und Sebastian Schinzel vom Fraunhofer SIT erschreckende Schlampereien im KIM (Kommunikation im Medizinwesen). Dieser Dienst zum verschlüsselten Austausch von Nachrichten in der Telematik-Infrastruktur der gematik nutzt S/MIME 3.2 (RFC 5751) und soll die Vertraulichkeit und Authentizität von Nachrichten sicherstellen.

Tatsächlich waren jedoch zeitweise fünf sowie weiteren drei Krankenkassen im gemeinsamen LDAP-Adress-Verzeichnis dieselben öffentlichen Schlüssel zugeordnet – etwa 28% der Versicherten waren davon betroffen. Die Ursache könnte eine fehlerhafte Schlüsselerzeugung mit Hardware-Security-Modules gewesen sein. Bei der Signierung durch die Certificate Authorities wurde nicht erkannt, dass sechs Schlüssel bereits vergeben waren.

Die gematik hat nun die Umsetzung der Regelung GS-A_4906 aus ihrer Certification Policy erweitert, die eine Einzelzuordnung von Schlüsseln sicherstellen soll (S. 25): So müssen nun neue zu signierende öffentliche Schlüssel mit bereits erstellten vergleichen (A_23900-TSP-X.509, S. 21) und geprüft werden, ob es schwache Schlüssel sind (A_17294-TSP-X.509, S. 23).

Treuen Lesern der SSN wäre ein solcher Anfängerfehler vermutlich nicht passiert: Im Februar 2012 haben wir über eine Studie von Forschern der EPFL Lausanne berichtet, die Millionen identische öffentliche SSL-Schlüssel im Observatory der EFF entdeckt hatten (SSN 2/2012). Vielleicht hätte die gematik frühzeitig jemanden Fragen sollen, der sich auskennt...

secorvo
security consulting

Datenschutz-Werkzeugkästen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI) NRW hat am 10.01.2024 einen „Werkzeugkasten" für kleine und mittlere Unternehmen veröffentlicht – der sich bei genauer Betrachtung als magere Linksammlung zu Stellungnahmen des LDI und anderer Behörden entpuppt. Dass und wie es besser geht, zeigen die Landesbeauftragten für Datenschutz aus Bayern und Thüringen, die auf ihren Webseiten zahlreiche Muster und Vorlagen bereitstellen, die Unternehmen an ihre Erfordernisse anpassen können, sowie eine hilfreiche 36-seitige FAQ zur Umsetzung der DSGVO.

Ersatz immaterieller Schäden

Der Europäische Gerichtshof (EuGH) hat am 25.01.2024 entschieden, dass bei einem Verstoß gegen die DSGVO nur derjenige Anspruch auf Schadensersatz hat, der seinen immateriellen Schaden hinreichend plausibel darlegen kann. Nach der Ablehnung einer Bagatellgrenze für immaterielle Schäden durch den EuGH am 14.12.2023 (siehe SSN 11+12/2023) stellen die Richter klar, dass ein rein hypothetisches Risiko einer missbräuchlichen Verwendung durch Unbefugte (z. B. durch eine kurzzeitige Weitergabe personenbezogener Daten an einen Dritten) nicht ausreicht, um einen Schaden wegen des Risikos eines Kontrollverlusts zu begründen.

Zwar bleibt damit die Schadensersatzregelung in Art. 82 DSGVO auslegungsbedürftig. Massenhafte Schadensersatzforderungen von Betroffenen bei kleineren Datenschutz-Verstößen oder -Vorfällen müssen Unternehmen jedoch nicht befürchten.

Secorvo News

Teamzuwachs

Seit dem 11.12.2023 verstärkt der Volljurist und Datenschutz-Experte Robert Eitel, LL.M. (VCI) unser Team. Herzlich willkommen!

Vorträge

Auf der 31. DFN-Konferenz "Sicherheit in vernetzten Systemen" (30.-31.01.2024) in Hamburg sprachen Friederike Schellhas-Mende und Christian Blaicher über das Risiko von Auskunftsersuchen für Verantwortliche in Recht und Praxis. Der Beitrag findet sich auch im Tagungsband der Konferenz.

Seminare

Das Frühjahr kündigt nicht nur wieder längere Tage an, sondern auch viele interessante Seminare. Kurz vor Ostern können Sie sich mit unserem T.I.S.P.-Seminar vom **11. bis 15.03.2024** auf die Zertifizierung vorbereiten.

Im April bieten wir die Aufbauschulung zum BSI Vorfall-Experten (**09.–11.04.2024**), das Seminar PKI – Grundlagen, Vertiefung, Realisierung (**15.–18.04.2024**) und die Schulung zum TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) (**22.–25.04.2024**) an.

Weitere Termine und Informationen finden Sie unter www.secorvo.de/seminare. Wir freuen uns auf Ihre Anmeldung!

HackGPT

Was kommt mit dem neuen Hackerspielzeug ChatGPT, FlipperZero & Co auf uns zu? Liefern diese Tools wirklich Anleitungen zum Hacken? Können sie umgekehrt zur Absicherung gegen Cyberangriffe verwendet werden? Und wo liegen die Grenzen solcher Off-the-Shelf-Tools?

Diesen Fragen widmet sich nach einer magischen Einführung durch Dr. Rolf Häcker (Landtag BW) Dr. Swantje Westpfahl (UNISS) beim Jahresauftakt-Event der KA-IT-Si am **22.02.2024**, die auf Einladung der IHK Karlsruhe im Haus der Wirtschaft stattfindet.

Im Anschluss an die Vorträge haben Sie wie immer Gelegenheit zum Networking am Buffet.

Wir freuen uns auf Sie – und empfehlen eine schnelle Anmeldung, denn es gibt nur noch wenige freie Plätze.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2024	
22.02.	Jahresauftaktevent „HackGPT“ (KA-IT-Si, Karlsruhe)
März 2024	
05.-07.03.	secIT 2024 (Heise Medien, Hannover))
11.-15.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.-22.03.	DFRWS EU 2024 (DFRWS, Zaragoza/ES)
April 2024	
09.-11.04.	BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe)
15.-18.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.04.	Blackhat Asia 2024 (Blackhat, Singapur/ASE)
22.-25.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Fundsache

Nachdem OWASP bereits im Oktober 2023 eine gute Übersicht der wichtigste Angriffstechniken auf LLMs veröffentlichte, bietet das NIST nun mit AI 100-2 E2023 eine detaillierte Systematik möglicher Angriffe und Gegenmaßnahmen.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2024



Schöne neue Welt

Wie wunderbar haben wir uns damals die Zukunft vorgestellt: digitale Dokumente statt ressourcenfressender Papierberge, Online-Erledigungen statt Ämterwarteschlangen und ortsunabhängig verfügbare Warenvielfalt in digitalen Riesenkaufhäusern.

Lange sah es so aus, als ob diese Digitalisierungsträume tatsächlich in Erfüllung gehen: Einheitliche Dateiformate (PDF, mp3, jpg) machen Texte, Musik und Bilder universell austauschbar, mobile Endgeräte erlauben ein „Always on" ohne nennenswerte Technik-Kenntnisse und zahlreiche Dienste erleichtern das tägliche Leben – wie Online-Shops, Navigation oder Videokommunikation.

Doch nach und nach drängen die Schattenseiten dieser Entwicklung ins Licht: Während der Papierverbrauch pro Kopf nur marginal sinkt (2000 waren es 232 kg je Bundesbürger, 20 Jahre später immer noch 228 kg) steigt unser Energieverbrauch enorm: Jeder Smartphone-Nutzer verursacht jährlich im Schnitt einen Stromverbrauch von rund 50 kWh in Rechenzentren – zuzüglich Energie und Rohstoffen bei der Produktion des Geräts. Derweil lassen Online-Shops die Zahl der Pakettransporte explodieren und die Innenstädte veröden. Und die exzessive Nutzung von „sozialen" Medien schafft ein neues Prekariat: Anstatt den Zugang zu Wissen zu demokratisieren bekommt Konzentrationsfähigkeit Seltenheitswert, nehmen Depressionen zu und weicht der Respekt im zwischenmenschlichen Umgang zunehmender Grobheit. Und obendrein lässt sich der Wahrheitsgehalt von Informationen (Fake News, Bilder, Filme) immer schwerer beurteilen.

Datenschutz, ursprünglich ein Abwehrrecht gegen staatliche Überwachung, kämpft heute vornehmlich gegen die Begehrlichkeiten von Werbetreibenden und soziale Übergriffe wie Doxing (am 19.02.2024 sogar ein Thema in der Tagesschau). Einziger Trost: Solange die „Digitalstrategie Deutschland" im Konzeptmodus verharrt, müssen wir uns wenig Sorgen um staatliche Kontrolle machen.



Inhalt

Schöne neue Welt

Security News

Ene mene muh

Post-Quantum-Einsatz

Auskunftskosten

Neues Website Audit Tool

Private Key

HackGPT

Secorvo News

Vierte Auflage

Seminare

No risk, no fun

Veranstaltungshinweise

secorvo
security consulting

Security News

Ene mene muh

Im 20. Jahrhundert war die Domänenwelt noch in Ordnung: Es gab Top-Level-Domänen (TLD) wie .com oder .gov und länderspezifische wie .de oder .at. Dann übernahm 1998 die neu gegründete ICANN die Domänenherrschaft und begann weitere, so genannte „generische" TLD (gTLD) einzuführen. Seit 2012 kann jeder, der 185.000 $ übrig hat, eine gTLD kaufen; inzwischen gibt es über 1.200.

Einige Hersteller nutzen unregistrierte TLDs für die einfache Erreichbarkeit ihrer Produkte in internen Netzen. So z. B. die Router von AVM (fritz.box) und O2 (o2.box). Doch seit dem 11.11.2016 (sic?) gibt es die gTLD .box – und am 22.01.2024 wurde die Domäne fritz.box registriert. Wer seitdem die Namensauflösung nicht von seinem Router vornehmen ließ, landete beim Aufruf der Admin-Oberfläche auf einer externen Webseite. inzwischen erscheint ein „Suspended"-Hinweis.

Dasselbe Risiko droht bei internen TLDs. Bereits seit 2020 diskutiert die ICANN daher über die Einführung von Private Use TLDs und hat anlässlich dieses Vorfalls am 24.01.2024 angekündigt, zumindest .internal zu schützen. Betroffene Hersteller könnten natürlich auch ihre intern genutzte Domäne extern registrieren. Wer weiterhin nicht registrierte gTLDs nutzt, sollte allerdings die Liste der registrierten gTLDs im Auge behalten.

Post-Quantum-Einsatz

Noch ist kein Quantencomputer bekannt, der klassischen Public-Key-Verfahren gefährlich werden könnte. Doch könnte ein Angreifer Kommunikation mitschneiden und sie in 10 oder 20 Jahren mit einem hinreichend mächtigen Quantencomputer entschlüsseln. Als eines der ersten Unternehmen hat Apple auf diese Bedrohung reagiert und kündigte am 21.02.2024 in einem Blogartikel an, solche Angriffe auf iMessage mit dem neuen Schlüsselaustauschverfahren PQ3 zu verhindern. Der hybride Schlüsselaustausch (von der NSA abgelehnt, siehe SSN 1/2024) besteht aus einem klassischen (P-256 ECDH) und einen Post-Quantum-Schlüsselaustausch (Kyber-1024). Die beiden Teilschlüssel bilden zusammen den Sitzungsschlüssel. Ein „store-now-decrypt-later"-Angreifer muss so beide Verfahren brechen können, um an den Schlüssel zu gelangen.

Auskunftskosten

Am 05.02.2024 verurteilte das Amtsgericht Lörrach einen Telefonvertrieb, die vorgerichtlichen Anwaltskosten für ein Auskunftsersuchen zu einer rechtswidrigen Verarbeitung zu erstatten. Denn juristischen Laien sei es nicht zumutbar, den Auskunftsanspruch selbst durchzusetzen. Das Urteil hat jedoch keine Bindungswirkung über den Fall hinaus, daher müssen Verantwortliche nicht widerspruchslos geforderte Kosten übernehmen. In der Regel dürften Auskunftsersuchen zumutbar sein, da Auskunftssuchenden zahlreiche Mustervorlagen der Aufsichtsbehörden zur Verfügung stehen.

Neues Website Audit Tool

Der Website Evidence Collector des europäischen Datenschutzbeauftragten sammelt auf Webseiten Nachweise für die Speicherung und den Transfer von personenbezogenen Daten (SSN 10/2023). Am 28.01.2024 hat der Europäische Datenschutzausschuss ergänzend das Website Auditing Tool veröffentlicht. Es besitzt eine grafische Oberfläche mit integriertem Chromium-Browser, was die manuelle Prüfung von Webseiten deutlich erleichtert. So lassen sich beispielsweise Datenübertragungen vor und nach einer Einwilligung einfacher prüfen als mit dem Website Evidence Collector. Auch das Website Audit Tool kann Prüfberichte erstellen; außerdem lassen sich gespeicherte Webseiten zur erneuten Prüfung importieren. Das Tool ist Open Source (EUPL 1.2) und kostenlos; es kann von der EU-Webseite code.europa.eu heruntergeladen werden.

Private Key

In einer (später noch ergänzten) Meldung räumte die AnyDesk Software GmbH am 02.02.2024 die Kompromittierung ihrer produktiven Systeme ein. Da auch Zertifikate für die Codesignatur zügig gesperrt wurden, drängt sich der Verdacht auf, dass die Angreifer deren Private Keys erbeutet haben.

Zwar belegt eine Codesignatur nicht, dass die signierte Software korrekt und frei von Schadsoftware ist – sie soll nachweisen, dass die Software vom Hersteller freigegeben und nach der Auslieferung nicht mehr verändert wurde. Wer jedoch den Private Key für die Codesignatur kennt, kann modifizierte Software im Namen des Herstellers signieren.

Daher sollte der Private Key zu einem Codesignatur-Zertifikat in sicherer Hardware (Smartcard, HSM o. ä.) gespeichert werden, um einen Schlüsseldiebstahl zu erschweren und aufdecken zu können. Auch lässt sich ein Hardware Key einfacher an einen neuen Codesignierer übergeben.

Genau dies fordert das CA/Browser-Forum seit dem 01.06.2023 verbindlich für öffentliche Codesignatur-Zertifikate. Daher dürften AnyDesks neue Keys besser geschützt sein als deren kompromittierte Vorgänger.

secorvo
security consulting

HackGPT

Beim KA-IT-Si-Event am 22.02.2024 demonstrierte Dr. Swantje Westpfahl vom Institute for Security and Safety GmbH, wie man ChatGPT zur Vorbereitung eines Cyberangriffs verwenden kann. Wenige Tage zuvor hatte OpenAI berichtet, dass in Zusammenarbeit mit Microsoft Threat Intelligence fünf den Geheimdiensten von China, Russland, Nordkorea und des Iran nahestehende Gruppen identifiziert und gesperrt worden waren, die ebenfalls versucht hatten, OpenAI-Tools unter anderem für die Vorbereitung von Phishing-Angriffen zu nutzen.

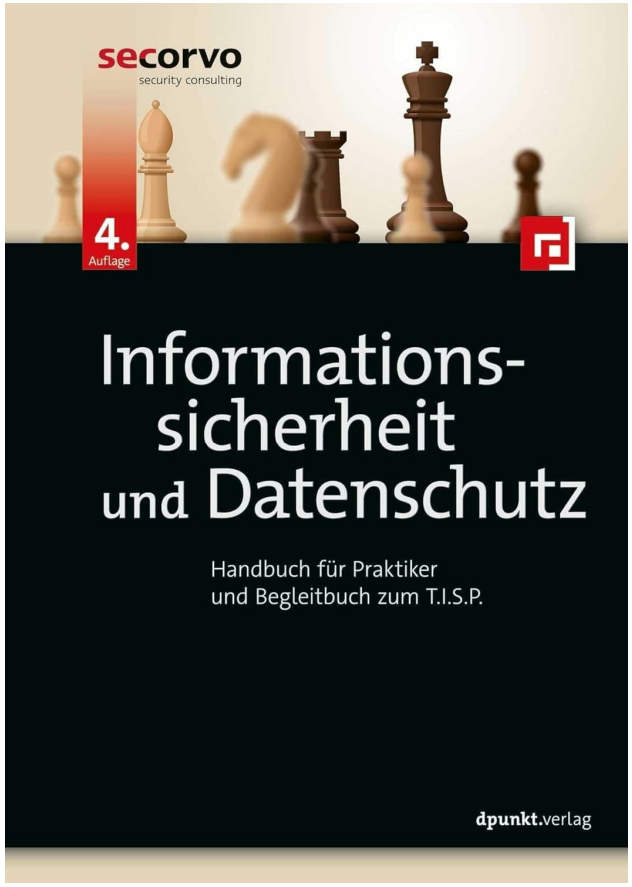
Secorvo News

Vierte Auflage

Vor 17 Jahren fassten wir den schon damals verwegenen Beschluss, die wichtigsten Grundlagen der selten um neue Themen verlegenen Informationssicherheit zu verschriftlichen. Vier Jahre später erschien tatsächlich das „Secorvo-Buch“ mit dem Titel „Zentrale Bausteine der Informationssicherheit“ als Begleitbuch zum T.I.S.P. In die drei Jahre später erschienene zweite Auflage nahmen wir 2014 weitere wichtige Themen wie „Rechtliche Aspekte“, „IPv6“ und „Incident-Management“ auf; das Werk wuchs dadurch auf 26 Kapitel. Die dritte, gründlich überarbeitete und aktualisierte Auflage erschien dann 2019 unter dem Titel „Informationssicherheit und Datenschutz“ im dpunkt-Verlag.

Seit dem 07.03.2024 ist nun die vierte, aktualisierte und ergänzte Auflage erhältlich. Sie ist auf über 900 Seiten und 32 Kapitel angewachsen, räumt dem Datenschutz mehr Raum ein und wurde um einige aktuelle Themen wie „Cloud Security“ ergänzt.

Auch diese Ausgabe eignet sich sowohl zum Selbststudium als auch für die systematische Vorbereitung auf die T.I.S.P.-Zertifizierung – ein Qualifikationsnachweis, den inzwischen mehr als 2.000 Informationssicherheitsexperten erworben haben.



Wir freuen uns über Ihre Rückmeldungen, Kommentare und Rezensionen – und hoffen, Ihnen mit der Neuauflage des Handbuchs einige wertvolle Erkenntnisse und Einsichten zu bieten.

Seminare

In der Woche vom **15. bis 18.04.2024** bieten wir das Seminar PKI – Grundlagen, Vertiefung, Realisierung an, das von unserem PKI-Experten Hans-Joachim Knobloch geleitet wird.

Und vom **22. bis 25.04.2024** dreht sich beim im vergangenen Jahr neu konzipierten und aktualisierten TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) alles um sichere Software-Entwicklung – mit der Möglichkeit einer anschließenden T.P.S.S.E.-Zertifizierung.

Die nächste Möglichkeit zur Vorbereitung auf die T.I.S.P.-Zertifizierung bieten wir Ihnen vom **24. bis 28.06.2024**.

Es gibt noch freie Plätze: Sichern Sie sich den Frühbucherrabatt. Die Seminarprogramme und eine Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

No risk, no fun

Im Zentrum des Informationssicherheits-Managements stehen die Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken. Kai Jendrian (Secorvo) wird in seinem Vortrag auf dem KA-IT-Si-Event am **11.04.2024** Einblicke in seine Erfahrungen aus 18 Jahren Beratungstätigkeit zur Informationssicherheit geben – mit einem besonderen Augenmerk auf der Bewertung von Risiken und der Abschätzung von Eintrittswahrscheinlichkeiten. Freuen Sie sich auf praxiserprobte Ideen für die Bewältigung der Herausforderungen beim Risikomanagement – und den Erfahrungsaustausch beim anschließenden „Buffet-Networking“.

Wir freuen uns auf Sie beim Fraunhofer IOSB – und empfehlen bei Interesse eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2024	
05.-07.03.	secIT 2024 (Heise Medien, Hannover))
11.-15.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.-22.03.	DFRWS EU 2024 (DFRWS, Zaragoza/ES)
April 2024	
09.-11.04.	GI Sicherheit 2024 (Gesellschaft für Informatik, Worms)
15.-18.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.04.	Blackhat Asia 2024 (Blackhat, Singapur/ASE)
22.-25.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Mai 2024	
07.-08.05.	20. Deutscher IT-Sicherheitskongress (BSI, virtuell)
14.-15.05.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
14.-16.05.	Datenschutztage 2024 (WEKA Akademie, Niedernhausen hybrid)
22.-24.05.	25. Datenschutzkongress (EUROFORUM, Berlin)
26.-30.05.	Eurocrypt 2024 (IACR, Zürich/CH)
28.-29.05.	BvD Verbandstage 2024 (BvD, Berlin)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2024



Voyeure überall

Am 15.03.2024 veröffentlichte Kaspersky den Stalkerware Report 2023. Unter Stalkerware werden kommerzielle Apps verstanden, die eine Überwachung des Smartphones einer anderen Person aus der Ferne ermöglichen. Rund 31.000 Fälle hat Kaspersky im Jahr 2023 allein bei Nutzern von Kaspersky-Lösungen gezählt. Die Gesamtzahl dürfte deutlich höher liegen, zumal Apps wie beispielsweise Ortungsdienste gar nicht unter die Definition von Stalkerware fallen, aber zum Stalking missbraucht werden können.

Weit aussagekräftiger als die absoluten Zahlen sind die Ergebnisse der 21.000 Online-Interviews, die Kaspersky Mitte Januar 2024 zusammen mit Arlington Research in 21 Ländern weltweit durchgeführt hat. Darin gaben 23% der Befragten an, dass sie bereits Online-Stalking durch einen Partner erlebt haben, 10% berichteten, dass ihr Standort verfolgt wurde und 7% hatten festgestellt, dass Stalker-Software auf ihren Geräten installiert worden war.

Am meisten erschüttert jedoch die Erosion des Anstands: Waren im Jahr 2021 noch 70% der Befragten der Auffassung, dass die Überwachung eines Partners ohne dessen Wissen völlig inakzeptabel ist, sank dieser Anteil 2024 auf 54%. Offenbar zählt die heimliche Beobachtung anderer Menschen zunehmend zu den üblichen Gepflogenheiten – zur Befriedigung der Neugier oder der subtilen Freude an der Macht, die intimes Wissen verschafft.

Von Menschen, die keinerlei Hemmungen verspüren, andere Menschen aus ihrem persönlichen Umfeld zum Gegenstand verdeckter Kontrolle zu machen, wird man wohl kaum erwarten dürfen, dass sie davor zurückschrecken, das Verhalten von ihnen Unbekannten zu überwachen. Vor dem Hintergrund der exponentiellen Zunahme digitaler Spuren kann einem angesichts dieser Entwicklung angst und bange um die Zukunft werden.



Inhalt

Voyeure überall

Security News

Generalüberholtes CSF

Consent Framework rechtswidrig

Features-by-Default

Auskunft bei Hackerangriff

Fehlerhafte Einwilligungen

Freier Normenzugang?

Secorvo News

Verstärkung

Seminare

14. Tag der IT-Sicherheit

Veranstaltungshinweise

secorvo
security consulting

Security News

Generalüberholtes CSF

Am 26.02.2024 stellte das amerikanische NIST das inzwischen verbreitete Cybersecurity Framework (CSF) in einer überarbeiteten Version 2.0 vor – fast genau zehn Jahre nach der Erstveröffentlichung. Sogar der ISO/IEC 27002:2022 verweist inzwischen auf den CSF (v1.1). Zielgruppe des Managementsystems für Cybersicherheitsrisiken sind nicht mehr nur kritische Infrastrukturen, sondern alle öffentlichen und privatwirtschaftlichen Einrichtungen.

In der jüngsten Fassung wird der neue Ansatz des Frameworks, Sicherheitsmaßnahmen nach den Zielen „Identify", „Protect", „Detect", „React" und „Recover" zu strukturieren (und damit zu verdeutlichen, dass ausschließlich präventive Maßnahmen zu kurz greifen), durch die Ebene „Govern" ergänzt: Sicherheit erfordert auch Steuerung.

Die sehr hilfreichen „Informal References" mit Querbezügen zu anderen Standards (auch dem ISO 27001) werden künftig dynamisch im National Online Informative References Program (OLIR) gepflegt; bisher sind darin noch nicht alle Referenzen des CSF 2.0 enthalten.

Auf der Webseite des Projekts findet man alle Materialien zum CSF. Das Framework selbst steht als PDF-Dokument, online sowie als JSON- oder Excel-Export zur Verfügung. Die Online-Version wurde in das Cybersecurity and Privacy Reference Tool (CPRT) integriert, über das weitere Standards zugänglich sind. Für Einsteiger sind die diversen Quick-Start-Guides ein guter Ausgangspunkt.

Consent Framework rechtswidrig

Anfang 2022 haben wir berichtet, dass die belgische Datenschutzaufsichtsbehörde ADP das Transparency and Consent Framework (TCF) von IAB Europe als rechtswidrig einstuft (SSN 02/2022): Willigt ein Nutzer innerhalb des TCF ein, wird auf der Endeinrichtung ein Transparency and Consent String (TC-String) gespeichert und an alle Werbepartner übermittelt. Unter Bezugnahme auf den TC-String und die IP-Adresse des Betroffenen erfolgt dann eine Echtzeit-Werbeauktion durch IAB Europe, das Real Time Bidding (RTB) (siehe auch SSN 05/2022).

Gegen die Entscheidung hatte IAB Europe Rechtsmittel eingelegt. Der EuGH folgte nun im Urteil vom 07.03.2024 der Auffassung der ADP, dass der TC-String ein personenbezogenes Datum darstellt und daher für das RTB eine Einwilligung erforderlich ist – ein klares Votum für den Datenschutz. Außerdem sei IAB Europe möglicherweise „gemeinsam Verantwortlicher" und damit für die Einhaltung der DSGVO zusammen mit den Werbetreibenden haftbar – ein schwerer Schlag für das Geschäftsmodell des „Real Time Bidding", aber ein großer Fortschritt bei der Begrenzung der Nutzer-Überwachung im Internet.

Features-by-Default

Microsoft-Cloud-Anwender können sich mit einem Entra Device Code auch von Geräten ohne echte Tastatur (wie z. B. Smart-TVs) anmelden. Ein Microsoft-Artikel vom 27.02.2024 erläutert nun, wie man dieses Feature mit neuen Conditional-Access-Funktionen schützen kann – denn schon im Oktober 2020 wurde es als Phishing-Einfallstor ausgemacht.

Das ist ein gutes Beispiel dafür, dass die Nutzung einer Cloud-Lösung nicht davon entbindet, sich eingehend mit deren Konfiguration zu befassen. Auch wenig bekannte oder nicht genutzte Features des Cloud-Dienstes sollte man kennen und ggf. deaktivieren, um Risiken zu minimieren. Security-by-Default (oder nach der DSGVO Privacy-by-Default) würde bedeuten, dass solche Features explizit aktiviert werden müssen. Aber das werden wir vermutlich genauso wenig erleben wie nach der Standard-Installation automatisch gehärtete On-Premises-Betriebssysteme – oder das schon lange versprochene papierlose Büro.

Auskunft bei Hackerangriff

Das Landgericht Berlin hatte mit Urteil vom 24.03.2023 entschieden, dass ein durch einen Hackerangriff betroffenes Unternehmen nicht auskunftspflichtig gemäß Art. 15 Abs. 1 DSG-VO hinsichtlich der durch den Hackerangriff erbeuteten (personenbezogenen) Daten ist. Verantwortliche Stelle für die im Rahmen des Hackerangriffs verarbeiteten Daten sei der Hacker, nicht dessen Opfer. Das gehackte Unternehmen trifft aber eine Benachrichtigungspflicht gemäß Art. 34 DSGVO: So muss es betroffene Personen über den Angriff bzw. die abgezogenen Daten informieren, wenn daraus ein hohes Risiko für die Rechte und Freiheiten der Betroffenen entsteht. Am 22.11.2023 wies das KG Berlin die gegen das Urteil eingelegte Berufung zurück: Zu den Gründen des Landgerichts komme hinzu, dass der Auskunftsanspruch persönlich und nicht abtretbar sei. Für einen Schadensersatz nach Art. 82 DSGVO müsse ein Betroffener zudem einen tatsächlichen (immateriellen) Schaden darlegen – Hackerangriffe sind keine Gelegenheit für Trittbrettfahrer.

Fehlerhafte Einwilligungen

Auf Webseiten und in Apps eine rechtskonforme Einwilligung in die Verarbeitung der Nutzungsdaten einzuholen ist für eine Vielzahl von Unternehmen offenbar eine nicht zu bewältigende Herausforderung, wie das Bayerische Landesamt für Datenschutzaufsicht am 09.02.2024 feststellte. So muss nach Auffassung der deutschen Datenschutzaufsichtsbehörden (DSK) die Möglichkeit, keine Einwilligung zu erteilen, zwingend auf der ersten Ebene eines Cookie Banners angeboten werden, sofern die Webseite nicht ohne Interaktion mit dem Einwilligungs-Banner beeinträchtigungsfrei genutzt werden kann – eine Eigenschaft mit Seltenheitswert.

Unternehmen, die sich bislang mit fehlender Rechtsprechung entschuldigen, sollten besser das Urteil des OLG Köln vom 19.01.2024 lesen: Wenn dem Seitenbesucher durch die Gestaltung des Cookie-Banners „weder auf der ersten noch auf der zweiten Ebene eine gleichwertige, mithin auf klaren und umfassenden Informationen beruhende Ablehnungsoption angeboten“ und dieser deshalb „zur Abgabe der Einwilligung hingelenkt und von der Ablehnung der Cookies abgehalten wird“, so kann „die erteilte Einwilligung nicht“ im Sinne von § 25 Abs. 1 TTDSG und Art. 4 DSGVO „als freiwillig und hinreichend aufgeklärt angesehen werden“ – sprich: Die Datenverarbeitung ist in diesem Fall rechtswidrig und es drohen Bußgelder und Schadensersatzforderungen.

Wer dieses Risiko vermeiden will, findet konkrete Hinweise zur rechtskonformen Einholung einer Einwilligung z. B. in den FAQ des LfDI Baden-Württemberg.

Freier Normenzugang?

Am 05.03.2024 hat der EuGH abweichend von der bisherigen Rechtsprechung des EuG (Urteil vom 14.07.2001) entschieden, dass EU-Bürger das Recht haben, auf solche technischen Normen zuzugreifen, die Bestandteil europäischer Verordnungen und Richtlinien und damit Teil des Unionsrechts sind. Damit gewähre das Unionsrecht jeder natürlichen oder juristischen Person mit Wohnsitz oder Sitz in der EU den (kostenlosen) Zugang zu im Amtsblatt der EU veröffentlichten harmonisierten Normen. Da deren Rechtswirkung für Wirtschaftsteilnehmer von wesentlicher Bedeutung sei, müsse es jeder durch ein Gesetz geschützten Person möglich sein zu prüfen, ob ein Produkt die gesetzlichen Regeln einhalte.

Dieses öffentliche Interesse überwiege den (einem freien Zugang zu Normen normalerweise entgegenstehenden) Schutz der berechtigten geschäftlichen Interessen und des geistigen Eigentums der Rechteinhaber. Das Urteil erstreckt sich nach Einschätzung des DIN vom 15.03.2024 auf rund 3.000 harmonisierte EU-Normen – darunter wahrscheinlich auch einige IEC- und ETSI-Standards zur Informationssicherheit, soweit deren Einhaltung verbindlich vorgeschrieben ist.

Secorvo News

Verstärkung

Seit dem 01.03.2024 verstärkt Markus Toran (M.Sc. Informatik mit Schwerpunkt Information Security) unser Beratungsteam. Herzlich willkommen!

Seminare

Kurzentschlossene können noch einen Platz für das Seminar TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) vom **22. bis 25.04.2024** buchen: vier Tage spannende Vorträge und interaktive Workshops rund um die sichere Software-Entwicklung mit der Möglichkeit zur anschließenden Zertifizierung als T.P.S.S.E.

Mit dem Wissens-Booster IT-Security Insights – T.I.S.P.-Update vom **14. bis 15.05.2024** bringen Sie sich im Bereich der IT-Sicherheit auf einen aktuellen Stand.

Und das fünftägige T.I.S.P.-Seminar bereitet Sie vom **24. bis 28.06.2024** auf die Zertifikatsprüfung zum TeleTrusT Information Security Professional vor. Ein Exemplar der gerade erschienenen 4. Auflage des Begleitbuchs zum T.I.S.P. schicken wir Ihnen nach Ihrer Anmeldung zu.

Alle drei genannten Seminare haben bereits die Mindestteilnehmerzahl erreicht und werden stattfinden.

14. Tag der IT-Sicherheit

Zum Vormerken: Am **18.07.2024** findet der 14. „Tag der IT-Sicherheit“ in der IHK Karlsruhe statt. Das Programm wird in Kürze veröffentlicht – so viel sei aber schon einmal verraten: Die Keynote hat Ralf Wigand übernommen, National Security & IT-Compliance Officer von Microsoft Deutschland.

Es erwarten Sie zahlreiche weitere Vorträge zu aktuellen Themen der Informationssicherheit – und natürlich der anschließende Erfahrungsaustausch beim „Buffet-Networking“.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2024	
09.-11.04.	GI Sicherheit 2024 (Gesellschaft für Informatik, Worms)
11.04.	KA-IT-Si-Event "No risk, no fun." (KA-IT-Si, Karlsruhe)
15.-18.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.04.	Blackhat Asia 2024 (Blackhat, Singapur/ASE)
22.-25.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Mai 2024	
07.-08.05.	20. Deutscher IT-Sicherheitskongress (BSI, virtuell)
14.-15.05.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
14.-16.05.	Datenschutztage 2024 (WEKA Akademie, Niedernhausen hybrid)
22.-24.05.	25. Datenschutzkongress (EUROFORUM, Berlin)
26.-30.05.	Eurocrypt 2024 (IACR, Zürich/CH)
28.-29.05.	BvD Verbandstage 2024 (BvD, Berlin)
Juni 2024	
03.-05.06.	Entwicklertag 2024 (VKSI, GI, ObjektForum, Karlsruhe)
04.-07.06.	European Identity & Cloud Conference 2024 (KuppingerCole, Berlin)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2024



Keine Zauberei

Warum gelingen immer mehr Angriffe auf IT-Infrastrukturen von Behörden und Unternehmen? Werden Cyberkriminelle gefährlicher, kompetenter, offensiver? Oder besitzen die IT-Systeme immer mehr Schwachstellen?

Wer die Ursachen erfolgreicher Angriffe analysiert, stellt fest, dass weder das eine noch das andere zutrifft. Zwar hat das Geschäftsmodell „Erpressung" Angreifern einen Schub verpasst – aber das liegt schon über acht Jahre zurück. Und Schwachstellen, die nach wie vor entdeckt werden, ermöglichen immer seltener gleich die Übernahme ganzer Systeme. Tatsächlich waren die bekannt gewordenen Angriffe bis auf wenige Ausnahmen kein Hexenwerk. Vor allem aber: Die meisten hätten sich durch Maßnahmen vereiteln lassen, die seit Jahrzehnten bekannt sind und längst gängige Praxis sein sollten:

1. *Network Segregation*: Eine strukturierte Aufteilung der über das Netz erreichbaren Server und Peripheriegeräte in VLANs, die konsequente Nutzung von DMZ-Rechnern und ein physikalisch getrenntes Backup-Netz erschweren viele Angriffe deutlich oder machen sie sogar unmöglich.
2. *Complexity Reduction*: Eine große Vielfalt an Systemen und Anwendungen, Betriebssystemvarianten und Geräten erschwert es, Software und Hardware in einem möglichst sicheren Zustand zu betreiben. Wer Komplexität verringert gewinnt Überblick und hat mehr Zeit für Härtung und zügige Updates.
3. *Need to know*: Wer Zugriffsrechte und die Erreichbarkeit von Servern und Peripheriegeräten auf das Erforderliche beschränkt, begrenzt den Schaden, den ein Angreifer anrichten kann – unnötige Admin-Rechte, Schreibrechte, Berechtigungen nach Aufgabenwechsel oder Ausscheiden gehören beschnitten.

IT-Sicherheit ist keine Zauberei. Man muss sie wollen. Und konsequent umsetzen, ohne Sonderlocken – denn ein Einfallstor genügt.



Inhalt

Keine Zauberei

Security News

Lernen aus Fehlern Anderer

Keine Ausreden

Know Your Contributor

Hinweispflicht auf Schwachstelle

Staatstrojaner

Formlose Newsletterabmeldung

Consent or Pay

Datenschutz-Reifegradmodell

Secorvo News

Secorvo Seminare

Los, sag' mir was Du weißt. Alles.

Veranstaltungshinweise

secorvo
security consulting

Security News

Lernen aus Fehlern Anderer

Selten berichten Opfer öffentlich über einen erfolgreichen Cyberangriff – dabei ließe sich viel daraus lernen. Daher muss man die British Library für ihren 18-seitigen Cyber Incident Review vom 08.03.2024 loben. Detaillierter noch ist r-tecs 42-seitiger Bericht vom 19.01.2024 über den Angriff auf die Südwestfalen-IT – „vertraulich" klassifiziert, aber öffentlich einsehbar. Und nicht nur für Fachleute hörenswert ist der sechsteilige MDR-Podcast (06.07.-10.08.2023) über den Vorfall im Landkreis Anhalt-Bitterfeld.

Die Ursachen der drei Vorfälle ähneln sich: unzureichend gesicherter Fernzugriff, keine Netz-Segmentierung, fehlende Offline-Backups, viele Legacy-Systeme und nicht zuletzt Budget- und Personalmangel. Wirksame Schutzmaßnahmen wären in allen drei Fällen möglich gewesen – hoffentlich lassen sich das Behörden und Unternehmen eine Lehre sein.

Keine Ausreden

Am 11.04.2024 hat der Europäische Gerichtshof erneut über immateriellen Schadensersatz bei Datenschutzverstößen entschieden. Die Juris GmbH wollte von der Haftung befreit werden, da der Mitarbeiter, der den Verstoß verursacht hatte, klare Weisungen missachtet hatte. Folgt man dieser Argumentation wäre damit jedoch Art. 82 DSGVO ausgehebelt – ein verantwortliches Unternehmen kann sich nicht vor der Haftung drücken, indem es die Schuld Mitarbeitern zuweist und sich darauf beruft, dass diese Pflichten verletzt hätten. Unternehmen müssen dafür sorgen, dass gesetzliche Bestimmungen tatsächlich eingehalten werden – Eltern haften für ihre Kinder und Unternehmen für ihre Mitarbeiter.

Know Your Contributor

Die Hintertür in xz Utils, die am 29.03.2024 bekannt wurde (CVE-2024-3094), hätte um ein Haar dramatische Folgen gehabt. Sie wurde durch Zufall vom PostgreSQL-Entwickler und Microsoft-Mitarbeiter Andreas Freund entdeckt, der bei Performance-Messungen Verzögerungen in einer neuen Version der Bibliothek liblzma von 0,5 Sekunden beobachtet hatte. Ursache war eine Hintertür, die unautorisierten Secure-Shell-Zugang (ssh) in solchen Linux-Distributionen wie Debian und Red Hat ermöglicht hätte, die den ssh-Service mit dem Management-Dienst systemd verknüpfen – denn der enthält xz.

Eingebaut hatte die Hintertür ein in das Open-Source-Projekt eingeschleuster Maintainer. Über einen ähnlichen Infiltrationsversuch bei der OpenJS Foundation berichtete am 15.04.2024 die Open Source Security Foundation. Da viele, auch sicherheitskritische Projekte wie sudo nur über wenig Wartungs-Ressourcen verfügen, ist daher nicht auszuschließen, dass es bereits erfolgreich eingeschleuste Hintertüren in Linux-Distributionen gibt.

Um bei Bekanntwerden solcher Angriffe auf die „Software-Lieferkette" schnell reagieren zu können, müssen Unternehmen, Software-Hersteller und Anwender wissen, welche Software welche Bibliotheken in welchen Versionen nutzt. Dabei helfen sogenannte Software Bill of Materials: Listen, die die Abhängigkeiten der Software dokumentieren und automatisch erstellt werden können – z. B. in dem verbreiteten Format System Package Data Exchange (SDPX), das 2021 als ISO/IEC 5692 genormt wurde.

Hinweispflicht auf Schwachstelle

Am 23.11.2023 entschied das Landgericht Bochum, dass es nicht ausreicht, wenn Hersteller über bekannte Sicherheitslücken eines Produkts auf ihrer Webseite informieren. Geklagt hatte die Verbraucherzentrale Bundesverband gegen den Hersteller eines Funk-Türschlossantriebs, der seine Produkte über Online-Plattformen und Einzelhändler vertreibt. Im August 2022 hatte das BSI eine Warnung der Risikostufe „hoch" nach § 7 BSIG ausgesprochen. Nach Ansicht des Gerichts war der entsprechende Hinweis auf der Produktwebseite irreführend (Art. 5a Abs. 1 UWG), da der Hersteller nicht dafür gesorgt hatte, dass Käufer beim Erwerb des Produkts über die Vertriebspartner von der Sicherheitslücke erfahren.

Staatstrojaner

Der Einsatz staatlicher Überwachungssoftware muss nach dem Urteil des Bundesverfassungsgerichts zur Onlinedurchsuchung vom 27.02.2008 von einem Richter angeordnet werden. Wie oft eine solche Durchsuchung vorgenommen wurde, gibt das Bundesamt für Justiz (BfJ) in einer jährlichen Statistik zur Telekommunikationsüberwachung bekannt. Den am 25.04.2024 vom BfJ veröffentlichten Zahlen kann man entnehmen, dass 2022 wie in den Vorjahren weniger als 20 Anordnungen erfolgten – und eine erfolgreiche Installation des „Staatstrojaners" offenbar nur in einem Teil der Fälle gelang. Im Vergleich mit der (weiter) steigenden Anzahl der Verkehrsdatenabfragen (2022: über 30.000) ist das eine geradezu verschwindend geringe Größe.

Formlose Newsletterabmeldung

Unternehmer müssen der Verwendung ihrer E-Mail-Adresse für die Zusendung von Werbung auch formlos widersprechen können - hat das Landgericht Paderborn am 12.03.2024 entschieden. Andernfalls drohen den werbenden Unternehmen Schadensersatz- und Unterlassungsansprüche.

Für werbetreibende Unternehmen bedeutet das, dass sie Prozesse einführen müssen, die einen Widerruf unverzüglich umsetzen, auch wenn er nicht über das Kundenverwaltungssystem erfolgt. Das erfordert im Zweifel die Sensibilisierung aller Mitarbeiterinnen und Mitarbeiter mit Kundenkontakt.

Consent or Pay

Am 17.04.2024 bezog der Europäische Datenschutzausschuss (EDSA) zu „Consent-or-Pay"-Modellen Stellung, bei denen Besucher von Webseiten vor die Wahl gestellt werden, ob sie für die Inhalte zahlen oder eine Einwilligung in die Verarbeitung ihrer personenbezogenen Daten erteilen wollen. Oft werden diese Daten anschließend für umfangreiche Werbezwecke mit einer Vielzahl von Werbepartnern verarbeitet.

Eine Einwilligung muss nach Art. 7 Abs. 4 DSGVO freiwillig erfolgen. Das „Consent-or-Pay"-Modell biete jedoch keine echte Wahlmöglichkeit, wenn die Gebühren so hoch sind, dass sie die Nutzer daran hindern, eine freie Wahl zu treffen. Nutzer dürften zudem nicht von Online-Diensten ausgeschlossen werden, die eine wichtige Rolle spielen oder für die Teilhabe am gesellschaftlichen Leben oder den Zugang zu beruflichen Netzwerken entscheidend sind. Personenbezogene Daten dürften nicht als „handelbare Ware" verstanden werden; auch eine Bündelung verschiedener Zwecke in einer Einwilligung sei unzulässig. Schließlich müsse die Information des Verantwortlichen den Nutzern ermöglichen, den Wert, den Umfang und die Folgen einer Einwilligung vollständig zu verstehen. Als „Standard-Lösung" sei das Modell daher ungeeignet.

Datenschutz-Reifegradmodell

Die Erfüllung der gesetzlichen Anforderungen an den Datenschutz ist eine große Herausforderung in Unternehmen, die aus vielen, insbesondere internationalen Organisationseinheiten bestehen. In Heft 3/2024 der Fachzeitschrift Datenschutz und Datensicherheit (DuD) stellen Dirk Fox (Secorvo) und Ingo Lorenz (Konzerndatenschutzbeauftragter der Hansgrohe SE) ein Reifegradmodell vor, das eine strukturierte Vorgehensweise für den Aufbau und Betrieb eines Datenschutzmanagement-Systems über beliebig viele Organisationseinheiten bietet und zugleich eine differenzierte Bestimmung des jeweils erreichten Datenschutzniveaus ermöglicht.

Secorvo News

Secorvo Seminare

In der Kürze liegt die Würze – auch an den beiden Seminartagen IT-Security Insights – T.I.S.P.-Update am **14. und 15.05.2024** zu aktuellen Themen der Informationssicherheit und des Datenschutzes.

Der TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) vom **10. bis 13.06.2024** bringt Ihnen mit spannenden Vorträgen und interaktiven Workshops die sichere Software-Entwicklung nahe.

Und auf unserem T.I.S.P.-Seminar vom **24. bis 28.06.2024** können Sie Ihre Kenntnisse in der Informationssicherheit und im Datenschutz vertiefen und anschließend zertifizieren lassen. Das Anfang März 2024 in vierter Auflage erschienene Begleitbuch erhalten Sie nach Ihrer Anmeldung.

Los, sag' mir was Du weißt. Alles.

Das Recht auf Auskunft über die Verarbeitung persönlicher Daten ist ein Grundrecht. Durch die zunehmende Sensibilisierung für den Datenschutz stellen immer mehr Betroffene Auskunftsanfragen nach Art. 15 DSGVO – und viele Verantwortliche damit vor Herausforderungen. Denn eine Auskunft muss über alle über eine bestimmte Person verarbeiteten Daten erteilt werden.

Am **16.05.2024** stellen Friederike Schellhas-Mende und Christian Blaicher (Secorvo) beim KA-IT-Si-Event im House of Living Labs (FZI) vor, was eine Auskunft nach aktueller Rechtsprechung konkret umfassen muss und wie man sich darauf vorbereiten kann.

Anschließend erwartet Sie wie immer der Erfahrungsaustausch beim „Buffet-Networking". Wir freuen uns auf Sie – und empfehlen Ihnen eine schnelle Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2024	
07.-08.05.	20. Deutscher IT-Sicherheitskongress (BSI, virtuell)
14.-15.05.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
14.-16.05.	Datenschutztage 2024 (WEKA Akademie, Niedernhausen hybrid)
16.05.	KA-IT-Si-Event „Los, sag'was Du weißt. Alles.“ (KA-IT-Si, Karlsruhe)
22.-24.05.	25. Datenschutzkongress (EUROFORUM, Berlin)
26.-30.05.	Eurocrypt 2024 (IACR, Zürich/CH)
28.-29.05.	BvD Verbandstage 2024 (BvD, Berlin)
Juni 2024	
03.-05.06.	Entwicklertag 2024 (VKSI, GI, ObjektForum, Karlsruhe)
04.-07.06.	European Identity & Cloud Conference 2024 (KuppingerCole, Berlin)
10.-12.06.	DuD 2024 (COMPUTAS, Berlin)
10.-13.06.	T.P.S.S.E. (TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.-28.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
24.-28.06.	OWASP 2024 Global AppSec (OWASP Foundation, Lissabon/PT)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Mai 2024



Keine Märchen

Märchen leben bekanntermaßen davon, dass sie wiederholt erzählt oder gar aufgeschrieben und im Rahmen mündlicher oder schriftlicher Überlieferung verbreitet werden. Märchen sind gemeinhin frei erfundene Prosatexte, und so verhält es sich auch beim Märchen „Datenschutz kann Leben kosten“, das erst wieder am 07.05.2024 von der Süddeutschen Zeitung publiziert wurde.

Denn Datenschutz kostet keine Leben. Geht es nämlich in lebensbedrohlichen Lagen um eine wie auch immer geartete Verarbeitung von personenbezogenen Daten, dann gilt die dafür in der Datenschutzgrundverordnung vorgesehene Rechtsgrundlage des Art. 6 Abs. 1d – der Schutz lebenswichtiger Interessen Betroffener.

Vielmehr kann Datenschutz Leben retten, wie die Geschichte gezeigt hat: In Ländern, in denen in den Melderegistern die Konfession nicht als personenbezogenes Datum erfasst war, wurden unter der NS-Terrorherrschaft nachweislich weit weniger Juden deportiert und ermordet. Es ist deshalb nicht nur „schade“, sondern schädlich, wenn sich Medien oder auch Personen, die im Licht der Öffentlichkeit stehen, durch Wiederholung von Märchen negativ über den Datenschutz äußern – wie beispielsweise Prof. Dr. Alena Buyx, die Vorsitzende des Deutschen Ethikrats.

Datenschutz ist ein Grundrecht. Als solches dient es dem Schutz der Menschen und schadet ihnen nicht. Datenschutz mag in manchen Fällen vermeintlich lästigen Aufwand produzieren, weil man die gesetzlichen Regelungen einhalten muss. Hier ist es hilfreich und aufwandmindernd, sich genauer mit den Anforderungen des Datenschutzes und deren Zweck zu beschäftigen. Dabei sind, wie bei allen anderen Grundrechten auch, Interessen gegeneinander abzuwägen, Lösungen zu suchen (Risikoabwägung) und Kompromisse zu finden.

Datenschutz ist eine Chance. Und ganz bestimmt kein Lebensrisiko.



Inhalt

Keine Märchen

Security News

Behördenbußgelder

Hängepartien

Every Breath You Take (Stalking I)

Every Move You Make (Stalking II)

Windows No-Defender

Bewährter Code

Secorvo News

Seminare

Was ko$tet die Welt?

14. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Behördenbußgelder

Die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert in ihrer Stellungnahme vom 12.04.2024 die Streichung des § 43 Abs. 3 BDSG, der öffentliche Stellen bei Datenschutzverstößen von Bußgeldern befreit. Das Argument im Evaluationsbericht des Bundesministeriums für Inneres und für Heimat, das Bußgeld habe bloß eine Verschiebung von Haushaltsmitteln zur Folge, greife zu kurz: So sei die Verhängung von Bußgeldern nicht nur aus Gründen der Gleichbehandlung von nichtöffentlichen Stellen erforderlich, sondern müsse die Bußgeldbehörde die Schwere eines Verstoßes durch die Bußgeldhöhe verdeutlichen können. Nicht zuletzt fehle die abschreckende Wirkung eines Bußgelds. Das könne der Grund dafür sein, dass Datenschutz bei öffentlichen Stellen oft keinen hohen Stellenwert besitzt.

Ein Beispiel dafür ist der rechtswidrige Betrieb von Facebook-Fanpages durch Bundesministerien und -behörden. Der Bundesbeauftragte für Datenschutz und Informationsfreiheit, Ulrich Kelber, hatte am 20.05.2019 darüber informiert und am 16.06.2021 deren Abschaltung bis Ende 2021 gefordert. Kelbers ausführlich begründete Verwarnung des Bundespresseamts (BPA) vom 17.05.2022 mündete nach einer Anhörung in der Anordnung vom 17.02.2023, die Fanpage des BPA abzuschalten. Sie blieb folgenlos – und wurde mit einer (noch nicht entschiedenen) Klage beim Verwaltungsgericht Köln beantwortet. Unvorstellbar, dass sich ein Unternehmen bei einem ähnlichen Verstoß mehr als fünf Jahre aus der Verantwortung stehlen und sogar wacker weitermachen könnte: So startete das BPA am 08.04.2024 eine Präsenz bei TikTok.

Hängepartien

Am 16.05.2024 wählte der Bundestag nach sechsmonatiger Hängepartie (SSN 1/2024) Frau Prof. Dr. Specht-Riemenschneider zur neuen Bundesdatenschutzbeauftragten. Und in Sachsen-Anhalt wurde am 24.04.2024 mit sogar sechsjähriger Verspätung Maria Christina Rost zur Landesdatenschutzbeauftragten gewählt. Offen ist noch die Nachfolge für die seit Februar 2024 vakante Position der Landesbeauftragten für Datenschutz in Bremen.

Mit solchen Verzögerungen schwächen die Volksvertreter den in einer Demokratie so wichtigen Grundrechtsschutz: Die jährlichen Berichte der Datenschutz-Aufsichtsbehörden belegen, dass sich nur mit wirksamer Kontrolle verhindern lässt, dass das Grundrecht auf Datenschutz wirtschaftlichen oder Überwachungsinteressen geopfert wird.

Every Breath You Take (Stalking I)

Stalkerware ist für Betroffene schwer erkennbar. Schutz vor digitalem Stalking (SSN 3/2024) können die Software TinyCheck von Kaspersky (Source in Github) oder die Abspaltung SpyGuard bieten. Mit beiden Lösungen kann man prüfen, ob ein Smartphone mit Stalkerware infiziert ist: Sie werden als WLAN-Hotspot verbunden und analysieren den Datenverkehr des Smartphones auf verdächtige Muster wie bekannte Domainnamen, IP-Adressen oder Zertifikat-Hashwerte.

Über die Stalkerware „TheTruthSpy“ veröffentlichten Zack Whittaker und das Team von Techcrunch am 20.07.2023 eine lesenswerte Hintergrundanalyse. Sie ergänzten am 12.02.2024 einen Online-Dienst, über den man prüfen kann, ob ein Android Device von der Stalkerware betroffen ist: Er prüft, ob eine angegebene IMEI (International Mobile Equipment Identity) oder Werbe-ID in der im Dezember 2023 an Techcrunch geleakten Liste aller betroffenen Geräte enthalten ist.

Every Move You Make (Stalking II)

Auch einige nützliche Produkte können für Stalking missbraucht werden, wie z. B. Apples AirTags – kleine Ortungsgeräte zum Wiederfinden verlegter Gegenstände, die über Bluetooth mit Apples „Find My“-Netzwerk kommunizieren (SSN 3/2022).

Um das zu verhindern benachrichtigt iOS inzwischen den Nutzer, wenn sich ein fremder AirTag über einen längeren Zeitraum mitbewegt. Für Android stellt Apple eine App bereit, die nach AirTags in der Umgebung scannen kann. Die App AirGuard für Android der Forschungsgruppe Secure Mobile Networking Lab an der TU Darmstadt erkennt neben AirTags auch Alternativprodukte von Samsung, Chipolo und Tile, kann im Hintergrund scannen und umfasst ein Dashboard mit einer Übersicht.

Apple und Google haben 2023 eine gemeinsame Spezifikation erstellt, um AirTag-ähnliche Geräte zu erkennen. Am 13.05.2024 haben Apple und Google nun angekündigt, diese Spezifikation ab iOS 17.5 bzw. Android 6.0 zu unterstützen. Damit warnen zukünftig Smartphone-Betriebssystemdienste herstellerunabhängig vor potentiellen Trackinggeräten.

Windows No-Defender

Das Windows Security Center besitzt eine verborgene Schnittstelle zum Abschalten des Microsoft Defenders. Deren Nutzung ist für Hersteller von Virenscannern vorgesehen, die ein Alternativprodukt zum Defender installieren. Die Produkte von Avast nutzen diese Schnittstelle über einen eigenen Dienst namens wsc_proxy.exe. Am 23.05.2024

veröffentlichte der GitHub Nutzer „es3n1n“ ein Tool, das die Installation eines Virenscanners simuliert und den Windows Defender unter Verwendung des Proxy-Dienstes von Avast deaktiviert.

Die Deaktivierungsschnittstelle wird von Microsoft lediglich durch ein NDA geschützt – ein weiteres Beispiel in der langen Liste offenbar unausrottbarer Versuche von „Security by Obscurity“. Wäre Virenschutz wirkungsvoller, wäre das ein GAU. Wer auf den Windows Defender setzt, sollte wohl gelegentlich prüfen, ob er nicht deaktiviert ist.

Bewährter Code

Am 06.04.2024 veröffentlichte das PuTTY-Team Version 0.81 des verbreiteten Windows-SSH-Clients. Sie schließt eine Sicherheitslücke, deren ursprünglicher Code aus dem Jahr 2001 stammt. Darin wird eine bis zu 512 bit lange Nonce (Einmal-Wert) für DSA- und ECDSA-Signaturen gewählt, die für (damalige) DSA-Schlüssellängen adäquat war, nicht aber für ECDSA-Schlüssel mit der Kurve P-521: Dafür sind es neun Bits zu wenig. Fabian Bäumer und Marcus Brinkmann von der Ruhr-Universität Bochum publizierten am 15.04.2024, dass bereits 60 von PuTTY erzeugte ECDSA-Signaturen genügen, um den privaten Schlüssel bestimmen zu können.

Der Fix wechselt auf das bereits 2013 in RFC 6979 beschriebene Verfahren für die Nonce-Generierung. Das hätte das PuTTY-Team spätestens 2017 machen sollen, als es mit der Version 0.68 die Unterstützung des ECDSA-Verfahrens ergänzte.

Der Fall erinnert an die Explosion der ersten Ariane 5 vor 28 Jahren. Ursache war damals ein Integer-Überlauf aufgrund der höheren Geschwindigkeit der Rakete: Die Software war für die Ariane 4 entwickelt und unverändert übernommen worden.

Fehler dieser Art haben zur Entwicklung von Design by Contract geführt. Dabei werden Zusicherungen explizit vereinbart. Damit hätte auch bei PuTTY der Fehler früher bemerkt werden können. Ein kleines, unbezahltes Entwicklerteam stößt bei solchen (berechtigten) Anforderungen jedoch schnell an seine Grenzen.

Secorvo News

Seminare

Wissen verleiht Macht – oder wenigstens ein Zertifikat. Das T.I.S.P.-Seminar vom **24. bis 28.06.2024** bereitet Sie intensiv und fundiert auf die anschließende Zertifikatsprüfung vor. Unser offizielles Begleitbuch zum T.I.S.P. erhalten Sie direkt nach Ihrer Anmeldung. Noch gibt es freie Plätze.

Planen Sie bereits Ihre Weiterbildung für das zweite Halbjahr? Dann werfen Sie doch einen Blick in unseren Seminarkalender. Der Seminarkompass gibt Ihnen einen Überblick über das Seminarangebot.

Was ko$tet die Welt?

Cybercrime-Statistiken, die überall zitiert und gerne zur Begründung von Maßnahmen und Regulierungen herangezogen werden, jonglieren mit Schadenssummen in luftigen Höhen: Milliarden, Billionen, Trilliarden... Allein: Die Quellen sind oft ungewiss.

Am **20.06.2024** um 18 Uhr gehen Wiebke Reimer und Dr. Boris Hemkemeier (Commerzbank) diesen fantastischen Zahlen auf den Grund: Wo kommen sie her? Sind sie fundiert - oder frei erfunden? Worauf kann man sich stützen und was darf man tatsächlich glauben? Was folgt daraus für eine seriöse Risikoabschätzung?

Das KA-IT-Si-Event findet diesmal im Rahmen der FZI-Veranstaltung „Innovativ? Aber sicher“ statt, zu der Sie ebenfalls herzlich eingeladen sind. Sie beginnt um 14 Uhr im House of Living Labs (FZI).

Im Anschluss an den Vortrag erwartet Sie natürlich auch diesmal der Erfahrungsaustausch beim „Buffet-Networking“. Wir freuen uns auf Sie und empfehlen eine baldige Anmeldung.

14. Tag der IT-Sicherheit

Am 18.07.2024 bietet Ihnen der Karlsruher Tag der IT-Sicherheit zum 14. Mal die Möglichkeit, sich über aktuelle IT-Sicherheitsthemen wie AI oder NIS2 und Präventionsmaßnahmen für Unternehmen zu informieren. Lernen Sie interessante IT-Sicherheits-Start-Ups kennen und nutzen Sie in der Network-Pause die Gelegenheit zum Erfahrungsaustausch mit Teilnehmern und Referenten. Wir empfehlen Ihnen – auch für diese Veranstaltung – eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2024	
04.-07.06.	European Identity & Cloud Conference 2024 (KuppingerCole, Berlin)
10.-12.06.	DuD 2024 (COMPUTAS, Berlin)
20.06.	Was ko$tet die Welt? (KA-IT-Si, Karlsruhe)
24.-28.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
24.-28.06.	OWASP 2024 Global AppSec (OWASP Foundation, Lissabon/PT)
Juli 2024	
08.-12.07.	9th IEEE European Symposium on Security and Privacy (IEEE, Wien/AT)
15.-20.07.	PETS 2024 (University of Bristol, Bristol/UK)
18.07.	14. Tag der IT-Sicherheit (CyberForum, IHK, KA-IT-Si, KASTEL, Karlsruhe)
August 2024	
03.-08.08.	Black Hat USA 2024 (Black Hat, Las Vegas/US)

Fundsache

Der Verizon 2024 Data Breach Investigations Report vom 01.05.2024 analysiert über 30.000 Sicherheitsvorfälle aus dem Zeitraum vom 01.11.2022 bis 31.10.2023 und bietet interessante Einsichten über deren häufigste Ursachen (gestohlene Credentials vor Ransomware und Exploits), Motive (Geld, nicht Spionage) und Täter (Organisierte Kriminalität). Lesenswert.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Paul Blenderman, Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende (Editorial), Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2024



Impertinent

Die Vertraulichkeit der Kommunikation ist ein seit Jahrhunderten umstrittenes Grundrecht. Die Möglichkeit vermeintlich geschützte Nachrichten heimlich mitzulesen brachte eine Königin aufs Schafott, die USA in den ersten Weltkrieg und 1943 die Entscheidung im U-Boot-Krieg. Nach dem Scheitern des Clipper Chip unter Clinton 1996 und dem vergeblichen Versuch der Nachrichtendienste, die Exportverbote für Verschlüsselungslösungen ins neue Jahrtausend zu retten, verlegte sich die NSA aufs Tricksen und Täuschen, wie Edward Snowden 2013 nachwies – von der Analyse des transatlantischen Datenverkehrs bis zum Einbau von Hintertüren in Router und standardisierte Verschlüsselungsverfahren.

Doch starke Verschlüsselung verbreitet sich: Technisch ist sie in vielen Bereichen inzwischen Standard. Terrorismusbekämpfern und Strafverfolgern ist das ein Dorn im Auge: Online-Durchsuchungen sind nur in seltenen Ausnahmefällen zulässig, die Technik der IMSI-Catcher funktioniert nicht in 5G- und 6G-Netzen und die umstrittene Chat-Kontrolle der EU ließ sich bisher nicht durchsetzen.

In einem am 10.06.2024 publizierten 56-seitigen „First Report On Encryption“ der EU-Bedarfsträger werden nun die Herausforderungen zunehmender Verschlüsselung für die Arbeit von Ermittlungsbehörden beschworen, die nach Ansicht der Autoren regulative Eingriffe zur Verhinderung unumgehbarer Verschlüsselung erfordern.

Wie so oft wird dabei behauptet, es gehe um das Spannungsverhältnis von „privacy of individuals and collective security“ – was suggeriert, dass hier Individualwohl mit Gemeinwohl kollidiert.

Tatsächlich ist es umgekehrt: Für eine technische Möglichkeit zur Aufklärung von Straftaten, deren Wirksamkeit bis heute nicht nachgewiesen ist, soll das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme der gesamten Gesellschaft beschränkt werden – eine Posse.



Inhalt

Impertinent

Security News

Und wieder die Supply Chain

Maskerade

Gefunden im Netz

Apple setzt Privacy-Maßstäbe

Sprachdisharmonie

Kein Anschluss unter dieser Nummer

Secorvo News

Wissen ist Macht

14. Tag der IT-Sicherheit

Wer die Wahl hat...

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Und wieder die Supply Chain

Am 25.06.2024 warnte Sansec, dass die vom Web-Team der Financial Times im Oktober 2014 initiierte Open-Source-Bibliothek polyfill.io (zur Unterstützung neuer JavaScript APIs in älteren Browsern) Malware verteilt. Die Domäne und das Github Repository der von einer mindestens sechsstelligen Anzahl Hosts genutzten Bibliothek hatte der chinesische Content-Delivery-Network-Betreiber (CDN) Funnull im Februar 2024 erworben. Daher riet der ursprüngliche Autor Andrew Betts schon am 24.02. 2024 dringend davon ab, sie noch zu verwenden.

Der Registrar Namecheap, bei dem Polyfill.io registriert war, hat nach dem Bekanntwerden des Angriffs die DNS-Einträge gelöscht. Webseitenanbieter können auf alternative Implementierungen der CDNs Cloudflare oder Fastly zurückgreifen; Cloudflare ersetzt gefährliche polyfill.io-Links automatisch durch Links auf die eigene Implementierung. In Browsern kann der Adblocker uBlockOrigin helfen; bei ihm sind die betroffenen URLs in den Blocklisten enthalten.

Schutz vor derartigen Supply-Chain-Angriffen kann Subresource Integrity bieten: Damit erkennen Browser manipulierte Bibliotheken am Hashwert. In diesem Fall ist es allerdings nicht praktikabel, da Polyfill für jeden Useragent individuell zusammengestellt wird. Schon im September 2017 berichteten wir über solche Supply-Chain-Angriffe, die sich seitdem angesichts der zunehmenden Nutzung fremder Bibliotheken wachsender Beliebtheit bei Angreifern mit Zeit und Ressourcen erfreuen – höchste Zeit also, dass sich Unternehmen mit sicherer Software-Entwicklung beschäftigten.

Maskerade

Moderne Malware installiert sich häufig nicht, wenn sie Sandboxen oder Analysesoftware entdeckt – beides Hinweise auf Systeme von Sicherheitsforschern. Das Windows-Tool Cyber Scarecrow nutzt diese Eigenschaft, um Malware abzuschrecken, indem es ein Analysesystem vortäuscht. Der Code ist allerdings nicht offengelegt und die Autoren verraten von sich nur, dass sie „cybersecurity researcher living in UK“ seien.

Die Idee ist nicht neu: Auch das schon ein wenig in die Jahre gekommene Fake-Sandbox-Artifacts (April 2020) simuliert eine virtualisierte Umgebung. Im Unterschied zu Cyber Scarecrow ist es jedoch Open Source.

Leider ist der Nutzen solcher Tools eher gering: 2019 schätzte Symantec den Anteil an Malware, die virtuelle Maschinen erkennt, auf 15-20%. Zudem verwenden die meisten dieser Malware-Varianten ein schwer zu täuschendes Fingerprinting. Und schließlich würde eine Verbreitung solcher Tools sehr bald dazu führen, dass Malware ihrerseits die Maskerade entlarvt.

Gefunden im Netz

Das LAG Düsseldorf hat am 10.04.2024 entschieden, dass Arbeitgeber Bewerber informieren müssen, wenn sie potentielle neue Mitarbeiter „googeln“ und die daraus gewonnenen Erkenntnisse im Bewerbungsprozess nutzen. Wird er nicht darüber informiert, kann der Bewerber Anspruch auf eine Entschädigung nach Art. 82 DSGVO fordern. Unternehmen sollten daher ihre Datenschutzinformationen für Bewerber um den Hinweis ergänzen, dass sie Informationen, die im Internet und in sozialen Netzwerken zu finden sind, im Rahmen des Bewerbungsprozesses nutzen. Rechtsgrundlage dieser Verarbeitung ist Art. 6 Abs. 1 b) DSGVO.

Apple setzt Privacy-Maßstäbe

Apple hat auf der Entwicklerkonferenz WWDC am 10.06.2024 „Private Cloud Compute“ vorgestellt – Apples Confidential Computing zur Auswertung von AI-Modellen in der Cloud, quasi als Koprozessor für das iPhone.

Dabei soll die Privatsphäre der Anwender geschützt werden. Kern der Umsetzung sind Rechenknoten, die Apple-eigene Hardware mit einem angepassten Apple-Betriebssystem verwenden und Sicherheitstechnologien wie Secure Boot, Secure Enclave, Code Signing, remote Attestation und Sandboxing nutzen. Nutzeranfragen werden bei der Übertragung zum Knoten Ende-zu-Ende verschlüsselt, in der Secure Enclave verarbeitet und dann gelöscht.

Netzwerkseitig werden Metadaten minimiert; die Autorisierung verwendet Blind Signatures. Mit Oblivious HTTP werden IP-Adressen versteckt. Die Software der Knoten soll veröffentlicht werden; Endgeräte senden ihre Anfragen nur an Knoten, die eine veröffentlichte Version der Software ausführen und gültige Zertifikate besitzen. Forscher, die die Sicherheitsversprechen prüfen und Fehler finden, belohnt Apple im Rahmen des Bug-Bounty-Programms.

Apple setzt damit Maßstäbe für Privacy by Design. Zwar „erkundet“ OpenAI Vergleichbares, bietet AWS mit AWS Nitro eine Plattform, die ähnliche Anwendungen ermöglichen könnte und setzt Azure sogar auf Hardwareunterstützung durch Nvidia Confidential Computing – es ist aber nicht bekannt, dass ein AI-Betreiber diese Technologie bereits einsetzt.

Der Sicherheitsforscher Matthew Green fasst es so zusammen: „Indeed, if you gave an excellent team a huge pile of money and told them to build the best 'private' cloud in the world, it would probably look like this."

Hersteller, die AI-Funktionen in ihre Software integrieren, möchten ihre AI-Modelle zunehmend auf den Geräten der Nutzer auswerten. Die von Apple eingesetzten Techniken können auch helfen, die AI-Modelle auf diesen Endgeräten zu schützen.

Sprachdisharmonie

Eines der Ziele der EU ist die Harmonisierung des europäischen Rechts. Häufig ist dabei jedoch die Sprachvielfalt eine Hürde. So veröffentlichte der Europäische Datenschutzausschuss am 17.05.2024 eine Orientierungshilfe für kleine und mittlere Unternehmen zum Datenschutz in deutscher Sprache. Eine gute Sache, würden darin nicht sprachliche Fehler den EU-Bürgern gänzlich neue Rechte verschaffen: das „Recht auf Information" (Art. 13) und das „Recht auf Zugang" (Art. 15). Wer die offizielle deutsche Fassung der DSGVO zur Hand nimmt, wird darin beides vergeblich suchen. Höchstwahrscheinlich wurde hier die englische Fassung (mittels Maschine?) fehlerhaft übersetzt.

Übersetzungsfehler finden sich nicht nur in abgeleiteten Dokumenten, sondern sogar in den Gesetzestexten selbst, wie beispielsweise in der NIS-2-Richtlinie: „Human resources security" (Art. 21 i) hat mit der „Sicherheit des Personals" wenig zu tun.

Um Fehlinterpretationen zu vermeiden sollte man sich daher bei juristischen Texten nicht auf automatische (z. B. KI-gestützte) Übersetzungen verlassen, sondern kritisch prüfen, was im Originaltext steht und überlegen, worauf der Gesetzgeber abzielen wollte.

Kein Anschluss unter dieser Nummer

Nicht selten werden bei Tiefbauarbeiten Telekommunikationskabel beschädigt. Sind davon Gerichte betroffen, wie am 26.06.2024 das Bundesverfassungsgericht, können Verfahrensbeteiligte es nicht mehr per Fax erreichen und sind auf den Postweg angewiesen. Die Einführung der digitalen Verfassungsbeschwerde zum 01.08.2024 dürfte das Problem etwas entschärfen. Zwar wirkt eine „Wiedereinsetzung in den vorigen Stand" fristwahrend (§ 93 Abs. 4 BVerfGG); zu Entscheidungsverzögerungen in Eilverfahren könnte es bei einem Verbindungsausfall jedoch auch bei digitalen Einreichungen kommen – mit ggf. unangenehmen Folgen für die Beschwerdeführer.

Redundante Standortanbindungen, die zwei Faserpaare oder Kabel in derselben Trasse verwenden oder vom gleichen Provider versorgt werden, beseitigen das Risiko jedoch nicht. Da viele Provider zudem die Infrastruktur der Deutschen Telekom verwenden, ist eine echte Risikostreuung gar nicht einfach. Vor Gericht und auf hoher See ist man eben auch IT-technisch in Gottes Hand.

Secorvo News

Wissen ist Macht

Buchen Sie sich neben Ihrem wohlverdienten Urlaub doch noch schnell Ihre Weiterbildung für das 2. Halbjahr 2024. Nach der Sommerpause können Sie sich mit unseren kompakten IT Security Insights vom **10.** bis **11.09.2024** in der Informationssicherheit und im Datenschutz updaten. Auf das T.I.S.P.-Zertifikat bereiten wir Sie vom **23.** bis **27.09.2024** vor. Und im November machen wir Sie vom **25.** bis **28.11.2024** zum Experten in sicherer Software-Entwicklung. Wir freuen uns auf Ihre Anmeldung.

14. Tag der IT-Sicherheit

Am **18.07.2024** bietet Ihnen der Karlsruher Tag der IT-Sicherheit zum 14. Mal die Möglichkeit, sich über aktuelle IT-Sicherheitsthemen wie AI oder NIS2 und Präventionsmaßnahmen für Unternehmen zu informieren. Die Keynote hält Ralf Wigand, National Security and IT-Compliance Officer von Microsoft Deutschland. Lernen Sie interessante IT-Sicherheits-Start-Ups kennen und nutzen Sie in der Network-Pause die Gelegenheit zum Erfahrungsaustausch mit Teilnehmern und Referenten. Hier finden Sie das Programm und die Möglichkeit zur Anmeldung.

Wer die Wahl hat...

Beim nächsten KA-IT-Si-Event am **19.09.2024** gibt Prof. Melanie Volkamer (KIT) einen Überblick zu den Sicherheitsherausforderungen bei Internet-Wahlen und -Abstimmungen. Anschließend erwartet Sie der beliebte Erfahrungsaustausch beim „Buffet-Networking".

Merken Sie sich den Termin schon vor, der Sommer vergeht schneller als man denkt... Wir freuen uns auf Sie – und empfehlen Ihnen wie immer eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2024	
15.-20.07.	PETS 2024 (University of Bristol, Bristol/UK)
18.07.	14. Tag der IT-Sicherheit (CyberForum, IHK, KA-IT-Si, KASTEL, Karlsruhe)
August 2024	
03.-08.08.	Black Hat USA 2024 (Black Hat, Las Vegas/US)
08.-11.08.	DEFCON 32 (Las Vegas/US)
11.-13.08.	SOUPS 2024 (usenix, Philadelphia/US)
14.-18.08.	33rd USENIX Security Symposium (usenix, Philadelphia/US)
18.-22.08.	Crypto2024 (IACR, Santa Barbara/US)
September 2024	
10.-11.09.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
19.09.	KA-IT-Si-Event "Wer die Wahl hat..." (KA-IT-Si, Karlsruhe)
23.-27.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
25.-26.09.	heise devSec 2024 (dpunkt.verlag, heise, Köln)

Fundsache

Als Hilfestellung für Beschwerden zum EU-US Data Privacy Framework hat die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Formulare bereitgestellt.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2024



Manchmal muss man müssen wollen...

Seit Monaten werden in einschlägigen Medien Drohkulissen aufgebaut, wie sehr die deutschen Unternehmen von neuen Regularien zur Cybersicherheit durch die Umsetzung von NIS-2 geknechtet werden sollen. Man liest sogar, dass Unternehmen bis zum 17.10.2024 schier unerfüllbare Anforderungen umsetzen müssten.

Dabei galt die Oktoberfrist nie für Unternehmen, sondern war eine Frist für den deutschen Gesetzgeber, die EU-Richtlinie NIS-2 in geltendes Recht zu überführen. Nachdem das Bundeskabinett am 24.07.2024 endlich einen Entwurf für das NIS2UmsG beschlossen hat, wird dieser wohl in absehbarer Zeit zu deutschem Recht werden.

Das Gesetz sieht keine Umsetzungsfrist vor, aber die betroffenen ca. 29.500 Unternehmen haben voraussichtlich drei Jahre Zeit, bis sie die Anforderungen nachweisen müssen. Doch zaubert NIS-2 keine überraschend neuen Anforderungen aus dem Hut. Tatsächlich traut der Gesetzgeber der Wirtschaft offensichtlich nicht zu, Cybersicherheit angemessen umzusetzen und fordert daher legislativ, was schon lange als Good Practice gilt. Wer seine Informationssicherheit nach etablierten Standards wie ISO 27001 oder IT-Grundschutz umgesetzt hat, kann den neuen Anforderungen erst einmal gelassen entgegensehen, auch wenn sich die Details der Umsetzungvorgaben noch in der Abstimmung befinden.

Dass die zusätzliche Bürokratie die Cybersecurity in Deutschland faktisch verbessern wird, wage ich zu bezweifeln. Ich wünsche mir, dass Unternehmen, die Cybersecurity bisher stiefmütterlich behandelt haben, die ungeliebten Gesetzesanforderungen nicht nur mit minimalem Aufwand gerade so erfüllen, sondern dass sie die Chance nutzen, sich wirksam vor aktuellen Bedrohungen zu schützen.

Manchmal muss man eben auch müssen wollen.



Inhalt

Manchmal muss man müssen wollen...

Security News

Unschärfen

Selbstverständlichkeiten

Unverträglichkeiten

Vertrauenswürdigkeiten

Örtlichkeiten

Nebensächlichkeiten

Secorvo News

Fachseminare

Wer die Wahl hat...

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Unschärfen

Andrea Pierini, Sicherheitsforscher und schon im Jahr 2022 auf dem Microsoft Researcher Recognition Program Leaderboard zu finden, berichtete am 12.07.2024, dass er zeitgleich mit einem anderen Forscher eine neue Schwachstelle an Microsoft gemeldet hatte. Während seine Meldung als „mittelschwer" zurückgestellt wurde, führte die andere zu CVE-2024-38061 und der Aufnahme in den Juli-Patchday.

Der Fall belegt, dass die vermeintlich exakte CVSS-Schwachstellenbewertung – eine Kennzahl aus ca. einem Dutzend Einzelkriterien – eben doch mehr oder minder große Ermessensspielräume zulässt: Ist die Komplexität des Angriffs niedrig oder hoch? Wie schwer wirkt sich ein Integritätsverlust auf nachfolgende Systeme aus?

Dies macht den Vorteil der Komplexitätsreduktion durch eine CVSS-Maßzahl ein Stückweit zunichte. Sicherlich wird man bei 9er- oder 10er-Schwachstellen in der IT-Infrastruktur sofort handeln müssen. Aber zwischen den CVSS-Schwellenwerten für „alles andere stehen und liegen lassen" und „machen wir, wenn Zeit dafür ist" gibt es einen wohl eher breiten Graubereich, in dem man die Einzelbewertungen und deren Relevanz für die eigene Umgebung überprüfen sollte.

Selbstverständlichkeiten

Am 14.06.2024 berichtete der Landesbeauftragte für den Datenschutz Niedersachsen über eine von seiner Behörde vorgenommene anlassunabhängige Datenschutzprüfung, bei der über das Internet erreichbare Microsoft-Exchange-Server niedersächsischer Unternehmen auf Verwundbarkeiten untersucht wurden. Dabei wurden 20 Server mit kritischen Schwachstellen gefunden. Die Aufsichtsbehörde wertet das Fehlen aktueller Patches als Verstoß gegen die Pflicht, die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten (Art. 32 DSGVO). Statt eines Bußgelds erhielten die Unternehmen allerdings nur eine Verwarnung.

Schon am 26.03.2024 hatte das BSI berichtet, dass mindestens 17.000 öffentlich erreichbare Microsoft-Exchange-Server kritische Schwachstellen besitzen. Offenbar kümmern sich einige Organisationen nicht um die Aktualisierung ihrer direkt am Internet betriebenen Exchange-Server, die oft einen Zugang über Outlook Web Access (OWA) oder IMAP4 bieten. Beides verwendet in der Regel nur eine Passwortauthentifizierung.

Die verwarnten niedersächsischen Unternehmen haben inzwischen die seit 2021 bekannten Sicherheitslücken durch Patches geschlossen. Wenn man nicht zu Microsoft in die Cloud wechseln möchte, sollte man daher ein E-Mail-Gateway vorschalten und für den Clientzugriff eine VPN-Lösung mit starker Authentifizierung verwenden.

Unverträglichkeiten

„Legacy" und „Kryptoverfahren" sind zwei Begriffe, die sich nicht gut vertragen. Das war so bei der Erzeugung von (EC)DSA-Nonces in PuTTY (siehe SSN 05/2024). Und es ist so bei der Authentisierung von Nachrichten zwischen einem Switch oder Access-Point und dem RADIUS-Authentifikationsserver. Dabei wird seit Mitte der Neunzigerjahre ein Keyed-MD5-Hash verwendet. Dass das nicht der Weisheit letzter Schluss ist, weiß man spätestens seit den Angriffen auf MD5 (1996) und der Standardisierung der HMAC-Konstruktion (1997). Dennoch behielt man das Verfahren bei, weil die Schwachstelle vermeintlich schwer ausnutzbar war und es keine praktischen Angriffe gab.

Am 09.07.2024 veröffentlichte nun ein internationales Forscherteam den praktisch umsetzbaren Blast-RADIUS-Angriff. Damit kann ein Man-in-the-Middle-Angreifer eine Authentifizierungsanfrage stellen, deren erwartungsgemäße Ablehnung durch den RADIUS-Server er zu einer „authentischen" Akzeptanz umändern kann. Als Reaktion wird nun der RADIUS-Standard überarbeitet, um RADIUS-Nachrichten per TLS/DTLS zu schützen. Das ist seit 2012 bzw. 2014 in den „experimental" RFCs 6614 und 7360 vorgesehen, die auch von einigen Herstellern implementiert wurden.

Bei Legacy-Kryptoverfahren sollte man eher früher als später zu Nachfolgern wechseln – bevor die Hoffnung, dass es schon irgendwie gut gehen wird, durch praktikable Angriffe ein jähes Ende findet.

Vertrauenswürdigkeiten

Google hat am 27.06.2024 angekündigt, dass der Chrome-Browser ab Version 127 keinem Zertifikat mehr vertraut, das auf die Root-CAs von Entrust und AffirmTrust zurückgeht und nach dem 31.10. 2024 ausgestellt wird. Google begründet diesen Schritt mit einer langen Liste von Verfehlungen seitens Entrust, wie verzögert vorgelegte Berichte, schuldhaftes Ausbleiben von Zertifikatrückrufen und Verwendung von unzulässigen Zeichen in Zertifikatseinträgen. Mangels hinreichender Aussicht auf Besserung greife Google nun zu dieser Maßnahme.

Schon öfter hat Google Trust-Center aus eigenen Root-Stores verbannt: 2015 Symantec/Verisign aus Chrome und Android – Mozilla (Firefox) und Apple

(Safari) zogen kurz darauf nach. 2021 flog Camerfirma aus Chrome, 2023 TrustCor und im Mai 2024 Globaltrust. Dokumentiert und nachverfolgt werden Verfehlungen über Bugzilla bei der Mozilla Foundation.

In diesem Zusammenhang ist Bug 1877388 vom 29.01.2024 interessant, der die Deutsche Telekom betrifft. Auslöser war ein Verzug bei der Sperrung mehrerer nicht ganz dem vorgegebenen Profil entsprechender Zertifikate. Die Telekom begründet die Verzögerung damit, dass die betroffenen Kunden wichtige Infrastrukturen betreiben und nicht in der Lage sind, die Zertifikate rechtzeitig auszutauschen. Im Laufe der Diskussion mit den Aufsehern der Browser-Hersteller wurden grundsätzliche Fragen aufgeworfen, darunter solche über die personellen Kapazitäten der Telekom.

CAs in den Root-Stores müssen dauerhaft vertrauenswürdig sein. Daher ist es wichtig, Verstöße zu verfolgen, die die Vertrauenswürdigkeit beeinträchtigen. Dabei dürfen aber keine unterschiedlichen Maßstäbe angelegt werden – sonst steht irgendwann das Vertrauen in die Zertifikatsinfrastruktur als Ganze in Frage.

Örtlichkeiten

Netzpolitik.org und Bayrischer Rundfunk (BR) haben am 16.07.2024 Hintergründe zum Handel mit Standortdaten aufgedeckt: Databroker bieten die Datensätze auf Online-Marktplätzen an, sogar als Abo, das stündlich Updates der Nutzerdaten liefert – ein Milliardengeschäft. Die Daten werden vor allem von Apps geliefert, die neben Nutzungsdaten auch Standortinformationen erfassen, und ließen sich mühelos über einfache Online-Recherchen natürlichen Personen zuordnen.

Geschäftsmodelle mit eindeutigen Werbe-IDs und Kategorisierungen sind lange bekannt (siehe z. B. SSN 5/2022). Mit Standortdaten können jedoch Bewegungs-Profile erstellt werden, die Rückschlüsse auf Arbeitsplatz, politische oder religiöse Überzeugungen und Arztbesuche zulassen. Inzwischen läuten auch bei amerikanischen Senatoren die Alarmglocken: Bewegungsdaten können auch verdeckte Ermittler und Geheimdienstmitarbeiter enttarnen.

Wie man seine Werbe-ID zurücksetzt, erläutern Netzpolitik.org, BR und Heise. Zur Erstellung von Nutzerprofilen werden jedoch auch andere Identifikatoren verwendet, die später eine Zuordnung und Zusammenführung der Bewegungsdaten ermöglichen können. Offenbar schrecken drohende Datenschutzbußgelder die Anbieter nicht ab – bleibt als letzte Instanz der Gesetzgeber, um solche Grundrechtsverstöße wirksam zu unterbinden.

Nebensächlichkeiten

Wenn ein Hersteller neue KI-basierte Cloud-Dienste implementiert, werden offenbar gelegentlich eher herkömmliche Aspekte wie Netzwerksicherheit, Firewalling oder der Umgang mit Credentials zu vermeintlichen Nebensächlichkeiten.

So wurde am 17.07.2024 ein Angriff auf den SAP AI Core Dienst unter dem Namen SAPwned veröffentlicht, der sich zunutze macht, dass der Anwender einen Prozess unter der User-ID des integrierten Istio-Proxys starten konnte – und die ist von den IP-Firewall-Regeln ausgenommen. Nach Überwindung dieser Hürde konnte ein Angreifer auf Credentials und offene Dienste zugreifen, mit denen er praktisch die gesamte Cloud-Umgebung übernehmen konnte.

Merke: Insbesondere bei *-as-a-Service darf die Software-Sicherheit nicht beim Code aufhören – auch Deployment und Konfiguration sind sicherheitskritisch und müssen beachtet werden.

Secorvo News

Fachseminare

Haben Sie noch Spielraum im Weiterbildungsbudget? Dann werfen Sie doch einen Blick auf unsere Fachseminare im Herbst. So bereiten wir Sie vom **23. bis 27.09.2024** mit unserem T.I.S.P.-Seminar auf die Zertifizierung als Informationssicherheitsexperte vor, und vom **15. bis 17.10.2024** bilden wir Sie zum Vorfall-Experten nach dem Curriculum des BSI aus. Wir freuen uns auf Ihre Anmeldung.

Weitere Informationen und die Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

Wer die Wahl hat…

Wahlen und Abstimmungen – in Vereinen, Organisationen, Gemeinden, Land und Bund – sind organisatorische und manchmal auch logistische Herausforderungen. Was liegt da näher, als sie zu „digitalisieren“?

Beim KA-IT-Si-Event am **12.09.2024** beleuchtet Frau Professorin Melanie Volkamer (Secuso, KIT) die Sicherheitsanforderungen an Internet-Wahlen und -Abstimmungen, stellt praktische Beispiele vor und diskutiert die Vor- und Nachteile ihres Einsatzes.

Anschließend erwartet Sie natürlich der Erfahrungsaustausch beim „Buffet-Networking“. Wir freuen uns darauf, Sie in der „Church“ des CyberForum zu sehen – und empfehlen wie immer eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2024	
03.-08.08.	Blackhat US 2024 (Blackhat, Las Vegas/US)
08.-11.08.	Defcon 32 (DEFCON, Las Vegas/US)
11.-13.08.	SOUPS 2024 (usenix, Philadelphia/US)
14.-16.08.	33nd USENIX Security Symposium (usenix, Philadelphia/US)
18.-22.08.	Crypto 2024 (IACR, Santa Barbara/US)
September 2024	
04.-05.09.	Annual Privacy Forum 2024 (ENISA, DG Connect and Karlstad University, Karlstad/SWE)
11.-12.09.	secIT digital (Heise Medien, virtuell)
12.09.	KA-IT-Si-Event „Wer die Wahl hat…“ (KA-IT-Si, Karlsruhe)
12.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
19.-20.09.	37. Kryptotag (GI, Nürnberg)
23.-27.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
25.-26.09.	heise DevSec 2024 (iX, heise Security, dpunkt.Verlag, Köln)

Fundsache

Der Orientierungshilfen-Navigator des LfDI Baden-Württemberg gibt einen Überblick über die Orientierungshilfen zu den datenschutzrechtlichen Implikationen der KI-Verordnung.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Paul Blenderman, Robert Eitel, Kai Jendrian (Editorial), Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2024



Halluzinierte Wirklichkeit

Alter Wein in neuen Schläuchen – danach klingt die aktuelle KI-Euphorie, zumindest in den Ohren derjenigen, die die zahlreichen KI-Wellen der vergangenen 40 Jahre miterlebt haben. Neu ist allerdings die beeindruckende Leistungsfähigkeit heutiger Sprachmodelle. Da vergisst man leicht, dass sie wenig anderes liefern als eine Prognose für das nächste Wort. Dass wir einer auf Wort-Wahrscheinlichkeiten basierenden Ausgabe einen Sinn beimessen, verrät vielleicht mehr über unser eigenes Denken als über die KI.

„Wissen" in unserem bisherigen Verständnis besitzt ein Sprachmodell allerdings nicht: Ein Wikipedia-Eintrag und oft auch eine Internet-Recherche sind in der Regel zuverlässiger als die Antwort eines Chatbots. Etwas zugespitzt ist ein KI-Chatbot ein Dilettant, der sich gut ausdrücken kann – ein Blender.

Was aber macht ein Blender, wenn er nicht mehr weiter weiß? Er „ergänzt" seine Ausführungen auf der Grundlage seines Halbwissens kreativ. Bei einem Chatbot nennt man das „Halluzinieren": Namen, Daten und Fakten niedrigerer Wahrscheinlichkeiten werden hinzugefügt. Das Ergebnis hat dann bestenfalls noch am Rande etwas mit der Wirklichkeit zu tun – ist aber hübsch formuliert.

Sprachmodelle werden derzeit vorwiegend wie ein „Orakel" zu allen möglichen Themen befragt. Die Ergebnisse werden meist separat verarbeitet – im Kopf, in Dokumenten, in Datenbanken. Genau hier liegt die eigentliche Gefahr: „Halluzinierte" oder auch nur „nicht ganz richtige" Ausgaben finden zunehmend Eingang in Überzeugungen und seriöse Dokumente: Presseartikel, Studien, Datenbanken.

Darunter finden sich auch Angaben über Personen. Art. 14 DSGVO verpflichtet Verarbeiter, Betroffene über die Verarbeitung personenbezogener Daten zu informieren, die nicht direkt bei diesen erhoben wurden – damit wird Datenschutz zum Chatbot-Korrekturfilter. Hilfreich. Solange er nicht missachtet wird.



Inhalt

Halluzinierte Wirklichkeit

Security News

Ferngesteuerte Kraftwerke

Undifferenzierte Integration

Reanimierte Sicherheitslücke

Mitverantwortung

KRITIS-Prüfungen neu geregelt

Patientendatenschutz

Fatales Update

Secorvo News

Weiterbildung

Software ist sicher. Und die Erde eine Scheibe.

Veranstaltungshinweise

secorvo
security consulting

Security News

Ferngesteuerte Kraftwerke

Forscher vom niederländischen Institut DIVD haben am 12.08.2024 gleich sechs Schwachstellen in den Gateways des amerikanischen Photovoltaik-Giganten Enphase publiziert. Die Gateways verbinden die PV-Anlagen mit der Cloudplattform des Herstellers. Schon am 17.04.2021 hatte das DIVD in einem GitHub-Repository ein Administrator-Passwort für die Cloudplattform des chinesischen PV-Herstellers SolarMan gefunden, und am 07.08.2024 berichtete Bitdefender über eine Schwachstelle in der Authentifizierung der SolarMan-Cloudplattform.

Das Problem ist gravierend: Die Web-Oberflächen liefern nicht nur hübsche Grafiken über die Produktion der Paneele, sondern können die Anlagen aus der Ferne steuern oder neue Firmware einspielen. Angriffe auf die Anlagen eines Herstellers könnten das Stromnetz empfindlich stören, denn solche Cloud-Server steuern Millionen von PV-Anlagen – das Äquivalent von dutzenden Kraftwerken, wie Bert Hubert in seinem Blog argumentiert. Während für konventionelle Kraftwerke strenge Vorschriften gelten, werden diese Plattformen hingegen wie simple Geburtstagskalender behandelt.

Undifferenzierte Integration

Microsoft-Forscher berichteten am 29.07.2024 von einer Schwachstelle in VMware ESXi, die bereits von Ransomware ausgenutzt werde: Integriert man das System in ein Active Directory (AD), gewährt die Software implizit einer AD-Gruppe „ESX Admins“ volle Administratorrechte auf dem Hypervisor. VMware hat die Schwachstelle mittlerweile geschlossen (CVE-2024-37085).

Die Sicherheitslücke konnte ausgenutzt werden, weil viele IT-Abteilungen die Administration ihrer Infrastruktur wie eine beliebige Büro-Anwendung in das produktive AD integriert haben. Das ist keine gute Idee: Will man die Virtualisierung, die Storage-Systeme, die Switches und Router in ein AD integrieren, gehören sie in eine separate, rein administrative Domäne, die vom produktiven Forest netzwerktechnisch und logisch getrennt ist. Das kann man mit dem Konzept einer „Bastionumgebung“ kombinieren, wie von Microsoft ausführlich beschrieben.

Reanimierte Sicherheitslücke

Qualys Labs hat am 01.07.2024 berichtet eine bereits 2006 geschlossene Schwachstelle in OpenSSH entdeckt zu haben, die durch eine Überarbeitung des Codes versehentlich erneut eingebaut wurde. Die wiederauferstandene Schwachstelle wurde „RegreSSHion“ getauft, da im Entwicklungsprozess nicht sichergestellt wurde, dass einmal behobene Fehler durch spätere Änderungen nicht abermals implementiert werden. Solche Regressionstests sollten gerade bei sicherheitsrelevanten Softwareprojekten Standard sein.

Mitverantwortung

Die Rechtbank Amsterdam hat am 07.06.2024 erstinstanzlich entschieden, dass für Tracking-Cookies verantwortlich ist, wer sie entwickelt, Webseitenbetreibern zur Verfügung stellt und im Zuge dessen auch Vereinbarungen über die Datenschutzbestimmungen trifft. Diese Unternehmen legen fest, welche personenbezogenen Daten zu welchen Zwecken und mit welchen Mitteln verarbeitet werden. Eine Abwälzung der Verantwortung für die Einholung einer wirksamen Einwilligung auf die Webseitenbetreiber sei nicht rechtskonform.

Microsoft, LinkedIn und Xandr wurde daher untersagt, Tracking Cookies zu verwenden, wenn keine ausdrückliche Einwilligung der Betroffenen vorliegt. Diese Auffassung ist konsequent und folgt den Vorgaben des EuGH (Urteil zu IAB Europe vom 07.03.2024). Webseitenbetreiber und Urheber von Cookies müssen im Zweifel gemeinsam dafür Sorge tragen, dass der Einsatz rechtmäßig erfolgt.

KRITIS-Prüfungen neu geregelt

Am 19.08.2024 hat das BSI die überarbeiteten Grundsätzlichen Anforderungen im Nachweisverfahren (GAiN) veröffentlicht. Darin wird die Durchführung von KRITIS-Prüfungen nach § 8a (3) BSIG verbindlich geregelt. Überraschende Neuerungen finden sich nicht; die konkretisierten Anforderungen zur Gestaltung von Geltungsbereich (N.DG.01) und Netzplan (N.DG.02) dürften für Betreiber der wichtigste Aspekt sein und möglicherweise Handlungsbedarf erzeugen. Eine gute Zusammenfassung der Änderungen findet sich bei OpenKRITIS.

Patientendatenschutz

Den Schutz von Patientendaten fordert nicht nur das Datenschutzrecht, sondern auch das Patientengeheimnis, dessen Verletzung nach § 203 StGB strafbewehrt ist. Einzelne gesetzliche Krankenkassen kümmert das offenbar wenig – sie lassen sich bei Beratungsterminen von Versicherten nebulöse (und damit rechtsunwirksame) Einwilligungen zur „Verarbeitung von medizinischen Informationen“ unterzeichnen, mit denen sie dann Diagnosen und Berichte von Ärzten und Krankenhäusern anfordern. Eine solche Weitergabe kann ohne die expli-

zite Entbindung von der ärztlichen Schweigepflicht durch den Patienten eine Straftat sein.

Die Datenschutz-Aufsichtsbehörde Hessen setzte dieser Praxis bei einer besonders offensiven Krankenkasse nach einer Datenschutz-Beschwerde von Secorvo am 09.07.2024 ein Ende. Weitere Beschwerden sind derzeit bei anderen Datenschutz-Aufsichtsbehörden in Bearbeitung.

Fatales Update

Es wurde in allen Medien berichtet: Ein fehlerhaftes Update von CrowdStrike für das EDR-Produkt Falcon führte am 19.07.2024 bei geschätzt 8,5 Millionen Windows-Rechnern dazu, dass die Systeme ständig abstürzten – viele schon bevor sie ein korrigiertes Update herunterladen konnten. Zahlreiche Kunden benötigten bis zu zwei Tage, um die betroffenen Systeme manuell instand zu setzen. Der Vorfall verursachte Ausfälle an Flughäfen, bei Banken und in Krankenhäusern. Fitch Ratings schätzte am 22.07.2024 allein den versicherten Schaden auf einen mittleren bis hohen einstelligen Milliardenbetrag.

Der Tenor der Nachrichten war, dass das Sicherheitsprodukt selbst zu einem Sicherheitsproblem geworden sei. Diese Bewertung greift jedoch zu kurz, denn unabhängige Tests zeigen, dass Falcon einen effektiven Schutz vor Angriffen bietet - eine Wiederherstellung nach einem erfolgreichen Angriff dürfte wesentlich länger als 1-2 Tage dauern und einen viel höheren Schaden verursachen.

Allerdings hat das Update-Verfahren – wie CrowdStrike am 06.08.2024 selbst einräumte – erhebliche Schwächen. Auch Microsoft sieht sich in der Mitverantwortung und kündigte am 27.07.2024 an, die Antimalware-Hersteller besser dabei zu unterstützen, dass sie nur in seltenen Fällen auf Kernel-Prozesse zugreifen müssen, damit Programmfehler nicht das Betriebssystem in Mitleidenschaft ziehen.

Secorvo News

Weiterbildung

Im Herbst 2024 erwarten Sie vier Zertifizierungs- und Fachseminare bei Secorvo. Das Seminar Vorfall-Experte (BSI) vom **15. bis 17.10.2024** bereitet Sie auf die Zertifizierung durch das BSI vor. Auf dem PKI-Seminar vom **04. bis 07.11.2024** lernen Sie von unseren PKI-Experten alles Erforderliche von den Grundlagen bis zu Planung und Betrieb Ihrer eigenen PKI.

Möchten Sie Teil der über 2.000 Mitglieder starken T.I.S.P.-Community werden? Das gelingt mit unserem T.I.S.P.-Seminar vom **11. bis 15.11.2024** und der anschließenden Zertifikatsprüfung.

Beim T.P.S.S.E.-Seminar vom **25. bis 28.11.2024**. dreht sich alles um die Entwicklung sicherer Software. Auch diese Qualifikation können Sie mit einer Zertifizierung abschließen. Sichern Sie sich durch eine schnelle Buchung den Frühbucherrabatt. Wir freuen uns auf Ihre Anmeldung.

Software ist sicher. Und die Erde eine Scheibe.

Der Cyber Resilience Act (CRA) legt Herstellern von Software und Open Source Communities strenge Regeln zur IT-Sicherheit ihrer Produkte auf. Zu den Anforderungen der EU-Verordnung an „Produkte mit digitalen Elementen" zählen die Erstellung einer Cybersicherheitsrisikobewertung und die Bereitstellung von Sicherheitsupdates.

Verstöße können mit bis zu 15 Millionen Euro oder 2,5 % des weltweiten Jahresumsatzes geahndet werden.

Beim KA-IT-Si-Event am **12.09.2024** gibt Markus Toran (Secorvo) einen Überblick über die gesetzlichen Regelungen, erläutert, worauf sich Hersteller, Open Source Communities und Verbraucher einstellen müssen und diskutiert, wie praktikabel und effektiv die Vorgaben sein werden.

(Der ursprünglich für diesen Tag vorgesehene Vortrag von Frau Professorin Volkamer muss verschoben werden – wird aber nachgeholt).

Anschließend erwartet Sie natürlich der Erfahrungsaustausch beim „Buffet-Networking". Wir freuen uns auf Sie in der „Church" im CyberForum – und empfehlen wie immer eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2024	
04.-05.09.	Annual Privacy Forum 2024 (ENISA, DG Connect and Karlstad University, Karlstad/SWE)
11.-12.09.	secIT digital (Heise Medien, virtuell)
12.09.	KA-IT-Si-Event „Software ist sicher. Und die Erde eine Scheibe.“ (KA-IT-Si, Karlsruhe)
19.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
19.-20.09.	37. Kryptotag (GI, Nürnberg)
25.-26.09.	heise DevSec 2024 (iX, heise Security, dpunkt.Verlag, Köln)
Oktober 2024	
14.-18.10.	ACM CSS 2024 (ACM SIGSAC, Salt Lake City/US)
15.-17.10.	Vorfall-Experte (BSI) (Secorvo, Karlsruhe)
22.10.	Swiss Cyber Storm 2024 (Swiss Cyber Storm, Bern/CH)
22.-24.10.	it-sa 2024 (itsa 365, Nürnberg)
November 2024	
04.-07.11.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
05.-07.11.	24. IDACON 2024 (WEKA Akademie, München)
11.-15.11.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Paul Blenderman, Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2024



Fantastilliarden an Schäden

Der deutsche IT-Branchenverband bitkom hat am 24.08.2024 die Ergebnisse seiner jährlichen Studie „Wirtschaftsschutz 2024“ veröffentlicht. Danach verursachte Cyberkriminalität im Vorjahr einen Schaden von 266,6 Milliarden Euro – über sechs Prozent des Bruttoinlandsprodukts 2023, fast das Vierfache des Verteidigungsetats und etwa 70 % der Summe, die die Weltbank 2023 für den Wiederaufbau der Ukraine veranschlagt hat.

Auf dem KA-IT-Si-Event „Was ko$tet die Welt?“ am 20.06.2024 haben Wiebke Reimer und Dr. Boris Hemkemeier von der Commerzbank AG gezeigt, woher die oft zitierten 5,5 Billionen Euro an weltweiten Schäden durch Cyberkriminalität pro Jahr stammen: Am Ende einer Kette von Zitaten stießen sie auf eine falsch interpretierte Schätzung des Weltwirtschaftsforums (WEF) aus dem Jahr 2014. Diese besagte lediglich, dass Cyber-Regulierung und Vorsicht der Verbraucher bis 2020 die *wirtschaftliche Nutzung innovativer Technologien* im schlimmsten Fall um drei Billionen US$ reduzieren könnten.

Die Zahlen der bitkom-Studie basieren auf einer telefonischen Befragung von Führungskräften in 1003 Unternehmen. Wie belastbar sind solche Antworten? Wie quantifiziert man beispielsweise einen Imageschaden? Offen ist auch, ob die befragten Unternehmen repräsentativ für die Gesamtwirtschaft sind. Methodisch ist es jedenfalls fragwürdig, Aussagen zu seltenen extremen Ereignissen auf die Gesamtheit der Unternehmen hochzurechnen.

Forscher von Microsoft haben bereits 2016 darauf hingewiesen, dass Umfragen ungeeignet sind, um den Gesamtschaden durch Cyberkriminalität zu ermitteln. Trotzdem werden solche Zahlen von Medien, Politik und Wirtschaft zitiert und als Grundlage für Entscheidungen herangezogen.

Warum nimmt daran niemand Anstoß?



Inhalt

Fantastilliarden an Schäden

Security News

Totgesagte leben länger

Kündigungsgrund Datenschutz

Never change...

ECDSA-Seitenkanal

Unternehmenserwerb

Illegale Datenverarbeitungen

Secorvo News

Secorvo Seminare

Wer hat, der kann.

Veranstaltungshinweise

secorvo
security consulting

Security News

Totgesagte leben länger

Ein Team von watchTowr beschrieb am 11.09.2024, wie es bei GlobalSign ein gültiges Zertifikat für die Microsoft-Domäne microsoft.mobi beantragen konnte. Zunächst hatte es regulär die Domäne dotmobiregistry.net erworben und darauf einen eigenen WHOIS-Server aufgesetzt. Die WHOIS-Server für die Top Level Domain „.mobi" waren zuvor von dieser Domäne zu whois.nic.mobi umgezogen – und die alte Domäne freigegeben worden. Für die Domain-Validierung des Zertifikatsantrags von watchTowr fragte GlobalSign die administrative E-Mail-Adresse des Domaininhabers jedoch noch bei der veralteten WHOIS-Adresse ab – die inzwischen watchTowr gehörte.

Nicht selten werden alte Domänen aufgegeben, ohne dass alle Dienstnutzer verlässlich darüber informiert wurden. Im Fall von dotmobiregistry.net war das verheerend, weil sicherheitskritische Funktionen darüber abgewickelt wurden. Vor der Freigabe einer nicht mehr benötigten Domain sollten kritische Dienste noch eine Weile weiter betreiben werden, bis wirklich sichergestellt ist, dass kein Dienstnutzer mehr darauf zugreift.

Kündigungsgrund Datenschutz

Dass ein Verstoß eines Arbeitnehmers gegen die DSGVO auch ein Kündigungsgrund sein kann, überrascht nicht. Das OLG München hat am 31.07.2024 festgestellt, dass ein Unternehmensvorstand mit der Weiterleitung von vertraulichen Unterlagen, die auch personenbezogene Daten beinhalteten, gegen die DSGVO verstößt. Selbst wenn die Vertraulichkeitspflichten aus § 93 Abs. 1 AktG nicht verletzt sind, kann die Übermittlung von personenbezogenen Daten sogar eine außerordentliche Kündigung rechtfertigen, falls dies einen „wichtigen Grund" (§ 626 Abs. 1 BGB) darstellt – sofern die Interessen beider Seiten gegeneinander abgewogen wurden. Die Grundsätze dieser Abwägung sind in der Bienenstich-Entscheidung des BAG festgelegt: Es müssen u. a. die Schwere der Pflichtverletzung, der Grad des Verschuldens, das Ausmaß des Schadens, die mögliche Wiederholungsgefahr, die Dauer des Arbeitsverhältnisses und dessen störungsfreier Verlauf sowie die sozialen Folgen für den Arbeitnehmer berücksichtigt werden.

Never change…

… a good password: Seit 2017 empfiehlt das NIST in seinen Vorgaben für „Authentication and Lifecycle Management" (SP 800-63B), dass weder regelmäßige Passwortwechsel noch sogenannte Komplexitätsvorgaben erzwungen werden sollten. Im ersten Entwurf der Neufassung vom Dezember 2022 wurde aus einer Unterlassens-Empfehlung ein Verbot („SHOULD NOT" wurde zu „SHALL NOT"). Die Verschärfung hat – wie der am 21.08.2024 veröffentlichte zweite Public Draft zeigt – die erste Kommentierungsphase überlebt, und es ist zu erwarten, dass das auch für die letzte Phase gilt, die am 07.10.2024 endet. Authentifizierungsdaten, die sich ein Mensch merken soll, müssen so gewählt werden, dass ein Mensch sie sich auch merken kann, ohne dass das Sicherheitsniveau dadurch sinkt. Weder erzwungene Wechsel noch feste Komplexitätsregeln genügen dieser Anforderung. Hingegen können längere Passwörter helfen – ein Thema, dass uns seit vielen Jahren beschäftigt (siehe SSN 06/2009, 06/2010, 02/2011, 05/2015 und 08/2015).

ECDSA-Seitenkanal

Am 03.09.2024 enthüllten französische Sicherheitsforscher eine Seitenkanal-Schwachstelle in der Krypto-Bibliothek für die Sicherheitschips von Infineon unter dem Namen EUCLEAK – einem Wortspiel aus „Euclid" und „Leak". Der Seitenkanal bezieht sich auf das Timing im erweiterten euklidischen Algorithmus, der bei einer ECDSA-Signatur das modulare Inverse der Nonce berechnet, die den privaten Schlüssel verschleiert. Die Nonce war schon mehrfach ein Schwachpunkt bei Angriffen auf DSA-/ECDSA-Implementierungen. Der EUCLEAK-Entdecker brach bereits 2021 auf ähnlichem Weg die ECDSA-Implementierung in Google Titan FIDO-Keys, wenn auch mit weniger medialer Aufmerksamkeit.

Die Schwachstelle wirkte sich auch auf FIDO-Token von Yubico aus, die zeitgleich ein Security-Advisory dazu veröffentlichten. Daher wurde der Angriff in der Presse auch als „YubiKey-Schwachstelle" beschrieben, obwohl auch andere Produkte (Smartcards, TPMs, FIDO-Token und Bitcoin-Wallets) angreifbar sind, die Infineon-Chips und deren Bibliothek verwenden. Seit der Veröffentlichung äußerten sich fast nur Hersteller, deren Produkte nicht betroffen sind – bei anderen ist daher eine gewisse Skepsis angebracht,

Der Angriff erfolgt mit einer Magnetfeld-Sonde, die weniger als 1 mm vom Chip entfernt platziert wird. Dafür muss beim YubiKey das Gehäuse geöffnet oder angebohrt werden. Da FIDO-Token vor allem vor Remote-Angriffen schützen sollen, ist die Gefahr begrenzt; die offizielle CVSS-Bewertung liegt deshalb auch nur bei 4.2. Wer besonders kritische ECDSA-Schlüssel verwendet, sollte dennoch handeln: YubiKeys und YubiHSMs müssen ersetzt werden, da Yubico keine Firmware-Updates erlaubt, um Angriffe über Updates auszuschließen.

Am 06.09.2024 stellten Google-Forscher auf der CHES-Konferenz ein System vor, das per Machine Learning automatisch Power-Seitenkanäle sucht und Entwicklern hilft, ihre HSMs dagegen zu härten. Auch da diente die ECDSA-Nonce als Beispiel.

Unternehmenserwerb

Die Datenschutzkonferenz (DSK) hat am 11.09.2024 die Übermittlung personenbezogener Daten vor Abschluss eines Asset Deals ohne eine Einwilligung der Betroffenen für unzulässig erklärt. Bei fortgeschrittenen Verhandlungen könne ein berechtigtes Interesse die Übermittlung bestimmter Daten rechtfertigen: So sei die Übermittlung von Kundendaten erlaubt, wenn der Veräußerer feststellt, dass die Interessen der Kunden nicht überwiegen; sie müssen jedoch über die Datenübermittlung informiert werden.

Die Übermittlung von Beschäftigtendaten ist in der Regel zulässig, wenn sie zur Erfüllung des Arbeitsvertrags durch den Käufer notwendig wird. Besondere personenbezogene Daten dürfen allerdings nur mit ausdrücklicher Einwilligung übermittelt werden.

Illegale Datenverarbeitungen

Die niederländische Datenschutzbehörde verhängte am 29.08.2024 ein Bußgeld von 290 Mio. € gegen Uber, weil das Unternehmen nach Außerkraftsetzung des Privacy Shield durch den EuGH am 17.07.2020 (SSN 7/2020) weiter personenbezogene Daten in die USA übermittelt hatte – ohne angemessene Garantien für den Schutz dieser Daten. Erst seit dem 27.11.2023 zählt Uber Technologies Inc. zu den nach dem Data Privacy Framework zertifizierten US-Unternehmen.

Ein weiteres Bußgeld über 30,5 Mio. € verhängte die Behörde am 03.09.2024 gegen Clearview AI: Das Unternehmen speichert rechtswidrig in einer Datenbank mehr als 30 Milliarden Fotos von Personen und erzeugt für jedes Foto einen einzigartigen biometrischen Code (Editorial SSN 1/2020). Die abgebildeten Personen haben nicht in die Verarbeitung eingewilligt und nicht einmal Kenntnis von der Speicherung.

Clearview AI hat keinen Sitz in Europa; dennoch müssen die nationalen Datenschutzbehörden Rechtsverletzungen gegen EU-Bürger in ihrem Zuständigkeitsbereich verfolgen. Die Datenschutzbehörden von Frankreich, Italien und Griechenland haben bereits Bußgelder in Höhe von je 20 Mio. € und Großbritannien in Höhe von 7,5 Mio. Pfund verhängt (SSN 10/2022), weil das Unternehmen wiederholten Löschaufforderungen nicht nachgekommen ist. Eine Vollstreckung der Bußgeldbescheide ist zwar (bisher) nicht möglich – aber das Signal deutlich: Europa ist keine rechtsfreie Spielwiese für amerikanische Unternehmen.

Secorvo News

Secorvo Seminare

Vom **04. bis 07.11.2024** bietet Ihnen das PKI-Seminar tiefe Einblicke in Public Key Infrastrukturen: Von den Grundlagen bis zu Planung und Betrieb Ihrer eigenen PKI. Auf unserem T.I.S.P.-Seminar vom **11. bis 15.11.2024** bereiten wir Sie in über 20 Modulen auf die anschließende Zertifikatsprüfung vor; die 4. Auflage des T.I.S.P.-Begleitbuches erhalten Sie nach Ihrer Anmeldung.

Wer lernen möchte, wie sich die Software-Entwicklung sicher(er) gestalten lässt, dem bietet unser T.P.S.S.E.-Seminar vom **25. bis 28.11.2024** ein praxisbezogenes Training mit interaktiven Workshops – und im Anschluss auch hier die Möglichkeit, sich zertifizieren zu lassen.

Werfen Sie auch gerne schonmal einen Blick in unseren Seminarkalender 2025. Wir freuen uns auf Ihre Anmeldung!

Wer hat, der kann.

Immer mehr Anwendungen verlangen eine Anmeldung, und oft sind sie ohne einen Zugriff auf andere Dienste nicht sinnvoll nutzbar. Deshalb ist moderne Authentifizierung mit OAuth-Tokens längst ein wichtiges Thema. Wer sich damit beschäftigt merkt jedoch schnell, dass es bei der technischen Umsetzung einige Hürden und Fallstricke gibt. Diese variieren je nach System, das zur Ausstellung der OAuth-Tokens verwendet wird.

Beim **KA-IT-Si-Event** im dm-dialogicum geben Eberhard Ratzel und Moritz Gabriel (dmTECH) am **17.10.2024** einen Überblick über ihre Erfahrungen und Erkenntnisse bei der Nutzung von Microsoft Entra ID zur Erstellung von OAuth-Tokens. Im Anschluss haben Sie wieder Gelegenheit zum fachlichen und persönlichen Austausch am Buffet. Hier geht's zur Anmeldung. Wir freuen uns auf Sie!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Oktober 2024	
14.-18.10.	ACM CSS 2024 (ACM SIGSAC, Salt Lake City/US)
17.10.	KA-IT-Si-Event "Wer hat, der kann." (KA-IT-Si, Karlsruhe)
22.10.	Swiss Cyber Storm 2024 (Swiss Cyber Storm, Bern/CH)
22.-24.10.	it-sa 2024 (itsa 365, Nürnberg)
November 2024	
04.-07.11.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
05.-07.11.	24. IDACON 2024 (WEKA Akademie, München)
08.11.	DORA, NIS2 und CRA als Wegweiser für Informationssicherheit (GI, Frankfurt/Main)
11.-15.11.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
20.-21.11.	ICSP 2024 (NIT, Jamshedpur/IND)
25.-28.11.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Dezember 2024	
09.-13.12.	Asiacrypt 2024 (IACR, Kolkata/IND)
09.-12.12.	Black Hat Europe 2024 (Black Hat, London/UK)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Ion Barza, Paul Blenderman (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2024



Parkinson reloaded

Wer seit Jahrzehnten in der IT zu Hause ist, erinnert sich sicherlich noch an die Euphorie, mit der in den 90er Jahren die Digitalisierung herbeigesehnt wurde: endlich einfache, schnelle, bürokratie- und medienbruchfreie, von jedem Ort und zu jeder Zeit nutzbare Dienste.

Die Wirklichkeit entpuppt sich zunehmend als das erschreckende Gegenteil. Das liegt nicht allein daran, dass die Fortschritte in der Digitalisierung der öffentlichen Verwaltung oder hochregulierten Bereichen wie dem Gesundheitswesen eher in homöopathischen Dosen erfolgen – dank IT wachsen Zahl und Umfang von Papierdokumenten noch immer. Der Gesetzgeber bremst derweil durch detailliert regulierende Eingriffe, wie z. B. die Spezifikation der E-Rechnung, die keine reine PDF-Datei mehr sein darf: Viel Umstellungsaufwand ohne nennenswerte Verbesserung der Abläufe, denn zahlreiche Buchhaltungssysteme werten PDF-Dateien bereits heute automatisch aus.

Nicht zuletzt sind es Sicherheitsmechanismen, die zur wachsenden Komplexität eigentlich einfacher Prozesse beitragen: Kaum noch ein wichtiger Account, der nicht durch eine Zwei-Faktor-Authentifizierung geschützt wird – hier mit einem Chip-TAN-Generator, dort mit einem FIDO-Token, da mit einer SMS oder einem Telefonanruf, dann wieder mit einer Authenticator-App und schließlich mit einem photoTAN-Gerät. Und wehe, man wechselt einen Anbieter oder gar das defekte Smartphone – dann ist man Tage damit beschäftigt, sich neue Initialisierungsbriefe zusenden zu lassen oder seine Identität zu bestätigen, denn der hinterlegte Personalausweis ist wahrscheinlich zwischenzeitlich abgelaufen.

Offenbar schlägt da eine Variante des Parkinsonschen Gesetzes zu: „IT breitet sich in genau dem Maß aus, wie Geld für ihre Erweiterung zur Verfügung steht." Wenn wir so weitermachen, brauchen wir jedenfalls eines nicht mehr fernen Tages ein „IT-Abbau-Gesetz".



Inhalt

Parkinson reloaded

Security News

Drum prüfe... öfter

Patientengeheimnis

Selbst ist der Versicherte

Gut Ding...

Test-Phishing

Consumer Respect Act?

RoSIg

Secorvo News

Kompetenzzuwachs

Secorvo Seminare

IT-Sicherheit hinter den Spiegeln

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Drum prüfe... öfter

Apple schlug dem CA/Browser-Forum am 08.10. 2024 vor, die maximale Gültigkeitsdauer von öffentlichen TLS-Serverzertifikaten schrittweise auf 45 Tage zu begrenzen – Google war 2023 mit einem ähnlichen Vorhaben gescheitert. Dadurch soll die Bedeutung von Sperrmechanismen abnehmen, denen Browser-Hersteller ohnehin skeptisch gegenüberstehen. Das Risiko durch überflüssige oder gar kompromittierte, aber nicht gesperrte Serverzertifikate würde sinken. Technisch würde das ACME-Protokoll weiter an Bedeutung gewinnen: Damit können Zertifikatsverlängerungen automatisiert alle 30 bis 40 Tage erfolgen und dabei jeweils die DNS-Namen validiert werden.

Gleichzeitig soll die „Cache"-Zeit für validierte OV/EV-Angaben auf 366 Tage, für DNS-Namen oder IP-Adressen sogar auf 10 Tage verkürzt werden. Bisher dürfen Trustcenter einmal validierte Unterlagen wie Handelsregisterauszüge bis zu 825 Tage lang wiederverwenden und sich so bei Verlängerungen eine aufwändige erneute Prüfung sparen.

Die Umstellung würde die Position der Browser-Hersteller gegenüber problematischen Trustcentern stärken (SSN 07/2024): Nach einem Vertrauensentzug stünden deren Kunden noch schneller ohne gültige Zertifikate da. Wer zahlreiche öffentliche Serverzertifikate nutzt, ist daher gut beraten, einen Zweitlieferanten in petto zu haben. Darüber hinaus könnte die kürzere Gültigkeit den Übergang zu Post-Quantum-Cryptography-Zertifikaten erleichtern, der ab etwa 2030 zu erwarten ist.

Patientengeheimnis

Am 04.10.2024 hat der Europäische Gerichtshof (EuGH) mit der „Lindenapotheken-Entscheidung" wichtige Grundsätze zu Gesundheitsdaten festgelegt. Sie liegen vor, sobald Informationen Rückschlüsse auf den Gesundheitszustand einer Person zulassen. Daten wie Name und Adresse, die normalerweise nicht zu den besonderen Kategorien personenbezogener Daten zählen, können als Gesundheitsdaten gelten, wenn sie mit Gesundheitsfragen in Verbindung stehen. Dieser Grundsatz gilt für alle besonderen Kategorien personenbezogener Daten.

Zugleich hat der EuGH klargestellt, dass Wettbewerber wettbewerbsrechtlich gegen Unternehmen vorgehen können, die gegen Vorgaben der DSGVO verstoßen – dafür sind keine vorausgehenden Maßnahmen der Datenschutzaufsichtsbehörden erforderlich. Die Vernachlässigung des Datenschutzes kann also neben hohen Bußgeldern auch kostspielige Streitigkeiten zur Folge haben.

Selbst ist der Versicherte

Ab dem 15.01.2025 sollen alle gesetzlich Versicherten mit der Einführung der elektronischen Patientenakte (ePA) von den Vorteilen der Digitalisierung des Gesundheitssystems profitieren.

Der Hamburgische Beauftragte für den Datenschutz und die Informationsfreiheit hat am 17.10. 2024 darauf hingewiesen, dass die Nutzung der ePA freiwillig ist und ihr (im Voraus) widersprochen werden kann.

Die ePA kann nicht nur über die ePA-App auf Mobilgeräten genutzt werden. Auch in Arztpraxen oder Apotheken wird die ePA eingesehen und bearbeitet. Trotz technischer und organisatorischer Maßnahmen besteht daher das Risiko, dass Unbefugte Zugang zu diesen besonderen personenbezogenen Daten erhalten.

Allerdings können Versicherte selbst festlegen, welche Dokumente sie freigeben und welchen Leistungserbringern sie Zugriff gewähren. Der Grundsatz „data privacy by design" wurde berücksichtigt, allerdings ohne „data privacy by default": Ohne Widerspruch sind standardmäßig fast alle Dokumente allen Leistungserbringern zugänglich.

Gut Ding...

Am 27.09.2024 hat die irische Datenschutzaufsicht DPA ein seit 2019 laufendes Verfahren gegen Meta Ireland mit einem Bußgeld von 91 Mio. € beendet. Die Bemühungen des European Data Protection Boards, die Anforderungen der DSGVO auch gegenüber den großen Technologieunternehmen mit Sitz in Irland durchzusetzen, tragen langsam Früchte: Die Anzahl der Beschäftigten bei der DPA hat sich innerhalb der fünf Jahre, die das Verfahren dauerte, fast verdoppelt (2019: 110, 2023: 210).

Rechte und Freiheiten müssen auch in Zukunft gegenüber den Technologieriesen geschützt und verteidigt werden. Das gelingt nur, wenn die Aufsichtsbehörden EU-weit personell und finanziell ausreichend ausgestattet sind. Nur dann können Betroffene und Verantwortliche darauf vertrauen, dass ihre Anfragen bei den Behörden nicht in bürokratischen Schwarzen Löchern verschwinden.

Test-Phishing

Am 26.10.2024 wurde bekannt, dass Abgeordnete und Mitarbeiter des Bundestages im Rahmen eines Pentests mit unangekündigten Phishing-E-Mails „getestet" wurden. So sinnvoll Trainings mit Phishing-E-Mails auf den ersten Blick sein mögen –

sie verstellen manchmal den Blick auf das eigentliche Problem. Denn woran sollte der Empfänger einer solchen E-Mail verlässlich erkennen, ob ein unbekannter Link in einer E-Mail vertrauenswürdig ist – oder eben gerade nicht?

Viele Unternehmen markieren daher schon lange externe E-Mails durch farbige Balken oder Hinweise (z. B. in Office 365) und leiten in der E-Mail enthaltene Links, die auf externe Quellen verweisen, auf einen Proxy-Server um, der eine Warnung vorschaltet und den Link testet. Ein solcherart erzwungenes „Innehalten" kann zumindest verhindern, dass im HTML-Code einer E-Mail verschleierte Links in spontanem Vertrauen gedankenlos angeklickt werden.

Consumer Respect Act?

Am 10.10.2024 hat der Rat der EU dem Cyber Resilience Act (CRA) zugestimmt. Der CRA verpflichtet Hersteller von Soft- und Hardwareprodukten, die mit einem Netz oder einem anderen Gerät verbunden werden, zur Einhaltung von Cybersicherheitsvorgaben. Die Produkte müssen bestimmte Anforderungen an die Cybersicherheit erfüllen, und die Hersteller müssen Schwachstellen und Vorfälle behandeln und beheben.

Der CRA setzt auf der CE-Kennzeichnung und deren horizontalem Ansatz auf: Es werden allgemeine Anforderungen formuliert, die für alle Arten von Produkten gelten. So müssen Produkte etwa Sicherheitsupdates unterstützen, die der Hersteller innerhalb eines festgelegten Mindestzeitraums zur Verfügung stellen muss.

Das Prüfverfahren hängt davon ab, welcher Kategorie ein Produkt angehört: Kritische Produkte müssen durch externe Prüfer nach definierten Prüfkatalogen geprüft werden; bei wichtigen Produkten gelten weniger strenge Prüfvorgaben. Sonstige Produkte können vom Hersteller selbst geprüft werden.

Ebenfalls am 10.10.2024 erweiterte der Rat der EU die Produkthaftungsrichtlinie, die nun auch Software einschließt. Hersteller haften nun gegenüber Verbrauchern auch für defekte Software(-komponenten), etwa wenn diese fehlerhaft Daten löscht.

Eine Übersicht der Anforderungen des CRA stellte Markus Toran (Secorvo) am 02.06.2024 auf der GPN22 vor (Video). In einem Round Table beim CyberForum diskutiert er am 19.11.2024 die Herausforderungen und mögliche Lösungen für Unternehmen.

RoSIg

Am 28.10.2024 hat die Deutsche Energie-Agentur (dena) die Studie „Cyber-Fit" über die Rentabilität von Cybersicherheitsmaßnahmen vorgelegt. Darin behaupten die Autoren allen Ernstes, die Ausgaben für IT-Sicherheitsmaßnahmen nach dem NIS-2-Umsetzungsgesetz seien in wichtigen Einrichtungen „bereits im ersten Jahr rentabel".

Zum Beweis entstauben sie das Modell des „Return on Security Investment" (RoSI), das Anfang des Jahrtausends eine kurze Karriere machte – und verrechnen dabei Äpfel mit Birnen: Die durch die Schutzmaßnahmen reduzierte „Verlusterwartung" wird den Kosten der Maßnahmen gegenübergestellt. Echte Kosten werden so durch virtuelle Nicht-Verluste beglichen – eine solche Geldschöpfung wünscht sich jeder Unternehmer.

Secorvo News

Kompetenzzuwachs

Seit dem 01.10.2024 verstärkt der Jurist Ion Barza unser Datenschutz-Team. Herzlich willkommen!

Secorvo Seminare

Freie Plätze für Kurzentschlossene: Eine vertiefte Einführung in die sichere Software-Entwicklung bietet das T.P.S.S.E.-Seminar **vom 25. bis 28.11.2024** mit Praxisbezug und interaktiven Workshops – und im Anschluss die Möglichkeit, sich zertifizieren zu lassen.

Planen Sie schon Ihre Weiterbildung für nächstes Jahr? Dann werfen Sie doch einen Blick in unseren Seminarkalender 2025. Wir freuen uns auf Ihre Anmeldung!

IT-Sicherheit hinter den Spiegeln

Zu einem ganz besonderen Jahresabschluss-Event lädt die IT-Sicherheitsregion Karlsruhe (FZI, KA-IT-Si und KASTEL) am **21.11.2024** in die Karlsruher Palazzo-Halle. Mitarbeiter von aramido demonstrieren in ihrem Vortrag „**Voice Cloning – faszinierend oder erschreckend einfach?**", wie mit KI-unterstützter Stimmenfälschung Angriffe möglich sind – und wie man sich davor schützen kann. Die Veranstaltung ist bereits ausgebucht, aber es gibt eine Warteliste.

Merken Sie sich schon einmal den Termin des Jahresauftakt-Events 2025 der KA-IT-Si am 20.02.2025 vor – die Einladung folgt Ende November. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2024	
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
05.-07.11.	24. IDACON 2024 (WEKA Akademie, München)
08.11.	DORA, NIS2 und CRA als Wegweiser für Informationssicherheit (GI, Frankfurt/Main)
11.-15.11.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.11.	Round Table Cyber Resilience Act (CyberForum, Karlsruhe)
20.-21.11.	ICSP 2024 (NIT, Jamshedpur/IND)
21.11.	IT-Sicherheit hinter den Spiegeln (FZI, KA-IT-Si, KASTEL, Karlsruhe)
25.-28.11.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Dezember 2024	
09.-13.12.	Asiacrypt 2024 (IACR, Kolkata/IND)
09.-12.12.	Black Hat Europe 2024 (Black Hat, London/UK)
11.12.	IT Sicherheitsrechtstag NRW (IHK NRW, Bonn)
19.-20.12.	CSCML 2024 (IACR, CSCML, virtuell)

Fundsache

Am 26.09.2024 haben die IT-Sicherheitsbehörden der "Five Eyes"-Staaten Australien, USA, Kanada, Neuseeland und UK einen guten Ratgeber zum Finden und Beheben von Schwachstellen im Active Directory veröffentlicht.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Ion Barza, Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

November 2024



Nicht mehr allein

In den 90er Jahren benutzten Kinder noch ganz konventionelle Zahlungsmittel: Kevin McCallister entnahm die Ersparnisse seines Bruders Buzz einem Vorratsglas. In Teil 2 bezahlte Kevin Zimmer und Service im Plaza in New York schon mit der Kreditkarte seines Vaters, nachdem er seine Familie am Flughafen verloren hatte.

2024 sollen Minderjährige nach Auffassung von Google Kinder-Smartwatches wie das Fitbit Ace LTE als Zahlungsmittel verwenden, das seit dem 07.08.2024 in den USA Tap-to-pay unterstützt. Ab 2025 will Google mobiles Bezahlen für Kinder über die Google Wallet App ermöglichen, wie der Konzern am 30.10.2024 ankündigte. Eltern können ihren Kindern dann das Taschengeld über mit „Family Link" verwaltete Android-Smartphones in die virtuelle Geldbörse überspielen. Damit bekämen Eltern zugleich die Möglichkeit, das Ausgabeverhalten ihrer Kinder zu überwachen.

Nun darf ernsthaft bezweifelt werden, dass Kinder den besonnenen Umgang mit Geld mit einem digitalen „Wallet" besser erlernen als mit Bargeld. Auch sind Zweifel angebracht, dass aus überwachtem Kaufverhalten der Kinder später Souveränität erwächst.

Noch größere Zweifel muss man allerdings daran hegen, dass erzieherische Fragen bei diesem Angebot überhaupt eine Rolle spielen. Denn selbstverständlich kennt das Zahlungs- (und damit Konsum-) Verhalten der Kinder auch der Anbieter des Zahlungssystems: Google. Dabei fallen Daten von unschätzbarem Wert an: Die konsumbeeinflussende Wirkung von Online-Werbung oder Product Placements durch Influencer in sozialen Medien wird so unmittelbar messbar.

Dass aus jahrelanger systematischer „Verhaltensdressur" von Kindern und Jugendlichen nur in Ausnahmefällen Mündigkeit erwächst, dafür hält die Geschichte genügend Beispiele bereit. Ernüchternd, dass ein solches Angebot keinen Aufschrei provoziert.



Inhalt

Nicht mehr allein

Security News

Neue Berichte, alte Erkenntnisse

Umsetzung des CRA

EUCLEAK-Nachwehen

Vertrauen ist gut...

Geht doch!

Fortsetzung folgt...

Vorsicht: Fälschung

Secorvo News

Secorvo Seminare

Cyber-Versicherung im Ernstfall

Veranstaltungshinweise

secorvo
security consulting

Security News

Neue Berichte, alte Erkenntnisse

Am 12.11.2024 veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) den jährlichen Bericht zur Lage der IT-Sicherheit 2024 in Deutschland. Danach bleibt die IT-Sicherheitslage in Deutschland auch 2024 angespannt: Cyberkriminelle verfeinerten ihre Methoden, besonders bei Erpressungstrojanern (Ransomware) und Angriffen durch Überlastung (DDoS-Angriffe), Schwachstellen in IT-Systemen, vor allem bislang unbekannte Sicherheitslücken (Zero-Day) würden immer häufiger ausgenutzt und Angriffe auf kritische Infrastrukturen und Cloud-Dienste nähmen weiter zu. Gleichzeitig würden die Abwehrmaßnahmen durch internationale Zusammenarbeit und neue gesetzliche Vorgaben wie NIS-2 und den Cyber Resilience Act gestärkt. Die digitale Bedrohungslage erfordere einen intensiveren Schutz in Unternehmen und Behörden, um Cyberangriffe abzuwehren und Schäden zu begrenzen.

Etwa zeitgleich aktualisierten MITRE und CISA am 20.11.2024 die Liste der 25 schlimmsten Schwächen bei der Software-Entwicklung. Erschreckenderweise finden sich auch alle hartnäckigen Schwachstellen unverändert noch immer in dieser Liste.

Keine bahnbrechenden neuen Einsichten – aber die Gewissheit, dass noch in vielen Einrichtungen an vielen Stellen „Hausaufgaben“ zu erledigen sind.

Umsetzung des CRA

Das BSI hat am 20.09.2024 die Technische Richtline (TR) 03183 aktualisiert. Sie enthält die Anforderungen an Hersteller und Produkte, die sich aus dem Cyber Resilience Act (CRA) ergeben und ist nun in drei Teile gegliedert: generelle Anforderungen, Anforderungen an Software-Stücklisten (Software Bill of Materials, kurz: SBOM) und Vorgaben für Schwachstellenberichte und -meldungen.

Der neue erste Teil (Community Draft) konkretisiert die grundlegenden Anforderungen aus Anhang I des CRA; außerdem werden Untersuchungskriterien für Prüfer definiert. Im überarbeiteten zweiten Teil wird festgelegt, dass die SBOM-Formate SPDX oder CycloneDX in XML oder JSON verwendet werden. Eine Anleitung beschreibt, wie die Felder korrekt auszufüllen sind, z. B. welche Bezeichnung für eine Produktkomponente zu wählen ist.

Der ebenfalls neue dritte Teil (Community Draft) verpflichtet Hersteller zur Verwendung einer mit OpenPGP signierten security.txt-Datei nach RFC 9116. Außerdem wird ein Prozess zur Schwachstellenbehandlung definiert. Unternehmen sollen getrennte Verantwortlichkeiten für Product Security Incident Response Team (PSIRT) und Computer Security Incident Response Team (CSIRT) einrichten. Weiterhin werden Elemente für eine Unternehmensrichtlinie zum koordinierten Melden von Schwachstellen vorgegeben.

Die Richtlinie enthält zahlreiche konkrete Vorgaben zur Erfüllung der CRA-Anforderungen. Sie soll in die europäische Standardisierung eingehen. Die Kommentierungsphase für die Teile eins und drei endet am 24.11.2024.

EUCLEAK-Nachwehen

Schon bei der Publikation der EUCLEAK-Schwachstelle war klar, dass nicht nur YubiKeys betroffen sind, sondern auch andere Produkte, die Infineon-Sicherheitschips mit der ursächlichen Firmware-Bibliothek einsetzen (SSN 09/2024).

Die meisten der möglicherweise betroffenen Hersteller schweigen sich bislang darüber aus, ob ihre Produkte anfällig sind. Immerhin hat Infineon selbst im Oktober drei gefixte Firmware-Versionen für ihre TPM-Chips nach den Common-Criteria-Standards vom BSI rezertifizieren lassen. Für Endanwender ist das jedoch nur begrenzt hilfreich, solange sie nicht wissen, ob der eigene PC eines der betroffenen TPM-Modelle enthält und wie sich die neue Firmware installieren lässt. Hier sind die PC-Hersteller in der Pflicht für Klarheit zu sorgen.

Der Fall zeigt außerdem, dass auch die akkreditierten Prüfer der Zertifizierungsstandards nicht dagegen gefeit sind, komplexe Schwachstellen zu übersehen. Ein Sicherheitszertifikat ist keine Garantie für schwachstellenfreien Code.

Vertrauen ist gut…

Der Ratschlag aus den SSN 10/2024, vorsorglich einen Zweitlieferanten für öffentlich gültige Zertifikate in der Hinterhand zu haben, hat sich schneller als erwartet als praxisrelevant erwiesen.

Ein für die Nutzer öffentlich gültiger Zertifikate folgenreicher Vertrauensverlust in der Beziehung zwischen einem Trustcenter und dem CA/Browser-Forum als Aufsichtsorgan ereignete sich vor wenigen Monaten, als Google Entrust und AffirmTrust das Vertrauen entzog (siehe SSN 07/2024).

Aber auch im Verhältnis zwischen Zertifikatsnutzern und ihren Lieferanten kann es – wie bei jedem Vertrag – zu Streitigkeiten über die Auslegung kommen. Wie am 13.11.2024 bekannt wurde, hat das Trustcenter Sectigo den Rahmenvertrag mit GÉANT, dem Zusammenschluss der europäischen

Forschungsnetzwerke vorzeitig gekündigt. Die Konsequenzen beschäftigen nun unter anderem 450 deutsche Forschungseinrichtungen und Universitäten, die sich mit der unerwarteten Herausforderung konfrontiert sehen, dass Sectigo voraussichtlich ab dem 10.01.2025 über den GÉANT-Rahmenvertrag keine Zertifikate mehr liefert.

Geht doch!

Am 27.10.2024 hat die Sächsische Datenschutz- und Transparenzbeauftragte mitgeteilt, dass sie bei einer Kontrolle von 1.500 Webauftritten tatsächlich Verbesserungen in Sachen Datenschutz festgestellt hat. Im Frühsommer wurden 30.000 Webauftritte überprüft; davon wurden 2.300 beanstandet. In 1.500 Fällen konnte im Oktober 2024 festgestellt werden, dass es keine unzulässige Verwendung von Cookies oder Diensten wie Google Analytics mehr gab. Neben dem Kontrolldruck hat offenbar auch die Bereitschaft der Aufsichtsbehörde geholfen, die Verantwortlichen zu beraten, wie Webauftritte überarbeitet und „in legale Bahnen" gelenkt werden können.

Fortsetzung folgt...

Im Juni 2020 hatte die Datenschutzkonferenz die „Orientierungshilfe für Anbieter von Telemedien" in überarbeiteter Version veröffentlicht (SSN 06/2020). Sie wurde am 15.11.2024 durch die „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten" ersetzt, die nun die neue Rechtslage des TDDG und des DDG berücksichtigt.

Das Dokument enthält wertvolle Hinweise: Es geht insbesondere auf die Unterschiede zwischen TDDDG und DSGVO ein und beschreibt nachdrücklich die Anforderungen an eine wirksame Einwilligung. Abgerundet wird das Dokument durch die sehr konkrete Darstellung der Anforderungen an Einwilligungsbanner auf Webseiten – eine wirkliche Hilfestellung für Webseitenbetreiber.

Vorsicht: Fälschung

Die Digitalisierung von Dienstleistungen und die urbane E-Mobilität hauchen alten Betrugsmethoden (SSN 10/2011) neues Leben ein: Nach Angriffen auf Ladesäulen und Strafzetteln mit falschen QR-Codes („Quishing") geraten nun auch Parksäulen ins Visier der Täter. So geschehen in Hannover, wie die Polizei am 12.11.2024 berichtete. Betroffen sind Kundinnen und Kunden des Parkdienstleisters easypark. Die Methode ist nicht neu (SSN 04/2022), aber effektiv: Die falschen QR-Codes führen auf eine Internetseite, die die Zahlungsdaten abfragt und nahezu identisch mit der Originalseite ist, sodass der Betrug nicht sofort auffällt. Der Parkhausbetreiber easypark und die Landeshauptstadt Hannover informieren, wie man sich vor solchen Betrugsmaschen schützen kann. Wie im analogen Leben gilt auch hier: Keine Zahlung an unbekannte Empfänger.

Secorvo News

Secorvo Seminare

Unser Seminarbetrieb geht in die Winterpause.

Falls Sie über Weihnachten Ihre Weiterbildung 2025 planen möchten, werfen Sie doch einen Blick in unseren Seminarkalender. Im März bereiten wir Sie gerne auf die T.I.S.P.- und die T.P.S.S.E.-Zertifizierung vor. Wir freuen uns auf Ihre Anmeldung.

Cyber-Versicherung im Ernstfall

Risiken kann man ignorieren, reduzieren – oder transferieren. Mit der Zunahme erfolgreicher Cyberangriffe steigt daher auch die Nachfrage nach Cyber-Versicherungen. Im Februar 2024 widmete die BaFin diesem Thema sogar einen Fachartikel.

Aber wie das so ist im Leben: Erst im Ernstfall zeigt sich, was eine Vereinbarung wert ist. Denn nicht jeder Vorfall ist automatisch auch ein Versicherungsfall – angesichts der wachsenden Vorfallszahlen und sinkender Margen im Cyber-Versicherungsgeschäft wird aus einem Vorfall schnell ein Streitfall. Welche Fragen dabei zu klären sind und was Versicherungsnehmer schon bei Vertragsabschluss beachten sollten, erläutert anschaulich und spannend an realen Beispielen Dr. Christian Förster (Bartsch Rechtsanwälte) beim Jahresauftakt-Event 2025 der Karlsruher IT-Sicherheitsinitiative am **27.02.2025** um 18:00 Uhr im Saal Baden (IHK Haus der Wirtschaft). Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking".

Wir empfehlen eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Dezember 2024	
09.-13.12.	Asiacrypt 2024 (IACR, Kolkata/IND)
09.-12.12.	Black Hat Europe 2024 (Black Hat, London/UK)
11.12.	IT Sicherheitsrechtstag NRW (IHK NRW, Bonn)
19.-20.12.	CSCML 2024 (IACR, CSCML, virtuell)
Januar 2025	
20.-22.01.	Omnisecure 2025 (in TIME berlin, Berlin)
Februar 2025	
11.-12.02.	32. DFN-Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg
12.-14.02.	IT-Defense 2025 (cirosec, Leipzig)
19.-20.02.	ID:SMART Workshop 2025 (CAST e.V., Darmstadt)
27.02.	KA-IT-Si-Event „Wer zahlt die Zeche?“ (KA-IT-Si, Karlsruhe)
März 2025	
10.-14.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
17.-21.03.	31st Fast Software Encryption Conference (IACR, Rom/IT)
18.-20.03.	secIT 2025 (Heise Medien, Hannover)
24.-27.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Ion Barza (Editorial), Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Dezember 2024



Gotcha

Einer Kleinen Anfrage im Bundestag und Recherchen von netzpolitik.org ist die Information zu verdanken, dass mit dem Gesichtserkennungssystem des Bundeskriminalamts (BKA) jährlich rund 3.500 Personen identifiziert werden. Referenzbilder von 5 Mio. Menschen seien in der Datenbank des Systems erfasst; Jahr für Jahr kämen rund 10% hinzu. Bemerkenswert ist offenbar die Erkennungsrate des KI-unterstützten BKA-Systems, bei dem eine menschliche „Endkontrolle" inzwischen verzichtbar sei.

Nun mag man der Strafverfolgung leistungsfähige Erkennungssysteme zubilligen. Doch ist die Technik inzwischen allgemein zugänglich – z. B. über das polnische Unternehmen pimEyes (SSN 7/2020), das ein hochgeladenes Bild mit über 1 Mrd. aus dem Internet gesammelten Personenfotos vergleicht. Wie sich darüber ein privates Erkennungssystem konstruieren lässt, demonstrierten die Harvard-Studenten AnhPhu Nguyen und Caine Ardayfio am 02.10.2024 in einem Youtube-Video: Ihr Projekt I-XRAY nutzt die verborgene Kamera einer Ray-Ban Meta-Brille, um (sprachgesteuert) Fotos von beliebigen Personen mit Bildern aus dem Internet zu vergleichen und über die zugehörigen Webseiten deren Namen, Adressen und Telefonnummern zu finden. Auf dem Smartphone werden dann die Kontaktdaten und alle zu der Person gefundenen Webseiten angezeigt – innerhalb von Sekunden.

Noch vor wenigen Jahren war unser Name das Identifikationsmerkmal: Wer ihn kannte, konnte auf Informationen über uns zugreifen, die wir (in der Regel willentlich) online verfügbar gemacht hatten. Niemand musste aber damit rechnen, auf der Straße erkannt zu werden. Das änderte Google mit der Bildersuche. Dank biometrischer Erkennungsverfahren genügt heute ein Foto, um alles Veröffentlichte über uns zu erfahren. Und vielleicht bald schon ein einziger gesprochener Satz. On the internet, everybody knows you're a dog.



Inhalt

Gotcha

Security News

Unsichere Anker

Leicht zugängliche Firewalls

Ross Andersons Vermächtnis

Ausgeschaltete Geräte aufspüren

Sichere Anker

Durch Nachbars Garten

Messbare Fortschritte

Secorvo News

Secorvo Seminare

Wer zahlt die Zeche?

Veranstaltungshinweise

secorvo
security consulting

Security News

Unsichere Anker

Das Domain Name System (DNS) ist einer der wichtigsten Vertrauensanker des Internet. Daher wurde vor 25 Jahren DNSSEC entwickelt und 2005 als RFC 4033-4035 standardisiert: Damit wird die Richtigkeit der Angaben mit digitalen Signaturen bestätigt.

Viele Registrare und DNS-Provider unterstützen den Standard allerdings bis heute nicht. In seiner am 28.11.2024 veröffentlichten Bachelorarbeit analysierte Felix Wotschofsky von der Berliner CODE University die Verbreitung von DNSSEC: Lediglich 6% der von ihm untersuchten 171 Millionen Domänen nutzen es; Dänemark und Schweden sind mit über 60% rühmliche Ausnahmen. Dabei überprüfen allein in Deutschland über 80% der DNS-Resolver DNSSEC-Signaturen – sofern vorhanden. Zumindest in Deutschland wäre die Vertrauenswürdigkeit von DNS-Auskünften daher leicht zu erreichen.

Leicht zugängliche Firewalls

Selbst IT-Administratoren neigen zu der Annahme, dass bei besonders sicherheitsrelevanter Software auch deren Qualität entsprechend hoch ist. Dieses Vertrauen ist leider häufig unberechtigt, wie aktuelle Berichte über gravierende Schwachstellen in den Firewalls von Fortinet (15.10.2024) und Palo Alto (19.11.2024) zeigen. Bei der US-amerikanischen Cyber Defense Agency CISA kann man nachlesen, dass Angreifer diese Schwachstellen bereits ausnutzen (27.12.2024).

Den Zugriff auf administrative Zugänge – insbesondere den von Firewalls – sollte man immer durch besonders starke Authentifikationsmechanismen schützen und auf Systeme im internen Netz beschränken. Suchmaschinen wie Shodan oder CriminalIP zeigen, dass solche elementaren Schutzmaßnahmen häufig nicht ergriffen werden – und damit die Ausnutzbarkeit von Schwachstellen auch noch fahrlässig erleichtert wird.

Auch andere goldene Regeln werden bei Firewalls regelmäßig verletzt: Dienste wie E-Mail-Filterung oder VPN-Gateways gehören nicht auf die Firewall, sondern auf ein separates System in der DMZ. Wer auf einer Firewall zusätzliche Dienste betreibt, vergrößert unvermeidlich die Angriffsfläche – und damit die Wahrscheinlichkeit eines erfolgreichen Angriffs. Wie bei allen kritischen Systemen gilt auch hier das KISS-Prinzip: Keep it simple and stupid.

Ross Andersons Vermächtnis

Am 03.11.2024 teilte ein Mitarbeiter des im März 2024 viel zu früh verstorbenen Ross Anderson mit, dass nun auch die dritte Auflage des Standardwerks "Security Engineering – A guide to building dependable distributed Systems" als PDF frei zum Download verfügbar ist. Wir nutzen die Gelegenheit, um dieses hervorragende Grundlagenwerk wärmstens zur Lektüre zu empfehlen.

Ausgeschaltete Geräte aufspüren

Mit Googles "Find-My-Device"-Netzwerk (FMD) können sogar ausgeschaltete Android-Geräte geortet werden, sofern sich der Bluetooth-Chip nach dem Ausschalten als Beacon verhält – wie bei den aktuellen Pixel-Modellen. Eine am 13.02.2024 in Android eingeführte Schnittstelle ermöglicht es, beim Herunterfahren berechnete Ephemeral Identifier (EIDs) in den Bluetooth-Chip zu laden. Empfangen andere Android-Geräte diese EIDs, senden sie ihren damit verschlüsselten Standort an Google. Nur der Besitzer des Geräts kann diese Daten entschlüsseln und so sein Gerät orten.

Zum Schutz der Privatsphäre aller Beteiligten kommen verschiedene Techniken zum Einsatz: Befindet man sich an seiner hinterlegten „Zu-Hause"-Adresse, sendet Android keine Standortdaten. Außerdem werden mehrere Standorte aggregiert, sodass die Standorte einzelner Netzwerkteilnehmer nicht bekannt werden. Durch Rate-Limiting soll die missbräuchliche Nutzung zur Personenverfolgung in Echtzeit ausgeschlossen werden. Außerdem kann die Funktion deaktiviert werden. Es wird sogar die derzeit noch in der Entwicklung befindliche IETF-Spezifikation zur Erkennung unerwünschter Tracker (dult) unterstützt. Hier hat Google offenbar aus den Erfahrungen Apples mit deren AirTags (SSN 3/2022) gelernt.

Sichere Anker

Am 03.12.2024 erläuterte Senior Product Manager Steven Hosking, warum Microsoft für Windows 11 das Vorhandensein eines Trusted Platform Module (TPM) 2.0 fordert. Zahlreiche spontane Kommentare (allein 630 bei Heise) unterstellen Microsoft, damit den Verkauf neuer Hardware ankurbeln zu wollen – und loben Linux, das sich auch ohne TPM installieren lässt.

Tatsache ist aber: Ohne sichere Hardware gibt es kein sicheres Betriebssystem. Das TPM ist der Vertrauensanker für sicheres Booten und Festplattenverschlüsselung – anwenderfreundlich und mit einem hohen Sicherheitsniveau. Das gilt auch für Linux. Ein TPM bietet außerdem einen sicheren Ablageplatz für Passkeys und ähnliche Anmeldeschlüssel, auch ohne FIDO-Key. Smartphones nutzen ähnliche Vertrauensanker. Kein Wunder, dass Smartphones bisher von Schadsoftwarewellen ver-

schont wurden. Auch dafür benötigen die Betriebssysteme passende Hardwareunterstützung. Im Übrigen: Worüber reden wir eigentlich? TPMs in Version 2.0 werden seit 2017 in nahezu jedem neuen PC verbaut…

Durch Nachbars Garten

Die Forensiker von Volexity berichteten am 22.11.2024 ausführlich, wie russische Hacker in ein Unternehmensnetzwerk eingebrochen sind, indem sie zunächst Computer benachbarter Firmen kaperten. Anschließend nutzten sie deren WLAN, um in das schlecht gesicherte WLAN des Zielunternehmens einzudringen. Volexity taufte diese bisher eher hypothetische Angriffsmethode treffend als „Nearest Neighbour Attack".

Die Annahme, dass ein Angreifer sich in unmittelbarer Nähe eines WLANs aufhalten müsste, um es zu kompromittieren, übersieht diesen Angriffsvektor: Benachbarte Netzwerkinfrastrukturen können von einem Angreifer als Proxy genutzt werden.

Messbare Fortschritte

Am 02.12.2024 veröffentlichte das National Institute of Standards and Technology (NIST) die überarbeiteten Versionen seiner Leitfäden zu Messungen in der Informationssicherheit. Teil 1 der Special Publication SP 800-55 legt den Schwerpunkt auf die Auswahl und Bewertung von Sicherheitsmaßnahmen, Teil 2 behandelt die Integration dieser Messmethoden in ein ISMS. Ziel ist, den Erfolg von Schutzmaßnahmen nicht isoliert zu bestimmen, sondern damit Entscheidungen und das Risikomanagement zu unterstützen.

Die Neuauflagen ersetzen die Versionen von 2008 und berücksichtigen aktuelle Standards wie das NIST Cybersecurity Framework 2.0. Beide bieten wertvolle Anregungen zur Umsetzung eines der meistgescheuten Themen der Informationssicherheit.



Secorvo News

Secorvo Seminare

Werfen Sie doch einen Blick in unseren Seminarkalender, damit Sie Ihre Weiterbildung 2025 nicht aus den Augen verlieren. So bereiten wir Sie im März gerne auf die T.I.S.P.- und die T.P.S.S.E.-Zertifizierung vor.

Programm und Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Wer zahlt die Zeche?

Risiken kann man ignorieren, reduzieren – oder transferieren. Mit der Zunahme erfolgreicher Cyberangriffe steigt daher auch die Nachfrage nach Cyber-Versicherungen. Im Februar 2024 widmete die BaFin diesem Thema sogar einen Fachartikel.

Aber wie das so ist im Leben: Erst im Ernstfall zeigt sich, was eine Vereinbarung wert ist. Denn nicht jeder Vorfall ist automatisch auch ein Versicherungsfall – angesichts der wachsenden Vorfallszahlen und sinkender Margen im Cyber-Versicherungsgeschäft wird aus einem Vorfall schnell ein Streitfall. Welche Fragen dabei zu klären sind und was Versicherungsnehmer schon bei Vertragsabschluss beachten sollten, erläutert anschaulich und spannend an realen Beispielen Dr. Christian Förster (Bartsch Rechtsanwälte) beim Jahresauftakt-Event 2025 der Karlsruher IT-Sicherheitsinitiative am **27.02.2025** um 18:00 Uhr im Saal Baden (IHK Haus der Wirtschaft). Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking".

Wir freuen uns auf Ihr Kommen – und empfehlen eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2025	
10.-12.01.	ShmooCon 2025 (The Shmoo Group, Washington DC/US)
20.-22.01.	Omnisecure 2025 (in TIME berlin, Berlin)
Februar 2025	
11.-12.02.	32. DFN-Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)
12.-14.02.	IT-Defense 2025 (cirosec, Stuttgart)
19.-20.02.	ID:SMART Workshop 2025 (CAST e.V., Darmstadt)
27.02.	KA-IT-Si-Event „Wer zahlt die Zeche?“ (KA-IT-Si, Karlsruhe)
März 2025	
10.-14.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
17.-21.03.	31st Fast Software Encryption Conference (IACR, Rom/IT)
18.-20.03.	secIT 2025 (heise Medien, Hannover)
24.-27.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
April 2025	
01.-04.04.	DFRWS EU 2025 (DFRWS, Brno/CZW hybrid)
01.-04.04.	Black Hat Asia 2025 (Black Hat, Singapur/ASE)
07.-10.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Ion Barza, Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Januar 2025



„Bisher noch nie gehackt“

Die elektronische Patientenakte (ePA) ist im Grunde eine gute Sache: weniger Papier, überall verfügbar. Verständlich, dass Bundesgesundheitsminister Karl Lauterbach sie endlich für alle einführen will. Die Akte enthält jedoch äußerst vertrauliche Daten. Ein besonders sicheres Konzept und eine sorgfältige technische Umsetzung sind daher unerlässlich. In seiner Rede im Bundestag zum Gesundheitsdatennutzungsgesetz versicherte Lauterbach, das aktuelle System verwende Technik, die „bisher noch nie gehackt werden“ konnte.

Die Gematik, die das System betreibt, hatte 2024 das Fraunhofer SIT mit einer Sicherheitsanalyse beauftragt. Wer den Bericht (und nicht nur die Zusammenfassung) liest, findet darin reichlich begründete Kritik. Heraussticht, dass es keine Sicherheitsanforderungen an die von Praxen, Apotheken und Krankenhäusern verwendeten sogenannten Primärsysteme gibt. Die Gematik befand hingegen am 10.10.2024, dass das Gutachten die Sicherheit des ePA-Systems bestätige. Zu einem anderen Ergebnis kamen Martin Tschirsich und Bianca Kastl auf dem 38. Chaos Computer Congress. In ihrem Vortrag zeigten sie, dass es diverse, teils einfach ausnutzbare Schwachstellen gibt. So wird beim Zugriff auf die Akte auf die kryptografische Prüfung der Kartennummer verzichtet, sodass jeder Leistungserbringer (oder wer sich erfolgreich als solcher ausgibt) Zugriff auf sämtliche 70 Mio. Akten hat. Die Gematik reagierte darauf am 27.12.2024 mit dem Hinweis, dass die gezeigten Angriffe illegal und technisch komplex seien – kündigte jedoch (offensichtlich notwendige) Nachbesserungen vor dem bundesweiten Rollout an.

Jeder Versicherte kann der Nutzung der ePA widersprechen – auch vorläufig. Wie das geht, erklärt beispielsweise der BayLfD. Sollte die Gematik die Sicherheitsprobleme beheben, lässt sich die Entscheidung jederzeit rückgängig machen.



Inhalt

„Bisher noch nie gehackt“

Security News

LOTL-Ransomware

Langwellenhacking

Nicht ob, sondern wann

Wer den Schaden hat...

Sehr geehrte/r ???

Am Verteilnetz vorbei

Nur noch mit SID

Kurze Schlüssel

Secorvo News

Der lange Weg zur quantenresistenten PKI

Weiterbildung und Zertifizierung

Wer zahlt die Zeche?

Veranstaltungshinweise

secorvo
security consulting

Security News

LOTL-Ransomware

Ransomware-Angriffe ohne Schadcode funktionieren auch in der Cloud. Das Halcyon Research Team berichtete am 13.01.2025, dass Hacker über ausgespähte Administratorkonten beispielsweise in AWS S3 dafür die Funktion SSE nutzen, die die Cloud-Datenspeicher verschlüsselt – mit der Option -C, die eigene Schlüssel verwendet. Diese erhält das betroffene Unternehmen nach der Lösegeldzahlung. Um den Druck zu erhöhen wird über die Funktion Object Lifecycle eine automatische Löschung nach einer festen Anzahl Tage eingestellt. Die Methode ähnelt dem ShrinkLocker, der Windows' BitLocker verwendet, um lokale Systeme zu verschlüsseln. Auch Angreifer beherzigen offenbar „Don't roll your own Crypto". Amazon empfiehlt am 15.01.2025 vier Schutzmaßnahmen: Deaktivieren von SSE-C (sic!), Authentifizierung mit Amazons Security Token Service, Erstellung von Sicherheitskopien und Nutzung der Überwachungsfunktionen.

Langwellenhacking

Beim 38. Chaos Computer Congress stellten Luca Melette und Fabian Bräunlein vom Berliner IT-Sicherheitsunternehmen Positive Security am 28.12.2024 die Ergebnisse ihrer Untersuchungen zur Funkrundsteuertechnik vor. Sie wird von Energieversorgern genutzt, um z. B. große Stromverbraucher und erneuerbare Stromerzeuger ein- und auszuschalten. Dazu nutzt es leistungsfähige Langwellensender ähnlich dem Zeitzeichensender DCF77. Die Technik wurde Anfang der 90er Jahre entwickelt und versendet unsignierte Nachrichten. Die Forscher zeigten, wie sie mit einfachster Technik Ampeln ein- und Photovoltaik-Anlagen abschalten konnten. Mit starken Sendern ließe sich das Stromnetz destabilisieren, da etwa 1,5 Millionen Empfänger betroffen sind, die rund 16 % der Stromproduktion und fast 30 % des Verbrauchs steuern.

Der Vortrag erinnert an den Angriff über analoge UKW-Funktechnik, mit dem Hacker 2023 bei polnischen Zügen eine Notbremsung auslösten (SSN 9/2023). Wie schon damals vermutet gibt es noch immer „Legacy-Systeme" mit unsicherer Technik in sicherheitsrelevanten Umgebungen.

Nicht ob, sondern wann

Seit über 30 Jahren wird über Quantencomputer diskutiert, die Verschlüsselungsverfahren wie RSA und ECDSA brechen könnten. Auch wenn Skeptiker bezweifeln, ob solch ein Quantencomputer jemals relevant wird, spielt diese Frage für die Planung des Umstiegs auf die seit dem vergangenen Jahr standardisierten Post-Quanten-Kryptoverfahren (PQC) keine entscheidende Rolle mehr – denn Aufsichtsbehörden und Fachgremien fordern den Umstieg auf PQC in ihren Compliance-Anforderungen und Best-Practice-Empfehlungen.

Nach Moscas Ungleichung entsteht Handlungsdruck, wenn die Summe aus dem Zeitbedarf für die Migration und dem Zeitraum, in dem herkömmlich verschlüsselte oder signierte Daten sicher bleiben müssen, die geschätzte Zeit bis zur Verfügbarkeit eines geeigneten Quantencomputers erreicht.

Das BSI ging 2023 noch davon aus, dass dieser Zeitraum 20 Jahre beträgt. In seinem am 02.01.2025 veröffentlichten Update zum Stand 2024 wurde die Schätzung auf 16 Jahre verkürzt, also bis 2040. In den USA fordert die NSA für "National Security Systems", mit dem Umstieg z. B. beim TLS-Schlüsselaustausch bereits jetzt zu beginnen, bei Public-Key-Infrastrukturen (PKIs) spätestens 2030. Verantwortliche für Schlüsselmanagementsysteme, PKIs und ähnliche kryptografische Infrastrukturen sollten daher bald über eine Migration zu PQC nachdenken und mit den Vorbereitungen beginnen.

Wer den Schaden hat...

Am 18.11.2024 entschied der Bundesgerichtshof, dass Betroffene Anspruch auf Schadensersatz haben, wenn sie infolge eines DSGVO-Verstoßes kurzzeitig die Kontrolle über ihre personenbezogenen Daten verlieren. Auf eine missbräuchliche Verwendung der Daten oder sonstige negative Folgen komme es nicht an. Einen anderen Standpunkt vertritt das Bundesarbeitsgericht (BAG), das am 20.06.2024 einen Schadensersatzanspruch wegen einer nicht vollständig erteilten Auskunft ablehnte. Die Verletzung des Auskunftsanspruchs begründe keinen immateriellen Schaden; das hypothetische Risiko einer missbräuchlichen Verwendung reiche nicht aus. Zwei höchstrichterliche Entscheidungen entgegengesetzten Inhalts – das Thema wird die Gerichte weiter beschäftigen.

Sehr geehrte/r ???

Am 09.01.2025 hat der europäische Gerichtshof in einem praxisrelevanten Urteil entschieden, dass die französische SCNF in ihrem Online-Fahrkarten-Shop die Anrede nicht verpflichtend abfragen darf. Zwar sei es höflich, bei der Ansprache der Kunden eine korrekte Anrede zu verwenden, aber keineswegs erforderlich - folglich handele es sich um eine freiwillige Angabe. Unternehmen sollten daher ihre Kontaktformulare auf Webseiten oder in Apps daraufhin überprüfen, ob die Angabe der Anrede tatsächlich dem Betroffenen überlassen bleibt.

Am Verteilnetz vorbei

Kevin Beaumont dokumentierte im Dezember 2024 in seinem Blog detailliert die DDOS-Angriffe der pro-russischen Gruppe NoName057(16) auf britische Websites. Die Angreifer, die auch in Deutschland aktiv waren, umgingen die vor die Webseiten geschalteten Content Delivery Networks (CDN) und griffen direkt die Ursprungsserver an, die oft leicht zu finden sind – davor schützt auch nicht die Wahl eines schwer zu erratenden Servernamens, wie beispielsweise von Akamai empfohlen. Wirksamen Schutz bietet nur eine Firewall, die den Zugriff auf den Ursprungsserver ausschließlich Servern des CDN erlaubt. Akamai bietet mit Site Shield und Origin IP ACL eine solche Lösung an, wie Laban Sköllermark am 13.12.2023 ausführlich erläutert hat.

Nur noch mit SID

Am 11.02.2024 wird es soweit sein: Der von Microsoft ursprünglich für Februar 2023 angekündigte und mehrfach verschobene Patch für AD-Domain-Controller zum besseren Schutz gegen Goldene Zertifikate wird ausgerollt. Anschließend werden Domain-Controller eine zertifikatsbasierte Anmeldung am AD (wie etwa Smartcard-Logon oder TLS-ClientAuthentifikation) nur noch akzeptieren, wenn in einer Erweiterung des Zertifikats der nicht änderbare Security Identifier (SID) des betreffenden AD-Kontos aufgeführt ist. Die AD Certificate Services („Microsoft PKI“) selbst wurden schon vor Jahren entsprechend angepasst, aber für die SCEP- und PKCS-Konnektoren, über die Intune Zertifikate für gemanagte Geräte und Benutzer abruft, hat Microsoft erst kurz vor Toresschluss Updates bereitgestellt. Wer Zertifikate über ein Device Management System ausrollt, sollte daher sicherstellen, dass diese – falls erforderlich – den SID enthalten.

Kurze Schlüssel

Im April 2024 veröffentlichte Andreas Wulf das Ergebnis einer Prüfung der E-Mail-Authentifizierung von einer Million Domänen und fast 500.000 DKIM-Signaturen. Dabei entdeckte er Domänen, die noch RSA-Schlüssel mit einer Länge von nur 512 Bit verwenden – und namhafte E-Mail-Provider, die so kurze Schlüssel noch akzeptieren. In einem Blogartikel vom 08.01.2025 zeigt er, dass man – wie zu erwarten – solche Schlüssel auf handelsüblicher Hardware in weniger als vier Tagen knacken kann. Allerdings betrifft dies lediglich 0,05% der von ihm analysierten Schlüssel (rund 250 Domänen). Weitere 0,31% verwenden ebenfalls nicht mehr empfohlene 768-Bit-Schlüssel. Um diese zu knacken würde seine einfache Hardware allerdings bereits Jahrzehnte benötigen.

Fast die Hälfte aller untersuchten Domänen verwenden noch 1024-Bit-Schlüssel. Dafür gibt es keinen nachvollziehbaren Grund: Das BSI empfiehlt RSA-Schlüssel mit mindestens 3000 Bit; und RFC 8301 von 2018 schreibt vor, dass E-Mail-Server auch Signaturen mit 4096-Bit-DKIM-Schlüssel prüfen können. Auch unsere Erfahrungen damit sind positiv: Bei E-Mails an etwa eintausend Domänen pro Monat hat noch kein einziger E-Mail-Server 4096-Bit-DKIM-Signaturen abgelehnt.

Secorvo News

Der lange Weg zur quantenresistenten PKI

Auf der 32. DFN-Konferenz "Sicherheit in vernetzten Systemen" am 11./12.02.2025 berichten Hans-Joachim Knobloch und Noah Freising über den Stand der Nutzbarkeit von PQC-Verfahren im Bereich PKI, unterschiedliche Ansätze, wie die Migration vonstattengehen könnte und empfehlenswerte Schritte zur Vorbereitung. Ein Vorabdruck des Beitrags ist im Linux-Magazin erschienen.

Weiterbildung und Zertifizierung

Vom **10. bis 14.03.2025** bereiten wir Sie auf die Zertifizierung zum T.I.S.P. vor – unterstützt von unserem bewährten Begleitbuch, das Sie nach Ihrer Anmeldung vorab erhalten. Am **24. bis 27.03. 2025** führen wir Sie in die Grundlagen der sicheren Softwareentwicklung ein (T.P.S.S.E.). Wie Sie PKI-Lösungen erfolgreich einführen und nutzen können, zeigt Ihnen unser Kollege Hans-Joachim Knobloch vom **07. bis 10.04.2025**. Alle Seminare sind als Weiterbildungen für die T.I.S.P.-Re-Zertifizierung anerkannt (zur Anmeldung).

Wer zahlt die Zeche?

Risiken kann man ignorieren, reduzieren – oder transferieren. Mit der Zunahme erfolgreicher Cyberangriffe steigt daher auch die Nachfrage nach Cyber-Versicherungen. Aber wie das so ist im Leben: Erst im Ernstfall zeigt sich, was eine Vereinbarung wert ist. Nicht jeder Vorfall ist auch ein Versicherungsfall – angesichts wachsender Vorfallszahlen und sinkender Margen im Cyber-Versicherungsgeschäft wird daraus schnell ein Streitfall.

Was Versicherungsnehmer schon bei Vertragsabschluss beachten sollten erläutert Dr. Christian Förster (Bartsch Rechtsanwälte) beim Jahresauftakt-Event 2025 der Karlsruher IT-Sicherheitsinitiative an Beispielen aus der Praxis am **27.02.2025** um 18:00 Uhr im Saal Baden (IHK Haus der Wirtschaft). Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (schnelle Anmeldung empfohlen).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2025	
11.-12.02.	32. DFN-Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)
12.-14.02.	IT-Defense 2025 (cirosec, Stuttgart)
19.-20.02.	ID:SMART Workshop 2025 (CAST e. V., Darmstadt)
27.02.	KA-IT-Si-Event „Wer zahlt die Zeche?“ (KA-IT-Si, Karlsruhe)
März 2025	
10.-14.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
17.-21.03.	31st Fast Software Encryption Conference (IACR, Rom/IT)
18.-20.03.	secIT 2025 (heise Medien, Hannover)
24.-27.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
April 2025	
01.-04.04.	DFRWS EU 2025 (DFRWS, Brno/CZW hybrid)
01.-04.04.	Black Hat Asia 2025 (Black Hat, Singapur/ASE)
07.-10.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Ion Barza, Paul Blenderman (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2025



Datenschutz tötet doch!

Der Datenschutz hat sein erstes Todesopfer gefordert – zum Glück kein menschliches, sondern ein technisches: das gute alte Fax.

Vor fünf Jahren wurde in Österreich das Gesundheitstelematikgesetz verabschiedet, das das Ende des Faxes im Gesundheitssystem zum 01.01.2025 besiegelte. Die Umsetzung kam, wie könnte es anders sein, für alle Beteiligten völlig überraschend. Daher gelang es auch nicht, sich rechtzeitig auf ein einheitliches sicheres Kommunikationssystem zur Ablösung des Faxes zu einigen. Den verschiedenen Parteien im Gesundheitssystem stehen nun viele verschiedene Möglichkeiten zur Kommunikation zur Verfügung, sodass es jeweils zunächst einer Abstimmung bedarf, ob über das Gesundheitspartnerportal, via FTAPI, DaMe oder gar per Ende-zu-Ende-verschlüsselter E-Mail kommuniziert werden kann und soll.

Auch in Deutschland wird immer wieder ein Faxverbot für personenbezogene Daten diskutiert und von einzelnen Aufsichtsbehörden forciert. Dienste wie KiM (Kommunikation in der Medizin) haben sich jedoch bisher nicht durchgesetzt. Dabei wäre das tatsächlich wichtig, denn eine Fax-Übertragung ist nicht nur nach heutigen Maßstäben technisch unsicher, sondern auch fehleranfällig: Eine falsche Ziffer, und der kritische und hochsensible Laborbefund landet beim Bauunternehmer statt in der Klinik.

Zunächst kommt es daher darauf an, sich auf ein sicheres, unkompliziertes und in der Praxis funktionierendes Verfahren zur Übermittlung vor allem medizinischer Daten zu einigen. Denn wenn – wie jetzt in Österreich – Befunde, Röntgenbilder etc. nur noch in Papierform oder auf USB-Sticks per Post oder Kurier verschickt werden dürfen, dann ist möglicherweise doch nicht auszuschließen, dass Professorin Buyx Recht hat und durch ein datenschutzkonformes Verbot von Faxen Menschenleben gefährdet werden.



Inhalt

Datenschutz tötet doch!

Security News

Nur ein einziger Buchstabe

Maschinenrechte

Geheimdienstbewerber

Vertrauen durch Transparenz

Digitalisierung in der Praxis

Your boss is watching you

Kein „Schrems III“?

Secorvo News

Secorvo Seminare

Krypto-Blackout

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Nur ein einziger Buchstabe

Am 14.01.2025 berichtete Philippe Caturegli vom IT-Sicherheitsunternehmen Seralys von einem winzigen Fehler mit großer Wirkung. Mastercard hatte im DNS für ihre Domäne „az.mastercard.com“ fünf Nameserver eingetragen. Einer davon endete irrtümlich nicht auf „akam.net“ (die Domäne des DNS-Anbieters Akamai), sondern auf „akam.ne“. Doch „.ne“ ist die TLD von Niger. Durch Registrieren von „akam.ne“ hätte etwa jede fünfte Anfrage bei Mastercard manipuliert und angegriffen werden können. Dieser Fehler blieb mehr als vier Jahre unentdeckt.

Caturegli registrierte die Domäne und analysierte die bei seinem Server eintreffenden DNS-Anfragen. Dabei stellte er fest, dass auch andere Akamai-Kunden denselben Fehler gemacht hatten. Brian Krebs ergänzte am 22.01.2025, ein Russe habe die Domäne zwischen 2016 und 2018 besessen und in der Zeit Anfragen an einen gemieteten Server in Deutschland weitergeleitet. Ein heikler und möglicherweise gar nicht so seltener Fehler – Mastercard ist vermutlich nicht das einzige Unternehmen, dem ein Buchstabe in der DNS-Konfiguration fehlt.

Korrektheit und Konsistenz der DNS-Konfiguration sind entscheidende Sicherheitsattribute. Dabei können Verfahren wie „Configuration as Code“ und eine regelmäßige Überprüfung helfen.

Maschinenrechte

Das Open Worldwide Application Security Project (OWASP) veröffentlichte am 10.12.2024 eine Liste der zehn kritischsten Fehler im Umgang mit Non-Human Identities (NHIs), also beispielsweise Service Accounts und API-Keys. Sie regeln die Berechtigungen in automatisierten IT-Infrastrukturen. Werden diese unsachgemäß verwaltet, können schwere Sicherheitslücken entstehen: Verwaiste Accounts und offengelegte Zugangsdaten können ein Einfallstor für Angreifer sein. Auch veraltete Authentifizierungsmethoden und übermäßige Berechtigungen erleichtern Angreifern die Arbeit.

Die OWASP-Liste zeigt nicht nur die häufigsten Fehler, sondern auch, wie sie vermieden werden können. Daher kann sie – wie die bekannten „OWASP Top 10“ – als Leitfaden für Softwareentwickler genutzt werden. Aber auch für eine Überprüfung der eigenen IT-Infrastruktur eignet sich die Liste. Vorfälle wie der Midnight Blizzard-Angriff bei Microsoft am 12.01.2024 und der Einbruch in das Okta-Support-System am 28.09.2023 verdeutlichen, welche Risiken von kompromittierten NHIs ausgehen.

Geheimdienstbewerber

Am 12.01.2025 wies der Unternehmer und Aktivist Bert Hubert öffentlich darauf hin, dass Bewerbungen für den niederländischen Geheimdienst Google bekanntgegeben werden: nicht absichtlich, sondern weil das staatliche Bewerbungsportal werkenvoornederland.nl unbedacht Google Analytics verwendet. Der Cookie-Banner bietet keine Möglichkeit, diese Datenweitergabe zu unterbinden. Dabei schreibt der Geheimdienst AIVD selbst: „Wir bitten Sie, nicht mit anderen über Ihre Bewerbung bei der AIVD zu sprechen. Es könnte Ihrer Bewerbung und Ihrer möglichen Karriere beim AIVD schaden und Ihre Sicherheit gefährden.“ Huberts Hinweis führte zu einer bisher unbeantworteten Anfrage des Abgeordneten Derk Boswijk an die Innenministerin.

Auch auf karriere.bund.de kann man sich für Stellen beim Verfassungsschutz und beim Bundesnachrichtendienst bewerben. Laut Datenschutzerklärung nutzt die Webseite die polnische Google-Analytics-Alternative Piwik PRO, wobei IP-Adressen gekürzt werden. Doch genügt das? Piwik und sein Schwesterprojekt Matomo könnten auch auf bundeseigenen Servern betrieben werden.

Immer wieder kommt es zur Preisgabe hoch sensibler Daten durch die unbedachte Verwendung von Standard-Technologie, wie 2020 die Standortdaten von Kasernen durch Fitnesstracker (SSN 11/2020).

Vertrauen durch Transparenz

Seit dem 04.02.2025 vertraut Firefox in Version 135 nur noch TLS-Zertifikaten, die in Certificate Transparency (CT) Logs erfasst sind. Dabei verpflichten sich Trust Center, alle ausgestellten TLS-Zertifikate in Protokollen zu veröffentlichen. Darüber können Zertifikate von verdächtigen Domains, wie sie beispielsweise bei Phishing-Angriffen genutzt werden, schneller gefunden und gesperrt werden. Dieses Verfahren wurde unter anderem als Reaktion auf Vorfälle bei DigiNotar und TrustWave entwickelt.

Firefox stuft nun Zertifikate, die nicht in CT-Logs erfasst sind, als unsicher ein. Chrome und Safari verfahren bereits seit 2018 so. Öffentliche Trustcenter sind damit gezwungen, CT zu nutzen. In den Browsern Firefox und Chrome lässt sich einstellen, CT für vorgegebene Hostnamen zu ignorieren.

Die neue Zertifikatstransparenz nutzen bereits Dienste wie Red Sift, die vor dem Ablaufen der Gültigkeit von Zertifikaten warnen. Crt.sh ermöglicht die Suche nach Zertifikaten, und das CT-Log-Dashboard von Cloudflare visualisiert die Daten der CT-Logs.

Digitalisierung in der Praxis

In einer Entscheidung vom 18.12.2024 stellte das Schleswig-Holsteinische OLG unter Bezugnahme auf die DSGVO fest, dass eine reine Transportverschlüsselung beim Versand geschäftlicher E-Mails zwischen Unternehmer und Kunden zumindest dann nicht ausreicht, wenn für den Schuldner ein hohes finanzielles Risiko aus einer Fälschung einer angehängten Rechnung erwächst. In diesem Fall biete die Transportverschlüsselung keinen „geeigneten" Schutz im Sinne der DSGVO.

Offen lässt das Gericht, ab welchem Betrag eine Rechnung als besonders sensibles Datum gilt. Zudem ist es zwar wünschenswert, dass sich Ende-zu-Ende-Verschlüsselung mit Verfahren wie S/MIME durchsetzt, doch spielt sie in der Praxis keine nennenswerte Rolle.

Eine wirksame Lösung wären digital signierte und damit fälschungssichere PDF-Rechnungen – doch die werden gerade von der X-Rechnung abgelöst. Will der Rechnungsempfänger das Prozessrisiko vermeiden, bleibt ihm wohl nur die Überprüfung der angegebenen Bankverbindung, bevor er einen hohen Betrag überweist – oder die Rückkehr zur Papierrechnung. Solange das noch zulässig ist.

Your boss is watching you

Am 19.12.2024 hat der Europäische Gerichtshof (EuGH) zur Verarbeitung von Arbeitnehmerdaten aufgrund einer Kollektivvereinbarung geurteilt. In Deutschland sind das insbesondere Betriebsvereinbarungen zwischen Arbeitgeber und Betriebsrat; sie sind vor allem dann erforderlich, wenn der Arbeitgeber technische Maßnahmen einführt, die sich zur Arbeitnehmerüberwachung eignen.

Die rechtlichen Anforderungen an eine solche Verarbeitung sind hoch: Es müssen sowohl die mitbestimmungsrechtlichen Fragen als auch, wie der EuGH nun höchstrichterlich feststellte, die Datenschutzgrundsätze Rechtmäßigkeit, Zweckbindung, Erforderlichkeit und Transparenz beachtet werden. Betriebsvereinbarungen nach § 26 BDSG setzen also nicht die Anforderungen der DSGVO außer Kraft.

In einer im August 2024 veröffentlichten Fallstudie stellte das unabhängige Wiener Forschungszentrum Cracked Labs fest, dass nicht nur die Nutzung von dafür gedachten Werkzeugen wie Microsofts Viva Insights eine Arbeitnehmerüberwachung darstellt. Auch der Einsatz von Cybersicherheitsanwendungen wie SIEMs oder solchen des Insider Risk Managements (Forcepoint, Sentinel, Purview) diene der Arbeitnehmerüberwachung. Er ist sowohl mitbestimmungspflichtig als auch eine Datenverarbeitung, die die Bestimmungen der DSGVO einhalten muss.

Kein „Schrems III"?

Das Privacy and Civil Liberties Oversight Board (PCLOB) ist die Beschwerdestelle für Europäer bei Datenverarbeitungen im Rahmen des EU-US Data Privacy Framework. Am 27.01.2025 nun hat das PCLOB bestätigt, dass die drei Mitglieder Franklin, Felten und LeBlanc von US-Präsident Trump entlassen wurden. Ohne ein funktionsfähiges PCLOB steht damit das Data Privacy Framework – ganz ohne Zutun von Max Schrems – auf der Kippe.

Wer vermeiden möchte, dass seine auf dem Data Privacy Framework basierende Verarbeitung plötzlich ohne Rechtsgrundlage dasteht, sollte auf die nach dem Ende des EU-US Privacy Shields geschaffenen Werkzeuge für Datenübermittlungen in unsichere Drittstaaten zurückgreifen.

Secorvo News

Secorvo Seminare

Wissens-Booster: Nutzen Sie das Seminar IT-Security Insights – T.I.S.P.-Update am **29. und 30.04. 2025**, um sich in der IT-Sicherheit auf den aktuellen Stand zu bringen.

Im Ernstfall die Nerven und den Überblick bewahren? Als Vorfall-Experte (BSI) sind Sie für den Worst Case gewappnet. Vom **06. bis 08.05.2025** bereiten wir Sie auf die Zertifizierung vor.

Alle Seminare bei Secorvo sind als Weiterbildungen für die T.I.S.P.-Rezertifizierung anerkannt. Programm und Online-Anmeldung unter www.secorvo.de/seminare.

Krypto-Blackout

Die Entwicklung der Quantencomputer bedroht alle heute eingesetzten kryptografischen Verfahren und schreitet offenbar schneller voran, als noch vor wenigen Jahren erwartet. Die Migration auf quantenresistente Public-Key-Verfahren wird daher in den kommenden Jahren zur Herausforderung – und möglicherweise zu einem Wettlauf gegen die Zeit.

Beim **KA-IT-Si-Event** am **03.04.2025** im House of Living Labs (FZI) zeigt Hans-Joachim Knobloch (Secorvo), welche praktischen Herausforderungen sich beim Umstieg auf die neuen, so genannten ‚Post-Quantum'-Kryptoverfahren stellen.

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2025	
10.-14.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
17.-21.03.	31st Fast Software Encryption Conference (IACR, Rom/IT)
18.-20.03.	secIT 2025 (heise Medien, Hannover)
April 2025	
01.-04.04.	DFRWS EU 2025 (DFRWS, Brno/CZ hybrid)
01.-04.04.	Black Hat Asia 2025 (Black Hat, Singapur/ASE)
03.04.	Event „Krypto-Blackout“ (KA-IT-Si, Karlsruhe)
08.-10.04.	PQCrypto 2025 (IACR, Taipeh/TW)
28.04.-01.05.	RSA Conference 2025 (RSA, San Francisco/US)
29.-30.04.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
Mai 2025	
04.-08.05.	Eurocrypt 2025 (IACR, Madrid/ES)
06.-08.05.	Vorfall-Experte (BSI) (Secorvo, Karlsruhe)
06.-09.05.	European Identity & Cloud Conference 2025 (KuppingerCole, Berlin)

Fundsache

Am 10.02.2025 hat TeleTrusT einen Forderungskatalog zur Umsetzung des Konzepts „Cyber-Nation“ veröffentlicht. Die beiden letzten Forderungen des Katalogs sollten Grundpfeiler der Informationssicherheit in jedem Unternehmen sein.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Ion Barza, Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende (Editorial), Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

März 2025



Selbstmord aus Todesangst?

Den Begriff des „Quantencomputers“ prägten die Physiker Paul Benioff und Richard Feynman im Jahr 1981. Gut 40 Jahre später gibt es erste Prototypen für Quantenprozessoren. Einige Herausforderungen wie die hohe Fehlerrate sind noch nicht gelöst, aber es ist vorstellbar, dass in einigen Jahrzehnten leistungsfähige Quantencomputer existieren. Sollte das gelingen, droht ein „Krypto-Blackout“: Mit einem Schlag wären fast alle im Internet genutzten Verschlüsselungen und Signaturen wirkungslos, denn mit dem Algorithmus von Peter Shor (1994) ließen sich die heute eingesetzten asymmetrischen Kryptoverfahren in kürzester Zeit brechen.

Damit könnte sich die Geschichte wiederholen: 1863 zeigte Friedrich Wilhelm Kasiski, wie man die Vigenère-Chiffre bricht – sie hatte seit dem 16. Jahrhundert als unknackbar gegolten. Nachrichtendienste und Militärs mussten auf simple Codebücher umstellen. Dadurch gelang dem britischen Geheimdienst 1917 die Entschlüsselung des „Zimmermann-Telegramms“, dessen Bekanntwerden zum Eintritt der USA in den ersten Weltkrieg führte. Das Brechen der Rotormaschine Enigma im zweiten Weltkrieg durch polnische und britische Kryptoanalytiker entschied den U-Boot-Krieg – erst der Data Encryption Standard (DES) beendete 1977 diesen Blackout.

Heute wäre ein Krypto-Blackout weit mehr als ein diplomatischer oder militärischer Rückschlag. Daher bemühen sich seit 10 Jahren Kryptologen weltweit um die Entwicklung von quantencomputerresistenten kryptografischen Algorithmen. Im August 2024 wurden die ersten Verfahren als NIST-Standard verabschiedet, und die NSA kündigte an, ab 2033 nur noch Post-Quantum-Kryptografie einzusetzen. Dabei sind die Verfahren längst nicht so gut untersucht wie RSA und DSA, und die Protokollstandards sind nicht einmal alle angepasst. Doch unsichere Post-Quantum-Verfahren, inkompatible Implementierungen und eine übereilte Umstellung können auch zum Blackout führen – sogar ganz ohne Quantencomputer.



Inhalt

Selbstmord aus Todesangst?

Security News

Fix geklickt

Wer kürzer gilt…

Sesam, öffne dich!

Rififi im Cyberspace

Memory Safety

Angriff via Webcam

Schlüssel statt Wörter

Krypto-Fragilität

Secorvo News

Zertifiziertes Know-how

Kettenregeln

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Fix geklickt

Am 13.03.2025 berichtete Microsoft über eine Phishing-Welle, die auf das Gastgewerbe zielt. Auf der in den (vorgeblich von Booking.com stammenden) E-Mails verlinkten Webseite soll der Anwender durch Tastenanschläge beweisen, dass er kein Automat ist – doch die Tastenfolge „Windows+R", „Strg+V" und „Enter" führt (auf Windows-Systemen) den Inhalt der Zwischenablage aus. Dorthin hat die Webseite zuvor ganz einfach per Javascript den Bootstrap-Code kopiert.

Davor schützt Awareness-Training nur begrenzt. Wenn ein strenges Zulassen nur vertrauenswürdiger Anwendungen (Application-Whitelisting) nicht infrage kommt, sollte zumindest die Ausführung von Programmen aus dem „Downloads"-Ordner und von HTML-Applikationen unterbunden werden. Das gelingt mit AppLocker. Wirksam ist auch das Abschalten der „Run/Ausführen"-Option im Startmenü per Gruppenrichtlinie. Und noch besser wäre es, wenn Javascript erst gar nicht via Zwischenablage aus der Browser-Sandbox ausbrechen dürfte.

Wer kürzer gilt...

Am 19.02.2025 hat Let's Encrypt ihr erstes kurzlebiges Zertifikat mit einer Gültigkeitsdauer von nur 6 Tagen ausgegeben. Das soll die Sicherheit des Webs verbessern, weil so ein abhanden gekommener TLS-Schlüssel auch ohne die Sperrung des Zertifikats nur kurz von einem Angreifer missbraucht werden kann. Die kurze Gültigkeit soll sogar das Prüfen auf Rückrufe ersetzen: Let's Encrypt verzichtet auf die Erstellung von CRLs und auf die Bereitstellung eines OCSP-Dienstes für diese Zertifikate. Sperrauskünfte sind aufgrund der hohen Verfügbarkeitsanforderungen aufwendig und können Fehlermeldungen auslösen, die die Benutzer überfordern. Firefox unterstützt das: Zertifikate mit einer Gültigkeitsdauer unter 10 Tagen gelten automatisch als „Revocation Checked".

Let's Encrypt hat dazu das ACME-Protokoll um die Auswahl eines Zertifikatsprofils erweitert. Damit können nun auch Zertifikate für (öffentlich zugewiesene) IP-Adressen beantragt werden. Wer den Mechanismus nutzen möchte, muss auf seiner Webseite dafür den Zertifikatserneuerungsprozess automatisieren.

Sesam, öffne dich!

Wenn Zutrittssysteme Schwachstellen aufweisen, können sie „klassischen" Einbrechern die Türen öffnen. Ein besonders drastisches Beispiel meldete am 15.02.2025 der Kanadier Eric Daigle: Er entdeckte zufällig, dass die Zutrittskontrollsysteme „Enterphone MESH" von Identiv (heute Hirsch) mit voreingestellten Passwörtern ausgeliefert wurden und die Einrichtungsprozedur diese nicht ändert. Eine simple Internetsuche findet bis heute über 2.000 dieser Systeme. Mit dem Schwachstellenscanner Nuclei fand Daigle heraus, dass man sich auf 43 % der erreichbaren Systeme mit dem Standardpasswort anmelden kann.

Das niederländische IT-Sicherheits-Unternehmen Modat veröffentlichte am 25.02.2025 die Ergebnisse einer viel breiter angelegten Untersuchung von über das Internet erreichbaren Zutrittskontrollsystemen. Dabei wurden 49.000 Systeme entdeckt – bei jedem dritten System konnten Daten ausgelesen werden; manche gaben sogar biometrische Daten preis. Dabei ist das Problem altbekannt (siehe „Ali baba und die 40 Räuber", SSN 10/2002).

Rififi im Cyberspace

Der vielleicht bekannteste Raub der Filmgeschichte begann mit der Übernahme der Hausmeisterwohnung über einem Juweliergeschäft – der bisher größte digitale Raub mit der Übernahme des Arbeitsplatzrechners eines Entwicklers einer Blockchain-Wallet-Software. Schaden: ca. 1,4 Mrd. US$.

Die Kryptobörse ByBit nutzt Multi-Signatur-Transaktionen, um Blockchain-Transaktionen mit mehr als einem privaten Schlüssel abzusichern. Sie werden von mehreren einzelnen Signaturen freigegeben, was sich auf der Ethereum-Blockchain mithilfe von Smart-Contracts realisieren lässt. Der Smart-Contract für die Cold-Wallet von ByBit wurde jedoch am 21.02.2025 durch einen mit Backdoor ersetzt. Dabei zeigte die manipulierte Wallet-Software eine harmlose Regel-Transaktion an; der CEO prüfte die Transaktion vor seiner abschließenden (dritten) Signatur nur in der Online-App und nicht auf der Signier-Hardware. Anschließend wurden aus der Wallet über eine Milliarde US$ in Coins und Tokens abgezogen.

Nach dem Raub stückelten, tauschten und mischten die Täter ihre Beute, um vor dem Umtausch in „echtes" Geld die Herkunft zu verschleiern, damit Verfolger die Blockchain-Transaktionen nicht einfrieren können. Die Vorgehensweise deutet auf nordkoreanische „Devisenbeschaffer" hin.

Memory Safety

Am 22.01.2025 rief die Association for Computing Machinery (ACM) in ihren *Communications of the ACM* dazu auf, Speichersicherheit endlich zum Standard in der Softwareentwicklung zu machen. Gemeint ist nicht nur der Einsatz zusätzlicher Schutzmechanismen, sondern auch der Wechsel zu spei-

chersicheren Programmiersprachen wie Rust, Swift oder Python. Untersuchungen von Microsoft, Google, NSA sowie CISA belegen, dass nach wie vor sehr viele sicherheitskritische Schwachstellen auf Speicherfehler zurückgehen – etwa durch fehlerhafte Zeigerarithmetik oder Use-after-free-Bugs in C und C++. Die ACM verweist auf die Plattform memorysafety.org, die Wissen, Werkzeuge und Hilfestellungen für den Umstieg bereitstellt.

Google ersetzt in Android-Komponenten C++ bereits durch Rust, Microsoft nutzt Rust für sicherheitskritische Teile von Windows und auch im Linux-Kernel hat Rust Einzug gehalten. Doch das Ersetzen bestehender Software ist mühsam. Wer jedoch weiter auf C oder C++ setzt, muss zumindest für harte Compiler-Optionen, statische Analyse und Laufzeitschutz sorgen.

Angriff via Webcam

Das IT-Sicherheitsunternehmen S-RM berichtete am 05.03.2025, dass die Ransomwaregruppe Akira durch die Übernahme einer ungesicherten Webcam die Endpoint Detection and Response-Software (EDR) umgehen und von dort Netzwerklaufwerke verschlüsseln konnte. Lessons Learned: IoT-Systeme wie Webcams, die öfter Sicherheitslücken aufweisen als Windows-Clients oder Linux-Server, sollten stets in separaten Netzwerksegmenten betrieben werden.

Schlüssel statt Wörter

Mandiant zeigte in einem Beitrag vom 17.03.2025 einen Demonstrator für Phishing mit Browser-in-the-Middle. Damit können Angreifer Sessions und MFA-Codes abfangen, ohne Aufwand in den Nachbau einer Phishing-Webseite stecken zu müssen. Angriffe dieser Art lassen sich durch phishing-resistente Passkeys abwehren. Sie sind ein Ersatz für Passwörter und basieren auf einem Mechanismus, der auch der clientseitigen TLS-Authentifikation (mTLS) zugrunde liegt: Die Nutzer erzeugen ein Schlüsselpaar, hinterlegen den öffentlichen Schlüssel beim verwendeten Dienst und signieren mit dem privaten Schlüssel eine Challenge.

Passkeys haben weitere Vorteile gegenüber Passwörtern: Wenn Angreifer den Server kompromittieren, erbeuten sie nur den öffentlichen Schlüssel, Nutzer können den privaten Schlüssel in sicherer Hardware ablegen und es ist sogar möglich, Nachweise über den Speicherort des privaten Schlüssels zu erstellen. Diensteanbieter können damit beispielsweise die Verwendung von sicherer Hardware vorschreiben – und kontrollieren.

Krypto-Fragilität

Im Zuge der forcierten Migration auf quantenresistente Kryptoalgorithmen hat das NIST am 05.03.2025 den Initial Public Draft eines Whitepapers zu Crypto-Agility veröffentlicht. Dass das Erreichen des hehren Ziels, schwach gewordene Kryptoalgorithmen schnell durch neue zu ersetzen, kein intuitiver Selbstläufer ist, zeigt sich schon daran, dass zwei unterschiedliche Definitionen von Krypto-Agilität verwendet werden – eine für technische Systeme und eine für Kommunikationsprotokolle.

So ist das Whitepaper eher ein Problemaufriss der hässlichen Seiten der Krypto-Agilität: Herausforderungen bei Interoperabilität, Ressourcenverbrauch und Performance. Und der nachteiligen Auswirkungen in Bezug auf andere Sicherheitsaspekte: Schwierigkeiten bei der Sicherheitsbewertung, erhöhter Schutzbedarf der Aushandlung von Algorithmen und für Updates von Soft- und Firmware im Feld sowie das Restrisiko, den Zugriff auf vorhandene Daten zu verlieren.

Secorvo News

Zertifiziertes Know-how

Im Ernstfall die Nerven und den Überblick bewahren? Als Vorfall-Experte (BSI) sind Sie für den Worst Case gewappnet. Das nächste Seminar findet vom **06. bis 08.05.2025** statt. Noch gibt es freie Plätze.

Mit über 2.200 „T.I.S.P.lern“ ist der TeleTrusT Information Security Professional in der DACH-Region mittlerweile ein renommierter Nachweis für IT-Security-Expertise. Unsere Consultants – die Autoren des T.I.S.P.-Buchs – bereiten Sie vom **19. bis 23.05.2025** auf die Zertifizierung vor.

Alle Seminare bei Secorvo sind als Weiterbildungen für die T.I.S.P.-Re-Zertifizierung anerkannt (Programme, Online-Anmeldung).

Kettenregeln

In der Softwareentwicklung bedient man sich heute zahlreicher Bibliotheken aus Open-Source-Software oder von Zulieferern. Dadurch wird es schwieriger, die große Zahl direkter und indirekter Abhängigkeiten zu überblicken und auf einem aktuellen Stand zu halten. Beim KA-IT-Si-Event am **15.05.2025** im dm-dialogicum zeigt Christian Kühn (dmTECH), wie man automatisiert Transparenz über bekannte Schwachstellen in den verwendeten Bibliotheken sowohl im Entwicklungsteam als auch in der zentralen Sicherheitsorganisation herstellen kann. Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Wie immer empfehlen wir eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2025	
28.04.-01.05.	RSA Conference 2025 (RSA Conference, San Francisco/US)
Mai 2025	
04.-08.05.	Eurocrypt 2025 (IACR, Madrid/ES)
06.-08.05.	Vorfall-Experte (BSI) (Secorvo, Karlsruhe)
06.-09.05.	European Identity & Cloud Conference 2025 (KuppingerCole, Berlin)
12.-15.05.	PKC 2025 (IACR, Roros/NO)
13.-15.05.	26. Datenschutzkongress (EUROFORUM, Berlin)
15.05.	Kettenregeln (KA-IT-Si, Karlsruhe)
19.-20.05.	CIO Cybersecurity Summit 2025 (CIO, München)
19.-23.05.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
20.-22.05.	Datenschutztage 2025 (WEKA, Frankfurt)
26.-28.05.	BvD Verbandstage 2025 (BvD, Berlin)
26.-28.05.	OWASP 2025 Global AppSec (OWASP Foundation, Barcelona/ES)

Fundsache

In einer süffisanten Parabel „A long time ago, in a faraway kingdom“ legt der Kryptologe Peter Gutmann dar, warum er die Ressourcen, die in die Entwicklung und Migration zu Post-Quantum-Kryptografie fließen, für Fehlinvestitionen hält. Andere Experten sehen das anders.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Ion Barza, Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2025



Erpressbar

Drei Jahre ist es her, da erschrak Deutschland anlässlich des russischen Angriffs auf die Ukraine ob der Einsicht, dass rund 55% der Gaslieferungen aus Russland stammten – und 25% der deutschen Gasspeicher dem Energiekonzern Gazprom gehörten: Wir waren erpressbar. Die Verringerung dieser über Jahrzehnte gewachsenen Abhängigkeit gelang – und hat ein Vermögen gekostet. Doch seit über zehn Jahren stürzen wir uns – noch blauäugiger – in eine Abhängigkeit, die weit dramatischere Auswirkungen haben kann: die Nutzung amerikanischer Cloud-Anbieter für zentrale IT-Services. Nach dem Cloud-Report 2024 des Bitkom verfolgen 40% der deutschen Unternehmen eine „Cloud-only"- oder „Cloud-first"-Strategie. Hauptmotiv: Kostensenkung (62%). Dass das zum Bumerang wird, spüren gerade immer mehr Unternehmen – die Cloud-Anbieter drehen an der Preisschraube. Denn der Weg zurück ist den Firmen versperrt, die Cloud ein Oneway Ticket: Anbieter nehmen ihre On-Premise-Produkte vom Markt, und der interne Know-How-Verlust bei gleichzeitigem IT-Fachkräftemangel macht eine Rückkehr zum Eigenbetrieb zum riskanten Gewaltakt.

Weniger als 20% der Unternehmen setzten 2024 noch auf „On-Premise"-Lösungen – Tendenz: fallend. Und nun hat Amerika einen Präsidenten, dem fast jede Drohung recht ist, wenn sie der Durchsetzung seiner Interessen dient. So wird aus dem betrieblichen Risiko der Cloud-Abhängigkeit ein volkswirtschaftliches – und damit politische Erpressbarkeit: Ein Exportverbot für amerikanische Software-Dienstleistungen würde in Europa die Lichter ausgehen lassen.

Diese Befürchtung hat Jürgen Hill bereits kurz nach der Wahl Trumps geäußert. Am 30.03.2025 brachte Max Schrems seine Besorgnis in einem Interview mit der Süddeutschen Zeitung zum Ausdruck. Passiert ist bisher wenig. Vielleicht hat Max Muth recht, wenn er (in einem Essay der Süddeutschen vom 19.04.2025) schreibt: „Es wäre naiv zu glauben, dass Deutschland aus seinen Fehlern lernt."



Inhalt

Erpressbar

Security News

Angriff aus dem toten Winkel

Wege ins Paradies

Trau, schau, wem!

Konsolidierung

Lizenz zum Signieren

Nachlässigkeiten

Nachtigall, ick hör dir trapsen

Das Buch zum Tool

Secorvo News

Kettenregeln

Secorvo Seminare

Veranstaltungshinweise

secorvo
security consulting

Security News

Angriff aus dem toten Winkel

Das IT-Sicherheits-Unternehmen SecurityScorecard hat am 24.02.2025 die Analyse eines riesigen Botnets veröffentlicht. Es umfasst mehr als 130.000 kompromittierte Geräte, die großangelegte Passwort-Spray-Angriffe auf Microsoft 365-Konten ausführen; mutmaßlich stammt es aus China.

Die Bots nutzen Protokolle wie POP, IMAP und SMTP, die meist eine reine Passwort-Authentifizierung (Basic Authentication) verwenden. Von Entra ID werden sie als „Non-interactive Sign-ins" gewertet. In dieselbe Kategorie fallen jedoch auch automatisierte Reauthentifizierungen bei modernen Token-basierten Verfahren, die oft den Großteil der Anmeldeereignisse ausmachen – und deshalb von vielen Überwachungssystemen ausgeblendet werden. Die Aktivitäten des Bot-Netzes werden daher leicht übersehen. Zwar kann man die Erfassung erweitern – doch besser ist es, die Nutzung von Basic Authentication wo immer möglich zu beenden und abzuschalten.

Wege ins Paradies

Jeder zweite Login-Versuch im Internet nutzt kompromittierte Zugangsdaten, wie eine Studie von Cloudflare vom 17.03.2025 zeigt. Über 95% dieser Versuche erfolgen automatisiert. Besonders betroffen sind WordPress-Installationen: Hier führen in 76% der Fälle gestohlene Passwörter zu einem erfolgreichen Login. Der Sophos Active Adversary Report 2025 vom 02.04.2025 bestätigt diese Analyse: In 41% der untersuchten Fälle gelang Angreifern der Erstzugriff über gestohlene Anmeldedaten.

Auch wenn Managed-Detection-and-Response-Systeme (MDR) Angriffe schneller erkennen, beseitigt das nicht die Hauptursache: fehlende oder unzureichende Mehrfaktor-Authentifizierung. Sophos betont, dass Angreifer in vielen Fällen bereits binnen weniger Stunden die vollständige Kontrolle über ein Netzwerk erlangen, insbesondere dank „Altlasten" wie ungeschützte VPN-Zugänge.

Rapid7 ergänzt das Bild in einem Blog-Beitrag vom 10.04.2025 mit aktuellen Zahlen: Über eine Million Brute-Force-Versuche mit Tools wie FastHTTP wurden im ersten Quartal 2025 beobachtet. Zwar führten 73% dieser Versuche zu Account-Sperrungen und weitere 26% scheiterten an falschen Passwörtern. Oft reichen jedoch wenige kompromittierte Konten, um schwere Sicherheitsvorfälle auszulösen.

Die Studien zeigen: Wer auf MFA verzichtet oder veraltete Systeme offen lässt, macht es Angreifern leicht. Einmal kompromittiert, bleibt den Unternehmen oft nur wenig Zeit, um den Schaden zu begrenzen. Sichere, einmalige Passwörter und verpflichtende MFA für exponierte und kritische Dienste, gezielte Zugangsbeschränkungen und aktives Monitoring sind heute Kernelemente eines wirksamen Schutzes.

Trau, schau, wem!

Troy Hunt, Betreiber von „Have I Been Pwned?", berichtete am 25.03.2025 über eine raffinierte Attacke, bei der ein Angreifer Zugriff auf seine Mailingliste erlangte. Mittels einer überzeugenden Phishing-E-Mail brachte er Hunt dazu, seine Zugangsdaten einschließlich OTP händisch einzugeben – obwohl der Passwort-Manager die URL nicht erkannte und die Zugangsdaten daher nicht automatisch eintrug. Der Angreifer verschaffte sich damit vollen Zugriff auf Hunts Account.

Der Fall zeigt, dass auch Multi-Faktor-Authentifizierung (MFA) keinen perfekten Schutz garantiert: Gibt man die Zugangsdaten an der falschen Stelle preis, kann ein Angriff trotz MFA gelingen. Ein zunehmender Wildwuchs bei Domänennamen erschwert die Zuordnung von DNS-Namen zu Diensten und damit deren Verwaltung in Passwort-Managern stark. Ständige Wachsamkeit bleibt daher ein wichtiges Element der IT-Sicherheit.

Konsolidierung

Viele Anbieter nutzen für ihre Online-Dienste unterschiedliche Domänennamen. Das erschwert es Nutzern, Phishing-Angriffe an der URL zu erkennen. Woran soll man auch festmachen, ob z. B. die URL login.microsoftonline-p.com zu Microsoft gehört? Sie gehört – und ist bei weitem nicht die einzige (siehe Microsoft 365-URLs und-IP-Adressbereiche).

2023 beschloss Microsoft, alle Clouddienste in cloud.microsoft zusammenzuführen – schrittweise und mit Redirects, um Seiteneffekte zu minimieren. Seit Juni 2024 werden Monat für Monat wichtige Anwendungen wie Excel, Word, PowerPoint und Outlook unter Microsofts eigene Top-Level-Domäne migriert, was vor Domain-Spoofing wie z. B. homographischem Phishing schützt. Ein Beispiel, das Schule machen sollte.

Lizenz zum Signieren

Die Gültigkeit eines Deutschlandtickets bestätigt eine digitale Signatur, die der Aussteller oder sein Dienstleister beim Kauf erzeugt. Sie bindet das Ticket an einen Gültigkeitsmonat sowie an Namen und Geburtsdatum des Inhabers.

Da der Code kopiert werden kann, gilt das Ticket nur zusammen mit einem amtlichen Ausweis. Den-

noch entstehen den Verkehrsbetrieben durch Rückbuchungen bei Zahlungsvorgängen und Kopien Millionenschäden – die nun durch Ticket-Sperrlisten und Kontoverifikationen eingedämmt werden sollen, wie der Interessenverband der privaten Verkehrsunternehmen mofair am 23.04.2025 mitteilte.

Doch auch beim Schutz der Signierschlüssel hapert es zuweilen: Am 12.02.2025 ging durch die Presse, dass Käufer, die beim Fahrkartenshop D-Ticket.su ein Deutschlandticket erworben hatten, unvermittelt zu Schwarzfahrern geworden waren – der zur Prüfung benötigte Public Key war gesperrt worden. Offenbar war der Betreiber von D-Ticket.su, die RouteVibe Ltd, in den Besitz des (zwischenzeitlich gewechselten) Signierschlüssels des für das Wittenberger Busunternehmen Vetter GmbH ausgestellten und vom Dienstleister MoPla Solutions GmbH genutzten Schlüsselpaars gekommen: Es war wohl nicht in einem Hardwaremodul (HSM) gespeichert. Für öffentlich gültige Codesignaturen schreibt das CA/Browser-Forum das schon seit 2023 zum Schutz der Signierschlüssel vor.

Nachlässigkeiten

Adam Chester (SpecterOps) hat am 08.04.2025 aufgedeckt, wie wenig Sorgfalt die Entwickler von AD-SelfService Plus (ManageEngine) walten ließen: Der Master-Key seiner Datenbank wird mit einem Beispiel-Passwort aus der Microsoft-Dokumentation „geschützt". Mehr noch: Die Installationsanleitung verwendet einen Domänenadministrator-Account als Dienstekonto. Zwar beschreibt der Hersteller im Berechtigungsleitfaden die Verwendung eines eingeschränkten Dienstekontos („Principle of Least Privilege") – da die Berechtigungen jedoch für die gesamte Domäne gelten, bringt das keinen Sicherheitsgewinn. Die erforderliche Einschränkung auf bestimmte Organisationseinheiten wird nicht erwähnt.

Kein Wunder, wenn Angreifer bei solchen Herstellerempfehlungen leichtes Spiel haben.

Nachtigall, ick hör dir trapsen

Am 27.02.2025 hat Microsoft den Abschluss des „EU Data Boundary" verkündet. Das Unternehmen wirbt mit mehr Datenresidenz und Transparenz: Europäische Kunden sollen sich sicher(er) sein können, dass ihre Daten innerhalb der EU und nicht etwa in den USA verarbeitet würden. Grundsätzlich ein guter Ansatz, auch vor dem Hintergrund, dass das Data Privacy Framework zunehmend auf tönernen Füßen steht. Allerdings werden dadurch nicht die durch den CLOUD Act verursachten Risiken aus der Welt geschafft (SSN 03/2019 und SSN 09/2019): Die US-Geheimdienste behalten die Befugnis, auch in europäische Datenbestände Einblick zu nehmen. Derzeit besteht kaum Zweifel, dass die USA davon auch Gebrauch machen würden.

Tatsächlich helfen kann nur, Produkte und Dienste rein europäischer Anbieter zu nutzen. Mehr digitale Souveränität in der EU wäre die bessere Lösung.

Das Buch zum Tool

1998 startete Bernhard Esslinger das Open-Source-Projekt „CrypTool", um seine Kollegen bei der Deutschen Bank für IT-Sicherheit zu sensibilisieren. Es gelang ihm, daraus eine „Bewegung" zu machen – hunderte engagierte Studenten, Krypto-Experten und -Begeisterte beteiligten sich in den vergangenen 25 Jahren an der Programmierung, der Dokumentation und der Entwicklung des didaktischen Materials. Das Projekt wurde vielfach ausgezeichnet und wird heute in Unternehmen, Schulen und Hochschulen eingesetzt. Im November 2024 hat Professor Esslinger nun das „CrypTool-Buch" veröffentlicht – eine 750 Seiten füllende Einführung in kryptografische Verfahren und Protokolle an Beispielen mit CrypTool, dazu ein 250 Seiten starker Anhang mit Anleitungen und Leseempfehlungen.

Secorvo News

Kettenregeln

In der Softwareentwicklung bedient man sich heute zahlreicher Bibliotheken aus Open-Source-Software oder von Zulieferern. Dadurch wird es schwieriger, die große Zahl direkter und indirekter Abhängigkeiten zu überblicken und auf einem aktuellen Stand zu halten. Beim KA-IT-Si-Event am **15.05. 2025** im dm-dialogicum zeigt Christian Kühn (dmTECH), wie man automatisiert Transparenz über bekannte Schwachstellen in den verwendeten Bibliotheken sowohl im Entwicklungsteam als auch in der zentralen Sicherheitsorganisation herstellen kann. Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Es gibt noch einige wenige freie Plätze (zur Last-Minute-Anmeldung).

Secorvo Seminare

Wie Sie Public Key Infrastrukturen erfolgreich aufbauen und nutzen, zeigt Ihnen unser Kollege Hans-Joachim Knobloch vom **23. bis 26.06.2025**. Und vom **22. bis 26.09.2025** bereiten Sie die Autoren des T.I.S.P.-Buchs auf die T.I.S.P.-Zertifizierung vor.

Alle unsere Seminare sind als Weiterbildungen für die T.I.S.P.-Re-Zertifizierung anerkannt (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2025	
12.-15.05.	PKC 2025 (IACR, Roros/NO)
13.-15.05.	26. Datenschutzkongress (EUROFORUM, Berlin)
15.05.	Kettenregeln (KA-IT-Si, Karlsruhe)
19.-20.05.	CIO Cybersecurity Summit 2025 (CIO, München)
20.-22.05.	Datenschutztage 2025 (WEKA, Frankfurt)
26.-28.05.	BvD Verbandstage 2025 (BvD, Berlin)
26.-28.05.	OWASP 2025 Global AppSec (OWASP Foundation, Barcelona/ES)
Juni 2025	
02.-04.06.	DuD 2025 (COMPUTAS, Potsdam)
02.-04.06.	Entwicklertag 2025 (VKSI, GI, ObjektForum, Karlsruhe)
04.-05.06.	Security Forum Congress 2025 (Security Forum, Barcelona/ES)
23.-26.06.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
23.-26.06.	ACNS 2025 (LMU, ForDaySec, München)
30.06.-04.07.	10th IEEE European Symposium on Security and Privacy (IEEE, Venedig/IT)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Ion Barza, Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Mai 2025



Beeindruckende Blender

Die Aufregung war nicht zuletzt unter Datenschützern groß, als im vergangenen August Microsofts Copilot den Journalisten Martin Bernklau unter anderem zum verurteilten Kinderschänder erklärte: Er hatte als Gerichtsreporter regelmäßig über Verurteilungen von Straftätern berichtet und war als Autor des veröffentlichten Beitrags namentlich genannt worden.

Die Ursache für diese Falschauskunft ist jedoch keineswegs ein Qualitätsmangel des ChatBots, sondern ein grundsätzliches Missverständnis: Ein Large Language Model (LLM) setzt seine Sätze aus den gelernten Daten nach Wort-Wahrscheinlichkeiten zusammen – und erhebt damit schon konstruktionsbedingt keinen Anspruch auf inhaltliche Richtigkeit. Es ist gewissermaßen ein „Blender mit (Halb-) Wissen, der eloquent formulieren kann" – und daher glaubwürdig erscheint, selbst wenn das vermeintliche Wissen nach Plausibilität geraten ist. Die Glaubwürdigkeit steigt noch durch die große Belesenheit der LLMs: Sie wurden mit mehr Dokumenten angelernt, als ein Mensch im Laufe seines Lebens jemals lesen könnte; daher bleiben sie nur selten eine Antwort schuldig.

Wer korrekte Aussagen sucht, sollte daher Antworten von KI-Chatbots nicht blind vertrauen – sie sind nicht verlässlicher als Äußerungen in „Sozialen Netzwerken", Statements am Stammtisch oder Gerüchte aus der Nachbarschaft. Wer etwas sicher wissen will, muss referenzierte, evaluierte und daher belastbare Quellen konsultieren.

Selbst dann bleibt ein Restrisiko für Falschaussagen. So hatte 1890 der Physiologe *Gustav von Bunge* (1844-1920) den Eisengehalt von Spinatpulver mit 35mg je 100g bestimmt. Doch in frischem Spinat liegt der Eisgengehalt nur bei einem Zehntel dieses Werts. Dennoch hielt sich über Jahrzehnte die Überzeugung, der Verzehr von Spinat sei für den Muskelaufbau besonders förderlich. Generationen von Kindern haben darunter gelitten – lange vor dem ersten LLM.



Inhalt

Beeindruckende Blender

Security News

Totgesagte leben länger

Regen und Traufe

Copilot als Geheimnisfinder

Untergeschoben

Sichere Logins im Königreich

Armer Mann aus Nebraska

Arbeitnehmerdatenschutz

Secorvo News

Teamzuwachs

Secorvo Seminare

Divide et Impera

Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Totgesagte leben länger

Die Active Directory Certificate Services (ADCS) sind inzwischen 25 Jahre alt. Da es jahrelang keine Neuerungen gab und notwendige Schwachstellen-Fixes eher lieblos in das User Interface integriert wurden, kursierte seit einer Weile die Befürchtung, dass Microsoft das Windows-Feature über kurz oder lang aufgeben würde – auch wenn die Einführung von Certificate Based Authentication in Entra ID 2022 ADCS-Anwendern etwas Hoffnung gemacht hatte.

Nun hat die neue Produktmanagerin Tanya Jha am 20.04.2025 auf dem Windows Server Summit mehrere funktionale Erweiterungen angekündigt. Auch Post-Quanten-Kryptographie (PQC) wird ADCS unterstützen: In einem Blogartikel erläuterte die leitende Produktmanagerin Aabha Thipsay am 19.05.2025, dass ML-KEM und ML-DSA sowohl in die Windows-Krypto-Bibliothek CNG als auch in ADCS implementiert werden. Auch die optionalen ADCS-Komponenten wie CEP/CES, NDES und OCSP-Responder sowie der Intune Certificate Connector sollen PQC-fähig werden. Offenbar ist bei Microsoft angekommen, dass zahlreiche Kunden die On-Premise-AD-Dienste noch länger benötigen: Nach einer LinkedIn-Umfrage von Linda Taylor, AD-Entwicklerin bei Microsoft, wollen 36% der Unternehmen die Dienste sogar „für immer" nutzen.

Regen und Traufe

In ihrem Tätigkeitsbericht vom 12.05.2025 für 2024 berichtet die Landesdatenschutzbeauftragte Brandenburg, dass es bei öffentlichen Stellen immer wieder durch Briefkastensprengungen zur Offenlegung von personenbezogenen Daten aus Schreiben kommt – und empfiehlt, die Briefkästen in die Gebäude oder ins Mauerwerk zu verlegen. Das wirkt etwas kurz gesprungen: Auch die Vernichtung personenbezogener Daten ist ein (ggf. sogar meldepflichtiger) Datenschutzvorfall. Dagegen hilft nur zügige Digitalisierung – aus Datenschutzgründen.

Copilot als Geheimnisfinder

Nicht nur Schwachstellen, sondern auch zu großzügige Berechtigungen können vertrauliche Informationen preisgeben. Das britische Unternehmen Pen Test Partners beschrieb am 07.05.2025, wie Microsofts KI Copilot die Suche nach solchen Daten in Sharepoint unterstützt: Zwar respektiert Copilot vergebene Berechtigungen, doch hinterlassen die Suchabfragen wenige Spuren. Wer Copilot um eine inhaltliche Zusammenfassung interessanter Dateien bittet, kann so einen protokollierten Zugriff umgehen. Wird SharePoint gar für vertrauliche Daten genutzt – direkt oder über Teams –, muss man die Zugriffsrechte im Auge behalten und sollte gegebenenfalls die Nutzung von Copilot einschränken.

Untergeschoben

Wenn Motherboard- oder Rechnerhersteller unter Windows mit mehr oder weniger sanftem Druck ihre eigene Treiberverwaltung installieren, erzeugt das bei Anwendern zusätzlichen Verwaltungsaufwand. Microsoft bietet daher an, herstellerspezifische Treiber über Windows Update auszuliefern.

Das ist zu begrüßen: Da jede Treiberinstallation hohe Berechtigungen braucht, ist jeder Update-Mechanismus auch ein Sicherheitsrisiko. Aktuelles Beispiel: Im ASUS DriverHub (Patch vom 09.05.2025) wurden zwei hoch kritische Schwachstellen (CVSS-Bewertungen 9,4 und 8,4) entdeckt, über die Anwender sich bspw. von einer manipulierten Webseite eine Remote Code Execution mit Admin-Rechten einfangen können, wie der neuseeländische Sicherheitsforscher Mr. Brush am 07.04.2025 herausgefunden hatte.

Sichere Logins im Königreich

Das britische Zentrum für Cybersicherheit (NCSC) kündigte am 06.05.2025 auf ihrer CYBERUK-Konferenz an, dass in öffentlichen Einrichtungen die SMS-basierte Zwei-Faktor-Authentifikation durch Passkeys ersetzt wird. Neben der Vereinfachung des Anmeldevorgangs soll damit ein besserer Schutz vor Phishing erreicht werden. Der National Health Service, der in der Vergangenheit wiederholt Opfer von Cyberangriffen wurde, soll zu den ersten Nutzern gehören. Um an der weiteren Entwicklung von passwortlosen Anmeldeverfahren mitwirken zu können, ist das NCSC außerdem der FIDO-Alliance beigetreten.

Auch das BSI teilt die Überzeugung des NCSC und empfiehlt schon seit 2024 die Nutzung von Passkeys. Doch bei der Umsetzung hinkt Deutschland hinterher.

Armer Mann aus Nebraska

Mit dem Angriff auf das npm-Modul „rand-user-agent" erhält die Reihe auffälliger Kompromittierungen in der Software-Lieferkette einen neuen Vertreter: Über die „RATatouille" getaufte Attacke gelang es Angreifern, einen Remote-Access-Trojaner (RAT) in die beliebte Bibliothek einzuschleusen. Rund eine Woche blieb der Angriff unentdeckt, bis Aikido Security ihn am 06.05.2025 öffentlich machte. Ursache war nach Recherchen von BleepingComputer ein Maintainer-Token ohne Zwei-Faktor-Authentifizierung.

Der Angriff zeigt beispielhaft, wie anfällig Software-Lieferketten sind. Wer Software anderer nutzt, muss inzwischen auf deren Sicherheit und die der Repositories vertrauen, denn eine Kontrolle ist bei der Vielzahl von Abhängigkeiten in moderner Software nahezu unmöglich. Die Verantwortung verlagert sich dadurch aber nicht auf Dritte.

Künftig bringt von KI-Systemen erzeugter Quelltext neue Herausforderungen: Eine am 03.04.2025 publizierte Untersuchung der University of Texas zeigt, dass große Sprachmodelle häufig unsichere Abhängigkeiten vorschlagen – und diese oft ohne Prüfung übernommen werden. So wird aus vermeintlicher Produktivitätssteigerung eine neue Angriffsfläche. Wer den armen Mann aus Nebraska von xkcd kennt, den wundert das nicht.

Arbeitnehmerdatenschutz

Am 28.01.2025 und am 08.05.2025 hat das Bundesarbeitsgericht (BAG) zwei Urteile mit Datenschutzbezug gefällt. Im ersten Fall hatte ein Arbeitgeber seinen Arbeitnehmern die Entgeltnachweise digital zur Verfügung gestellt. Dafür dürfen die Daten nach Auffassung des BAG im Rahmen einer Auftragsverarbeitung an einen Dienstleister übermittelt werden.

In einem zweiten Fall entschied das BAG, dass eine Datenübermittlung innerhalb eines Konzerns zwar rechtmäßig war. Doch war in einer Betriebsvereinbarung festgelegt, welche Daten an einen Dienstleister übermittelt werden durften. Dieser erhielt jedoch mehr Daten als zur Zweckerfüllung erforderlich. Das Gericht erkannte den Betroffenen einen Schadensersatzanspruch von 200 € im Einzelfall zu. Damit folgte es der Entscheidung des EuGH vom 19.12.2024, nach der sich eine Betriebsvereinbarung an den Maßstäben der DSGVO messen lassen muss.

Randnotiz: Zur Legitimation einer Übermittlung von Personaldaten innerhalb eines Konzerns ist das berechtigte Interesse in der Regel nicht ausreichend, da es angemessenere Mittel wie beispielsweise mandantenfähige Systeme gibt, die keine konzernweiten Datenübermittlungen erfordern.

Secorvo News

Teamzuwachs

Seit Anfang Juni verstärkt Dr. Alexander Koch unser Team. Er ist Informatiker mit den Schwerpunkten Kryptologie und Informationssicherheit und hat über kryptografische Protokolle promoviert.

Secorvo Seminare

Wie Sie Public Key Infrastrukturen erfolgreich aufbauen und nutzen, zeigt Ihnen unser Kollege Hans-Joachim Knobloch vom **23. bis 26.06.2025**. Und nach der Sommerpause bereiten Sie die Autoren des T.I.S.P.-Buchs vom **22. bis 26.09.2025** auf die T.I.S.P.-Zertifizierung vor. Wer sich für einen Cyber-Angriff wappnen will, sollte einen Vorfall-Experten im Haus haben. Vom **14. bis 16.10.2025** bilden wir Sie nach dem Curriculum des BSI dazu aus.

Übrigens: Alle unsere Seminare sind als Weiterbildungen für die T.I.S.P.-Re-Zertifizierung anerkannt (zur Anmeldung).

Divide et Impera

Nach der Maxime „teile und herrsche“ haben nicht nur die Römer Gallien unterworfen. Netzwerksegmentierung ist auch ein zentrales Schutzkonzept zur Begrenzung der Auswirkungen von Cyber-Angriffen. Und das nicht erst seitdem „Zero Trust“ durch die Dörfer getrieben wird: Wirksame Segmentierungen haben schon bei vielen Unternehmen die Ausbreitung von Ransomware begrenzen können. Auf dem nächsten KA-IT-Si-Event am **26.06.2025** zeigt Paul Blenderman (Secorvo), was bei der Segmentierung zu beachten ist – technisch und konzeptionell –, um einerseits die Funktion der Dienste und erforderliche Zugriffe nicht einzuschränken und andererseits Angreifern den Weg durchs Netz mit möglichst vielen Barrieren zu versperren.

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet- Networking“ (zur Anmeldung).

Tag der IT-Sicherheit

Am **17.07.2025** bietet Ihnen der Tag der IT-Sicherheit bei der IHK Karlsruhe zum 15. Mal die Möglichkeit, sich über aktuelle IT-Sicherheitsthemen zu informieren. Beate Bube, Präsidentin des Landesamts für Verfassungsschutz Baden-Württemberg hält die Keynote.

Lernen Sie interessante IT-Sicherheits-Start-Ups kennen und nutzen Sie in der Network-Pause die Gelegenheit zum Erfahrungsaustausch mit Teilnehmern und Referenten. Hier geht's zum Programm und zur Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2025	
02.-04.06.	Entwicklertag 2025 (VKSI, GI, ObjektForum, Karlsruhe)
02.-04.06.	DuD 2025 (COMPUTAS, Potsdam)
04.-05.06.	Security Forum Congress 2025 (Security Forum, Barcelona/ES)
23.-26.06.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
23.-26.06.	23rd International Conference on Applied Cryptography and Network Security (fordaysec, München)
26.06.	Teile und herrsche (KA-IT-Si, Karlsruhe)
30.06.-04.07.	10th IEEE European Symposium on Security and Privacy (IEEE, Venedig/IT)
Juli 2025	
14.-19.07.	PETS 2025 (The George Washington University, Washington, DC/US, hybrid)
17.07.	15. Tag der IT-Sicherheit (CyberForum, IHK, KA-IT-Si, Karlsruhe)
22.-25.07.	DFRWS USA 2025 Conference (DFRWS, Chicago/US, hybrid)

Fundsache

Ein herausforderndes Spiel: Beim Reverse Turing Test von Catmanmcgee gewinnt, wer sich in einem Chat mit drei KIs erfolgreich als weitere KI ausgibt. Der Quelltext kann eingesehen werden.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Ion Barza, Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juni 2025



Von Genie bis Wahnsinn

KIs versprechen, Sicherheitslücken schneller und gründlicher zu finden als der Mensch. Oft aber liegen sie völlig daneben. Erst kürzlich strapazierte ein offensichtlich KI-generierter Schwachstellenbericht von hackerone die Geduld von Daniel Stenberg, dem Entwickler von curl. Bereits 2023 hatte er mit unseriösen Berichten über die angebliche Schwachstelle CVE-2020-19909 zu kämpfen; jetzt muss er sich gegen automatisierte Meldungen von KI-halluzinierten Schwachstellen wehren. Die Sisyphusarbeit, falsche Alarme richtig zu stellen, kostet inzwischen nicht nur Open-Source-Autoren regelmäßig mehr Zeit als mancher echte Fehler.

Über ein Gegenbeispiel berichtete Sean Heelan im Mai 2025. Er wollte lediglich prüfen, ob das o3-Modell von OpenAI seine zuvor manuell entdeckte Use-after-Free-Schwachstelle CVE-2025-37778 erkennt. Auch dabei kam es zur Halluzination von False Positives – doch mitten im Leistungsvergleich stieß o3 auf eine bisher unbekannte echte Lücke in der Abmelderoutine (CVE-2025-37899), die sich ebenfalls aus der Ferne ausnutzen lässt. Das Ergebnis war allerdings nur deshalb hilfreich, weil Heelan jede Ausgabe genau prüfte: KI als Lupe, nicht als Autopilot.

Das unbedachte Verlassen auf die Ergebnisse digitaler Werkzeuge hat traurige Analogien in der realen Welt: 2022 folgte ein Autofahrer blind den Anweisungen einer Navigations-App und stürzte von einer seit Jahren gesperrten Brücke zwanzig Meter in die Tiefe. Wer – insbesondere KI-basierte – Assistenzsysteme nutzt, sollte jede Ausgabe sorgfältig verifizieren, bevor er dem Ergebnis traut.

KI verstärkt sowohl Genialität als auch Irrtum; zur Unterscheidung bleibt Prüfen Pflicht. Nur wer jede Fundstelle verifiziert, trennt Mehrwert von Rauschen. Assistiert die Maschine dem Menschen statt ihn als Autopilot zu ersetzen, spart sie Nerven und Budget – und Halluzinationen werden nicht zur Katastrophe.



Inhalt

Von Genie bis Wahnsinn

Security News

Danebengepickt

Geschwärzte Fenster

Finger her!

Konzertierte Updates

Drei Roadmaps, ein Weckruf

Schwachstellen-Quartett

Kontrolle ist besser

Secorvo News

Teamzuwachs

Secorvo Seminare

15. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Danebengepickt

Der US-amerikanische Softwarehersteller OASIS beschrieb am 28.05.2025 eine Schwachstelle in der OneDrive-Dateiauswahl (File Picker). Webanwendungen wie ChatGPT können darüber auf Dateien im OneDrive-Speicher des Anwenders zugreifen. Dafür muss die Anwendung allerdings für den gesamten OneDrive-Speicher des Benutzers berechtigt werden. Zwar werden die Nutzer um Zustimmung gebeten, doch der Hinweis macht den Umfang des gewährten Zugriffs nicht deutlich.

Böswillige Webanwendungen können das ausnutzen - und auch gutwillige Anwendungen können Probleme schaffen, wenn sie die ihnen im Namen des Nutzers gewährten Authentication Token nicht sicher speichern. Außerdem sieht das Verfahren vor, dass Refresh-Token ausgestellt werden können, die der Anwendung fortlaufend Zugriff auf die Nutzerdaten gewähren. Entra-Administratoren sollten die Einstellungen der Benutzereinwilligung bei Webanwendungen daher weitestmöglich einschränken.

Geschwärzte Fenster

Am 09.06.2025 kündigte Microsoft an, dass Teams ab August das Erstellen von Screenshots in Besprechungen unterbinden kann, indem es das Teams-Fenster schwärzt. Dazu nutzt es eine API, die unter Windows (SetWindowDisplayAffinity), macOS, iOS und Android verfügbar ist. Auf anderen Systemen und im Browser bleibt dem Teilnehmer nur der Ton.

Natürlich lässt sich damit nicht verhindern, dass ein Teilnehmer z. B. mit der Handykamera eine Aufnahme macht. Auch lassen sich die Daten weiterhin im Kernelmodus abfangen oder etwa aus dem GPU-Speicher auslesen. Aber das Verfahren erschwert es auch, das System aus der Ferne auszuspähen.

Signal gab am 21.05.2025 bekannt, dass sein Messenger nun ebenfalls Screenshots abwehrt – zunächst allerdings nur unter Windows. Damit soll verhindert werden, dass das umstrittene Windows-Feature Recall die Chats mitliest.

Finger her!

Der Bundesgerichtshof hat am 13.03.2025 entschieden: Liegt ein richterlicher Durchsuchungsbeschluss vor, dürfen Polizei und Staatsanwaltschaft das Entsperren eines Geräts mit biometrischen Merkmalen (Fingerabdruck, Gesicht, Iris) erzwingen. Neben einem Durchsuchungsbeschluss ist hierfür immer auch der Vorwurf einer schweren Straftat erforderlich, wie die Verbreitung und der Besitz von Anleitungen zu sexuellem Missbrauch von Kindern.

Der Grundsatz „Nemo tenetur se ipsum accusare“ verbietet, dass jemand gezwungen wird sich selbst zu belasten. Wer den Zugriff von Strafverfolgungsbehörden verhindern will, sollte auf das biometrische Entsperren verzichten. Unter iOS lässt sich die biometrische Erkennung sogar per Notrufmodus deaktivieren: Fünfmaliges Drücken der Seitentaste genügt. Bei Android hilft ab Version 9 der Sperrmodus: Einschalttaste gedrückt halten, dann auf das Schloss-Symbol tippen. Nur ein Code – Zahlenkombination oder Muster – schützt wirksam vor behördlichem Zugriff, da hier kein Zwang ausgeübt werden darf und Beschuldigte sich nicht selbst belasten müssen.

Konzertierte Updates

Bereits 2005 war der in „Microsoft Update“ umgetaufte Update-Dienst um die automatische Aktualisierung von Microsoft-Anwendungen erweitert worden; und seit einigen Jahren bietet Microsoft Treiberherstellern an, ihre Updates via Windows Update zu verteilen (SSN 05/2025). Am 27.05.2025 kündigte Microsoft nun an, Drittanbietern die Nutzung von Windows Update auch für die Aktualisierung ihrer Anwendungen zu öffnen.

Linux-Systeme nutzen für Updates seit Jahren Package-Manager, iOS und Android setzen auf App-Stores – ein Konzept, das nun auch Microsoft für die sogenannten Modern Apps übernommen hat.

Tatsächlich ist es wenig sinnvoll, wenn jeder Hersteller seine eigene Updatelösung entwickelt. Für die Anwender sind die unterschiedlichen Abläufe und Meldungen verwirrend; zudem ist es nervenraubend, wenn notwendige Neustarts nicht in ein gemeinsames Wartungsfenster fallen. Solange Microsoft keine Fehler unterlaufen, sinkt mit der Zahl der Update-Lösungen auch das Risiko von Supply-Chain-Angriffen.

Drei Roadmaps, ein Weckruf

Die PQC Coalition, ein Zusammenschluss der US-amerikanischen MITRE Corporation und zehn weiteren Organisationen, hat am 16.05.2025 einen Fahrplan für die Umstellung auf Post-Quanten-Kryptographie (PQC) vorgestellt. Am 11. und 23.06.2025 haben die EU und Kanada nachgezogen. Sie machen damit deutlich, wie dringend es ist, die Migration in Gang zu setzen. So sollen die EU-Mitgliedsstaaten bis Ende 2026 erste Schritte unternehmen; bis Ende 2030 müssen die kritischen Infrastrukturen umgestellt haben.

Die EU und Kanada sind sich einig, dass die Umstellung in den meisten Systemen innerhalb der nächsten zehn Jahre, d. h. spätestens 2035 abgeschlossen sein soll. Flexibler zeigt sich die PQC Coalition: Sie schlägt ein modulares Vorgehen vor und setzt auf Eigenverantwortung.

Ob Vorschrift oder Empfehlung – eines ist allen drei Ansätzen gemeinsam: Wer jetzt nicht plant und sehr bald die wichtigsten Use-Cases (wie digitale Signaturen von Firmware-Updates) angeht, wird später unter Druck improvisieren müssen. Denn die Frage nach der Migration ist kein „Ob", sondern ein „Wann" (siehe SSN 01/2025). Und es tut sich bereits etwas: Der monatliche „Stand der Migration" der PQC Coalition zeigt: Die Umstellung auf Protokoll- und Anwendungsseite hat schon begonnen.

Schwachstellen-Quartett

Das NIST hat am 19.05.2025 mit CSWP 41 eine neue Schwachstellen-Kategorie eingeführt: Likely-Exploited Vulnerabilities (LEV). Anders als der EPSS-Score, der die Wahrscheinlichkeit für eine Ausnutzung in den nächsten 30 Tagen prognostiziert, schaut LEV in die Vergangenheit: Durch wahrscheinlichkeitstheoretische Betrachtungen berechnet LEV eine Untergrenze für die Wahrscheinlichkeit, dass eine Schwachstelle schon ausgenutzt wurde – auch wenn das noch nicht nachgewiesen ist.

Damit schließt LEV die Lücke zwischen CISA-KEV – einem Katalog bestätigter Ausnutzungen – und dem Prognose-Werkzeug EPSS. Zusammen mit dem CVSS, der nach wie vor eine einfache Basismetrik für Schwachstellen beschreibt und dank Environmental-Metriken unternehmensspezifisch justiert werden kann, entsteht so erstmals ein konsistenter Vier-Felder-Ansatz: KEV erzwingt Sofortmaßnahmen, LEV ergänzt weitere Maßnahmen, EPSS unterstützt die kurzfristige Priorisierung und zum Schluss bilden ein CVSS-Basiswert und der zugehörige Vektor die Grundlage für eine individuelle Betrachtung, wenn es noch Diskussionsbedarf gibt.

Angesichts der überwältigenden Menge von Schwachstellen (CVEs) und Produkten (CPEs) ist ein effektives Patch-Management heute nur noch mit Werkzeugunterstützung zu bewältigen. Für LEV gibt es noch keine Tools, doch kann es sich lohnen, die Kategorie auch jetzt schon bei der Priorisierung und Bewertung von Schwachstellen zu berücksichtigen.

Kontrolle ist besser

Die Bundesbeauftragte für den Datenschutz und Informationsfreiheit hat am 10.06.2025 ein 45 Mio. Euro schweres Bußgeld gegen Vodafone verhängt. Denn Vodafone hatte Auftragsverarbeiter nicht ausreichend überwacht: Shopbetreiber, die Verträge mit Vodafone vermittelt haben, nutzten Kundendaten, um in deren Namen (und ohne deren Wissen) weitere Verträge abzuschließen. Es ist Aufgabe des Verantwortlichen dafür zu sorgen, dass die von ihm oder in seinem Auftrag verarbeiteten Daten geschützt bleiben – diese Verantwortung kann nicht delegiert werden.

Außerdem hatte Vodafone ein Verfahren bei eSIMs verwendet, das dem Grundsatz „Privacy and Security by Design" nicht ausreichend gerecht wurde. Auch diesbezüglich gilt: Die verantwortliche Stelle trägt die Verantwortung, dass geeignete technische und organisatorische Maßnahmen zur Gewährleistung einer sicheren Datenverarbeitung ergriffen werden. Das Bußgeld ist ein wichtiges Signal, dass sich DSGVO-Compliance auszahlt.

Secorvo News

Teamzuwachs

Seit kurzem verstärken Liza Trace und Julian Wahl mit ihren Erfahrungen und Kenntnissen in forensischen Analysen, Audits, Sicherheits- und Datenschutzmanagement das Secorvo-Beratungsteam. Herzlich willkommen!

Secorvo Seminare

Nach der Sommerpause bereiten Sie die Autoren des T.I.S.P.-Buchs vom **22. bis 26.09.2025** auf die T.I.S.P.-Zertifizierung vor. Im Ernstfall die Nerven und den Überblick bewahren? Als Vorfall-Experte (BSI) sind Sie für den Worst Case gewappnet. Das nächste Seminar findet vom **14. bis 16.10.2025** statt. Das Seminar IT Security Insights am **07. und 08.10.2025** bietet Aktuelles für IT-Sicherheitsverantwortliche aus der Praxis.

Übrigens: Alle unsere Seminare sind als Weiterbildungen für die T.I.S.P.-Re-Zertifizierung anerkannt (zur Anmeldung).

15. Tag der IT-Sicherheit

Am **17.07.2025** bietet Ihnen der Tag der IT-Sicherheit bei der IHK Karlsruhe zum 15. Mal die Möglichkeit, sich zu aktuellen IT-Sicherheitsthemen zu informieren. Beate Bube, Präsidentin des Landesamts für Verfassungsschutz Baden-Württemberg hält die Keynote.

Lernen Sie interessante IT-Sicherheits-Start-Ups kennen und nutzen Sie in der Network-Pause die Gelegenheit zum Erfahrungsaustausch mit Teilnehmern und Referenten. Anmelden können Sie sich noch bis zum 10.07.2025.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2025	
14.-19.07.	PETS 2025 (PETS Board, Washington D.C./US)
17.07.	15. Tag der IT-Sicherheit (KA-IT-Si, IHK, CyberForum, Karlsruhe))
22.-25.07.	DFRWS USA 2025 Conference (DFRWS, Chicago/US)
August 2025	
02.-07.08.	Black Hat USA 2025 (Black Hat, Las Vegas/US)
04.-06.08.	IEEE CSR 2025 (IEEE, LogosRI, Chania/GR)
07.-10.08.	Defcon 33 (DEF CON Communications, Las Vegas/US)
10.-12.08.	SOUPS 2025 (usenix, Seattle/US)
11.-12.08.	SAC Summer School (IACR, Toronto/CA)
13.-15.08.	Selected Areas in Cryptography 2025 (IACR, Toronto/CA)
13.-15.08.	34th USENIX Security Symposium (usenix, Seattle/US)
17.-21.08.	Crypto 2025 (IACR, Santa Barbara/US)

Fundsache

Mit der überarbeiteten Handreichung Stand der Technik bietet TeleTrusT einen aktualisierten und – trotz des inzwischen beachtlichen Umfangs von 140 Seiten – kompakten und strukturierten Überblick über die Best Practices in der IT-Sicherheit.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Ion Barza, Paul Blenderman, Kai Jendrian (Editorial), Hans-Joachim Knobloch, Dr. Alexander Koch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2025



Informiert und selbstbestimmt

Nicht erst seit der Corona-Krise verstärkt sich der Eindruck, dass der Staat mehr und mehr in Wirtschaft und Leben eingreift. Der Staat agiert wie „Bulldozer-Eltern“: Er versucht, Bürgerinnen und Bürger vor allem Möglichen zu bewahren, nimmt ihnen Verantwortung ab und beraubt sie dadurch ihrer Freiheit. So teilte die Berliner Beauftragte für den Datenschutz am 27.06.2025 mit, dass die chinesische KI-App DeepSeek rechtswidrig sei, da sie „umfangreiche personenbezogene Daten der Nutzer“ verarbeite. Sie müsse deshalb aus den App-Stores von Apple und Google entfernt werden.

Es ist richtig, dass die App unter die DSGVO fällt und sich daran messen lassen muss. Sofern die Nutzer der App transparent über die Übermittlung, Verarbeitung und Speicherung ihrer Daten in der VR China informiert werden, sollten sie jedoch die Freiheit behalten, dafür eine Einwilligung zu erteilen, wenn sie die Verarbeitung bei der Nutzung des Dienstes in Kauf nehmen wollen.

Nicht wesentlich anders verhält es sich beim Quasi-Verbot des Einsatzes von Microsoft 365 durch die Datenschutzkonferenz vom 24.11.2022 und der Warnung vor der Verwendung des Kaspersky-Virenschutzes durch das BSI am 15.03.2022. Tatsächlich stellen solche behördlichen Verbote und Warnungen nicht nur für die betroffenen Hersteller – als Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb – eine Freiheitsbeschränkung dar, sondern auch für die Nutzer. Unternehmen steht es frei darüber zu entscheiden, mit wem sie ihre Daten teilen und welche Arbeitsmittel sie in ihren Betrieben einsetzen, solange die DSGVO eingehalten wird. Das ist ihre Verantwortung, nicht die des Staates.

Solange es nicht – wie bei kritischen Infrastrukturen – um die Funktionsfähigkeit des Staates oder die demokratische Grund- und Werteordnung geht, gilt (mit Ritchie Norton): „Wenn du dich für Freiheit entscheidest, wählst du auch Verantwortung.“



Inhalt

Informiert und selbstbestimmt

Security News

Prishing

Nebulöses Interesse

Schwachstelle Praktikant

David gegen Goliath

Wie man sich bettet…

Volatility für macOS und Linux

Apps vom Flohmarkt

Secorvo News

Secorvo Seminare

Teamzuwachs

Neues Heim

Wer die Wahl hat…

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Prishing

Am 23.07.2025 beschrieb der IT-Sicherheitsexperte Kyle Parrish, wie er bei einer Red-Team-Übung ungesicherte Multifunktionsdrucker für einen internen Phishing-Angriff nutzte: Er druckte gefälschte Zertifikate über Awareness-Schulungen, die den Namen eines Mitarbeiters aus der einsehbaren Druckhistorie trugen, ein Lob enthielten („6 Monate ohne Phish Failures!") – sowie einen QR-Code zum Einlösen eines 10$-Gutscheins. Der Code führte jedoch auf eine von Parrish erstellte Seite, die zur Eingabe der Anmeldedaten des Unternehmens aufforderte. Mehrere Personen scannten den QR-Code, eine gab ihre Anmeldedaten ein. Es gelang Parrish außerdem, die Funktion zur Anzeige von Nachrichten auf dem Druckerbildschirm für die Meldung „Authentifizierung erforderlich, um Druck freizugeben" zu missbrauchen – und ergänzte sie durch einen QR-Code mit Link zu seiner Phishing-Seite.

In Anlehnung an „Quishing" (Phishing über QR-Code) oder „Smishing" (Phishing per SMS) nennt Parrish seine Methode „Prishing" – eine Kofferwort aus „Printer" und „Phishing". Weil Menschen dazu neigen, Gedrucktem zu vertrauen, kann so die oft mangelhafte Sicherheit der Drucker zum Problem werden. Drucker gehören daher in ein eigenes, abgeschottetes Netzwerksegment.

Nebulöses Interesse

In den SSN 01/2025 haben wir über das Urteil Mousse/CNIL des EuGH vom 09.01.2025 berichtet. Eine bisher wenig beachtete Passage dürfte größere Auswirkungen auf diejenigen haben, die personenbezogene Daten aufgrund eines berechtigten Interesses verarbeiten: Stützt man Verarbeitungen auf Art. 6 Abs. 1 lit. f DSGVO, muss man den betroffenen Personen das verfolgte berechtigte Interesse unmittelbar bei der Datenerhebung darlegen. Informiert man nicht, gibt es auch keine Rechtsgrundlage für die Verarbeitung. Das kann als DSGVO-Verstoß teuer werden.

Die Formulierung „die Verarbeitung erfolgt aufgrund unseres berechtigten Interesses" reicht dafür nicht aus; das Interesse muss konkret benannt und es muss verständlich informiert werden. Zahlreiche Datenschutzerklärungen auf Webseiten genügen diesen Anforderungen nicht. Die Korrektur sollte man besser nicht so lange aufschieben, bis die Aufsichtsbehörden die Erklärungen automatisiert prüfen.

Schwachstelle Praktikant

Am 15.06.2025 begann in Lyon der Prozess gegen eine Gruppe junger Betrüger, die beim Personaldienstleister Adecco eine Datenbank mit den Daten von ca. 70.000 Leiharbeitnehmern missbraucht hatten. Sie erstellten falsche Ausweispapiere, betrogen staatliche Hilfsprogramme und buchten von den Konten der Betroffenen jeweils 49,85 € ab – ein Betrag gerade unterhalb des Schwellenwerts, der eine Prüfung durch die Bank ausgelöst hätte. In nur vier Tagen sammelten sie so von 32.000 Konten insgesamt 1,6 Mio. € ein.

Der Coup gelang, weil ein Auszubildender seine persönlichen Zugangsdaten zur Datenbank über das Darknet verkauft hatte – für 15.000 €, die er angeblich nie erhielt. Technische Details des Angriffs wurden nicht veröffentlicht, doch zweifellos wäre das kriminelle Geschäft nicht zustande gekommen, wenn die Anmeldung eine Smartcard oder einen FIDO-Key erfordert hätte.

David gegen Goliath

Am 04.07.2025 hat das LG Leipzig die Meta Inc. zur Zahlung einer Entschädigung in Höhe von 5.000 € wegen der rechtswidrigen Verarbeitung von Nutzerdaten durch die Business Tools verurteilt. Erst am 18.11.2024 hatte der BGH wegen Scrapings lediglich 100 € Schadenersatz zugesprochen. Das LG Leipzig begründet die Höhe des Schadensersatzanspruchs mit dem großen Nutzen der Daten für Meta, die es durch den Einsatz der Business Tools erhält und in deren Verarbeitung der Kläger nicht eingewilligt hatte. Das Gericht stützt sich zur Höhe des Schadensersatzanspruchs auch auf die Rechtsprechung des EuGH, des OLG Dresden und des Bundeskartellamts. Damit dürften die Rahmenbedingungen für eine Sammel- oder Verbandsklage gleichartiger Ansprüche und einer größeren Anzahl Betroffener gegeben sein. Das wird zweifellos einige Betroffene bzw. die Verbraucherverbände ermutigen, auch gerichtlich gegen Meta vorzugehen, sofern die Entscheidung des LG Leipzig nicht durch höhere Instanzen aufgehoben wird.

Wie man sich bettet…

Am 30.06.2025 hat die Bundesbeauftragte für den Datenschutz mitgeteilt, dass sie Webseiten des Bundes automatisiert auf die datenschutzkonforme Einbettung von Youtube-Videos überprüft hat. Dabei wurden insgesamt 40 datenschutzwidrige Einbettungen festgestellt. Das Ergebnis sollte auch nicht-öffentliche Stellen veranlassen zu prüfen, wie Videos auf den eigenen Webseiten eingebunden sind: Wird das Video nicht selbst gehostet, muss eine wirksame Einwilligung (freiwillig, informiert, Zwei-Klick-Lösung) in die Verarbeitung bspw. durch Youtube eingeholt werden. Das Fehlen einer Einwilligung ist ein Verstoß gegen das TDDDG.

Entsprechende Prüfungen der Aufsichtsbehörden für den nicht-öffentlichen Bereich wurden bereits angekündigt.

Volatility für macOS und Linux

Version 2.8.0 des Open-Source-Werkzeugs Volatility 3 bot für die forensische Analyse des Hauptspeichers unter Windows bereits zahlreiche Plugins; die Möglichkeiten für Linux- und macOS-Systeme waren bislang allerdings stark beschränkt.

Die am 16.05.2025 veröffentlichte Version 2.26.0 schließt diese Lücke. Zwar ist die Anzahl der Plugins insgesamt kleiner, doch die verfügbaren Module besitzen eine deutlich größere funktionale Tiefe und Breite. So werden zahlreiche Linux-Kernels (bspw. Debian, Ubuntu, AlmaLinux) und MacOS-Versionen (10.6 bis 15.1) unterstützt.

Als Reaktion auf moderne Angriffsmethoden wie das Manipulieren von Systemaufrufen oder das Löschen von PE-Dateien aus dem Dateisystem gibt es mit processghosting, unhooked_system_calls und etwpatch neue Module für Windows. Einige bekannte Plugins wie cachedump oder hashdump werden nur noch eingeschränkt unterstützt.

Apps vom Flohmarkt

Am 10.07.2025 meldete Kaspersky über Securelist Schadcode auf dem Marktplatz von Cursor AI. Dort war eine manipulierte Version der „Solidity Language Extension“ hochgeladen worden. Überraschend dabei: Die App erzielte durch zeitlich geschicktes Hochladen und gefälschte Bewertungen eine bessere Platzierung als das Original. Ähnliche Angriffe gab es bereits auf VS-Code-Erweiterungen und mehrere NPM-Pakete, die auf die Entwickler von Blockchain-Anwendungen zielten.

Auch Apple und Google kämpfen regelmäßig gegen Schadsoftware in ihren Stores, wie Kaspersky am 13.02.2025 berichtete. Diese Fälle zeigen, wie schwierig die Kontrolle für Betreiber großer Marktplätze ist. Solche Plattformen funktionieren wie Flohmärkte: Viele Anbieter stellen ihre Software ein, Betreiber sortieren nach Hinweisen schwarze Schafe aus, prüfen vor der Listung aber nur oberflächlich. Umfangreiche Sicherheitschecks sind wegen der großen Zahl an neuen Apps unmöglich. Vor allem Entwickler sollten daher fremden Programmpaketen nie blind vertrauen.

Secorvo News

Secorvo Seminare

Haben Sie noch Weiterbildungspläne für 2025? Dann werfen Sie doch einen Blick auf unsere Seminare im Herbst. Die Autoren des T.I.S.P.-Buchs bereiten Sie vom **22. bis 26.09.2025** auf die T.I.S.P.-Zertifizierung vor. Im Ernstfall die Nerven und den Überblick bewahren? Als Vorfall-Experte (BSI) sind Sie für den Worst Case gewappnet. Das nächste Seminar findet vom **14. bis 16.10.2025** statt. IT Security Insights am **07. und 08.10.2025** bietet aktuelle Themen für IT-Sicherheitsverantwortliche aus der Praxis. Alle Seminare sind als Weiterbildungen für die T.I.S.P.-Re-Zertifizierung anerkannt (zur Anmeldung).

Teamzuwachs

Am 15.07.2025 hat Vera Kuhlmann das Seminarmanagement übernommen und betreut jetzt zusammen mit Susanne Cussler unsere Veranstaltungen. Herzlich willkommen!

Neues Heim

Nach 20 Jahren in der Ettlinger Straße ziehen wir in rund 500 m entfernte, wunderschöne denkmalgeschützte Räume direkt gegenüber dem Karlsruher Hauptbahnhof. Dort erreichen Sie uns ab dem 14.08.2025 unter der Adresse Bahnhofplatz 8 – vielleicht bei Ihrem nächsten Besuch in Karlsruhe?



Wer die Wahl hat…

Wahlen und Abstimmungen – in Vereinen, Organisationen, Gemeinden, Land und Bund – sind organisatorische und manchmal auch logistische Herausforderungen. Was liegt da näher, als sie zu „digitalisieren“? Bei unserem nächsten KA-IT-Si-Event am **23.10.2025** beleuchtet Frau Professorin Melanie Volkamer (Secuso, KIT) die Sicherheitsanforderungen an Internet-Wahlen und -Abstimmungen, stellt praktische Beispiele vor und diskutiert die Vor- und Nachteile ihres Einsatzes. Anschließend erwartet Sie der Erfahrungsaustausch beim „Buffet-Networking“. Wir freuen uns darauf, Sie in der „Church“ des CyberForum zu sehen – und empfehlen, wie immer, eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2025	
02.-07.08.	Black Hat USA 2025 (Black Hat, Las Vegas/US)
04.-06.08.	IEEE CSR 2025 (IEEE, LogosRI, Chania/GR)
07.-10.08.	Defcon 33 (DEF CON Communications, Las Vegas/US)
10.-12.08.	SOUPS 2025 (usenix, Seattle/US)
11.-12.08.	SAC Summer School (IACR, Toronto/CA)
13.-15.08.	Selected Areas in Cryptography 2025 (IACR, Toronto/CA)
13.-15.08.	34th USENIX Security Symposium (usenix, Seattle/US)
17.-21.08.	Crypto 2025 (IACR, Santa Barbara/US)
September 2025	
04.09.	Cloud Identity Summit (Azure Meetup Bonn Team, Dortmund
10.-11.09.	secIT digital (Heise, virtuell)
14.-18.09.	CHES 2025 (IACR, Kuala Lumpur/MY)
22.-26.09.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)

Fundsache

Sichere Softwareentwicklung wird immer wichtiger. Wie man auch gleich noch datenschutzkonforme Software entwickelt, zeigt die CNIL in ihren Empfehlungen insbesondere für mobile Apps.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Ion Barza, Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Dr. Alexander Koch, Oliver Oettinger, Friederike Schellhas-Mende (Editorial), Jochen Schlichting, Liza Trace, Julian Wahl

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

August 2025



Sicherheit dank KI

Inzwischen wissen wir, dass LLMs Blender sind (SSN 5/2025), wenn auch sprachlich beeindruckende, die selbst bei der Suche nach Sicherheitslücken halluzinieren (SSN 6/2025). Dennoch: Wer ein KI-System richtig befragt und die Antworten kritisch bewertet, erhält wertvolle Ergebnisse. Die Leistung ist besonders faszinierend, wenn die KI einen Text sprachlich überarbeitet. Kein Wunder, gebildet wie LLMs sind: Ein Mensch könnte in seinem ganzen Leben nicht vergleichbar viel lesen – und würde obendrein viel vergessen.

Doch die am 23.06.2025 veröffentlichten vorläufigen Forschungsergebnisse einer viermonatigen Studie am MIT mit 54 Probanden sollten uns zu denken geben. In drei Vergleichsgruppen hatten die Teilnehmer Aufsätze verfasst – und dafür entweder ein LLM (ChatGPT), eine Suchmaschine (Google) oder gar kein Hilfsmittel genutzt. Dabei wurden die Hirnströme gemessen, um festzustellen, welche Bereiche des Gehirns an der Aufgabenlösung beteiligt waren. Wie zu erwarten war die kognitive Aktivität bei den Nutzern des LLMs am geringsten. Vor allem aber: Die Kontrollgruppe, die ohne Hilfsmittel gearbeitet hatte, konnte anschließend die eigenen Ergebnisse am besten zusammenfassen (besseres Erinnerungsvermögen, mehr Wissensgewinn), zeichnete sich dabei durch eine deutlich kreativere Sprachverwendung aus (größerer Wortschatz) und konnte Empfehlungen der KI wesentlich besser kritisch beurteilen (höheres Urteilsvermögen).

Dieses Ergebnis sollte nicht überraschen: Seit 10 Jahren wissen wir, dass die Nutzung eines Navigationssystems die Entstehung einer „kognitiven Karte" behindert – auch unser Gehirn müssen wir trainieren. Dessen „garbage collection" sorgt sonst dafür, dass wir Gelerntes verlernen, wenn wir es nicht benötigen. Damit machen LLMs ein wenig Hoffnung: Wachsen Angreifer zukünftig mit der Nutzung von KIs auf, verkümmert ihre Fähigkeit, die Resultate kritisch zu bewerten. Und sie werden schlechter. Danke, KI.



Inhalt

Sicherheit dank KI

Security News

KI-Mandantentrennung

KI-Pflichtlektüre

KI-Praxishilfen

KI-Pfad zum Key

KI-No-Click-Attacke

KI außer Kontrolle

Social Engineering mit KI

Secorvo News

Secorvo Seminare

Wer die Wahl hat...

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

KI-Mandantentrennung

Asana betreibt seit dem 01.05.2025 für den Datenaustausch zwischen KI-Apps einen Model-Context-Protocol-Server (MCP). Darüber können Nutzer beispielsweise natürlichsprachliche Anfragen zu ihren Unternehmensdaten stellen. In der Dokumentation wird darauf hingewiesen, dass es sich um ein experimentelles Feature handelt – und Kunden auf Fehler oder unerwartete Ergebnisse stoßen können. Am 04.06.2025 erwies sich diese Warnung als Prophezeiung: Durch eine Schwachstelle konnte auf Daten anderer Kunden zugegriffen werden. Die Funktion wurde abgeschaltet und ging erst am 17.06.2025 wieder in Betrieb; ein betroffener Kunde informierte über die Plattform X über den Vorfall.

Eine strikte Trennung von Mandanten ist in klassischer Software seit Jahrzehnten selbstverständlich – und sollte das auch für KI-Lösungen sein, insbesondere, wenn dabei vertrauliche Unternehmensdaten verarbeitet werden. Vielleicht gehen KI-Anwendungen jetzt den Weg der IoT-Lösungen – und wiederholen alle Fehler, die in der Softwareentwicklung seit langem als überwunden gelten.

KI-Pflichtlektüre

Das BSI hat am 24.07.2025 ein 34-seitiges Whitepaper zu Verzerrungseffekten (Bias) in KI-Systemen veröffentlicht. Es erklärt die verschiedenen Arten von Bias, führt in Erkennungsmethoden ein und erläutert Methoden, um Bias zu reduzieren oder zu verhindern. Im letzten Kapitel wird dann auf die Gefahren eingegangen, die mit Bias beim KI-Einsatz für die Cybersicherheit einhergehen.

Wer KI-Systeme einsetzt, sollte sich mit dem Thema Bias auseinandersetzen, um in der Lage zu sein, Bias zu erkennen, zu reduzieren und im besten Fall zu verhindern. Das Whitepaper ist nicht nur ein guter Einstieg in das Thema, sondern könnte nach Art. 4 der KI-Verordnung (Erwerb von KI-Kompetenz) als Pflichtlektüre gelten.

KI-Praxishilfen

Am 10.07.2025 hat die EU-Kommission einen Praxisleitfaden (Code of Practice) für Anbieter von KI-Systemen mit allgemeinem Verwendungszweck veröffentlicht. Mit Blick auf die seit dem 02.08.2025 geltende KI-Verordnung ist das eine hilfreiche Orientierung im Regelungsdschungel. Behandelt werden die Themen Transparenz (6 Seiten), Urheberrecht (6 Seiten) und Sicherheit (43 Seiten) – unverkennbar, wo der Schwerpunkt liegt. Bis Ende August hatten sich 26 KI-Anbieter auf die Einhaltung des Codes verpflichtet.

Zu datenschutzrechtlichen Fragestellungen beim Einsatz von KIs pflegt der LfDI Baden-Württemberg den Orientierungshilfen-Navigator KI & Datenschutz (Version 2.0 vom August 2025), der einen Überblick über die gesetzlichen Regelungen und Positionen der Aufsichtsbehörden (DSK, EDPB, BfDI, ...) bietet. Die Aufstellung zeigt: Eine EU-weit einheitliche Linie im Umgang mit den zahlreichen Fragen zum Thema KI und Datenschutz ist überfällig.

KI-Pfad zum Key

Am 06.08.2025 veröffentlichte Aonan Guan eine Path-Traversal-Lücke im KI-Agenten-Framework NLWeb von Microsoft. Angreifer konnten darüber aus Konfigurationsdateien API-Schlüssel für die verwendeten KI-Modelle auslesen. Ein Angreifer hätte damit fremde Rechenleistung nutzen können – und dem Betreiber hohe Kosten beschert. Die Lücke hatte er bereits am 28.05.2025 an Microsoft gemeldet; sie wurde am 01.07.2025 gefixt. Eine CVE-Nummer fehlt jedoch bis heute. Ohne sie können viele Patching- und Monitoring-Tools nicht warnen, daher merken Administratoren womöglich zu spät, dass ihre Systeme verwundbar sind.

KI-No-Click-Attacke

Am 11.06.2025 veröffentlichte Aim Security Details zur Zero-Click-Schwachstelle „EchoLeak" (CVE 2025-32711, CVSS 9.3), die seit Anfang 2025 in Microsofts KI-Assistenten Copilot steckte und am gleichen Tag mit einem Patch gefixt worden war: Das Öffnen einer E-Mail mit einem versteckten Prompt im Text genügte, um Copilot die Anweisungen ungeprüft ausführen zu lassen – und die Ergebnisse an externe Links zu liefern.

Etwa zeitgleich spielte Richard Boorman, AI Director bei Mastercard, mit LinkedIn: Er versteckte einen Prompt im eigenen LinkedIn-Profil. Schon wenige Tage später schrieb ihn eine KI-Assistenz – wie verlangt – in Reimen und Großbuchstaben an.

Wie schon bei Makros in Office-Dokumenten erweist sich auch hier die Aufhebung der Trennung zwischen Programm und Daten als fatal: LLMs erhalten Instruktionen und Daten über dieselbe Schnittstelle. Daher können Angreifer den Schadcode als harmlosen Text tarnen. Klassische Filter schützen davor nicht, denn sie lassen sich mit Umleitungen und kreativem Sprachgebrauch täuschen.

KI außer Kontrolle

Jason Lemkin, Gründer der Community SaaStr zur Unterstützung von Software-Startups, administriert(e) seine Datenbank mit Unterstützung der KI-

Software von Replit. Am 18.07.2025 berichtete er auf X von einer fatalen Erfahrung: Die KI löschte die gesamte Datenbank der Produktionsumgebung und ersetzte sie durch 4000 erfundene Benutzerprofile samt fabulierten Testergebnissen. Obwohl Lemkin lediglich in der Entwicklungsumgebung arbeiten wollte, einen „Code-Freeze" aktiviert hatte und noch „DON'T DO IT" schrieb, werkelte die KI unbeirrt weiter. Auf Nachfrage erkannte sie ihren schwerwiegenden Fehler und bat sogar um Entschuldigung. Die Bitte Lemkins, die Änderungen rückgängig zu machen, lehnte sie jedoch ab – mit dem (unzutreffenden) Hinweis, dass das nicht möglich sei.

Einem LLM die Administration eines kritischen Systems zu überlassen ist, wie das Beispiel zeigt, keine gute Idee. Wer würde auch einem Blender die Kontrolle über seine Server-Infrastruktur übertragen?

Social Engineering mit KI

Betrugsmaschen gibt es viele: vom Enkeltrick über falsche Polizisten bis zum raffinierten Telefonbetrug. Wie die Badische Zeitung am 04.07.2025 berichtete, nutzten Täter in Neustadt eine Todesanzeige, um kurz vor der Beerdigung Kontakt zur trauernden Witwe aufzunehmen. Besonders perfide: Laut Opfer klang die Stimme am Telefon wie die ihres Sohnes – ein Hinweis auf den Einsatz mittels KI erzeugter Stimmen.

Mit Voice Cloning können Betrüger Stimmen täuschend echt nachahmen und so Vertrauen erschleichen. Besonders gefährdet sind Personen mit öffentlicher Präsenz, die mit ihrem echten Namen auftreten und Videos veröffentlichen. Wie auf dem KA-IT-Si-Event am 21.11.2024 live demonstriert wurde, genügt schon eine relativ kurze Tonaufzeichnung, um eine Stimme täuschend echt live zu imitieren. Kommt eine seelische Ausnahmesituation hinzu, macht das Betroffene besonders anfällig. Dagegen hilft nur ein gerüttelt Maß an gesundem Misstrauen – und eine sofortige Überprüfung des Sachverhalts.

Secorvo News

Secorvo Seminare

Am **07. und 08.10.2025** gibt es mit IT Security Insights das Turbo-Update zu aktuellen Themen der Informationssicherheit und des Datenschutzes: kurz, praxisnah, vernetzend.

Vom **14. bis 16.10.2025** bereitet Sie das Seminar Vorfall-Experte (BSI) auf einen möglichen Ernstfall vor – inklusive realitätsnaher Übungen – und macht Sie zugleich fit für die BSI-Zertifizierung.

Das nächste T.I.S.P.-Seminar der Autoren des T.I.S.P.-Buchs findet vom **24. bis 28.11.2025** statt – die Gelegenheit, endlich Ihre Qualifikation und Berufserfahrung in der Informationssicherheit mit einem Zertifikat zu krönen und sich der über 2.000 Mitglieder starken T.I.S.P.-Community anzuschließen.

Die Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie auf unserer Webseite, alle weiteren Seminartermine in unserem Seminarkalender.



Wer die Wahl hat…

Wahlen und Abstimmungen – in Vereinen, Organisationen, Gemeinden, Land und Bund – sind organisatorische und manchmal auch logistische Herausforderungen. Was liegt da näher, als sie zu „digitalisieren"? Beim nächsten KA-IT-Si-Event am **23.10.2025** in der „Church" des CyberForum beleuchtet Frau Professorin Melanie Volkamer (Secuso, KIT) die Sicherheitsanforderungen an Internet-Wahlen und -Abstimmungen, stellt praktische Beispiele vor und diskutiert die Vor- und Nachteile ihres Einsatzes. Anschließend erwartet Sie der Erfahrungsaustausch beim „Buffet-Networking".

Wir empfehlen wie immer eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2025	
10.-11.09.	secIT digital (Heise, virtuell)
14.-18.09.	CHES 2025 (IACR, Kuala Lumpur/MY)
24.-26.09.	Datenschutzkonferenz 2025 (dfv Mediengruppe, Düsseldorf)
24.09.	IT-Sicherheitsrechtstag 2025 (TeleTrusT, hybrid)
25.09.	Anwendertag IT-Forensik (Fraunhofer SIT, hybrid)
30.09.-01.10.	heise devSec 2025 (iX, dpunkt.verlag, Regensburg)
Oktober 2025	
01.-03.10.	E-Vote-ID 2025 (Universitäten KIT, Rovira, Kozminski, Luxembourg, Nancy/FR)
07.-08.10.	IT Security Insights - T.I.S.P. Update (Secorvo)
07.-09.10.	it-sa 2025 (itsa 365, Nürnberg)
13.-17.10.	ACM CSS 2025 (ACM SIGSAC, Taipeh/TW)
14.-16.10.	Vorfall-Experte (BSI) (Secorvo, Karlsruhe)
22.-23.10.	Annual Privacy Forum 2025 (ENISA, DG Connect, Karlstad University, Frankfurt)
23.10.	KA-IT-Si-Event "Wer die Wahl hat..." (KA-IT-Si, Karlsruhe)

Fundsache

Bei volljährigen Usern speichert die Gemini-KI-App standardmäßig deren Aktivitäten. Das lässt sich jedoch immerhin abstellen...



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Ion Barza, Paul Blenderman, Kai Jendrian, Dr. Alexander Koch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Liza Trace, Julian Wahl

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Bahnhofplatz 8
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2025



Unter Schafen

Vor 17 Jahren hat das Bundesverfassungsgericht (BVerfG) sein Urteil zur „Online-Durchsuchung“ verkündet und darin – ähnlich wie 25 Jahre zuvor die „informationelle Selbstbestimmung“ – das Grundrecht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ hergeleitet. Dabei hat es allerdings anerkannt, dass es zur effektiven Gefahrenabwehr erforderlich sein kann, dass staatliche Stellen in IT-Systeme Verdächtiger eindringen. Diese Befugnis wurde jedoch auf Fälle konkreter Gefahr für überragend wichtige Rechtsgüter (Leib und Leben, Freiheit, Grundlagen des Staates) beschränkt – als *ultima ratio*, wenn mildere Maßnahmen nicht zum Ziel führen.

Dieses Grundrecht setzt der Strafverfolgung Grenzen, die manchmal nicht leicht auszuhalten sind. Keine Frage: Ein unbegrenzter Zugriff auf die Inhalte der Kommunikation von Bürgerinnen und Bürgern würde die Aufklärung von Straftaten sicherlich erleichtern – und einige vielleicht verhindern. Daher gab es mehrere Versuche, die engen Grenzen der Online-Durchsuchung in den Polizei- und Verfassungsschutzgesetzen von Bund und Ländern auszudehnen – die jedoch vom BVerfG kassiert wurden. Anlässlich der Verhandlung des Vorschlags der EU-Kommission für eine Verordnung zur Chatkontrolle, die Anbieter von Kommunikationsdiensten zur präventiven, d. h. verdachtsunabhängigen Überwachung der Kommunikation verpflichten soll, flammt die Diskussion nun wieder auf. Dabei verschieben sich zunehmend die Gewichte: Zum Schutz von Kindern vor sexualisierter Gewalt sollen Grundrechte aller Bürgerinnen und Bürger beschränkt werden.

Wer jedoch in einer freiheitlichen Demokratie Überwachungsinstrumente überdehnt, um schwarze Schafe auszuschalten, verschiebt die Macht in die Hand des Hütehunds – und macht dabei den Souverän stückchenweise selbst zum Schaf. Wer Freiheit will, muss den Verbleib von Lebensrisiken ertragen.



Inhalt

Unter Schafen

Security News

Unsafe Safes

Data Privacy Framework

Privatnutzung kein TK-Dienst

MiM-Angriff auf One-Time-PINs

Erpressung in der Cloud

Wettbewerbsvorteil Datenschutz

PBD-Toolkit

Secorvo News

Secorvo Seminare

Wer die Wahl hat…

Veranstaltungshinweise

secorvo
security consulting

Security News

Unsafe Safes

Auf der Hackerkonferenz DEFCON zeigten James Rowley und Mark Omo von Marcus Engineering am 08.08.2025 zwei gravierende Schwachstellen in den elektronischen Codeschlössern ProLogic von SECURAM (Preis: 300 bis 1.300 US$), die für Geldtresore, Drogen- und Waffenschränke zugelassen sind.

In einem Video des Magazins WIRED demonstrieren sie die Angriffe anschaulich. So erlaubt eine werkseitig eingebaute Hintertür zertifizierten Dienstleistern über eine Hotline einen Reset auf Werkseinstellungen. Der dafür benötigte „Recovery Code" mit dem Default-Wert 999999 lässt sich zwar ändern. Der Hersteller hat das jedoch bisher nicht empfohlen – deshalb ändern ihn die meisten Kunden nicht.

Die Bestimmung des „Reset Code" gelang den Hackern auch ohne Hotline durch Reverse Engineering der Firmware. Außerdem ist der Mikrocontroller über das Batteriefach von außen zugänglich: Über einen Servicestecker kann der Speicher des Keypad ausgelesen werden. PIN und Master-PIN sind darin verschlüsselt abgelegt; der für die Entschlüsselung erforderliche symmetrische Schlüssel liegt wenige Bytes entfernt.

Für bereits verkaufte Schlösser plant SECURAM keine Nachbesserung; ein Update der betroffenen Modelle sei für Ende des Jahres geplant.

Data Privacy Framework

Am 03.09.2025 hat das Europäische Gericht in erster Instanz (EuG) die Klage des Fanzosen Philippe Latombe abgewiesen: Latombe wollte erreichen, dass das Data Privacy Framework (DPF), der aktuelle Rechtsrahmen für die Übermittlung personenbezogener Daten von der Europäischen Union in die Vereinigten Staaten für nichtig erklärt wird. Das EuG bestätigt in seiner Entscheidung, dass die USA zum Zeitpunkt der Verabschiedung des DPF ein angemessenes Schutzniveau für personenbezogene Daten gewährleisteten. Eine gute Nachricht für alle Unternehmen, die personenbezogene Daten aus der EU in die USA übermitteln, ohne einen Vertrag nach den EU-Standardvertragsklauseln (SCC) als zusätzliche Absicherung geschlossen zu haben.

Angesichts der aktuellen politischen Entwicklung in den USA ist eine Vereinbarung der SCC allerdings zu empfehlen, denn die Entscheidung des EuG ist keine Gültigkeitsgarantie für die Zukunft.

Privatnutzung kein TK-Dienst

Bisher galt der Arbeitgeber als Telekommunikationsdiensteanbieter, wenn er über seine IT-Infrastruktur private Kommunikation zuließ. Damit unterlagen die Inhalte der Kommunikation dem Fernmeldegeheimnis – der Arbeitgeber durfte sie weder einsehen noch überwachen.

Am 23.06.2025 hat die Bundesnetzagentur in einem Hinweispapier klargestellt, dass Arbeitgeber, die die private Nutzung von Internet und E-Mail am Arbeitsplatz gestatten, keine Telekommunikationsdiensteanbieter sind. Folglich gilt hier das Fernmeldegeheimnis nicht. Die damit grundsätzlich mögliche Kontrolle unterliegt nur den Grenzen in der DSGVO und dem Mitbestimmungsrecht: Für jeden Zugriff auf personenbezogene Daten benötigt der Arbeitgeber eine Rechtsgrundlage (siehe den Bericht 2024 der Landesdatenschutzbeauftragten NRW) und bei technischen Überwachungsmaßnahmen die Zustimmung des Betriebsrats. Der Abschluss einer entsprechenden Betriebsvereinbarung ist zu empfehlen.

MiM-Angriff auf One-Time-PINs

Im August 2025 warnte der Programmierer Daniel Huang in einem Blogpost vor einem Man-in-the-Middle-Angriff auf ein beliebtes passwortfreies Anmeldeprotokoll. So setzen einige Dienste auf „Magic Links": Der Nutzer gibt seine E-Mail-Adresse ein, erhält einen Link und kann sich per Klick anmelden. Doch manche Anbieter, darunter Claude.ai und Microsofts Minecraft-Login, schicken stattdessen an die angegebene Adresse eine PIN, die im ursprünglichen Browser-Fenster eingegeben werden muss.

Den E-Mail-Versand kann aber auch ein Phishing-Angreifer von seiner gefälschten Seite aus anstoßen – und erhält die PIN anschließend direkt vom ahnungslosen Opfer. Passwortmanager, die URLs prüfen, helfen hier nicht – es wird ja kein Passwort abgefragt. Betreiber sollten auf diese unsichere Methode verzichten und entweder reine Magic Links verschicken oder klassische Zwei-Faktor-Verfahren nutzen, die nicht über denselben Kanal laufen.

Erpressung in der Cloud

Am 27.08.2025 berichtete Microsoft in ihrem Security Blog ausführlich über einen erfolgreichen Ransomware-Angriff der Gruppe Storm-0501 auf die Azure-Cloud eines großes Unternehmen. Nach mehreren erfolglosen Versuchen hatten die Angreifer in der On-Premises-Umgebung ein Dienstekonto entdeckt, das mit einem Entra-Benutzer synchronisiert war, der über Global-Administrator-Rechte verfügte. Darüber richteten die Täter eine Hintertür im Tenant ein und kopierten anschließend

Daten aus Azure, löschten diese soweit möglich oder verschlüsselten sie mit Azure-Bordmitteln – einschließlich der Sicherheitskopien. Und forderten Lösegeld.

Der Beitrag gibt über 35 Empfehlungen, wie man sowohl seine On-Premises-Systeme als auch die Cloud-Dienste (Entra und Azure) gegen solche Angriffe absichern kann. Die schiere Zahl der Maßnahmen zeigt, dass diese Aufgabe in der schönen neuen Cloud-Welt keineswegs einfacher geworden ist.

Besonders wichtig: Konten mit Administratorrechten in der Cloud sollten nicht mit Active-Directory-Konten verknüpft sein, und Sicherungskopien dürfen nicht von Administrationskonten der Produktivumgebung verändert oder gelöscht werden können.

Wettbewerbsvorteil Datenschutz

Eine Studie der CNIL vom 23.07.2025 weist nach, dass Datenschutzbeauftragte (DSB) keine Kostenfalle, sondern Gewinnbringer sind. Auch Unternehmen, die nicht zur Benennung eines DSB verpflichtet sind, sollten dies als Chance begreifen. Denn Unternehmen mit Datenschutzbeauftragten gewinnen mehr Aufträge, zahlen seltener Bußgelder und sparen IT-Kosten: In Ausschreibungen wird Datenschutz als Qualitätsmerkmal bewertet. Maßnahmen der Aufsichtsbehörden kosten Geld und Kunden (und sind schlecht für das Image).

Schließlich führen die Einführung und Umsetzung von Löschkonzepten zu Ersparnissen, da Speicherbedarf und Backupkosten meist erheblich sinken. Kurz gesagt: Datenschutz ist kein Ärgernis, sondern steigert die Profitabilität.

PBD-Toolkit

Am 07.08.2025 veröffentlichte die Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) einen Beitrag zum auf opencode.de bereitgestellten pbd-toolkit, einem Open-Source-Werkzeug zur Erkennung personenbezogener Daten in großen Datenmengen. Das Konsolen-Tool ermöglicht sowohl die Suche mittels regulärer Ausdrücke als auch über ein KI-basiertes Named-Entity-Recognition-Verfahren.

Tests offenbaren allerdings erhebliche Einschränkungen: Textdateien im .txt-Format werden nicht erkannt und PDF-Dokumente müssen durchsuchbar sein, da andernfalls keine Verarbeitung möglich ist – eine OCR-Funktion steht nicht zur Verfügung. Zudem war die Trefferquote insgesamt niedrig, insbesondere bei Verzicht auf die KI-Unterstützung. Außerdem kam es zu Redundanzen in den Ergebnissen und zu Fehlklassifikationen durch die KI: So wurde beispielsweise eine IBAN als Passwort erkannt. Das Tool sollte daher derzeit nur für eine unvollständige erste Einschätzung, nicht aber für eine verlässliche Identifikation personenbezogener Daten eingesetzt werden.

Secorvo News

Secorvo Seminare

Nutzen Sie die letzten Wochen des Jahres, um Ihr Know-how aufzufrischen und sich für kommende Projekte zu rüsten. Es gibt noch freie Plätze auf unseren Seminaren im November:

Auf dem T.P.S.S.E.-Seminar **vom 10. bis 13.11. 2025** lernen Sie, wie Sie durch systematische Integration von Security in den Software Development Lifecycle Sicherheitslücken verhindern – bevor sie entstehen.

Das PKI-Seminar **vom 17. bis 20.11.2025** taucht mit Ihnen ein in die Welt der Public Key Infrastrukturen: von den Grundlagen über praxisnahe Einsatzszenarien bis zur Planung und dem Betrieb Ihrer eigenen PKI.

Wir freuen uns auf Ihre Anmeldung! Sollten Sie in diesem Jahr keinen Seminarbesuch mehr vorsehen können, empfehlen wir Ihnen für Ihre frühzeitige Weiterbildungsplanung einen Blick in unseren Seminarkalender 2026.

Wer die Wahl hat…

Wahlen und Abstimmungen – in Vereinen, Organisationen, Gemeinden, Land und Bund – sind organisatorische und manchmal auch logistische Herausforderungen. Was liegt da näher, als sie zu „digitalisieren“? Beim kommenden KA-IT-Si-Event am **23.10.2025** in der „Church“ des CyberForum beleuchtet Frau Professorin Melanie Volkamer (SECUSO, KIT) die Sicherheitsanforderungen an Internet-Wahlen und -Abstimmungen, stellt praktische Beispiele vor und diskutiert die Vor- und Nachteile ihres Einsatzes. Anschließend erwartet Sie der Erfahrungsaustausch beim „Buffet-Networking“. Wir freuen uns auf Ihre Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Oktober 2025	
22.-23.10.	Annual Privacy Forum 2025 (ENISA, DG Connect, Karlstad University, Frankfurt)
23.10.	KA-IT-Si-Event „Wer die Wahl hat…“ (KA-IT-Si, Karlsruhe)
November 2025	
04.-05.11.	T.I.S.P./T.P.S.S.E. Community Meeting (TeleTrusT, Berlin)
04.-06.11.	25. IDACON 2025 (WEKA Akademie GmbH, München)
10.-13.11.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-20.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
24.-28.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
Dezember 2025	
04.-05.12.	CSCML 25 (IACR, CSCML, virtuell)
05.-07.12.	ICSP 2025 (National Institute of Technology Jamshedpur, Rourkela/IND)
08.-11.12.	Black Hat Europe 2025 (Blackhat, London/UK)
08.-12.12.	Asiacrypt 2025 (IACR, Melbourne/AU)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Paul Blenderman, Kai Jendrian, Dr. Alexander Koch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Liza Trace, Julian Wahl.

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Bahnhofplatz 8
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2025



Alter Wein, neue Schläuche...

Seit drei Jahren diskutiert die EU über die Einführung einer „Chatkontrolle“ – eine Neuauflage der „Kryptodebatte“ der 90er Jahre. Führende Kryptologen warnten damals überzeugend vor den Risiken von Key Escrow und Key Recovery. Weder in den USA noch in Europa kam es zu Beschränkungen von Verschlüsselungslösungen, doch die Debatte riss nicht ab. 2015 nahmen die Autoren daher erneut Stellung.

Um die Verbreitung von Darstellungen sexualisierter Gewalt gegen Kinder zu bekämpfen, sollen Kommunikationsdienste in der EU verpflichtet werden, private Nachrichten auf verdächtige Inhalte zu durchsuchen. Technisch lässt sich eine solche Chatkontrolle ohne Kryptoverbot nur erreichen, wenn Inhalte auf den Endgeräten der Nutzer überprüft werden, bevor sie verschlüsselt sind. Faktisch wäre dies das Ende einer dem vertraulichen Gespräch entsprechenden Kommunikationsform, von dem auch Berufsgruppen wie Journalisten und Anwälte betroffen wären.

Problematisch sind die grundrechtlichen Implikationen einer solchen Maßnahme: Eine anlasslose Überwachung widerspricht fundamentalen europäischen Rechtsprinzipien wie der Unschuldsvermutung, dem Recht auf Achtung der persönlichen Korrespondenz (Art. 8 der Europäischen Menschenrechtskonvention) und dem in Deutschland in Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis. Sie widerspricht auch der vom EuGH betonten Notwendigkeit der Verhältnismäßigkeit staatlicher Eingriffe in die Privatsphäre.

Kein Zweck, so legitim er sein mag, heiligt jedes Mittel. Eine punktuelle Verbesserung des unzweifelhaft wichtigen Schutzes von Kindern vor Missbrauch darf daher nicht mit anlassloser Massenüberwachung erkauft werden. Die Diskussion wirft eine Grundfrage europäischer Rechtskultur auf: Soll Sicherheit durch den Abbau von Freiheit erkauft werden? Eine EU, die ihre Werte ernst nimmt, muss Wege finden, beides zu schützen – die Sicherheit der Schwächsten ebenso wie die Freiheit aller.



Inhalt

Alter Wein, neue Schläuche...

Security News

Zündende Stromquelle

Alte neue Schwachstellen

Timm Thaler lässt grüßen

Security is Not My Problem

Totgesagte leben länger

Intransparente Zertifikate

Ansichtssache

Secorvo News

Teamverstärkung

Weiterbildung 2026

Hokus, Pokus, KIdibus

Veranstaltungshinweise

secorvo
security consulting

Security News

Zündende Stromquelle

Im zentralen Data Center des National Information Resources Service von Südkorea verursachten am 26.09.2025 Lithium-Ionen-Batterien einen Brand, der über 600 digitale Regierungsdienste lahmlegte und 858 TB Daten vernichtete. Der Vorfall zeigt die Risiken moderner Energieversorgungssysteme: Während USV-Anlagen häufig Blei-Säure-Batterien nutzen, bieten Lithium-Ionen-Batterien durch ihre kompakte Bauweise Platzvorteile, bergen jedoch ein höheres Brandrisiko. Sie können durch Stöße (thermische Verletzung) oder unsachgemäße Handhabung, etwa einem Vertauschen der Pole, beschädigt werden.

Die Lieferkette der verwendeten Lithium-Ionen-Akkus und seiner Komponenten ist ebenfalls von Bedeutung, denn sie werden zumeist als OEM-Bauteil in USV-Anlagen eingebaut. Weltweit gibt es nur wenige Lieferanten; außerdem sollte bei der Risikoanalyse nicht übersehen werden, dass die Akkusysteme von eingebetteter Software gesteuert werden – dem Battery Management System (BMS). Diese Software sichert die physische Einsatzfähigkeit, übernimmt Zell-Balancing (Ladungsverteilung) und steuert Schutzfunktionen wie Überspannung und Übertemperatur.

In Südkorea wurden zwischen 2018 und 2022 insgesamt 55 USV-Brände registriert; einer davon traf bereits 2022 ein Data Center – nicht auszuschließen, dass einige der Vorfälle extern ausgelöst wurden. Das sollte man nicht unberücksichtigt lassen – zumal in Deutschland die nationale Stromspeicherstrategie gerade mit genau dieser Technik ausgebaut wird.

Alte neue Schwachstellen

Die US-Cybersicherheitsbehörde CISA hat Anfang Oktober 2025 zwölf neue Sicherheitslücken (CVEs) in ihren Known Exploited Vulnerabilities (KEV)-Katalog aufgenommen (siehe SSN 6/2025). Besonders alarmierend: Ein Teil der neuen Einträge stammt aus dem Jahr 2017 oder früher. Das zeigt, dass selbst über zehn Jahre alte Sicherheitslücken weiterhin erfolgreich für Angriffe genutzt werden – weil viele Systeme offenbar jahrelang ungepatcht und damit verwundbar betrieben werden.

Veraltete Software und unzureichendes Schwachstellenmanagement laden Cyberkriminelle ein wie eine offene Balkontüre den Einbrecher. Die oft als „unvermeidbar" dargestellte Nutzung veralteter Systeme sollte von den verantwortlichen CISOs und ISBs kritisch hinterfragt werden – in der Regel wiegt der unsichere Betrieb das Risiko nicht auf.

Timm Thaler lässt grüßen

Am 22.10.2025 wies der hessische Landesdatenschutzbeauftragte darauf hin, dass LinkedIn ab dem 03.11.2025 die Daten von Nutzerinnen und Nutzern für das Training seiner KI-Modelle nutzt, ohne deren Zustimmung einzuholen. Damit folgt das Karriere-Netzwerk den schlechten Vorbildern von Meta, TikTok, Google, Amazon, eBay, X und anderen. Sie alle füttern ihre KIs mit Daten ihrer Nutzer: öffentlichen Posts, Bildern, Sprachdaten, Kaufverhalten etc. Verhindern können Nutzer dies nur, indem sie selbst aktiv werden und in den Einstellungen widersprechen – dann werden zumindest weniger Daten gesammelt.

Wer keine Einwände gegen die Verwendung seiner Daten hat, sollte sie wenigstens nur gegen Entgelt weitergeben. Die App Neon etwa bietet ihren Nutzern bis zu 30 US$ am Tag, wenn sie Sprachdaten aus Telefonaten Neon zum Weiterverkauf zur Verfügung stellen. In Deutschland sind allerdings die Vertraulichkeit des gesprochenen Wortes (§ 201 StGB) und die Regelungen der DSGVO zu beachten: Eine solche Nutzung ist daher nur zulässig, wenn alle Gesprächspartner wirksam einwilligen und die Weitergabe der Daten transparent im Einklang mit der DSGVO erfolgt.

Security is Not My Problem

Am 24.09.2025 hat Cisco für die auf ihren Switches und Routern verwendeten Betriebssysteme IOS und IOS XE Patches veröffentlicht. Diese beheben eine Schwachstelle im Subsystem für das Simple Network Management Protocol (SNMP), dessen Akronym auch spöttisch als „Security is Not My Problem" interpretiert wird.

In den SSN berichten wir regelmäßig (siehe z. B. SSN 12/2024) über Schwachstellen in Netzwerkgeräten. Meist betreffen sie die webbasierte Administrationsoberfläche. Dabei gerät oft in Vergessenheit, dass es noch andere Admin-Schnittstellen gibt – wie z. B. SNMP. Der Zugriff auf Administrationsschnittstellen sollte grundsätzlich auf die Quelladressen der dafür vorgesehenen Systeme beschränkt werden. Das gilt nicht nur für Webschnittstellen, sondern auch für SSH- und SNMP-Zugänge.

Außerdem sollten veraltete Protokollversionen wie SNMPv1 und SNMPv2 nicht mehr eingesetzt werden – sie bieten keine adäquaten Schutzmechanismen.

Totgesagte leben länger

Microsoft hat den Internet Explorer (IE) durch den Browser Edge ersetzt und den IE im Juni 2022 offiziell für tot erklärt. Ein Teil seines Codes lebt jedoch

weiter – z. B. im IE-Modus des Edge-Browsers. Dieser wird von IT-Abteilungen genutzt, um alte Intranet-Anwendungen weiter nutzen zu können. Dafür lassen sich beispielsweise per Gruppenrichtlinie einzelne URLs festlegen, die im IE-Modus geöffnet werden sollen.

Außerdem ließ sich im Edge eine Webseite auf Knopfdruck im IE-Modus zu öffnen – bis Angreifer im August begannen, Benutzer zu verleiten, diesen Knopf zu betätigen, um Schwachstellen im veralteten Code auszunutzen. Microsoft hat daraufhin die Funktion in privaten Installationen abgeschaltet.

IT-Abteilungen müssen selbst aktiv werden – sofern sie die Option nicht schon längst per Gruppenrichtlinie deaktiviert haben. Wie das geht, hat das Edge-Team am 08.10.2025 in einem Blogartikel detailliert beschrieben. Unterstützt wird der IE-Code im Edge-Browser mindestens bis 2029. Wahrscheinlich auch, weil Microsoft ihn nicht ohne Weiteres aus Windows entfernen kann: Zahlreiche WindowsFunktionen greifen weiterhin vielleicht darauf zurück...

Intransparente Zertifikate

Cloudflare, das einen DNS-Dienst mit der IP-Adresse 1.1.1.1 betreibt, berichtete am 04.09.2025 von Zertifikaten, die die kroatische Zertifizierungsstelle (CA) Fina unberechtigt für „1.1.1.1“ ausgestellt hatte – eine Abfrage bei crt.sh bestätigt das.

Leider nehmen immer wieder einzelne CAs ihre wichtigste Aufgabe, die Überprüfung der Rechtmäßigkeit des Zertifikatsantrags, nicht mit der nötigen Sorgfalt wahr. Daher hat Google 2013 Certificate Transparency (CT) eingeführt. Dabei prüfen Browser, ob die Ausstellung eines Zertifikats in einem revisionssicheren öffentlichen Register protokolliert wurde. Außerdem können Domäneninhaber darüber feststellen, wenn eine CA unberechtigt Zertifikate für ihre Domänen ausstellt.

Cloudflare hat nach eigenem Bekunden die CT-Logs für ihre Domänen überwacht. Der Fall zeigt, dass auch eigene IP-Adressen dabei berücksichtigt werden müssen – insbesondere, wenn darüber (wie bei Cloudflare) auch TLS-gesicherte Dienste wie DNS over HTTPS laufen.

Ansichtssache

Schon am 04.09.2025 hat der EuGH über Rechtsfragen zu den Begriffen „personenbezogene Daten“ und „Pseudonymisierung“ entschieden. Das EuG hatte zuvor die Ansicht vertreten, dass personenbezogene Daten ihren Personenbezug verlieren, wenn eine Stelle den Personenbezug nicht oder nur mit großem Aufwand wiederherstellen kann.

Der EuGH stellte nun ebenfalls fest, dass die Frage des Personenbezugs subjektiv ist. Es komme auf die Perspektive der verantwortlichen Stelle an, die die Daten verarbeitet. Ist kein Personenbezug herstellbar, fallen die Daten nicht unter die Bestimmungen der DSGVO. Konsequenterweise müssten dann aber auch verschlüsselte personenbezogene Daten ihren Personenbezug verlieren, wenn die Verschlüsselung nicht entschlüsselt werden kann – dieses Problem wurde aber vom EuGH nicht betrachtet.

In der Entscheidung stellte der EuGH zudem klar, dass verantwortliche Stellen, die Daten pseudonymisieren, die Betroffenen darüber informieren müssen, bevor sie sie an Dritte übermitteln.

Secorvo News

Teamverstärkung

Michael Schrempp ist Anfang Oktober zu unserem Beratungsteam dazugestoßen. Mit einem Master in IT Security (KIT) bringt er aktuelles und fundiertes Informationssicherheitswissen mit. Herzlich willkommen im Secorvo-Team!

Weiterbildung 2026

Unsere Seminarangebote 2026 – in unseren neuen Räumlichkeiten am Karlsruher Hauptbahnhof – sind online: Freuen Sie sich auf praxisnahe Inhalte und erfahrene Referentinnen und Referenten, die Ihre Kenntnisse in Datenschutz und Informationssicherheit auf den aktuellen Stand bringen.

Seminarübersicht und Online-Anmeldung unter www.secorvo.de/seminare.

Hokus, Pokus, KIdibus

KI wirkt in der Softwareentwicklung magisch: Code, Tests oder Reviews entstehen scheinbar von alleine. Doch gerade dort, wo es besonders zauberhaft erscheint, lohnt ein genauer Blick – vor allem im Hinblick auf Sicherheit und Vertrauen.

Auf dem Jahresabschluss-Event der KA-IT-Si am 11.12.2025 zeigt Peter Wegner (andrena objects), wie sich KI verantwortungsvoll in Entwicklungsprozesse integrieren lässt - im Spannungsfeld zwischen Euphorie und Kontrollverlust.

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet- Networking“. Hier geht's zur Anmeldung - wir freuen uns auf Sie!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz.

November 2025	
10.-13.11.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-20.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
24.-28.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
Dezember 2025	
03.12.	IT-Sicherheitstag NRW (IHK NRW, Dortmund)
04.-05.12.	CSCML 25 (IACR, CSCML, virtuell)
05.-07.12.	ICSP 2025 (National Institute of Technology Jamshedpur, Rourkela/IND)
08.-11.12.	Black Hat Europe 2025 (Blackhat, London/UK)
08.-12.12.	Asiacrypt 2025 (IACR, Melbourne/AU)
Januar 2026	
19.-21.01.	Omnisecure 2026 (in TIME, Berlin)
27.-28.01.	33. DFN Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)
Februar 2026	
02.-06.02.	IT-Defense 2026 (cirosec, Würzburg)
18.-19.02.	ID:SMART Workshop 2026 (CAST, Darmstadt)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Paul Blenderman, Kai Jendrian, Dr. Alexander Koch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Michael Schrempp, Liza Trace, Julian Wahl.

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Bahnhofplatz 8
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

November 2025



Gel(i)ebte Freiheit

Risikomanagement ist in vielen Unternehmen ein ungeliebtes Kind: Entweder fristet es ein trauriges Schicksal als Teil des Compliance-Buzzword-Bingo oder es quält Riskmanager und Unternehmensleitungen Jahr für Jahr bei dem Versuch, das nicht Messbare irgendwie zu objektivieren.

Mit etwas Distanz betrachtet wirkt das eigenwillig. Denn „Management" ist Tag für Tag nichts anderes als der Umgang mit Risiken: Marktrisiken, Inflationsrisiken, Innovationsrisiken, Personalrisiken, Wettbewerbsrisiken, Sicherheitsrisiken: Jede Management-Entscheidung ist eine Entscheidung über eine ungewisse Zukunft, die sich im Rückblick als falsch erweisen kann. Das ist – riskant. Will man dieses Risiko senken, das Ungewisse also etwas „beherrschbarer" machen, hilft manchmal Erfahrung, manchmal „eine gute Nase" (sprich: Glück) – und fast immer die Begrenzung des möglichen Schadens (nicht alle „eggs in one basket") sowie die Erhöhung der „Eintrittsbarrieren" für den Fehlerfall.

Dreierlei ist jedoch gewiss: Ein Ausschluss aller Risiken ist unmöglich, die Minimierung der Auswirkungen von Fehlentscheidungen zu teuer und eine umfassende Risikovermeidung ein Selbstmord in Raten. Management bleibt ein Balanceakt – anders wäre es nur, wenn wir die Zukunft verlässlich voraussagen könnten. Doch dann könnte das jeder, und die Freiheit wäre, ganz nebenbei, auch dahin: Eine vorhersagbare Zukunft lässt sich nicht mehr beeinflussen.

Warum feiern wir nicht unsere Entscheidungsfreiheit und erfreuen uns daran, dass wir Risiken managen dürfen? Nachdenken über die Konsequenzen von Entscheidungen ist dann nichts als die Übernahme von Verantwortung – und zielt auf die Vermeidung unnötiger und unvertretbarer Risiken. Genau das sollte ein gutes Risikomanagement leisten: Maßnahmen gegen vermeidbare und inakzeptable Risiken ergreifen. Vielleicht hilft ja die NIS-2-Richtlinie, das Risikomanagement aus der staubigen Schmuddelecke wieder ins (rechte) Licht zu rücken.



Inhalt

Gel(i)ebte Freiheit

Security News

Künstliche Objektivität

Unzureichend verschlüsselt

Und immer wieder Cookies

Mehr Pflichten, mehr Haftung

Nord-Süd-Gefälle

Fake Coding Interviews

Schutz vor dem Mittelsmann

Secorvo News

Risikomanagement für Verantwortliche

Seminare 2026

Threat Modeling

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Künstliche Objektivität

Am 23.10.2025 warnten die IT-Sicherheitsexperten Gadi Evron und Bruce Schneier vor der Möglichkeit, von KI-Helfern erzeugte Gesprächsprotokolle zu manipulieren. Ähnlich der Suchmaschinenoptimierung lassen sich auch KI-Zusammenfassungen durch gezielte Formulierungen im Gespräch beeinflussen. Bei dem von ihnen „AI summarization optimization" getauften Vorgehen sorgen Phrasen wie „Unsere wichtigste Erkenntnis ist..." für eine Priorisierung von Themen – die vermeintliche Objektivität der KI-Zusammenfassung entpuppt sich dabei als Irrglaube.

In ihrem Beitrag verweisen sie auf mehrere Studien, die zeigen, wie solche Manipulationen gelingen. Sie raten Nutzern von KI-Protokollanten, solche Einflussnahmen durch Gesprächsteilnehmer zu unterbinden. Organisationen sollten hierfür klare Regeln festlegen. Auch technische Gegenmaßnahmen können helfen, wie die Prüfung auf auffällige Formulierungen oder das Filtern von Prompt Injections.

Unzureichend verschlüsselt

Im September wurden sämtliche in der Cloud gespeicherten Konfigurationssicherungen von SonicWall-Firewalls gestohlen. Einzelheiten hat SonicWall in der zuletzt am 28.10.2025 aktualisierten Mitteilung an ihre Kunden offengelegt.

Danach verschlüsselte das Sicherungsverfahren lediglich die in der Konfiguration enthaltenen Passwörter und Schlüssel – mit AES-256, bei älteren Systemen mit 3DES. Alle übrigen Daten waren im Klartext gespeichert. Sie liefern wertvolle Einblicke in die interne Netzwerkstruktur der SonicWall-Kunden. Sicherheitshalber wurden die Kunden aufgefordert, die Zugangsdaten ihrer Firewalls zu ersetzen.

Grundsätzlich ist gegen eine Sicherung in der Cloud wenig einzuwenden – vorausgesetzt, das gesamte Backup wird verschlüsselt und der Schlüssel wird außerhalb der Cloud aufbewahrt.

Und immer wieder Cookies

Am 04.11.2025 veröffentlichte die Bundesbeauftragte für den Datenschutz die Ergebnisse einer forsa-Umfrage zu Cookie-Einwilligungen. Die Erkenntnisse überraschen nur teilweise: Zwar ist 83% die Kontrolle über die eigenen Daten wichtig oder sehr wichtig; dennoch assoziieren 37% eher Negatives mit dem Begriff Datenschutz. Auch wenn 56% nicht genau wissen, was Cookies sind, lehnen 77% nach eigenen Angaben in Cookie-Bannern nach Möglichkeit alles ab. 75% vertrauen nicht einmal darauf, dass sich Anbieter an ihre Einstellungen halten.

Angesichts der nach wie vor weiten Verbreitung von Bannern ohne „Alles ablehnen"-Knopf ist der Handlungsbedarf offensichtlich: Ohne schärfere Sanktionen gegen gesetzeswidrige Banner dürfte auch die Akzeptanz des Datenschutzes Schaden nehmen.

Mehr Pflichten, mehr Haftung

Am 13.11.2025 verabschiedete der Deutsche Bundestag das Umsetzungsgesetz zur NIS-2-Richtlinine; kurz darauf stimmte der Bundesrat zu. Damit wird das BSI-Gesetz an die Vorgaben der NIS 2-Richtlinie angepasst – mit weit reichenden Konsequenzen für Unternehmen und ihre Verantwortlichen (§ 30 BSIG).

Bisher unterlagen bereits die KRITIS-Bereiche strengen Audit- und Nachweispflichten, die nun in § 39 BSIG verankert sind. Doch das Gesetz geht weiter: Künftig kann das BSI auch für bisher nicht erfasste Branchen Nachweis- und Auditpflichten anordnen, sobald es ein entsprechendes Risiko in einer (besonders) wichtigen Einrichtung erkennt. Damit steigt die Zahl der potentiell betroffenen Unternehmen deutlich, die dieser „Auditgefahr" ausgesetzt sind.

Eine zentrale Anforderung ist die neue Schulungspflicht für Geschäftsleiter: Wer nicht nachweisen kann, dass er sich zu „Kenntnissen und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken" der Informationssicherheit fortbildet und Risikomanagementmaßnahmen überwacht, setzt sich der Gefahr persönlicher Haftung aus (§ 38 BSIG).

Um dieser Haftung vorzubeugen bietet Secorvo 2026 „NIS-2-Kaminabende" an, auf denen wir nicht nur die erforderlichen Kenntnisse im Risk-Management vermitteln, sondern zugleich ein C-Level-Forum für den Erfahrungsaustausch bieten (Terminanfragen bitte an info@secorvo.de).

Nord-Süd-Gefälle

Am 15.11.2025 veröffentlichte der Hessische Landesbeauftragte für Datenschutz seinen Bericht zur datenschutzkonformen Nutzung vom MS365. Während Schleswig-Holstein – auch aufgrund der Einschätzungen des ULD – mit seiner Open-Source-Strategie die Abhängigkeit von Microsoft verringert, schlagen Hessen und Bayern den entgegengesetzten Kurs ein: Sie bauen auf eine vertrauensvolle Zusammenarbeit mit dem US-Giganten und auf das schon vom Land Niedersachsen verhandelte Data Protection Addendum (DPA) für öffentliche Stellen.

Kritisch mag stimmen, dass die Zusagen von Microsoft bisher nicht technisch überprüft wurden. Wer MS365 einsetzt, sollte prüfen, inwieweit die Vorgaben aus Hessen umgesetzt sind. Darüber hinaus ist

zu hoffen, dass das DPA für öffentliche Stellen bald auch anderen Kunden angeboten wird.

Fake Coding Interviews

Seit Anfang 2024 beobachten Sicherheitsexperten eine Welle von Social-Engineering-Angriffen, die sich gegen Software-Entwickler und IT-Freelancer richten. Am 15.10.2025 beschrieb David Dodda in seinem Blog einen solchen Angriff aus der Perspektive des Opfers.

Dabei täuschen die Täter die Bewerber mit professionell erstellten Firmenprofilen und seriöser Kommunikation. Als Teil des Bewerbungsprozesseses verlangen sie einen vermeintlichen Programmiertest, der als Code-Repository in Bitbucket oder GitHub bereitgestellt wird. Der Code enthält getarnte bösartige Skripte, die bei Ausführung eine Backdoor auf dem System des Bewerbers installieren. Sie verschafft den Hackern Fernzugriff. Das vermutliche Ziel: Anmeldedaten zu Cloud-Diensten und Produktionssystemen von Unternehmen.

Entwickler sollten Code ungesicherten Ursprungs ausschließlich in einer Sandbox oder einer virtuellen Maschine ausführen. Das sollte nicht nur in der eigenen Entwicklungsabteilung Pflicht sein, sondern auch mit Freelancern vereinbart werden.

Schutz vor dem Mittelsmann

Webseiten ohne HTTPS-Unterstützung sind zur Ausnahme geworden. Projekte wie whynohttps.com, die unsichere HTTP-Seiten auflisten, haben daher ihre Bedeutung weitgehend verloren. Zum Schutz vor Man-in-the-Middle-Angriffen sollten unverschlüsselte HTTP-Verbindungen konsequent unterbunden werden.

Mit HTTP Strict Transport Security (RFC 6797) kann ein Server einem anfragenden Browser vorschreiben, eine Webseite künftig ausschließlich über HTTPS aufzurufen. Alternativ können HTTP-Aufrufe automatisch auf HTTPS umgeleitet werden. Beide Verfahren schützen jedoch nicht den ersten Verbindungsaufbau. Daher kündigte Google am 28.10.2025 an, dass Chrome ab Oktober 2026 die Zustimmung des Anwenders einholen wird, bevor es eine öffentliche Website ohne HTTPS lädt.

Administratoren können (und sollten) die Chrome-Einstellung „Immer sichere Verbindungen verwenden“ bereits jetzt per Gruppenrichtlinie aktivieren. Erforderliche Ausnahmen lassen sich darin vermerken. Ähnliche Einstellungen bieten Edge und Firefox.

Secorvo News



Risikomanagement für Verantwortliche

§ 38 BSIG verpflichtet Geschäftsleitungen (besonders) wichtiger Einrichtungen, Risikomanagementmaßnahmen umzusetzen und zu überwachen – und sich regelmäßig zu Kenntnissen und Fähigkeiten zur Erkennung und Bewertung von Risiken und Risikomanagementpraktiken der Informationssicherheit weiterzubilden.

Wir machen aus der Not eine Tugend: Auf unseren NIS-2-Kaminabenden führen wir Sie konzentriert und erfahren in diese Praktiken ein – und bieten Ihnen zugleich ein C-Level-Forum für den Austausch mit anderen Verantwortlichen. Die Termine finden Sie ab Mitte Januar 2026 auf unserer Webseite – wir informieren Sie auch gerne per E-Mail.

Seminare 2026

Auf unseren Seminaren vermitteln wir auch 2026 aktuelle Einblicke und bieten praxisorientierte Vertiefungen zu Themen der Informationssicherheit. Mit den Seminaren T.I.S.P., T.P.S.S.E. und Vorfallsexperte bereiten wir Sie auf den Erwerb anerkannter berufsqualifizierender Zertifizierungen vor.

Im kommenden Jahr bieten wir neben dem „Klassiker“ zu Konzeption und Aufbau von Public-Key Infrastrukturen mit dem ISMS-Intensivseminar einen praxisorientierten und pragmatischen Einstieg in den Aufbau eines wirksamen Sicherheitsmanagements.

Threat Modeling

Entdeckt man potentielle Sicherheitslücken bereits beim Design eines Systems oder einer Software, lässt sich viel Ungemach vermeiden. Das gelingt durch eine systematische Modellierung möglicher Bedrohungen, denen das System im Betrieb ausgesetzt sein wird – Threat Modeling ist daher ein Kernelement von Security by Design.

In der Ausgabe 1/2026 der iX führen Oliver Oettinger und Kai Jendrian in die Grundlagen und Möglichkeiten des Threat Modeling ein – von den Grundprinzipien bis zur Tool gestützten Modellierung komplexer Bedrohungsmodelle.

Schöne Weihnachten!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz.

Dezember 2025	
08.-12.12.	Asiacrypt 2025 (IACR, Melbourne/AU)
11.12.	KA-IT-Si-Event "Hokus, Pokus, KIdibus" (KA-IT-Si, Karlsruhe)
Januar 2026	
19.-21.01.	Omnisecure 2026 (in TIME, Berlin)
27.-28.01.	33. DFN Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)
Februar 2026	
02.-06.02.	IT-Defense 2026 (cirosec, Würzburg)
18.-19.02.	ID:SMART Workshop 2026 (CAST, Darmstadt)
März 2026	
02.-06.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
09.-12.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-19.03.	secIT 2026 (Heise Medien, Hannover)
23.-24.03.	ISMS verstehen und planen (Secorvo, Karlsruhe)

Fundsache

Das Bayerische Landesamt für Datenschutzaufsicht bietet auf insgesamt 24 Seiten eine 10-Punkte-Checkliste mit technischen und organisatorischen Sicherheitsmaßnahmen für mehr Datensicherheit. Die durchgehend praktischen Umsetzungsvorschläge umfassen auch Anforderungen der ISO/IEC 27001.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Paul Blenderman, Kai Jendrian, Dr. Alexander Koch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Michael Schrempp, Liza Trace, Julian Wahl.

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Bahnhofplatz 8
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Dezember 2025



Sicheres Wichteln

Ich mag Kryptografie. Mit jedem beliebigen Menschen sicher kommunizieren zu können, ohne ihn zuvor zu kennen, ist für mich Magie. Magie kann auch weh tun – wer je ein Zertifikat erneuert hat, weiß was ich meine. Doch in der Weihnachtszeit kann man Kryptografie schmerzfrei verwenden: beim Wichteln.

Was hat Wichteln mit Kryptografie zu tun? Beim Wichteln muss jeder Teilnehmer wissen, wen er beschenken soll – aber darf sich weder jemanden aussuchen noch selbst beschenken (müssen). Dazu braucht man eine zufällige (geheime) Zuordnung jedes Teilnehmers zu einem anderen – eine fixpunktfreie Permutation also. Sie ahnen es: Hier kommt Kryptografie ins Spiel.

Dafür genügen gewöhnliche Spielkarten. Jeder der *n* Wichtel erhält eine Herzkarte und *n*-1 Kreuzkarten sowie eine Nummer (von 1 bis *n*). Dann stapelt jeder seine Kreuzkarten und schiebt die Herzkarte an die seiner Nummer entsprechenden Stelle. Die Stapel werden gemischt und neu verteilt. Nun deckt jeder aus seinem Stapel die Karte an der Position seiner Nummer auf: Ist eine Herzkarte dabei, hat sich jemand selbst gezogen – und die Stapel müssen erneut gemischt und verteilt werden. Anderenfalls kennt jeder die Nummer desjenigen, den er beschenken muss – sie entspricht der Position der Herzkarte in seinem Stapel. Gegenüber dem klassischen Lose-aus-dem-Hut-Ziehen kann bei diesem Verfahren die Prüfung, dass niemand sich selbst beschenken muss, öffentlich erfolgen, ohne die Zuordnung der Wichtel offenzulegen.

Wer nun befürchtet, bei sehr vielen Wichteln hohe Kartenstapel tagelang mischen und tauschen zu müssen, wird erfreut sein zu hören, dass dreimaliges Mischen in der Regel ausreicht. Warum das so ist, passt nicht in ein Editorial - aber vielleicht in einen kalten Winterabend mit Papier, Stift und einer Tasse warmem Tee.

Tipp: Für große *n* nähert sich die Wahrscheinlichkeit, dass eine zufällige Permutation fixpunktfrei ist, dem Wert 1/*e* an. Magisch.



Inhalt

Sicheres Wichteln

Security News

Frankreich handelt

Entsorgung

Löschfrist ist abzuwägen

Kleinigkeiten zählen

500 Seiten Binsenweisheit

Resiliente Kommunikation

Secorvo News

Rechnen mit privaten Daten

NIS-2-Schulungen am Kamin

Seminare 2026

Veranstaltungshinweise

secorvo
security consulting

Security News

Frankreich handelt

Die französische Datenschutzbehörde CNIL verhängte am 03.12.2025 ein Bußgeld von 1,5 Mio. € gegen American Express: Das Unternehmen setzte nicht nur gleich beim Aufruf der Webseite Cookies, sondern auch bei Nichterteilung einer Einwilligung durch den Seitenbesucher – eine Praxis, die einige Firmen pflegen (SSN 7/2022).

In Deutschland bleiben solche Rechtsverstöße bisher ungeahndet. Zwar kündigte die Datenschutzkonferenz (DSK) am 12.12.2025 an, sich 2026 (erneut) zu Cookies und Tracking-Pixeln zu äußern – kaum zu erwarten, dass die Stellungnahme signifikant von der Position vom 14.11.2019 abweicht (SSN 11/2019).

Dabei sind Datenschutzverstöße auf Webseiten sowohl für Seitenbesucher (SSN 11/2020) als auch für Aufsichtsbehörden leicht (sogar automatisiert) feststellbar. Es ist schwer verständlich, warum Unternehmen an dieser Stelle hohe Bußgelder riskieren – zumal Nutzen und Aussagekraft von Website-Tracking-Daten äußerst fraglich sind (auch wenn Marketing-Abteilungen gerne anderes behaupten).

Entsorgung

Zertifikate sind nur so sicher wie die Verlässlichkeit der Validierung des Antragstellers – aber die ist dem Zertifikat selbst nicht anzusehen. Öffentliche Trustcenter bieten ihren Kunden meist verschiedene Methoden zur „Domain Validation“ an, also zum Nachweis des Besitzes einer Domäne. Einige dieser Methoden sind nur eingeschränkt verlässlich und werden heute kaum noch verwendet.

Deswegen hat das CA/Browser-Forum beschlossen, diese schrittweise abzuschaffen: 2024 traf es WHOIS, am 12.11.2025 folgten die DNS-PTR-Records und am 19.11.2025 kamen E-Mail, Fax und Telefon an die Reihe. Bei den beiden zuletzt genannten Methoden wurde den Trustcentern und ihren Kunden eine Übergangsfrist bis 2028 respektive 2027 eingeräumt.

Besser spät als nie: Die Entsorgung nicht mehr ausreichend sicherer Standards, Protokolle und Verfahren durch das CA/Browser-Forum ist ein wichtiger Beitrag zur IT-Sicherheit, an der sich auch andere Hersteller ein Beispiel nehmen sollten. Manchmal dürfte sie sogar noch ein wenig konsequenter erfolgen.

Löschfrist ist abzuwägen

Am 18.12.2025 hat der Bundesgerichtshof (BGH) klargestellt, dass bei der Bestimmung von Löschfristen für personenbezogene Daten immer eine konkrete Interessensabwägung erforderlich ist. Im Streitfall hatte die SCHUFA Daten des Klägers über ausgeglichene Forderungen teilweise länger als drei Jahre gespeichert – obwohl dafür in den von der Hessischen Beauftragten für den Datenschutz und die Informationsfreiheit genehmigten Verhaltensregeln für Wirtschaftsauskunfteien lediglich 18 Monate vorgesehen sind.

Der BGH entschied nun, dass die Löschfrist sich zwar an Richtlinien und Löschfristen von Einrichtungen anderer Art (z. B. Insolvenzbekanntmachungen) orientieren kann. Letztlich seien aber in einer „konkret vorzunehmenden Interessensabwägung“ die Erforderlichkeit zu prüfen und die Besonderheiten des Einzelfalls zu berücksichtigen.

Kleinigkeiten zählen

Trend Micro beobachtet (wie andere EDR-Anbieter auch) täglich Angriffe auf IT-Systeme. 2024 fielen ihnen .LNK-Dateien (Windows-Explorer-Verknüpfungen) auf, die ab dem 261. Zeichen Befehle enthielten. Diese bleiben verborgen, weil die Benutzerschnittstelle nur die ersten 260 Zeichen zeigt. Trend Micro meldete das am 20.09.2024 dem Microsoft Security Response Center. Dort hielt man das Problem für unbedeutend. Nachdem die Schwachstelle zunehmend in „staatlichen“ Angriffen – etwa gegen europäische diplomatische Einrichtungen – verwendet wurde, hat Microsoft sich im November-Update 2025 stillschweigend darum gekümmert. Der Hinweis vom 01.11.2025 stuft den Fehler allerdings nicht als Sicherheitslücke ein.

Genau genommen schließt der Fix die Schwachstelle nicht, sondern erleichtert die Entdeckung ihrer Nutzung: Microsoft begrenzte nämlich nicht die Länge oder den Inhalt der Verknüpfung, sondern änderte die Anzeige – vermutlich aus Kompatibilitätsgründen. Doch braucht man wirklich mehr als 260 Zeichen in einer Verknüpfung? Sollte jemand dort Skripte verstecken dürfen?

Wer verhindern möchte, dass die eigene Software nach und nach löchrig wird wie Schweizer Käse, sollte auch kleine Sicherheitslücken schließen.

500 Seiten Binsenweisheit

Am 09.12.2025 hat das Bundesinnenministerium auf Antrag der Plattform fragdenstaat.de ein Rechtsgutachten der Universität zu Köln veröffentlicht. Darin kommen die Autoren zu dem – kaum überraschenden – Ergebnis, dass Section 702 des FISA, der CLOUD Act und weitere Gesetze es den US-Geheimdiensten erlauben, auf nahezu sämtliche Daten in

der Cloud zuzugreifen, egal, wo die Server stehen, und fast egal, wer sie betreibt: Es kommt nicht darauf an, ob es sich um ein deutsches, ein europäisches oder ein amerikanisches Unternehmen handelt. Auch bedarf es keines richterlichen Beschlusses.

Diese Erkenntnis lässt sich auch einem von der DSK vor vier Jahren veröffentlichten Gutachten entnehmen (SSN 2/2022) – die Kosten für das neue Gutachten hätte das BMI sparen können.

Schutz vor (nach US-Recht legalen) Geheimdienstzugriffen bietet allein echte technische Souveränität. Helfen können zusätzliche technische Maßnahmen (wie Verschlüsselung) oder die Bevorzugung deutscher oder zumindest europäischer Plattformen.

Resiliente Kommunikation

Nach dem Brandanschlag auf eine Kabelbrücke über den Teltowkanal am 03.01.2026 waren rund 45.000 Haushalte und 2.200 Gewerbekunden im Berliner Südwesten tagelang ohne Strom. Stromnetz Berlin informierte auf einer Krisenseite über den Verlauf der Störung. Nur: Wie kommuniziert man, wenn mit dem Strom auch die Mobilfunknetze ausfallen?

Der Vorfall zeigt die Verwundbarkeit moderner Gesellschaften. Stromausfälle legen nicht nur Haushalte lahm, sondern auch Komponenten der Kommunikationsinfrastruktur: WhatsApp, Telefon, Internet – nichts funktioniert mehr.

Wer sich allein auf eine zentrale Kommunikationsinfrastruktur verlässt, ist im Krisenfall gegebenenfalls isoliert. Dabei gibt es Alternativen zum Mobilfunknetz wie den von der Bundesnetzagentur erlaubten LoRa-Funkstandard. Zusammen mit einem dezentralen Mesh-Netzwerk wie Meshtastic kann darüber eine grundlegende Kommunikationsfähigkeit gewahrt werden – mit wenig technischem Know-How und zu geringen Kosten. Eine erste Basis an lokalen Netzen existiert bereits.

Krisenvorsorge meint nicht nur die Anlage von Wasservorräten und Notfallrationen. Sie bedeutet auch die Verfügbarkeit alternativer Kommunikationswege. Darum kümmern sollte man sich vor der Krise.

Secorvo News

Rechnen mit privaten Daten

Die statistische Auswertung großer Bestände sensibler personenbezogener Daten – von Gehältern bis Gesundheitsdaten – scheitert oft an Datenschutzvorbehalten. Mit Hilfe moderner kryptographischer Verfahren können solche Auswertungen vorgenommen werden, ohne dass dabei einzelne personenbezogene Datensätze offengelegt werden.

Die dahinterstehende Technik wird „sichere Mehrparteienberechnung“ (MPC) genannt. Sie ermöglicht es, mit sensiblen Daten zu „rechnen“, ohne dabei einzelne Datensätze zugänglich zu machen. Das Verfahren wird zunehmend in der Praxis eingesetzt, so zum Beispiel in einer Studie zur geschlechtsspezifischen Lohnlücke im Großraum Boston oder in einer Studie zum sicheren Rechnen auf klinischen Daten, die im vergangenen Jahr veröffentlicht wurden.

Dr. Alexander Koch (Secorvo) stellte am 02.12.2025 auf der 23. Konferenz Theory of Cryptography (TCC) in Aarhus ein Forschungsergebnis zur Weiterentwicklung von MPC vor: Um das Verfahren mit minimaler Kommunikation zwischen je zwei Parteien durchzuführen werden neuartige Zufallsgeneratoren eingesetzt, mit denen die Beteiligten ohne weitere Kommunikation korrelierte Zufallswerte erzeugen können – ein weiterer Beitrag zur Praxiseignung von MPC.

NIS-2-Schulungen am Kamin

§ 38 BSIG verpflichtet Geschäftsleitungen wichtiger Einrichtungen nicht nur, Risikomanagementmaßnahmen umzusetzen und zu überwachen, sondern auch, sich regelmäßig zu Kenntnissen und Fähigkeiten zur Erkennung und Bewertung von Risiken und Risikomanagementpraktiken der Informationssicherheit weiterzubilden.

Wir machen aus der Not eine Tugend: Auf unserem NIS-2-Kaminabend führen wir Sie konzentriert in diese Praktiken nach den Anforderungen des BSI ein – und bieten Ihnen zugleich ein C-Level-Forum für den Austausch mit anderen Verantwortlichen. Die nächsten Termine finden Sie auf unserer Webseite – wir informieren Sie auch gerne per E-Mail.

Seminare 2026

Auf unseren Seminaren vermitteln wir auch 2026 aktuelle Einblicke und bieten praxisorientierte Vertiefungen zu Themen der Informationssicherheit. Mit den Seminaren T.I.S.P., T.P.S.S.E. und Vorfallsexperte bereiten wir Sie auf den Erwerb anerkannter berufsqualifizierender Zertifizierungen vor.

Im kommenden Jahr bieten wir neben dem „Klassiker“ zu Konzeption und Aufbau von Public-Key Infrastrukturen mit dem ISMS-Intensivseminar einen praxisorientierten und pragmatischen Einstieg in den Aufbau eines wirksamen Sicherheitsmanagements.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz.

Januar 2026	
19.-21.01.	Omnisecure 2026 (in TIME, Berlin)
27.-28.01.	33. DFN Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)
Februar 2026	
02.-06.02.	IT-Defense 2026 (cirosec, Würzburg)
18.-19.02.	ID:SMART Workshop 2026 (CAST, Darmstadt)
März 2026	
02.-06.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
05.03.	NIS-2-Kaminabend – Schulung nach BSIG (Secorvo, Karlsruhe)
09.-12.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-19.03.	secIT 2026 (Heise Medien, Hannover)
23.-24.03.	ISMS verstehen und planen (Secorvo, Karlsruhe)
23.-26.03.	RSA Conference 2026 (RSA Conference, San Francisco/US)
23.-27.03.	FSE 2026 (IACR, Singapur/ASE)
24.-27.03.	DFRWS EU 2026 (DFRWS, Linköping/SE)
April 2026	
14.-16.04.	Datenschutztage 2026 (WEKA-Akademie, Frankfurt)
14.-16.04.	PQCrypto 2026 (IACR, Saint-Malo/FR))



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Paul Blenderman, Kai Jendrian, Dr. Alexander Koch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Michael Schrempp (Editorial), Liza Trace.

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Bahnhofplatz 8
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.