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

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 Knobloch 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

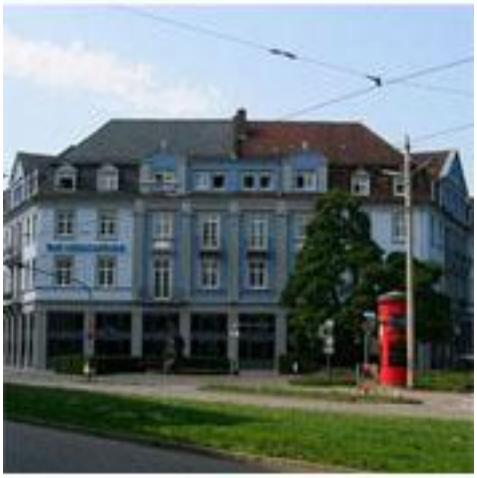
ISSN 1613-4311

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")

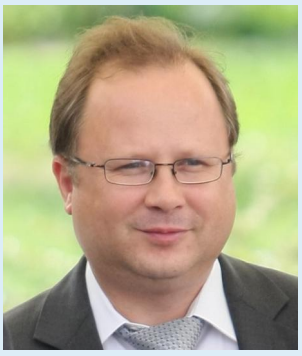
Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de



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

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

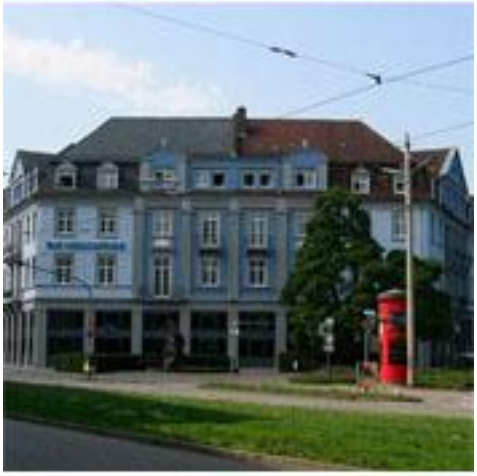
ISSN 1613-4311

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



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

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.

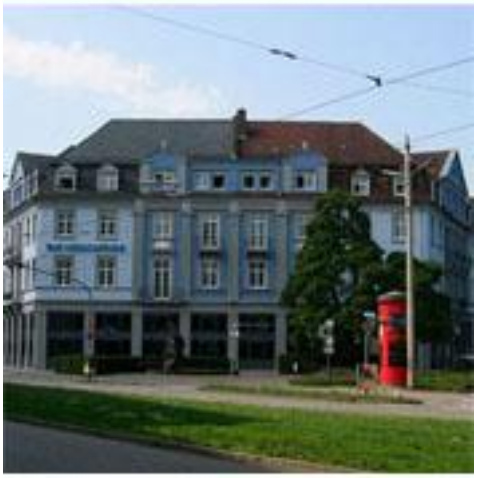
Veranstaltungshinweise

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

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

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!

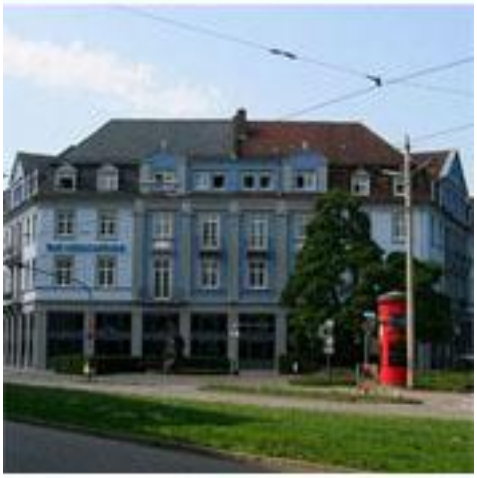
Veranstaltungshinweise

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

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

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

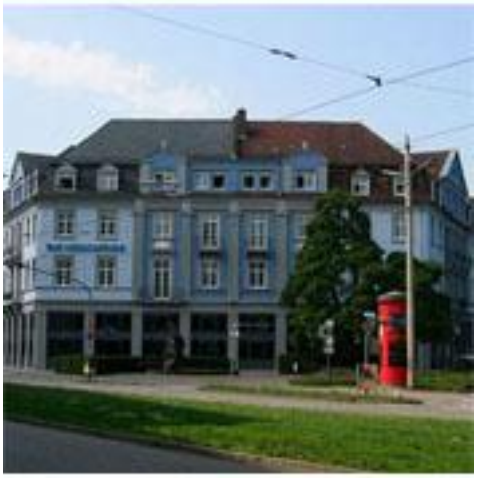
Auszug aus http://www.veranstaltungen-it-sicherheit.de

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

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

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

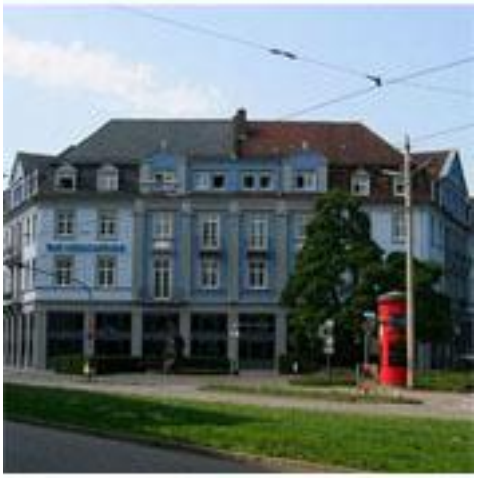
Veranstaltungshinweise

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

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

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!

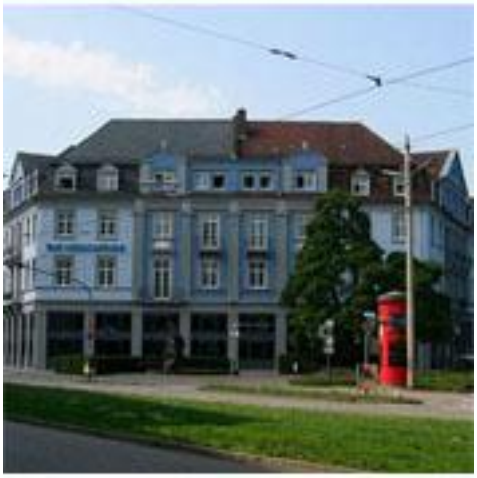
Veranstaltungshinweise

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

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

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!

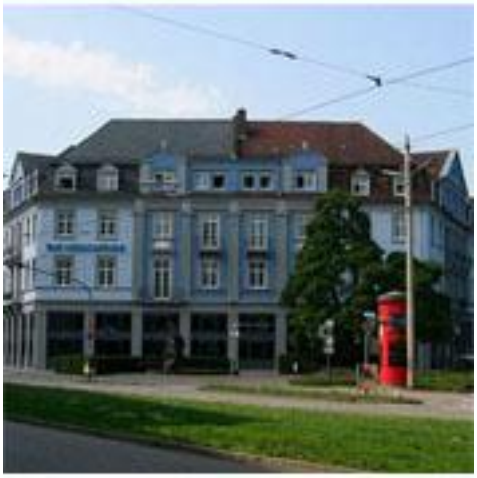
Veranstaltungshinweise

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

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

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!

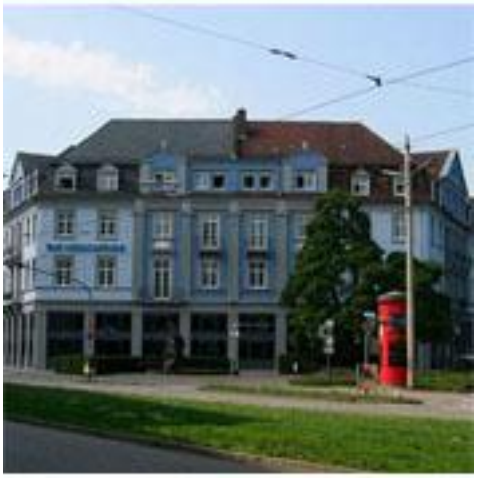
Veranstaltungshinweise

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

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

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!

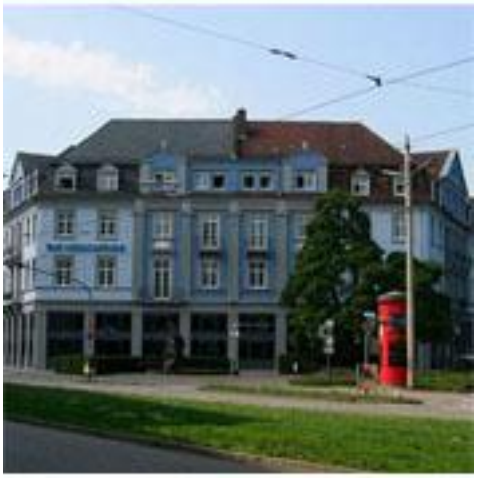
Die Zukunft ist mobil

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

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

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.

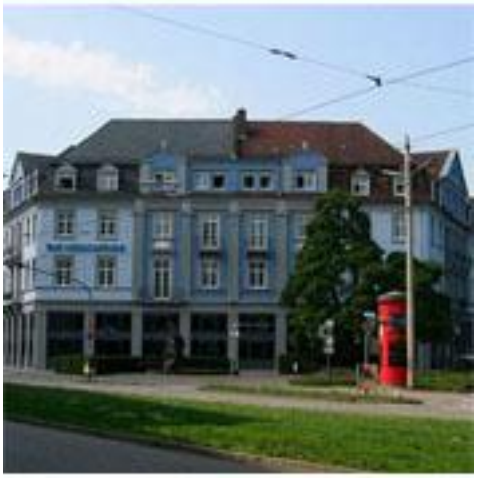
Veranstaltungshinweise

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

secorvo
security consulting

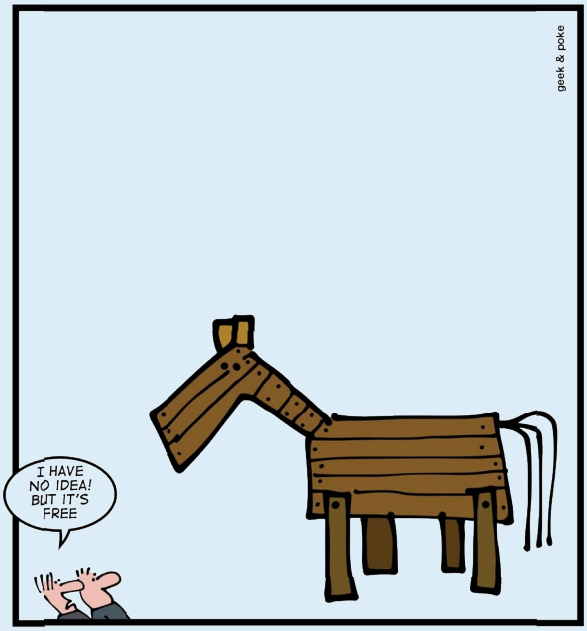
Secorvo Security News

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

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.

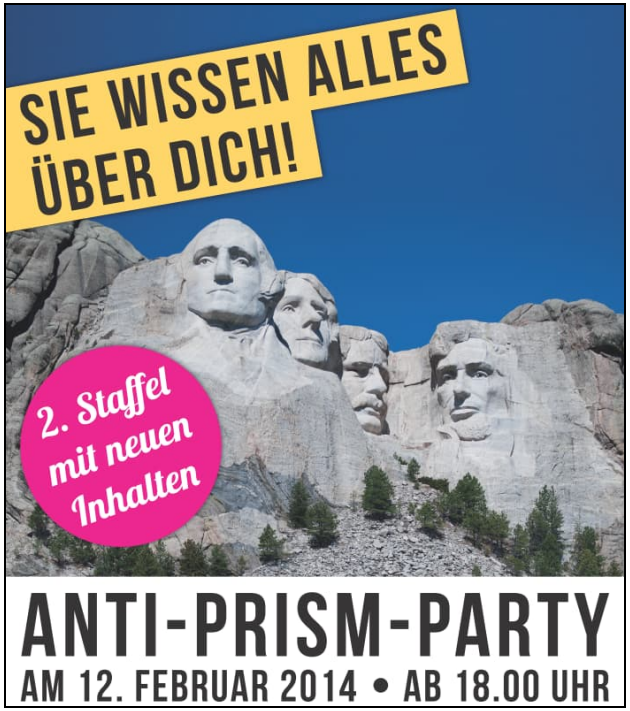
Sollte die Verordnung nicht rechtzeitig kommen, ist geplant, das Beschäftigtendatenschutzgesetz wieder auszugraben. Zum Ausgleich – da nun Sabine Leutheusser-Schnarrenberger als Justizministerin nicht mehr im Weg steht – soll, allen NSA-Affären zum Trotz, die Vorratsdatenspeicherung nach den Vorgaben 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.

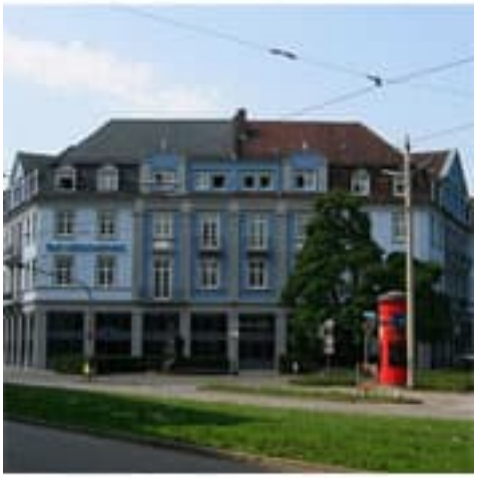
Veranstaltungshinweise

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