

Secorvo Security News

Januar 2011



Hornberger Schießen

Die Reaktionen sind vorhersagbar: CEOs bekommen beim Thema „Cloud Computing“ glänzende Augen, Datenschützer Bauchgrimmen. Hier die erwarteten Einsparungen durch Bedarfsabrechnung statt pauschaler Lizenzkosten, günstige Thin Clients und vorkonfigurierte Software mit zentraler Pflege, dort die Ungewissheit, welche Daten eigentlich wo, wie und von wem verarbeitet werden – unvorstellbar,

dass unter solchen Bedingungen eine [rechtskonforme](#) Auftragsdatenverarbeitung (schriftlicher Vertrag, Anweisung der Schutzmaßnahmen, Kontrolle des Auftragnehmers) möglich ist.

Tatsächlich sind die Auswirkungen des Cloud Computing-Konzepts schon heute sichtbar. Wer eine Suchmaschine für sich arbeiten lässt, einen Online-Routenplaner nutzt oder seine Kontakte in einem „Social Network“ pflegt, zahlt mit der Preisgabe personenbezogener Informationen. Auch Angreifer dürften sich nicht lumpen lassen und nutzen wahrscheinlich bereits verteilte Rechenpower, wie das Beispiel von Thomas Roth (siehe „Security News“) zeigt.

Bei genauerer Betrachtung werden die Fronten jedoch unscharf. So dürften viele Schutzmechanismen wie Virenschutz, Spam-Abwehr oder Patch-Services bei zentralen Diensten deutlich aktueller und wirksamer sein als in vielen heutigen IT-Infrastrukturen. Umgekehrt würden interne Informationen ungefiltert die Unternehmen verlassen – eine gruselige Vorstellung für die meisten Mittelständler. Dafür stiege der Schutz vor anderen Informationsabflüssen wie dem Verlust mobiler Geräte, wenn Unternehmensdaten nicht mehr lokal gespeichert sondern nur „in der Wolke“ zugänglich wären.

Voraussichtlich wird auch dieser Hype enden wie das Hornberger Schießen: Nach viel aufgewirbeltem Staub werden die Unternehmen versuchen, durch den Aufbau von Private Clouds die Vorteile zentraler Services mit einer kontrollierten Datenverarbeitung zu verknüpfen – nicht zur Freude der Service-Anbieter, die bereits neue Geschäfte wittern.



Inhalt

Hornberger Schießen	Smart, smarter, am smartesten
Security News	Lesestoff
Sandkastenleck	Neue Seminare
Krypto-Umbruch vertagt	Veranstaltungshinweise
Simple Foto-Tagging	Fundsache
Im Glashaus	
Undurchsichtige Wolke	
Secorvo News	

Security News

Sandkastenleck

Gleich am 04.01.2010 hat Billy Riot [in seinem Blog](#) zwei Schwachstellen in [einer der Sandboxes](#) von Adobes Flash-Player veröffentlicht. Wenngleich die Dokumentation [anderes verspricht](#), ist damit ein Zugriff auf eine lokale URL und so die Übermittlung von Informationen möglich. Bei der Analyse der zweiten Schwachstelle zeigt sich, dass Adobe sich zur Filterung der Protokolle für eine Blacklist entschieden hat. Damit sind alle Protokolle, die für un-gefährlich gehalten werden, auch für Zugriffe auf beliebige Systeme im Internet zugelassen. Auf diese Weise lassen sich aus der Flash-Sandbox heraus beliebige Daten an einen Server im Internet übermitteln.

Beunruhigend, dass Adobe auf die von Julia Wolf am 30.12. 2010 in Ihrem [Vortrag](#) auf dem Chaos Computer Congress 2010 ([27C3](#)) beschriebenen prinzipiellen Schwächen des Dateiformats PDF mit dem Hinweis auf ein Sicherheitsfeature in der aktuellen Version ihres PDF-Readers reagierte: einer Sandbox. Damit hat Adobe schon Erfahrung ...

Krypto-Umbruch vertagt

Der 2005 erschienenen und zuletzt 2007 überarbeiteten [NIST SP 800-57](#) zufolge hätte der 31.12.2010 das Ende aller Kryptoalgorithmen und Schlüssellängen der „80-Bit-Äquivalent“-Klasse markieren sollen: 1024-Bit-RSA und SHA-1 für digitale Signaturen sowie 2-Key-Triple-DES für die Verschlüsselung.

Die damaligen Abschätzungen waren jedoch sehr konservativ - und seither waren keine spektakulären Erfolge bei der Kryptoanalyse zu verzeichnen. So

erteilt die am 13.01.2011 erschienene [NIST SP 800-131A](#) diesen Algorithmen nochmals drei bzw. fünf Jahre Gnadenfrist. Dazu wurde zwischen „acceptable“ und „disallowed“ die Kategorie „deprecated“ eingeführt - frei übersetzt: „eigentlich sollst Du nicht, aber wenn es partout nicht anders geht und Du Dir über die Risiken im klaren bist ...“. Und bei Verwendung des 2-Key-Triple-DES muss nach maximal 8 MByte Daten der Schlüssel gewechselt werden - wie praktikabel das in der Praxis ist, wenn eine Dateilänge dieses Limit übersteigt, sei einmal dahin gestellt.

Zwar richten sich die [NIST](#)-Empfehlungen formal nur an US-Bundesbehörden; sie gelten aber gemeinsam mit dem am 22.12.2010 in der Fassung für 2011 erschienenen [SigG-Algorithmenkatalog](#) der [BNetzA](#) als Referenz für den Stand der Technik bei Kryptoalgorithmen und Schlüssellängen.

Simple Foto-Tagging

... ist das Thema eines auf den ersten Blick unscheinbaren [Eintrags](#) vom 16.12.2010 im [Facebook-Blog](#). Als erstes „Soziales Netzwerk“ beginnt Facebook damit, im großen Stil biometrische Informationen über seine Mitglieder (und darüber hinaus) zu sammeln: Die Kombination von automatischer Gesichtserkennung und vereinfachter Markierung von Personen in Fotos wird Facebook dank der Beliebtheit des Fotodienstes absehbar mit einer der größten personenbezogenen Bilddatenbanken ausstatten.

Die Datenbank wird allen europäischen Datenschutzbestimmungen zum Trotz auch Aufnahmen von Personen enthalten, die weder der Bereitstellung eines Bildes in Facebook noch der Markierung zugestimmt haben - möglicherweise nicht einmal Nutzer des „Sozialen Netzwerks“ sind. Das wird

zweifellos Begehrlichkeiten wecken - sofern diese Begehrlichkeiten nicht bereits eins der Motive für diesen Datenbankaufbau darstellen.

Für die Facebook-Nutzer ist dies ein Danaergeschenk, das Erziehungsberechtigte an die Warnung Laokoons in Vergils Aeneis erinnern sollte: „Quidquid id est, timeo Danaos et dona ferentes.“¹ Die Geschichte hat ihm Recht (und Schadsoftware einen illustren Namen) gegeben.

Im Glashaus

... sitzend warf der Hamburger Datenschutzbeauftragte Prof. Johannes Caspar am 10.01.2011 mutig [mit Steinen](#): Bei seiner für Google Deutschland zuständigen Datenschutzaufsichtsbehörde stand nach einer Reihe von Beschränkungsforderungen an Street View und dem Entwurf eines auf Google zugeschnittenen neuen [BDSG-Paragrafen 4a \(SSN 5/2010\)](#) nun Google Analytics auf der Agenda.

Bereits am 26./27.11.2009 hatte der Düsseldorfer Kreis einen [Entschluss über Zulässigkeitsbedingungen für Trackingdienste \(SSN 8/2010\)](#) gefasst. Im Wesentlichen wurden darin die verkürzte, anonyme Verarbeitung von IP-Adressen beim Tracking, die Möglichkeit zum Widerspruch und eine ausreichende Information in den Datenschutzerklärungen gefordert.

Da Google dem [eher verhalten nachgekommen](#) war, hatte Caspar angekündigt, nun mit Bußgeldern gegen Nutzer von Google Analytics vorgehen zu wollen. Entgangen war ihm jedoch, dass seine eigene Website sowie die der Stadt Hamburg gleich

¹ Was auch immer es ist, ich fürchte die Danaer und ihre überbrachten Geschenke.

mehrere nicht gesetzeskonforme Trackingdienste – darunter Google Analytics – verwendete. Nach seiner eher unglücklichen Verteidigung auf der [Blog-seite des Rechtsanwaltes Stadler](#) ging die Webseite der Aufsichtsbehörde dann „trackerfrei“ [offline](#).

Dem Datenschutz wird diese Komödie nicht gedient haben. Obwohl die Nutzung von Google Analytics [weiterhin gegen geltendes Datenschutzrecht verstößt](#), dürfte glaubwürdigen Maßnahmen der Aufsichtsbehörden damit bis auf weiteres der Boden entzogen sein.

Undurchsichtige Wolke

Das Verlagern von Rechenaufgaben in die Cloud ist nicht nur für Unternehmen ein Thema. Am 10.01.2011 [beschrieb](#) Thomas Roth, wie diese „Demokratisierung von Rechenleistung“ genutzt werden kann, um für wenige Euro per Wörterbuchangriff in der Cloud das WLAN-Passwort (WPA-PSK) des Nachbarn zu knacken, und präsentierte auf der [Black Hat DC](#) am 19.01.2011 seine „Cloud Cracking Suite“, mit der die Wolke zum Hacker-Tool mutiert.

Zwar verdankte er den schnellen Erfolg beim Nachbarn einem schlecht gewählten Passwort – dennoch wirft der Fall eine wichtige Frage auf: Muss ein Cloud-Anbieter prüfen, zu welchem Zweck sein Kunde die Rechenleistung nutzt? Und falls ja: Wie kann er das beurteilen? Eine ähnliche Frage stellte sich beim [SETI@Home](#) und dem inzwischen eingestellten [RC5-Wettbewerb](#). Zwar dürfte jede „missbräuchliche“ Verwendung der Ressourcen in den AGB der meisten Cloud-Anbieter untersagt sein – in der Praxis ist jedoch eine tatsächliche Bewertung der Nutzung unmöglich.

Mit Cloud-unterstützten Angriffen muss daher zukünftig verstärkt gerechnet werden. Das könnte die

eine oder andere Annahme über die einem Angreifer typischerweise zur Verfügung stehende Rechenleistung Makulatur werden lassen.

Secorvo News

Smart, smarter, am smartesten

Das „intelligente Stromnetz“ (vulgo: „Smart Grid“) verspricht in vielerlei Hinsicht Vorteile: So sollen sich Spitzen in Stromerzeugung und -abnahme verringern lassen, wodurch wiederum eine gleichmäßigere Bereitstellung von Energie und der Verzicht auf Kraftwerke ermöglicht werden soll.

Doch eine Beeinflussung von Geräten birgt auch enormes Missbrauchspotenzial, wie die [Analyse von Lastprofilen](#), die detaillierte Einblicke in die Vorgänge in einem Haushalt erlauben, bis zur unautorisierten Fernsteuerung elektrischer Geräte.

In seinem [Vortrag](#) über Sicherheits- und Datenschutzaspekte des Smart Grid auf dem nächsten KA-IT-Si-Event am 24.02.2011 im Schlosshotel Karlsruhe beleuchtet [Klaus J. Müller](#) beide Seiten. Um [Anmeldung](#) wird gebeten.

Lesestoff

Nicht nur in den Security News, sondern auch in einschlägigen Fachzeitschriften meldet sich Secorvo regelmäßig zu Wort. So hat sich in den vergangenen Monaten Michael Knopp zu [WLAN-Haftung](#) (DuD 9/2010) und der [Datenschutzherausforderung Webtracking](#) (DuD 11/2010) geäußert, Dirk Fox zur [betriebswirtschaftlichen Bewertung von Security Investments in der Praxis](#) (DuD 1/2011) Stellung genommen und Kai Jendrian und Klaus J. Müller Features und Maßnahmen gegen Browser-Angriffe beleuchtet (IX 2/2011).

In Kürze wird ein Beitrag zu Herausforderungen bei IPv6 von Dr. Safuat Hamdy und Hans-Joachim Knobloch in der <kes> (Ausgabe 1/2011) erscheinen.

Eine Übersicht der mehr als 350 Publikationen von Secorvo finden Sie auf unserer [Webseite](#).

Neue Seminare

Mit dem Thema Web-Anwendungs-Sicherheit erweitern wir ab Frühjahr 2011 unser Seminarangebot. Jedem, der Web-Anwendungen entwirft, entwickelt, spezifiziert, oder prüft bietet das Seminar alles Wichtige über die Bedrohungen, denen Web-Anwendungen ausgeliefert sind, sowie Lösungen, die einen verlässlichen Schutz bieten.

Zudem werden relevante rechtliche Rahmenbedingungen und insbesondere Datenschutzaspekte beleuchtet. Am 12. und 13.04.2011 startet das Seminar [„Verlässliche Web-Anwendungs-Sicherheit“](#).

Ab diesem Jahr werden die unabhängige Prüfung und Zertifizierung zum [T.I.S.P.](#) (TeleTrusT Information Security Professional) vom TÜV PersCert durchgeführt, einem Tochterunternehmen des TÜV Rheinland. Die nächste [T.I.S.P.-Schulung und -Prüfung](#) bieten wir vom 23.03. bis 02.04.2011 an.

Programme und Online-Anmeldung aller Seminare unter <http://www.secorvo.de/college>.

Veranstaltungshinweise

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

Februar 2011	
01.-02.02.	Smart Grid Symposium (Secorvo, Ettlingen/KA)
02.-03.02.	21. SIT-SmartCard Workshop (SIT, Darmstadt)
08.-10.02.	CPSSE-Schulung (Secorvo College)
15.-16.02.	18. DFN-Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
März 2011	
01.-05.03.	CeBIT (Deutsche Messe, Hannover)
22.-24.03.	Sicherheitsmanagement heute (Secorvo College)
28.03.- 01.04.	T.I.S.P.-Schulung (Secorvo College)
April 2011	
04.-06.04.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
07.-08.04.	Datenschutzaudit: Best Practice (Secorvo College)
12.-13.04.	Datenschutztag 2011 (FFD Forum für Datenschutz, Frankfurt)
Mai 2011	
10.-13.05.	Public Key Infrastrukturen (PKI) (Secorvo College)

Fundsache

Das US-amerikanische NIST hat dem Thema Datenschutz und Datensicherheit beim Cloud Computing ein 60seitiges Dokument gewidmet: „[Guidelines on Security and Privacy in Public Cloud Computing](#)“, erschienen am 28.01.2011 als SP 800-144 (Draft) zur Kommentierung.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

Februar 2011



Falsche Freunde

Im Englischen nennt man sie „false friends“. Wörter einer Fremdsprache, die einem Wort der Muttersprache phonetisch oder orthografisch ähneln, aber eine gänzlich andere Bedeutung besitzen, und so zu falschen Übersetzungen verleiten. So z. B. *become* (nicht bekommen, sondern werden), *sensible* (nicht sensibel, sondern fühlbar) oder *pathetic* (nicht pathetisch, sondern erbärmlich).

Ein ähnliches Phänomen lässt sich in der Informationssicherheit beobachten. Damit sind weniger die verbreiteten begrifflichen Unschärfen („persönliche Daten“) oder unterschiedlichen Definitionen von Sicherheit (*safety* versus *security*) gemeint, die gelegentlich zu Missverständnissen führen. Weit schlimmer sind Schutzmaßnahmen, die manchmal sogar Profis ein „Sicherheitsgefühl“ vermitteln – aber im Kern teure [potemkinsche Dörfer](#) sind.

So ist es heute in größeren Unternehmen üblich, den Gebäudezugang durch Betriebsausweise mit Foto zu kontrollieren. Tatsächlich werden die Fotos jedoch selten aktualisiert und oft sogar bei der Neuausgabe von Ausweisen wieder verwendet. Konsequenterweise überprüft das Sicherheitspersonal Ausweisfotos gar nicht erst auf Übereinstimmung mit dem Gesicht des Trägers. Zumeist genügt daher ein selbst gebastelter Pappausweis mit beliebigem Passfoto, um Zugang zu erhalten. Verhindert eine elektronische Schranke den unberechtigten Zugang, hilft ein großer Trolley (oder Rollstuhl), damit der „barrierefreie Zugang“ bereitwillig entriegelt wird.

Am Rechnerarbeitsplatz finden sich dann weitere Angriffserleichterungen: Die (ohnehin oft mickrige) Passwortlänge wird durch die Erzwingung regelmäßiger Wechsel effektiv weiter verringert – schließlich werden die letzten Stellen als Folgezähler benötigt (was den Zweck des Passwortwechsels konterkariert). Nicht selten gelingt eine Passwortrücksetzung durch Anruf beim Helpdesk – häufig wird dies durch keine wirksame Anruferauthentisierung verhindert.

Es wäre nicht nur billiger, auf derartigen Schein-Schutz zu verzichten. Denn die Illusion von Sicherheit reduziert die Wachsamkeit.



Inhalt

Falsche Freunde

Security News

Vorgedacht

Nachgedacht

Zu kurz gedacht

Umgedacht

Kompliziert gedacht

Neu gedacht

Speziell gedacht

Zu Ende gedacht

Secorvo News

Grundlagenseminare ...

... und der T.I.S.P.

Sicherheit von IPv6

Veranstaltungshinweise

Fundsache

Security News

Vorgedacht

Im vergangenen Jahr war es der Datenschutz, der [Bewegung](#) in das Thema Smart Metering brachte - nun rückt auch die Datensicherheit in den [Fokus](#). Am 28.01.2011 stellte das BSI einen [ersten Entwurf](#) eines Schutzprofils für die Kommunikationseinheit des Messsystems vor, das auch auf dem [Smart Grid Symposium](#) in Ettlingen diskutiert wurde. Die Planung sieht vor, das Schutzprofil noch im Jahr 2011 fertig zu stellen.

Da Smart Grids in den USA vor allem eine höhere Robustheit und Netzverfügbarkeit bewirken sollen, genießen Sicherheitsfragen in der amerikanischen Diskussion einen sehr hohen Stellenwert. So hat das NIST bereits im September 2010 600seitige „[Guidelines for Smart Grid Cyber Security](#)“ (aktuelle Fassung vom 25.10.2010) veröffentlicht. Es wäre zu begrüßen, wenn sich die darin enthaltenen Überlegungen und Erkenntnisse auch im deutschen Schutzprofil wiederfinden.

Nachgedacht

Der Bundesgerichtshof hat am 13.01.2011 über die derzeitige Praxis der Access-Provider zur ca. einwöchigen benutzerbezogenen Speicherung der IP-Adresszuordnung ([Urteilsbegründung](#) vom 08.02.2011) entschieden. Nach dem Telekommunikationsgesetz (TKG) bestehen zwei Rechtfertigungsmöglichkeiten: die Speicherung zu Abrechnungszwecken ([§ 97 Abs. 1 S. 1, Abs. 2 Nr. 1 TKG](#)) und die Speicherung zur Störungsanalyse und -beseitigung ([§ 100 Abs. 1 TKG](#)). Der BGH hat nun deutlich gemacht, dass die Geeignetheit und Erforderlichkeit der Speicherung zu beiden Zwecken detailliert unter

Beweis zu stellen ist. Die Instanzgerichte hatten die Erforderlichkeit und mögliche Alternativen gar nicht erst geprüft und eine diesbezügliche Beweislast des beklagten Telekommunikationsunternehmens verneint.

Tatsächlich bestehen begründete Zweifel, denn auch einzeln abzurechnende Dienste innerhalb einer Flatrate rechtfertigen keine generelle Speicherung zu Abrechnungszwecken. Die Begründungen für eine Speicherung zur Störungsbeseitigung beziehen sich bislang überwiegend auf die Störerermittlung bei SPAM- oder DoS-Attacken - dabei ist eine Speicherung jedoch nur für eine anschließende Rechtsverfolgung erforderlich. Ob diese von § 100 Abs. 1 TKG erfasst wird, ist äußerst fraglich. Nun ist das OLG Frankfurt am Zug. Die Prüfanforderungen zur Begründung von IP-Adressspeicherungen sind mit dem Urteil jedoch deutlich schärfer geworden.

Zu kurz gedacht

Die am 26.01.2011 von Alex Rice im Facebook-Blog [vorgestellte Reaktion](#) auf Session-Hijacking-Angriffe, die mit Tools wie Firesheep ([SSN 10/2010](#)) einfach durchzuführen sind, erweitert das Benutzerprofil um die Option „Facebook mit einer sicheren Verbindung (https) durchstöbern, wenn möglich“. Nach Aktivierung werden dann nicht nur die Login-Daten mit SSL geschützt an Facebook übertragen, sondern alle Daten, inklusive des Session-Cookie.

So weit, so gut. Was ist aber mit „wenn möglich“ gemeint? Da nicht alle Facebook-Apps den Umgang mit gesicherten Verbindungen beherrschen, erhält ein Benutzer beim Zugriff auf eine solche App den Warnhinweis: „Es tut uns leid, aber wir können diese Inhalte nicht anzeigen, während du Facebook über eine sichere Verbindung (https) benutzt. Um diese Anwendung nutzen zu können, musst du zu

einer regulären Verbindung (http) wechseln.“ Das wäre verschmerzbar - wenn das Wechseln auf eine ungeschützte Verbindung temporär erfolgen würde. Tatsächlich schaltet Facebook in diesem Fall die Option zum sicheren Surfen dauerhaft ab.

Umgedacht

Mit der verantwortungsvollen Veröffentlichung von Schwachstellen (Stichwort „[responsible disclosure](#)“) beschäftigt sich die vom Intrusion Detection Hersteller Tipping Point (HP) betriebene [Zero Day Initiative \(ZDI\)](#) seit ihrer Gründung. Die Kernidee ist, dass festgestellte Schwachstellen zuerst dem Hersteller gemeldet werden, um diesem Zeit zu geben, Gegenmaßnahmen zu ergreifen oder einen Patch bereit zu stellen. Danach erst wird die Schwachstelle öffentlich gemacht. Vorausgesetzt wird dabei, dass die betroffenen Hersteller ein Interesse daran haben, gefundene Schwachstellen umgehend zu beheben. Dass dies nicht immer der Fall ist, zeigt eine am 06.02.2011 von Sami Koivu veröffentlichte [Schwachstelle](#), die er bereits 2008 an Sun gemeldet hatte - und die bis heute nicht behoben wurde.

Die Zero Day Initiative verfolgt daher nun ein „responsible disclosure mit Ultimatum“: Festgestellte Schwachstellen werden nach 180 Tagen [veröffentlicht](#), unabhängig davon, ob ein Patch verfügbar ist - zum einen, um betroffene Nutzer möglichst frühzeitig über vorhandene Schwachstellen zu informieren, und zum anderen, um den Druck auf die Hersteller zu erhöhen. Von den aktuellen Veröffentlichungen sind unter anderem Adobe (Acrobat Reader, Flashplayer), Microsoft (Visio, Powerpoint, Excel), EMC, CA, Hewlett-Packard und IBM (Lotus Notes) betroffen. Betroffenen Nutzern empfehlen wir bis zur Bereitstellung von Updates temporär zusätzliche Schutzmaßnahmen.

Kompliziert gedacht

Die SHA-2 Familie bekommt Zuwachs: Neben den beiden unterschiedlichen Algorithmen SHA-256 und SHA-512 definiert [FIPS 180-3](#) vom 17.10.2008 ([SSN 10/2008](#)) den SHA-224 als SHA-256 mit unterschiedlichem Initialwert, dessen Ausgabe auf 224 bit gestutzt wird, und SHA-384 als auf 384 Ausgabebits zurechtgestutzten SHA-512, auch diesen mit abweichendem Initialwert.

Der am 11.02.2011 vom NIST veröffentlichte [Draft FIPS 180-4](#) ergänzt nun entsprechend zurechtgestutzte Versionen des SHA-512 als SHA-512/224 und SHA-512/256. Interessanterweise wird als Begründung für die neuen Familienmitglieder nicht die höhere Sicherheit angeführt, sondern die Tatsache, dass SHA-512 mit 80 Runden auf 64-Bit-Prozessoren schneller ist als der für 32-Bit-Architekturen entworfene SHA-256 mit 64 Runden. Einfach ist anders.

Neu gedacht

Dass Linux-Systeme nicht „per se“ sicherer sind als Windows-Systeme zeigen die inzwischen zahlreichen Sicherheitswarnungen und Patches zu den verschiedenen Distributionen. Allerdings hält sich hartnäckig die Überzeugung, dass Windows-Systeme der Ergonomie Vorzug vor der Sicherheit geben und daher – wie bei der Autorun-Funktion von DVD und USB-Sticks – mehr Einfallstore bieten. Tatsächlich wurden solche Einfallstore durch Softwareupdates inzwischen weitgehend dicht gemacht.

Für Linux-Systeme gilt das offenbar nicht, wie Jon Larimer auf der [Shmoocon](#) am 30.01.2011 [nachwies](#). Das Einstecken eines USB-Sticks genügt, um beispielsweise über Schwachstellen im Dateisystemtreiber oder (wie im konkreten Fall) des GNOME

Filemanagers „Nautilus“ Schaden zu stiften – sogar bei aktivierter Bildschirmsperre. Dagegen hilft nur, das automatische Mounten von Wechseldatenträgern manuell zu deaktivieren.

Speziell gedacht

Am 14.02.2011 erschienen gleich drei neue (Web)-Application-Firewalls: [OpenWAF](#), [IronBee](#) und [Oracle Database Firewall](#). Bei OpenWAF und IronBee handelt es sich um Open-Source-Lösungen von Herstellern mit Erfahrung – OpenWAF ist aus dem kommerziellen [Hyperguard](#) entstanden, IronBee entstammt der Feder von [Ivan Ristic](#), dem Autor von [mod_security](#). Oracles Lösung soll SQL-Datenbanken aller Art vor Angriffen schützen.

So schön die Verfügbarkeit dieser Schutzlösungen ist, drängt sich die Frage auf, wie viele Produkte eigentlich noch hintereinander geschaltet werden müssen, um einen ausreichenden Schutz von Anwendungen zu erreichen? Viel wichtiger wäre es wohl, Hersteller und Entwickler in die Lage zu versetzen, sichere Anwendungen auszuliefern, die nicht auf zusätzlichen Schutz angewiesen sind.

Zu Ende gedacht

Aufgrund der positiven Erfahrungen beim Betrieb des [DNSSEC Testbeds](#) ([SSN 01/2010](#)) kündigte DENIC am 08.02.2011 an, dass ab dem 31.05.2011 auch für die produktive .de-Zone [DNSSEC eingeführt](#) werden wird. Passend dazu gaben bei einer am 18.02.2011 präsentierten [Studie](#) von eco e.V. und VeriSign 61 % der befragten deutschen Domain-Anbieter an, DNSSEC bereits anzubieten oder innerhalb der kommenden zwölf Monaten anbieten zu wollen.

Viele Domaininhaber dürften in Bälde zur sichereren Version von DNS übergehen. Unternehmen und

Organisationen können also demnächst ihre DNS-Resolver am Übergang zum Internet DNSSEC-Signaturen prüfen lassen.

Secorvo News

Grundlagenseminare ...

Am 22.03.2011 startet die zweiteilige Seminarreihe „Grundlagen“ mit dem dreitägigen Seminar [Sicherheitsmanagement heute](#), einer Einführung in alle wesentlichen Bereiche des Informationssicherheitsmanagements. Mitte Mai folgt Teil zwei mit dem ebenfalls dreitägigen Seminar [IT-Sicherheit heute](#).

... und der T.I.S.P.

Experten in Sachen Informationssicherheit bietet das einwöchige T.I.S.P.-Seminar ab [28.03.2011](#) mit einer Kombination aus Schulung und zertifizierter TÜV-Prüfung einen aussagekräftigen und weithin anerkannten Kompetenznachweis.

Die Programme aller Seminare und die Möglichkeit zur Online-Anmeldung finden Sie unter <http://www.secorvo.de/college>.

Sicherheit von IPv6

Anlässlich der bevorstehenden Ausschöpfung des Adressraums von IPv4 haben sich Dr. Safuat Hamdy und Hans-Joachim Knobloch mit den Herausforderungen und Sicherheitsrisiken von IPv6 auseinander gesetzt. Die Ergebnisse ihrer Überlegungen sind nachzulesen in der aktuellen Ausgabe der Zeitschrift <kes> (Seiten 11-16).

Veranstaltungshinweise

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

März 2011	
01.-05.03.	CeBIT (Deutsche Messe, Hannover)
22.-24.03.	Sicherheitsmanagement heute (Secorvo College)
28.03.-01.04.	T.I.S.P.-Schulung (Secorvo College)
April 2011	
04.-06.04.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
07.-08.04.	Datenschutzaudit: Best Practice (Secorvo College)
12.-13.04.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College)
Mai 2011	
10.-13.05.	Public Key Infrastrukturen (PKI) (Secorvo College)
10.-12.05.	12. Deutscher IT-Sicherheitskongress (BSI, Bonn)
17.-20.05.	12. Datenschutzkongress (Euroforum, Berlin)
24.-27.05.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)

Fundsache

Die internationale [SAFECode-Initiative](#), die sich der Erhöhung der Vertrauenswürdigkeit informationstechnischer Systeme durch die Verbesserung und Verbreitung von Methoden sicherer Software-Entwicklung verschrieben hat, und in der sich neben EMC, Juniper und Microsoft insbesondere die SAP AG stark engagiert, veröffentlichte am 08.02.2011 die zweite Auflage der [Fundamental Practices for Secure Software Development](#). Das 56 Seiten starke Dokument enthält praxiserprobte Prinzipien und Empfehlungen für Design, Programmierung und Tests.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

März 2011



Krisenmanagement

Die entsetzliche Naturkatastrophe in Japan hat die Industrienationen dieser Welt in einen Schockzustand versetzt. Mehr noch als die gerne verdrängte Einsicht, dass lange drohende Naturkatastrophen eben doch eines Tages eintreten, erschreckt die Erkenntnis, dass das Krisenmanagement eines so hoch entwickelten und in Qualitätsfragen vorbildlichen Landes wie Japan geradezu hilflos wirkt.

So hielten die Hochhäuser dank präventiver Maßnahmen dem gewaltigen Erdbeben der Stärke 9 stand, nachdem das mit 20 Sekunden deutlich kürzere und schwächere Beben der Stärke 7 vor 16 Jahren in Kobe Häuser und Brücken wie Streichhölzer einknicken ließ.

Die Notfallvorsorge hingegen versagte. Stimmen die Berichte, dann haben Mängel in der Versorgung der Überlebenden des gigantischen Tsunami weitere Todesopfer gekostet. Angesichts der [Kritik am Krisenmanagement](#) nach der Kobe-Katastrophe erscheint dies wie ein Déjà-vu. Inzwischen ist zudem bekannt, dass der Betreiber des havariierenden Kernkraftwerks [zahlreiche Inspektionen versäumt](#) hatte – darunter die des Kühlsystems. Möglicherweise waren die Notstromaggregate also bereits vor dem Tsunami defekt.

Notfallvorsorge bedeutet, sich auf den Umgang mit einem Ereignis vorzubereiten, dessen Eintritt man zugleich durch präventive Maßnahmen zu verhindern sucht. Das ist ein „mentaler Spagat“, der oft zu Lasten der Notfallvorsorge ausgeht, da Menschen dazu neigen, die Wirksamkeit ihrer präventiven Maßnahmen zu überschätzen – weil „nicht sein kann, was nicht sein darf“.

Dafür gibt es auch in der IT-Sicherheit zahlreiche Beispiele – wie Backup-Bänder, deren Rückspielbarkeit nicht regelmäßig überprüft wird oder Notfallpläne, die auf falschen Annahmen beruhen (wie der Verfügbarkeit von Strom, Telefon oder Internet). Zwar geht es hier meist nicht um „Leib und Leben“. Dennoch gilt: Wer die Krisenreaktion nicht übt, wird sie im Ernstfall nicht beherrschen.



Inhalt

Krisenmanagement

Security News

Datenschutzkonformes
Webtracking

Legalisierte PIN-Weitergabe?

Desaster I

Desaster II

Schwierige Trennung

Rückkehr der Dialer

Secorvo News

PKI lesen und erleben

Alle IT-Sicherheit geht von
Karlsruhe aus

SSN-Symposium

Veranstaltungshinweise

Fundsache

Security News

Datenschutzkonformes Webtracking

Wer die Zugriffsstatistiken seiner Webseitenbesucher datenschutzkonform auswerten wollte, musste sich lange Zeit mühen, eine brauchbare Alternative zu Google Analytics zu finden. Zwar hat Google als Reaktion auf den „Bann“ der deutschen Aufsichtsbehörden ([SSN 08/2010](#)) im vergangenen Jahr eine Möglichkeit geschaffen, IP-Adressen der Seitennutzer so zu kürzen, dass sie nicht mehr zurückverfolgt werden können. Die Datenverarbeitung in den USA ohne angemessenen Schutz verhinderte jedoch nach wie vor einen rechtskonformen Einsatz in Deutschland. Die Datenschutz-Aufsichtsbehörden nahmen dies zum Anlass, den Einsatz von Google Analytics und anderer Tracking-Tools zunehmend abzumahnern – nicht immer mit glücklicher Hand ([SSN 01/2011](#)).

Als Alternative zu Google Analytics wird seit einer Weile das [Open-Source-Tool PIWIK](#) diskutiert. Für einen datenschutzkonformen Einsatz muss es allerdings angepasst werden – und genau dafür hat am 15.03.2011 das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) nach einer aufsichtsbehördlichen Analyse eine [Arbeitshilfe](#) publiziert. Unternehmen, die weiterhin Google Analytics auf ihren Webseiten nutzen, haben nun nicht einmal mehr eine schlechte Ausrede, wenn sie ein Bußgeldbescheid der Aufsichtsbehörde erreicht.

Legalisierte PIN-Weitergabe?

Am 09.03.2011 hat das Bundeskartellamt nach [Auskunft der Payment Network AG](#) eine Stellungnahme zu der am Landesgericht Köln anhängigen Klage der Giropay GmbH abgegeben. Darin wirft Secorvo Security News 03/2011, 10. Jahrgang, Stand 01.04.2011

Giropay dem Betreiber von [sfortüberweisung.de](#) wettbewerbswidriges Verhalten durch die Anstiftung zum Verstoß gegen die Muster AGB der Banken vor. Hintergrund ist das in diesen AGB verankerte Verbot, die Authentifizierungsmittel für das Online-Banking (Login-ID, PIN und TAN) an Dritte weiterzugeben. Genau [dies ist jedoch erforderlich](#), um im Rahmen von Internetgeschäften eine von sofortüberweisung.de unterstützte, in den Kaufprozess eingebundene Überweisung vorzunehmen. Das Bundeskartellamt sieht nach den eingeleiteten Ermittlungen Hinweise darauf, dass durch das Verbot der Weitergabe der Authentifizierungsmittel bankenunabhängigen Direktüberweisungsverfahren der Marktzutritt verwehrt wird.

Noch ist offen, wie das LG Köln und die vermutlich folgenden Instanzen den Sachverhalt bewerten werden. Allerdings erscheint fraglich, dass das Bundeskartellamt die Klausel der AGB in ihrer Bedeutung richtig erfasst hat. Für die Sicherheit des Online-Bankings ist die Geheimhaltungsklausel berechtigt, und es darf bezweifelt werden, dass ein Geschäftsmodell, das die Herausgabe der für einen persönlichen Authentifizierungsprozess verwendeten Geheimnisse an Dritte erfordert, überhaupt kartellrechtlichen Schutz genießen kann.

Desaster I

Mehrere Security-Unternehmen wurden in den vergangenen Wochen Opfer von viel beachteten Angriffen. Dabei betreffen die Angriffe auf RSA und Comodo auch die Sicherheit der Kunden und weiterer Anwender.

RSA – [Hersteller](#) der [SecurID](#) Einmalpasswort-Token und inzwischen Teil von EMC – [teilte](#) am 17.03.2011 [mit](#), dass das Unternehmen Opfer eines längerfristigen gezielten Angriffs ([Neusprech](#): [APT](#)) geworden

war. Aus der Mitteilung geht hervor, *dass* ein Schaden für SecurID eingetreten ist – lässt aber offen, *worin* dieser genau besteht und *wie* er sich auswirkt. Dem Vernehmen nach informiert RSA derzeit seine großen Kunden einzeln und unter [NDA](#) über Details. [Spekulationen zufolge](#) könnte zumindest ein Teil der Datenbank mit den Seed-Werten, aus denen sich alle One-Time-Passwörter aller registrierten Token rekonstruieren lassen, den Angreifern in die Hände gefallen sein. Dann würde nur noch ein Austausch der betroffenen Token helfen.

Desaster II

Am 15.03.2011 wurde eine für die Prüfung von SSL-Zertifikatsanträgen zuständige Registration Authority (RA) der von Comodo (Claim: „Creating Trust Online“) betriebenen CA [UTN-UserFirst-Hardware](#) kompromittiert. Der [vorgeblich iranische Angreifer](#) konnte mit deren Zugangsdaten fingierte Zertifikate für Domains wie Google.com und Yahoo.com beziehen – ein Blankoscheck für Phisher. Comodo [informierte](#) am 23.03.2011 darüber und veröffentlichte den zugehörigen [Incident Report](#).

Bereits zuvor hatten viele Browserhersteller [Patches erstellt](#), um die falschen Zertifikate unabhängig von den üblichen PKI-Sperrmechanismen zurückzuweisen. Besondere Übung hierin hat Microsoft, das bereits seit 22.03.2001 zwei [fingierte „Microsoft Corp.“ Code-Signing-Zertifikate](#) auf diese Weise [aus Windows aussperrt](#). Falls die Angreifer allerdings wie [behauptet](#) noch weitere, nicht identifizierte Zertifikate oder Zugangsdaten erbeutet haben, bliebe letztlich nur, die betroffenen CAs komplett als Vertrauensanker zu entfernen – mit unschönen Konsequenzen auch für alle legitimen Zertifikate.

Beide Fälle belegen, dass selbst in sicherheitskritischen Branchen noch nicht alle Unternehmen ver-

standen haben, dass das langfristige Vertrauen von Kunden und Anwendern in einem solchen Fall nur mit Offenheit, Kulanz und schneller Schadensbegrenzung zurück gewonnen werden kann – und nicht mit vagen Andeutungen, Geheimniskrämerei oder Verharmlosung. Gerade von Anbietern im Bereich der IT-Security sollte man zudem erwarten dürfen, dass sie Notfallpläne für „ihr“ Worst-Case-Szenario in der Schublade liegen haben.

Schwierige Trennung

Am 23.03.2011 hat das Bundesarbeitsgericht die vorangegangenen Urteile zum Umfang des Kündigungsschutzes eines betrieblichen Datenschutzbeauftragten [bestätigt](#). Kern des Streits war der gesetzliche Kündigungs- und Widerrufsschutz des betrieblichen Datenschutzbeauftragten aus den §§ [4f Abs. 3 BDSG](#), [626 BGB](#) einerseits und das Bestreben eines Unternehmens, konzernweit einen einheitlichen externen Datenschutzbeauftragten statt des internen zu etablieren andererseits. Sämtliche Instanzen haben den Wunsch nach einer Neuorganisation des Datenschutzes ebenso wie mögliche Konflikte durch die gleichzeitige Zugehörigkeit zum Betriebsrat nicht als wichtigen Grund gemäß § 626 BGB anerkannt.

Wie das klagende Unternehmen zu Recht vorgetragen hat, hat diese – auch schon zuvor in der einschlägigen Literatur vertretene – Rechtsauffassung zur Folge, dass ein unbefristet bestellter interner Datenschutzbeauftragter ohne sein Mitwirken praktisch nicht mehr abgelöst werden kann.

Rückkehr der Dialer

Bei der Sicherheit von VoIP wird der Fokus gern auf Vertraulichkeit, Integrität und Authentizität gelegt. Diese Sicherheitsziele sind meist jedoch weniger kri-

Secorvo Security News 03/2011, 10. Jahrgang, Stand 01.04.2011

tisch, solange VoIP nur hausintern betrieben wird. Eine erhebliche Gefahr ist hingegen der Gebührenbetrug. Durch die Vereinigung von Daten- und TK-Netzen werden Angriffe möglich, die die längst totgeglaubten Dialer wieder zum Leben erwecken. Insbesondere Softphones sind stark gefährdet.

So berichtete Mark Collier am 09.03.2011 in seinem [VoIP Security Blog](#) von einem Fall, in dem durch die Installation von Dialern acht Millionen US-Dollar „erwirtschaftet“ wurden. Der Urheber dieses Betruges wurde ermittelt und zu sieben Jahren Haft verurteilt. Solche Dialer können lange unbemerkt bleiben, wenn der Betrüger nicht zu gierig wird, denn gelegentliche kurze Anrufe an Servicenummern dürften in der Praxis kaum auffallen.

Bei Softphones kommen zudem zwei Angreiferwelten zusammen: Sofern es die Browser-Konfiguration zulässt, wird ein SIP-URI in einem HTML-Dokument an das Softphone weitergereicht – ein Himmelreich für Phisher. Von solchen Angriffen sind auch Smartphones betroffen, wie ein am 28.02.2011 bekannt gewordenes [Android-App](#) belegt.

Angesichts der geringen Aufmerksamkeit für diese Bedrohung steht zu befürchten, dass die schmerzlichen Lektionen mit herkömmlichen Endgeräten ignoriert und erneut gelernt werden müssen.

Secorvo News

PKI lesen und erleben

Seit dem 01.03.2011 stehen auf der Secorvo-Webseite zwei neue Whitepaper zum Download bereit: Eine Einführung in „[Public Key Infrastrukturen](#)“ von Petra Barzin und eine Schritt-für-Schritt-Anleitung zur Realisierung einer „[PKI von der Stange](#)“ von Hans-Joachim Knobloch. Vom **10.-13.05.2011**

können Sie auf dem viertägigen Secorvo College Seminar „[PKI – Grundlagen, Vertiefung, Realisierung](#)“ beide Autoren persönlich kennen lernen. Sie bieten Ihnen einen detaillierten und praxisorientierten Einblick in Konzeption, Implementierung und Nutzung von PKIs.

Alle IT-Sicherheit geht von Karlsruhe aus

Vor mehr als 25 Jahren wurden an der Universität Karlsruhe – dem heutigen KIT – die ersten Vorlesungen zu Kryptographie, technischem Datenschutz und Informationssicherheit in Deutschland gehalten. Zahlreiche Lehrstühle an deutschen Hochschulen und Unternehmen im Gebiet IT-Sicherheit haben ihre Wurzeln in Karlsruhe, ebenso wie das „Europäische Institut für Systemsicherheit (EISS)“.

Am 28.02.2011 wurde das EISS/KIT vom Bundesforschungsministerium zum „[Kompetenzzentrum für angewandte Sicherheits-Technologie](#)“ ernannt. Was KASTEL in der Zukunft zur IT-Sicherheit in und aus der Region Karlsruhe beitragen wird, stellt Prof. Dr. Jörn Müller-Quade, Leiter des EISS, auf dem kommenden [KA-IT-Si-Event](#) am **14.04.2011** vor. Beginn: 18 Uhr im Schlosshotel Karlsruhe, mit anschließendem Buffet-Networking ([Anmeldung](#)).

SSN-Symposium

Nach dem überschwänglichen Feedback zu unserem „Security News Symposium“ im vergangenen Jahr freuen wir uns, Sie heute zu unserem [zweiten SSN-Symposium](#) am **31.05.-01.06.2011** in die [Buhlsche Mühle](#) einladen zu können – mit spannenden Vorträgen und Diskussionen zu Security- und Datenschutzfragen rund um VoIP, IPv6, Webtracking, Skimming und Online-Banking. Wir freuen uns auf Ihre [Anmeldung](#)!

Veranstaltungshinweise

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

April 2011	
12.-13.04.	a-i3/BSI-Symposium 2011 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
Mai 2011	
10.-13.05.	Public Key Infrastrukturen (PKI) (Secorvo College)
10.-12.05.	12. Deutscher IT-Sicherheitskongress (BSI, Bonn)
12.-15.05.	Swiss Cyber Storm 3 Security Conference (Compass Security AG, Rapperswil/CH)
17.-20.05.	12. Datenschutzkongress (Euroforum, Berlin)
24.-27.05.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)
31.05.- 01.06.	2. Security News Symposium (Secorvo, Karlsruhe/Ettingen)
Juni 2011	
06.-07.06.	DuD 2011 (Computas, Berlin)
06.-11.06.	T.I.S.P.-Schulung und -Prüfung (Secorvo College)
06.-11.06.	OWASP Global AppSec Europe (OWASP Foundation, Dublin/IE)
28.-30.06.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)

Fundsache

Anfang März publizierte das US-amerikanische NIST die 88seitige [Special Publication 800-39](#) zum Thema „Managing Information Security Risk“ – ein lesenswerter systematischer und aktueller Überblick.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Karin Schuler

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

April 2011



Anonyme Kontrolle

Der eine oder andere „Datenschutzaufrerger“ mutet schon etwas skurril an. So wissen wir jetzt, dass der Navigationsgerätehersteller TomTom [Daten über Streckendurchschnittsgeschwindigkeiten](#) (die aus den Fahrdaten von TomTom-Kunden errechnet werden, um möglichst realistische Fahrzeiten zu prognostizieren) niederländischen Behörden zugänglich macht, um diesen die Beseitigung von

Engpässen und Stauabschnitten zu erleichtern. Die niederländische Polizei nutzte diese Daten unerwartet kreativ: Sie platzierte Radarfallen an Stellen, an denen die von TomTom bestimmten Durchschnittswerte über der örtlichen Geschwindigkeitsbegrenzung lagen. (Vielleicht hatte sie den [Datenschutzbericht der Telekom](#) gelesen.)

Aus der Perspektive des Steuerzahlers und Bürgers ist das eine sehr vernünftige Maßnahme: höchste Wirtschaftlichkeit der Geschwindigkeitskontrollen, wirksame Erhöhung der Verkehrssicherheit in kritischen Straßenabschnitten – und datenschutzrechtlich nicht zu beanstanden, da lediglich mit Zustimmung der Nutzer erstellte anonyme Statistiken verwendet wurden. Dennoch ist die Aufregung groß. Das mag daran liegen, dass TomTom-Nutzer den Eindruck gewonnen haben, dass sie mit ihrer Zustimmung zur Datenerhebung der Polizei die Ahndung eigener Verkehrsdelikte erleichtern.

Vielleicht aber versteckt sich hier ein sehr grundsätzliches Datenschutzproblem, das das geltende Recht nur unzureichend erfasst. Denn auch anonyme Statistiken – nach Definition gerade keine personenbezogenen Daten – können die freie Entfaltung beeinträchtigen. So könnten Stadtwerke in Abhängigkeit vom Mietniveau eines Wohnbezirks entscheiden, ob sie bei Zahlungsverzug den Kunden erst anrufen oder lieber gleich zwei kräftige Ableser vorbeischicken. Versandhändler könnten Bestellungen aus Städten mit hoher Arbeitslosigkeit ablehnen, um Zahlungsausfälle zu minimieren. Und Anbieter von Pillen gegen Harndrang könnten die Plakatierung in Gegenden verstärken, in denen die Smart Meter gehäuft nächtliche Toilettengänge registrieren. Schöne neue Welt.



Inhalt

Anonyme Kontrolle

Security News

Ein Goldchip ist keine Silberkugel

Erhöhtes Grundrauschen

Datenschutz zum Anfassen

Virencheck-Check

GPS-Daten in Smartphones

Personalausweis im Test

Smart Meter – mit Sicherheit

Secorvo News

Lizenz zum Entwickeln

Security News Symposium 2011

DuD 2011

College-Seminare

Veranstaltungshinweise

Fundsache

Security News

Ein Goldchip ist keine Silberkugel

Zu Jahresbeginn [forderte das BKA](#), zum Schutz gegen Skimming-Angriffe an Geldautomaten endlich komplett vom Magnetstreifen auf den EC-Karten-Chip umzusteigen. Bereits am 11.02.2010 hatten britische Forscher der BBC [demonstriert](#), wie sich eine Schwäche im dort verwendeten „Chip&PIN“ Verfahren am Point-of-Sale-Terminal ausnutzen lässt. Sie benötigten dazu allerdings einen Rucksack voller Elektronik und im Ärmel versteckte Kabel.

Am 10.03.2011 [präsentierten](#) amerikanische Wissenschaftler nun bei der [CanSecWest](#) Konferenz ein [Skimming-Gerät](#), das vollständig im Schlitz eines Kartenlesers verschwindet und sich als ultraflacher Man-in-the-Middle zwischen die Kontakte des Lesers und der Karte setzt. Ohne starke Krypto-Protokolle schützt auch ein Sicherheitschip nicht vor Missbräuchen an der Automatenchnittstelle.

Erhöhtes Grundrauschen

Am 19.04.2011 veröffentlichte der Sicherheitsdienstleister Verizon Business seinen [Data Breach Investigations Report](#) für 2011. Danach hat die große Zahl externer Hacking-Angriffe auf Zufallsopfer den Anteil an Insiderattacken gegenüber dem Vorjahr zurück gedrängt - nicht jedoch deren absolute Zahl.

Diesen Trend bestätigt eine [Meldung](#) vom 16.04.2011, nach der selbst von seriösen Webseiten wie den von [Amnesty International](#) aus Drive-By Downloads über die offenbar nicht auszurottenden [Schwachstellen des Flash Players](#) verteilt werden.

Die Empfehlung der Autoren des Reports für den Umgang mit dem damit verbundenen Risiko ist Wasser auf die Mühlen von Datenschützern: Man lösche alle nicht benötigten Daten, damit man die verbleibenden besser im Blick behalten kann.

Datenschutz zum Anfassen

Das Projekt „Autobahnmaut“ des Betreibers [Toll Collect](#) stand vor Beginn des Wirkbetriebs am 01.01.2005 wegen Startproblemen und der Erhebung der Mautdaten unter starker Kritik. Seither ist es ruhig geworden um Toll Collect - die Mauterhebung läuft reibungslos und der [BfDI](#) überzeugte sich 2006 von der [Wirksamkeit des Daten-Löschkonzepts](#).

Am 25.02.2011 ging Toll Collect mit der Eröffnung einer [Datenschutz-Ausstellung](#) in die Öffentlichkeit: Spannungsfelder zwischen Techniknutzung und Datenschutz werden in fünf Installationen aufbereitet, z. B. in Form einer Datenspur über einen Tag - mit überraschenden Einsichten. Drei weitere Installationen beschäftigen sich mit der beschlagnahmefesten [Zweckbindung der Mautdaten](#), der Löschkaskade für Kontrolldaten aus den Mautbrücken und den Löschrufen für Daten im Lebenszyklus eines Mautbenutzers. Die Besichtigung der Berliner Ausstellung ist nach [Anmeldung](#) möglich.

Bleibt zu wünschen, dass sich solche Best Practice in andere Unternehmen verbreitet - und der Gesetzgeber die strenge Zweckbindung der Mautdaten auch in der Zukunft aufrecht erhält.

Virencheck-Check

Viele IT-Nutzer erleben IT-Sicherheit vor allem beim Viren-Scan - häufig allerdings eher als (vermeintliche) Ursache für Performance- oder Funktionalitätseinschränkungen denn als wirksamen Schutz.

Am 14.04.2011 veröffentlichte nun das renommierte unabhängige Magdeburger AV-Testlabor aktuelle [Prüfergebnisse](#) für 22 führende Anti-Virus-Produkte. Seit Mitte 2010 erhalten Produkte, die 11 der maximal 18 zu vergebenden Testpunkte erreichen, von AV-Test ein Zertifikat. Ein zugehöriger Test-Report weist die vom Produkt für die Erkennung und Beseitigung von Viren sowie den Bedienkomfort erreichten Punkte aus.

Zwar kann man geteilter Meinung darüber sein, ob ein umfassender Client-Virenschutz auf rein geschäftlich genutzten Systemen noch zeitgemäß ist - denn eingehende E-Mails und Internet-Downloads lassen sich zentral wirksamer prüfen. Damit bleibt wenig mehr als das Einfallstörchen USB-Stick.

Bei privaten Systemen hingegen, die in der Regel durch keine Firewall und keinen zentralen Virenscanner geschützt sind, sind Anti-Viren-Produkte nach wie vor unverzichtbar - da kann es lohnen, vor der nächsten Verlängerung der Produktlizenz einen Blick auf die Testergebnisse zu werfen.

GPS-Daten in Smartphones

Der am 20.04.2011 publizierte [„iPhone Tracker“](#) von Alasdair Allan und Pete Warden, der die im iPhone gespeicherten GPS-Informationen eines Nutzers visualisiert, hat großen Wirbel ausgelöst - dabei ist die Speicherung von GPS-Daten auf dem iPhone [lange bekannt](#). Auch der primäre Zweck der Speicherung ist leicht zu raten: Da präzise GPS-Lokalisierungen zeit- und rechenintensiv (und damit auch energiehungrig) sind, suchen alle Smartphone-Hersteller nach Optimierungen - z. B. durch die Speicherung „bekanntere Wege“, denn Menschen neigen dazu, bestimmte Wege immer wieder zu nutzen. Nicht auszuschließen allerdings, dass Apple mit den Daten zukünftig auch anderes im Sinn hatte: Erst

im Juni 2010 hatte Apple in seine [Datenschutzrichtlinie](#) die Nutzung und Weitergabe (anonymisierter) Standortdaten aufgenommen.

Andere Anbieter haben sich da geschickter ange stellt. So erzeugt Vodafone mit seinem Ortungsservice „[Vodafone Locate](#)“ zur Handyortung, Routen- und Terminplanung Umsatz – statt eines Datenschuttskandals.

Personalausweis im Test

Am 21.04.2011 hat die Stiftung Warentest die Ergebnisse des Schnelltests der [Einsatzmöglichkeiten des neuen Personalausweises](#) veröffentlicht. Ganze 18 Angebote für die Online-Identifikation mit der eID zählten die Tester – davon ist ein Teil nur für registrierte Kunden nutzbar. Die [Testseite](#) des „Kompetenzzentrums neuer Personalausweis“ erzeugte z. T. merkwürdige Fehlermeldungen. Und einzig beim Angebot der Schufa erhält man bei deaktivierten Cookies eine aussagekräftige Meldung – alle anderen Angebote stellen sich „tot“.

Das nüchterne Fazit: Der praktische Nutzen der eID-Funktion hält sich (noch) stark in Grenzen, die wenigen Anwendungen gehören zudem zum Teil in die Kategorie „Bananen-Software“: Reift beim Kunden.

Smart Meter – mit Sicherheit

Seit Anfang 2010 ist der Einbau von Smart Metern in Neubauten und bei Renovierungen nach [§ 21b Abs. 3a/b Energiewirtschaftsgesetz](#) (EnWG) vorgeschrieben. Dass Sicherheitsprobleme in diesen Geräten weit reichende Auswirkungen haben können, ist [keine neue Erkenntnis](#). Daher wird derzeit unter der Federführung des BSI ein passendes [Schutzprofil](#) nach [Common Criteria](#) für die zugehörige Kommunika-

tionseinheit (auch „[Multi Utility Communication Controller](#)“ oder „MUC“ genannt) erarbeitet.

Am 26.04.2011 führte das BSI einen Workshop durch, bei dem die Gerätehersteller den Autoren des Schutzprofils Fragen stellen konnten. Offen blieb dabei, wie im Falle des Bekanntwerdens einer sicherheitsrelevanten Schwachstelle in zertifizierten Geräten vorzugehen ist. Denn bei einem MUC verbietet sich das schnelle Ausbringen einer neuen Version, da die bevorstehende Novelle des EnWG voraussichtlich den Betrieb von nicht-zertifizierten Systemen untersagen wird. Der Einsatz einer fehlerbereinigten, aber noch nicht nachzertifizierten Geräteversion würde also gegen geltendes Recht verstoßen. Denkbar wäre eine definierte Notfallstrategie mit einer Ad-hoc-Freigabe durch das BSI.

Während die für Mitte 2011 angekündigte endgültige Version des Schutzprofils inhaltlich wohl nur marginal von der aktuellen Vorversion abweichen dürfte, bleibt diese Nuss bis zur Markteinführung der Geräte noch zu knacken. Da die Hersteller vorher allerdings noch die Zertifizierung durchlaufen müssen, ist damit allerdings kaum vor Mitte 2012 zu rechnen.

Secorvo News

Lizenz zum Entwickeln

Software ohne Schwachstellen schützt Kunden und Anbieter: Vom 24.-27.05.2011 bieten wir mit dem Seminar „[Certified Professional for Secure Software Engineering \(CPSSE\)](#)“ eine praxisorientierte Einführung in die sichere Softwareentwicklung. Mit der sich anschließenden Prüfung können Sie das international anerkannte Qualifikations-Zertifikat zum CPSSE erwerben.

Security News Symposium 2011

Am 31.05.-01.06.2011 ist es wieder soweit – wir laden Sie herzlich ein zum zweiten „[Security News Symposium](#)“ in das Tagungszentrum [Buhlsche Mühle](#) in Karlsruhe/Ettlingen. Auch in diesem Jahr werden wir aktuelle Security- und Datenschutzfragen aufgreifen, die uns bereits in den SSN beschäftigt haben, und gemeinsam mit Ihnen in Vortrag und Diskussion vertiefen. Zusammen mit weiteren Fachexperten bieten wir Ihnen ein [spannendes Programm](#) rund um VoIP, IPv6, Webtracking, Skimming und Online-Banking – und freuen uns auf Ihre [Teilnahme!](#)

DuD 2011

Am 05.-06.06.2011 findet die 13. Fachkonferenz „Datenschutz und Datensicherheit“ ([DuD 2011](#)) in Berlin unter der fachlichen Leitung der Herausgeber der [Fachzeitschrift DuD](#) statt. Das Programm umfasst eine breite Themenpalette: von der Datenschutzaufsicht über aktuelle Entwicklungen im EU-Datenschutzrecht hin zu aktuellen Datenschutzfragen des Cloud Computing, Smart Metering, Sozialer Netzwerke, forensischer Analysen und der Videoüberwachung – einschließlich einer Führung durch die [Datenschutz-Ausstellung von Toll Collect](#).

College-Seminare

Eine sehr praxis- und anwendungsorientierte Einführung in die Computer-Forensik bieten wir vom 28.-30.06.2011 mit dem Seminar „[Forensik – Verfahren, Tools, Praxiserfahrung](#)“.

Die nächste Gelegenheit zur [T.I.S.P.-Zertifizierung](#) (TeleTrust Information Security Professional) bietet Secorvo College vom 06.-11.06.2011.

Veranstaltungshinweise

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

Mai 2011	
10.-12.05.	12. Deutscher IT-Sicherheitskongress (BSI, Bonn)
12.-15.05.	Swiss Cyber Storm 3 Security Conference (Compass Security AG, Rapperswil/CH)
17.-20.05.	12. Datenschutzkongress (Euroforum, Berlin)
24.-27.05.	Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
31.05.- 01.06.	2. Security News Symposium (Secorvo, Karlsruhe/Ettingen)
Juni 2011	
06.-07.06.	DuD 2011 (Computas, Berlin)
06.-11.06.	T.I.S.P.-Schulung und -Prüfung (Secorvo College)
06.-11.06.	OWASP Global AppSec Europe (OWASP Foundation, Dublin/IE)
28.-30.06.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
Juli 2011	
14.07.	3. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum und KA-IT-Si, Karlsruhe)

Fundsache

Satire findet sich bisweilen an Stellen, wo man sie am wenigsten erwartet. So z. B. in Bugzilla, dem Bug-Tracking-System von Firefox & Co. Ähnlichkeiten des dort am 06.04.2011 eingereichten [Antrags auf Aufnahme einer weiteren Root-CA](#) mit den Geschäftsmodellen [real existierender Trustcenter](#) sind bestimmt [rein zufällig](#).

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

Mai 2011



So schlau als wie zuvor

Wenn mein Gedächtnis nicht trügt, begann alles in den frühen 90er Jahren mit dem ISO-9000-Hype – einem Qualitätssiegel, das häufig eher das Vorhandensein einer bürokratisch-peniblen Dokumentation belegt als die materielle Qualität des Produkts. Heute sind Zertifikate so allgegenwärtig, dass uns bei einem Produkt ohne Zertifikat schnell das Gefühl beschleicht, dass damit etwas nicht stimmt.

Meist ist es einer von zwei Gründen, der dem Brancheneinzug eines Zertifikats den Weg ebnet: der Wunsch (oft eines neuen „Marktbegleiters“), sich von seinen Mitbewerbern abzusetzen – oder die Hoffnung, nach einem Skandal verlorenes Vertrauen zurückzugewinnen. Wenige Jahre später ist in der Regel die gesamte Branche zertifiziert – und das Gütesiegel zur „conditio sine qua non“ geworden.

Was für die zertifizierende Stelle (und ihren Umsatz) gut ist, ist jedoch nicht notwendig gut für einen Käufer. Denn die Aussagekraft eines Zertifikats hängt von zahlreichen – häufig nicht einmal öffentlich zugänglichen – Kriterien ab: in erster Linie von dem gewählten Prüfschema (was wird geprüft?), dann von der Prüftiefe (wie intensiv wird geprüft?), vom Prüfumfang (welche Aspekte werden geprüft?), dem Prüfzeitpunkt (wurde das fertige Produkt oder bereits in der Konzeptions- und Entwicklungsphase geprüft?), und nicht zuletzt auch von Qualifikation und Sorgfalt der Prüfer. Zwar mag man von der Prüfung eines unabhängigen Dritten grundsätzlich erwarten, dass sich mindestens in der Vorbereitung darauf Qualitätsverbesserungen einstellen – eine Garantie gibt es jedoch nicht dafür.

So bleibt auch nach einem Blick in den [Zertifizierungsbericht](#) des TÜV TrustIT Austria zum IE9 eher Ratlosigkeit zurück. Schützt das Zertifikat beim Surfen vor Malware – oder vor Programmierfehlern im IE9? Wem das alles zu unspezifisch ist, sollte den Browser lieber anhand objektiver Kriterien wählen – zum Beispiel nach ihrem [Stromverbrauch](#): das ist zeitgemäß, politisch korrekt und jederzeit überprüfbar. Zum Beispiel mit einem neuen Smart Meter.



Inhalt

So schlau als wie zuvor

Security News

BGH zum Accountmissbrauch

3544, 3653, 5072

EnWG-Novelle

Man-in-the-Middle XXS

Zensus 2011 – aber sicher!

Secorvo News

Einblick in die Forensik

Was nix koscht, isch au nix

3. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

Security News

BGH zum Accountmissbrauch

Am 11.05.2011 hat sich der BGH in einem [Grundsatzurteil](#) zur Haftung von ebay-Nutzern geäußert. Der Ehemann der Beklagten hatte ein Niedrigpreisangebot unter dem Account seiner Frau auf der Auktionsplattform ebay eingestellt, das diese vor Auktionsablauf zurückzog. Der zuletzt Höchstbietende hatte sie daraufhin auf Schadensersatz wegen entgangenen Gewinns verklagt.

Der BGH hat auf diese Konstellation das herkömmliche Stellvertreterrecht angewendet und eine Anscheinsvollmacht verneint: Danach kommt es ohne nachträgliche Billigung durch die Accountinhaberin nicht zum Vertragsschluss. Aus den bislang nur als Pressemitteilung verfügbaren Ausführungen zur Bindungswirkung der ebay-AGBs, die die Haftung des Account-Anbieters für Handlungen Dritter festschreiben, geht hervor, dass der BGH eine Geltung für Rechtsverhältnisse zwischen den Plattformnutzern verneint. Das hat Konsequenzen für Plattformbetreiber. Wenn sie sich weiterhin – wie ebay – aus den auf ihrer Plattform geschlossenen Geschäften heraushalten wollen, wird es für sie schwierig, Vertragsbedingungen zwischen ihren Nutzern wie den Umgang mit dem Account-Passwort durchzusetzen. Damit steht für Käufer und Verkäufer gegebenenfalls die Rechtsverbindlichkeit der Kaufverträge in Frage.

3544, 3653, 5072

Falls am 08.06.2011 Internetanbieter wie Google, Facebook & Co. nicht wie gewohnt erreichbar sein sollten, dann ist das vermutlich keinem [DoS](#)-Angriff geschuldet, sondern dem von der [ISOC](#) ausgerufenen

Secorvo Security News 05/2011, 10. Jahrgang, Stand 31.05.2011

nen [World IPv6 Day](#). An diesem Tag wird getestet, zu welchen Effekten es führt, wenn das Internet im Parallelbetrieb von IPv4 und IPv6 läuft. Auch Anwender, die nur das herkömmliche IPv4 einsetzen, könnten durch die IPv6-Adressauflösung in die Irre geführt werden, wenn Netzwerkfunktionen ungenügend oder fehlerhaft implementiert sind. Testen kann man das vorab über Webseiten wie z. B. [test-ipv6.com](#) – leider meist mit viel [JavaScript](#).

Der Test ist ein guter Anlass, zu überprüfen, wieviel unbeabsichtigte IPv6-Konnektivität im eigenen Netz besteht: In den [meisten neueren Betriebssystemen](#) ist IPv6 standardmäßig aktiviert. Zudem kann IPv6-Datenverkehr in IPv4-Paketen getunnelt u. U. Firewalls (auch eingehend!) aushebeln, die ausgehende Verbindungen nicht rigide kontrollieren. Man achte auf die drei im Titel genannten Zahlen: Das sind die UDP/TCP-Ports, die die Tunneling-Verfahren [Teredo](#), [TSP](#) bzw. [AYIYA](#) nutzen.

EnWG-Novelle

Am 11.05.2011 hat die Bundesregierung einen Entwurf zur Novellierung des Energiewirtschaftsgesetzes (EnWGÄndG) vorgelegt. Er enthält u. a. umfassende Ergänzungen zu Smart Metern sowie diesbezügliche Datenschutzregelungen.

In § 21 Abs. 1 werden ausschließliche Zwecke für die Nutzung der durch Smart Meter gewonnenen Daten und in Abs. 2 die zum Datenumgang berechtigten Stellen festgelegt. Dabei wird der Terminus „Datenumgang“ eingeführt, der zukünftig die „Erhebung, Verarbeitung und Nutzung“ personenbezogener Daten bereichern soll. Ein überflüssiger Abs. 3 ermöglicht explizit die Auftragsdatenverarbeitung.

In § 21e werden umfassender als bisher die Anforderungen an Smart Meter aufgegriffen. Im We-

sentlichen beschränkt sich der Entwurf jedoch auf einen Verweis auf eine zu erlassende Rechtsverordnung nach § 21i, die Forderung nach Verschlüsselung bei Versendung über offene Netze und den Hinweis auf den Stand der Technik.

Nach Abs. 5 dürfen Messsysteme, die vor Inkrafttreten der Neuerungen verbaut wurden, bis zum Ablauf der Eichgültigkeit (mindestens bis 31.12.2013) verwendet werden: Damit liegt die Höchstgrenze für „Alt“-Geräte bei acht Jahren. Die Pflicht zum Einbau von Smart Metern nach § 21c Abs. 1, beschränkt auf Neubauten und größere Renovierungen, kann bei Feststellung der wirtschaftlichen Vertretbarkeit durch das Bundeswirtschaftsministerium allgemein vorgeschrieben werden.

Substantielle Änderungen wie die [von den Datenschutzbeauftragten der Länder geforderte](#) Gestaltungsvorgabe, die Daten so weit wie möglich lokal und unter Kontrolle des Endnutzers zu verarbeiten, wurden jedoch nicht umgesetzt. Mit § 14a werden zudem von außen unterbrech- und steuerbare Verbrauchseinrichtungen eingeführt. Insgesamt gehen die Neuregelungen nicht weit über das bereits im BDSG Geregelte hinaus und verlieren sich teilweise in Details. Hinsichtlich der Sicherheitsanforderungen an Smart Meter werden nun mit Spannung die Endfassung des [Protection Profiles](#) des BSI sowie die zugehörige Rechtsverordnung erwartet.

Man-in-the-Middle XXS

Schon am 08.12.2010 [präsentierte Vasco](#) einen [Chip in einer Folie](#), der über die „echten“ Kontaktflächen einer [SIM-Karte](#) geklebt wird, um unabhängig vom jeweiligen Netzbetreiber Sicherheitsfunktionen für das Online-Banking per Handy zu ergänzen.

Genau wie viele andere Sicherheitslösungen ist das Konzept eine [Dual Use](#)-Technologie: Man stelle sich vor, dass eine derartige Folie über den Kontakten eines Geldautomaten klebt, um diesen mit „Zusatzfunktionen“ anzureichern. Das wäre noch eleganter als das in der [vorigen Ausgabe](#) der SSN vorgestellte [Chipkarten-Skimming-Gerät](#), das in den Schlitz des Kartenlesers passt. Es wird daher immer wichtiger, dass Chipkarten-Anwendungen auch gegen einen Man-between-Card-and-Reader-Angriff gefeit sind.

Zensus 2011 – aber sicher!

Derzeit wird zum Stichtag 09.05.2011 in Deutschland wieder gezählt. Im Rahmen des [Zensus 2011](#) werden in Form einer repräsentativen Stichprobe Informationen über die Bevölkerung in Deutschland erhoben. Dem Schutz der erhobenen Daten widmet das Statistische Bundesamt auf der Zensus-Webseite einen [ganzen Abschnitt](#). Darin bleiben allerdings Fragen offen: Wie steht es insbesondere um die Transportsicherheit bei der Befragung?

In der öffentlichen Berichterstattung entsteht der Eindruck, die Beantwortung der Fragen müsse in Form eines Interviews durchgeführt werden – in diesem Fall hinge die Sicherheit der persönlichen Daten stark vom [Erhebungsbeauftragten](#) ab. Dubiose Aufrufe zur Meldung als Erhebungsbeauftragte, wie der der [sächsischen NPD](#), geben Anlass, die Vertrauenswürdigkeit der Interviewer zumindest kritisch zu hinterfragen.

Etwas versteckt findet sich auf der offiziellen Webseite zum Zensus ein Hinweis auf [alternative Möglichkeiten zur Meldung](#) der Daten: Online oder durch Postversand an die Meldestelle. Aber auch dabei ist Vorsicht geboten: In drei Bundesländern wurden [externe Dienstleister](#) mit der Beleglesung beauf-

tragt. Bei Versand empfiehlt sich daher eine Prüfung der Rücksendeadresse auf dem Fragebogen.

Auch die Online-Meldung ist nicht ohne Risiken. Im Blog von Jan Schejbal finden sich [Angriffsbeschreibungen](#), und auch das [Statistische Bundesamt](#) und das [Bundesamt für Sicherheit in der Informationstechnik](#) halten Sicherheitshinweise zur Online-Meldung für erforderlich.

Die deutliche Fokussierung auf die Interview-Erhebung könnte sich mit den [Aufwandsentschädigungen](#) für Erhebungsbeauftragte erklären: Jeder analog ausgefüllte Fragebogen wird zusätzlich mit 7,50 Euro entlohnt.

Bei der Meldung der Daten ist also Sorgfalt angeraten. Dann sollten auch Erfahrungen ausbleiben, die [Volkszähler der TAZ](#) Berlinern und [clevere Betrüger auf der Suche nach Kontodaten](#) Münchner Bürgern bescherten.

Secorvo News

Einblick in die Forensik

Kurz vor der Sommerpause bietet Ihnen Secorvo College mit dem Seminar [Forensik – Verfahren, Tools, Praxiserfahrung](#) vom 28.-30.06.2011 einen praxisorientierten Einblick in die Computer-Forensik. Hier erleben Sie in realitätsnahen Übungen, worauf es bei IT-forensischer Arbeit ankommt.

Im September startet Secorvo College mit dem Seminar **Sicherheitsmanagement heute** vom 27.-29.09.2011 in den Herbst. Es folgen die Seminare **Verlässliche Web-Anwendungs-Sicherheit** (05.-06.10.2011), **IT-Sicherheitsaudit in der Praxis** (10.-12.10.2011) und **Datenschutzaudit: Best Practice** (13.-14.10.2011). Zudem bieten wir

Ihnen vom 17.-22.10.2011 die nächste Gelegenheit zur [T.I.S.P.-Zertifizierung](#). Alle Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter <http://www.secorvo.de/college>

Was nix koscht, isch au nix

„Sicherheit für umsonst“ lautet der Titel des kommenden Events der [Karlsruher IT-Sicherheitsinitiative \(KA-IT-Si\)](#) am 09.06.2011, bei dem Astaro-Technikvorstand Markus Hennig seine Erfahrungen und Einschätzungen zur Frage "Sicherheit durch OpenSource?!" vorstellen wird. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Im Anschluss an den Vortrag gibt es wie gewohnt die Gelegenheit zum „Buffet-Networking“. Wir freuen uns auf Ihre [Anmeldung](#).

3. Tag der IT-Sicherheit

Am 14.07.2011 findet zum dritten Mal der von der Karlsruher IT-Sicherheitsinitiative ([KA-IT-Si](#)) gemeinsam mit der IHK Karlsruhe und dem [CyberForum e.V.](#) veranstaltete „[Tag der IT-Sicherheit](#)“ statt.

Der Präsident des [Bundesamtes fuer Sicherheit in der Informationstechnik \(BSI\)](#), Michael Hange, wird in einer Keynote einen Ausblick auf die Bedrohungslage und die Arbeit des BSI in Deutschland geben. Außerdem erwarten Sie Praxisbeiträge zum elektronischen Personalausweis, De-Mail, Web-Angriffen und der Sicherheit im Online-Banking. Die Veranstaltung beginnt um 14 Uhr im Saal Baden der [IHK](#).

Direkt im Anschluss lädt die KA-IT-Si zum Jubiläumsempfang anlässlich ihres 10jährigen Bestehens. Das vollständige Programm und die Online-Anmeldung finden Sie unter www.karlsruhe.ihk.de.

Veranstaltungshinweise

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

Juni 2011	
06.-07.06.	DuD 2011 (Computas, Berlin)
06.-11.06.	OWASP Global AppSec Europe (OWASP, Dublin/IE)
09.06.	Sicherheit für umsonst (KA-IT-Si, Karlsruhe)
28.-30.06.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
Juli 2011	
14.07.	3. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum und KA-IT-Si, Karlsruhe)
30.07.- 02.08.	Blackhat USA 2011 (Blackhat, Las Vegas/US)
August 2011	
04.-07.08.	DEFCON 19 (DEFCON, Las Vegas/US)
14.-18.08.	Crypto 2011 (IACR, Santa Barbara/US)
September 2011	
20.-21.09.	8. Security Awareness Symposium (Secorvo, Karlsruhe-Ettingen)

Fundsache

Am 27.04.2011 veröffentlichte das BSI ein [Eckpunktepapier zu Sicherheitsempfehlungen für Cloud-Computing-Anbieter](#). Das 76seitige Dokument ist übersichtlich strukturiert und enthält – von einzelnen Skurrilitäten wie der Liste von Vorfällen im Kapitel Notfallmanagement abgesehen – viele wertvolle Hinweise. Eine Antwort auf die wichtige Frage, wie eine datenschutzkonforme Auftragsdatenverarbeitung in der Cloud funktionieren kann, bleibt es allerdings schuldig.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

Juni 2011



Editorial: Sieg der Vernunft

Das Schlimmste ist, dass wir die einfachsten Fragen mit Tricks zu lösen versuchen, darum machen wir sie auch so kompliziert. *Anton Tschechow (1860-1904)*

Manchmal kommt die Vernunft auf ganz leisen Sohlen. Diesmal versteckt sie sich im [Steuervereinfachungsgesetz 2011](#), das am 09.06.2011 vom Bundestag verabschiedet wurde. Darin wird [§ 14](#) Abs. 1 des Umsatzsteuergesetzes geändert – und damit [GDPdU](#) und deutsches Signaturgesetz ([SigG](#)) zugleich „geschleift“.

Aber der Reihe nach. Seit dem Inkrafttreten des „Gesetzes über Rahmenbedingungen für elektronische Signaturen“ im Jahr 2001 mangelte es nicht an Versuchen, der qualifizierten Signatur zum Durchbruch zu verhelfen. So führte der Gesetzgeber nicht nur die „elektronische Form“ im Bürgerlichen Gesetzbuch (BGB) ein, sondern schob auf der Suche nach einer „Killer-Applikation“ zahlreiche Initiativen an, darunter – um die prominentesten zu nennen – die elektronische Steuererklärung mit Signatur ([ELSTER](#)), das [ELENA-Verfahren](#), den [neuen Personalausweis](#) (nPA) mit Signierfunktion und zuletzt das am 03.05.2011 in Kraft getretene [De-Mail-Gesetz](#).

Jedoch signierte nur eine verschwindend geringe Zahl an Bürgern die elektronische Steuererklärung, ELENA wurde gestoppt und für die Signierfunktion des nPA gibt es auch acht Monate nach Einführung kein Trustcenter, das [die Nachladefunktion für Signaturzertifikate unterstützt](#). Daher waren die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU) vom 16.07.2001 die letzte Bastion: Milliarden elektronischer Rechnungen von TK-Unternehmen, Fluggesellschaften und Online-Shops mussten qualifiziert signiert und vom Empfänger geprüft und protokolliert werden.

Ab dem 01.07.2011 ist das Geschichte. Zwar darf weiterhin signiert werden. Eine Übermittlung per E-Mail ohne Signatur genügt jedoch für den Vorsteuerabzug. Trauern dürften darüber nur externe „GDPdU-Prozessdesigner“ – Unternehmer und Steuerberater hingegen werden die [FAQ des Finanzministeriums](#) mit ungläubigem Staunen lesen: So viel Bürokratieabbau war selten.



Inhalt

Editorial: Sieg der Vernunft

Security News

Key Escrow 2.0

Web 2.0

Alchemie 2.0

EnWG 2.0

Forensik 2.0

C++ 2.0

Secorvo News

TISP und mehr

3. Tag der IT-Sicherheit

Leseprobe

Veranstaltungshinweise

Fundsache

Security News

Key Escrow 2.0

Nachdem im März 2011 unbekanntem Hackern ein Einbruch bei RSA gelang (siehe [SSN 03/2011](#)), hat der [SecurID](#)-Hersteller am 06.06.2011 seinen Kunden [angeboten](#), alle One-Time-Password-Token auszutauschen. Dieser Schritt wird allgemein als ein Eingeständnis interpretiert, dass bei dem Einbruch tatsächlich die Seed-Werte vieler oder aller Token entwendet wurden – die Masterkeys, die es erlauben, alle von den Token angezeigten Einmalpasswörter nachzuberechnen.

Auch die Seed-Werte der neuen Token wird RSA archivieren, wenn auch vermutlich besser abgesichert. Da stellt sich die Frage, warum Anwender diese Art von Schlüssel hinterlegung („Seed Escrow“) so ohne weiteres akzeptieren sollten. Schließlich käme auch niemand auf die Idee, beim Ausstellen eines SSL-Zertifikats den privaten Schlüssel des betreffenden Webservers dem Trustcenter zum Archivieren zu überlassen, nur für den Fall, dass er dem Besitzer verloren ginge – oder eine Kopie des Fahrzeugschlüssels dem Autohändler oder des Haustürschlüssels dem Makler. Die Hinterlegung großer Mengen sensibler Schlüssel war noch nie ein gutes Konzept, sondern ein meist unnötiger „Single Point of Failure“.

Web 2.0

Das KG Berlin hat am 29.4.2011 über die Beschwerde wegen der Ablehnung einer einstweiligen Verfügung gegen einen Wettbewerber [entschieden](#), der den „[Gefällt-mir-Button](#)“ von Facebook nutzt. Einen abmahnungsfähigen Verstoß gegen eine Marktverhaltensvorschrift nach [§ 4 Nr. 11 UWG](#)

wegen fehlender Information über die Datenübermittlung ([§ 13 Abs. 1 TMG](#)) lehnte das Gericht ab.

Für Telemedienanbieter, die Social Plugins nutzen, stellt das Urteil dennoch keine Entwarnung dar: Es klammert die datenschutzrechtliche Bewertung der Fragen, wer verantwortliche Stelle beim Einsatz von Social Plugins ist, ob der Verwender ohne diesbezügliche Datenschutzerklärung seine Informationspflicht verletzt oder ob eine unerlaubte Datenübermittlung ohne Einwilligung vorliegt, gänzlich aus. Eine diesbezügliche Stellungnahme des „[Düsseldorfer Kreises](#)“ dürfte nicht lange auf sich warten lassen – vom Vorliegen einer bußgeldbewehrten Ordnungswidrigkeit ist weiterhin auszugehen.

Alchemie 2.0

In den letzten Wochen überschlugen sich die Meldungen über [Bitcoin](#), eine elektronische Währung, die ohne eine zentrale Ausgabestelle auskommt – jeder Teilnehmer kann als „Miner“ neue „Münzen“ erschaffen, wenn er Rechenzeit investiert, um bestimmte Krypto-Aufgaben zu lösen. Bitcoins können wie Bargeld anonym übertragen werden, da alle Teilnehmer nur unter Pseudonym bekannt sind. Dabei kontrollieren und beglaubigen in einem Peer-to-Peer-Verfahren andere Teilnehmer die Weitergabe und verhindern, dass digitale Münzen mehrfach ausgegeben werden.

Das Verfahren ist umstritten – die Bewertungen reichen von einem faszinierenden Stück [Kryptographie](#) oder einer [finanztechnischen Revolution](#) über [Geldwäschemechanismus](#) bis zur Unterstellung eines [Ponzi-Schneeball-Systems](#). Jedenfalls werden Bitcoins bereits in [Dollar oder Euro gewechselt](#), es wurden schon Razzien ([23.05.2011](#)) und echte oder vorgebliche Diebstähle ([13.06.2011](#)) gemeldet und erste Trojaner stehen entweder [Rechenzeit zum](#)

„[Mining](#)“ oder gleich die ganze [Bitcoin-Brieftasche](#). Seit dem 20.05.2011 gibt es überdies eine [JavaScript-Version](#), mit der Webseitenbetreiber ihre Besucher als Bitcoin-Miner für sich arbeiten lassen können.

Zwar sind Zweifel am Erfolg dieser Goldsuche des 21. Jahrhunderts angebracht – allerdings könnte Bitcoin das eine oder andere rätselhafte Verschwinden von Rechenleistung plausibel erklären.

EnWG 2.0

Am 06.06.2011 legte die Bundesregierung einen [Entwurf zur Novellierung des Energiewirtschaftsgesetzes](#) (EnWG) vor. Eine wesentliche Neuerung ist die Präzisierung des „Smart Meter“-Begriffs als „eine in ein Kommunikationsnetz eingebundene Messeinrichtung“. Während es bislang laut EnWG ausschließlich um die Verbrauchsanzeige ging, werden die Kommunikationsschnittstelle und deren Nutzung nun Standard. Über die tatsächlich übertragenen Daten sagt das noch nichts aus – jedoch ist zu befürchten, dass dies zu Stromprodukten führen wird, die mit der Übertragung personenbezogener Verbrauchswerte im 15-Minuten-Takt einhergehen.

In ihren Stellungnahmen plädieren sowohl der [BfDI](#) (zum Schutzprofil) als auch das [ULD](#) (zur EnWG-Novelle) für eine Lösung, die Datensparsamkeit bereits im Entwurf berücksichtigt. Die Tarifierung sollte im Haushalt vorgenommen und auch bei lastabhängigen Tarifen sollten nur aggregierte Daten übermittelt werden.

Immerhin ist in § 40 (5) verankert, dass „Lieferanten [...] stets mindestens einen Tarif anzubieten [haben], für den die Datenaufzeichnung und -übermittlung auf die Mitteilung der [...] verbrauchten

Gesamtstrommenge begrenzt bleibt“. Wenigstens könnte sich Datensparsamkeit als Unterscheidungsmerkmal etablieren – dann würde möglicherweise schon ein Anbieter mit einem attraktiven Stromprodukt („Datenschutztarif“) genügen, um datensparsame Tarifmodelle durchzusetzen.

Forensik 2.0

Die seit Anfang Juni 2011 im Betatest befindliche [Public Preview 2 von EnCase Forensic Version 7](#) weist lange erwartete Verbesserungen auf. Neben einer klareren Strukturierung der Oberfläche sticht besonders der neue „Evidence Processor“ hervor, der nun vor dem Beginn der inhaltlichen Analyse eine Reihe von derzeit neun Standardaufgaben (darunter eine Dateisignatur-Analyse und die Indexierung) konfigurierbar abarbeitet – für eine beliebige Anzahl forensischer Images. Erste Tests haben gezeigt, dass die Arbeitsabläufe deutlich komfortabler und schneller werden, solange man über ausreichend dimensionierte Hardware für den Evidence Processor verfügt.

In einer zehnten Standardaufgabe (Kategorie „Modules“) kann z. B. der File Carver für bestimmte Datentypen eingestellt werden. Noch ist offen, ob dieser Bereich durch Endkunden selbst erweitert werden kann, wie dies z. B. bei [EnScript](#) der Fall ist. Falls Erweiterungen bspw. für CAD-Daten benötigt werden, wird man sonst wohl auf EnCase 8 warten oder auf ein forensisches „Schweizer Offiziersmesser“ wie [X-Ways Forensics](#) ausweichen müssen.

Einen Schritt weiter geht Simson L. Garfinkel mit seinem [bulk_extractor V 1.0.0](#) vom 15.06.2011, der als Stream-basierter Ansatz mit [Named Entity Recognition](#) fast in Echtzeit große Datenmengen unterschiedlicher Formate (wie Bilder, Diskimages oder Dateien) nach Zielbegriffen wie z. B. Kredit-

kartendaten durchsucht. Solche Carving-Ansätze dürften zukünftig maßgeblich die Erfolgchancen einer IT-Forensik-Software bestimmen.

C++ 2.0

Im Juni 2011 hat [Michael Howard](#) (Microsoft) eine [Übersicht über gefährliche C und C++ Funktionen](#) im Microsoft Developer Network ([MSDN](#)) veröffentlicht. Dieser Auszug aus Kapitel 11 seines mit Steve Lipner verfassten und bereits am 31.05.2006 erschienenen Buch [The Security Development Lifecycle](#) ist als konkrete Handreichung für Software-Entwickler gedacht. In dem kurzen Artikel findet sich eine Übersicht über potenziell gefährliche Funktionen – und Empfehlungen für sichere Alternativen. Diese Übersicht sollte über jedem Entwicklerschreibtisch hängen.

Secorvo News

TISP und mehr

Mit Blick auf die steigenden Anmeldezahlen möchten wir Sie schon jetzt auf die nächste [T.I.S.P.-Schulung](#) vom 17.-22.10.2011 (einschließlich Prüfung) hinweisen. Nutzen Sie die Gelegenheit, Ihre Kenntnisse zu erweitern, und lassen Sie sich Ihr Wissen zertifizieren.

Nach den Sommerferien startet Secorvo College zunächst mit dem Seminar [„Sicherheitsmanagement heute“](#) vom 27.-29.09.2011. Es folgen die Seminare [„Verlässliche Web-Anwendungs-Sicherheit“](#) (05.-06.10.2011), [„IT-Sicherheitsaudit in der Praxis“](#) (10.-12.10.2011) und [„Datenschutzaudit: Best Practice“](#) (13.-14.10.2011). Alle Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter <http://www.secorvo.de/college>.

3. Tag der IT-Sicherheit

Gemeinsam mit dem [CyberForum e.V.](#) und der IHK Karlsruhe veranstaltet die Karlsruher IT-Sicherheitsinitiative ([KA-IT-Si](#)) am 14.07.2011 den „3. Tag der IT-Sicherheit“ im Saal Baden der [IHK Karlsruhe](#) (Beginn: 14 Uhr, Teilnahmebeitrag 75 Euro).

Der Präsident des [Bundesamtes für Sicherheit in der Informationstechnik \(BSI\)](#), Michael Hange, wird in seiner Keynote einen Ausblick auf die Bedrohungslage und die Arbeit des BSI in Deutschland geben. Außerdem erwarten Sie praxisnahe Beiträge zum elektronischen Personalausweis, De-Mail, Web-Angriffen und der Sicherheit im Online-Banking.

Im Anschluss lädt die KA-IT-Si anlässlich ihres 10-jährigen Bestehens zum Jubiläumsempfang. Bitte melden Sie sich rechtzeitig an, damit wir ausreichende Mengen Sekt kalt stellen... Nähere Informationen zum Programm und zur Online-Anmeldung finden Sie unter www.ka-it-si.de.

Leseprobe

Die Fachzeitschrift „Datenschutz und Datensicherheit“ (DuD) erscheint bereits im 35. Jahr und seit knapp 15 Jahren unter der Mitwirkung von Dirk Fox als Herausgeber. Dank des wachsenden Interesses am Thema und der Erweiterung des Herausgeber-teams um die Juristen [Prof. Dr. Benedikt Buchner](#) und [Dr. Britta Alexandra Mester](#) im Jahr 2009 wuchs der Umfang des Jahrgangs 2010 auf über 860 Seiten.

Von der Ausgabe 6/2011 ist nun eine [digitale Leseprobe](#) verfügbar. Auch ein [kostenloses Probeabonnement](#) wird angeboten – wer schnell ordert, erhält noch die Ausgabe 8/2011 mit dem Schwerpunkt „Smart Grids“.

Veranstaltungshinweise

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

Juli 2011	
14.07.	3. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum und KA-IT-Si, Karlsruhe)
30.07.- 02.08.	Blackhat USA 2011 (Blackhat, Las Vegas/US)
August 2011	
01.-03.08.	DFRWS 2011 (DFRWS, New Orleans/US)
04.-07.08.	DEFCON 19 (DEFCON, Las Vegas/US)
10.-12.08.	20th USENIX Security Symposium (Usenix, San Francisco/US)
14.-18.08.	Crypto 2011 (IACR, Santa Barbara/US)
September 2011	
19.-23.09.	OWASP Global AppSec North America (OWASP Foundation, Minneapolis/US)
27.-29.09.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Oktober 2011	
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)

Fundsache

Am 14.06.2011 hat das [PCI Security Standards Council](#) als Ergänzung zum [PCI Data Security Standard](#) das Dokument [PCI DSS Virtualization Guidelines](#) in der Version 2.0 veröffentlicht. In der 39seitigen Übersicht werden auf einem recht hohen Abstraktionsniveau Sicherheitsaspekte von Virtualisierung und Cloud Computing vorgestellt – für Nicht-Techniker ein lesenswerter Leitfaden.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

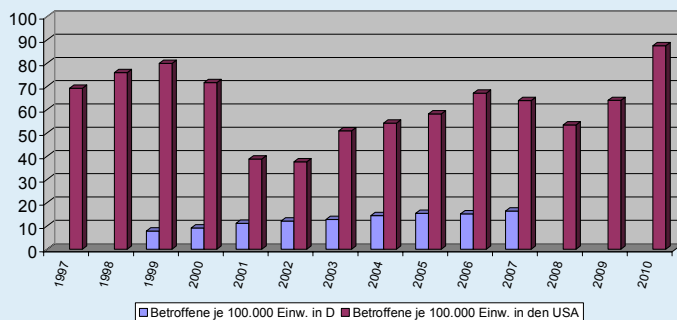
Juli 2011



TK-Überwachung im Vergleich

Die heimliche Überwachung von Telekommunikationseinrichtungen ist ein Eingriff in das Fernmeldegeheimnis ([Art. 10 GG](#)) – und den Strafverfolgungsbehörden nur bei begründetem Tatverdacht, schweren Straftaten und als „ultima ratio“ ([§ 100a StPO](#)) erlaubt. Sie erfordert zudem eine richterliche Anordnung ([§ 100b StPO](#)). Anders als in den USA, die die Richter verpflichten, das Ergebnis der Überwachung

in einem „Wiretap Report“ (Umfang, Anklagen und Verurteilungen) zu dokumentieren, unterliegt die TK-Überwachung in Deutschland keiner Erfolgskontrolle. Den tatsächlichen Umfang der Überwachung geben aber auch die amerikanischen [Wiretap Reports](#) nicht auf den ersten Blick preis. Im direkten Vergleich zeigt sich, dass die Zahl der von einer Überwachung Betroffenen je Einwohner und Jahr in den USA erheblich schwankt, während sie in Deutschland - auf niedrigerem Niveau - kontinuierlich wächst. Leider ist der deutschen [Statistik](#) die Zahl der Betroffenen nur bis 2007 zu entnehmen.



Bedenklicher stimmen die Ergebnisse empirischer Analysen, wie die von [Dr. Jens Eckhardt](#) (2009). Sein Fazit: „Die Erfolge stehen in keinem angemessenen Verhältnis zu den damit verbundene Eingriffen.“ Und: „Eine substantiierte Begründung der Überwachung war nur in einem geringen Maß festzustellen.“



Inhalt

TK-Überwachung im Vergleich

Security News

Böse Schnittstelle

IMSI-Catcher für jedermann

Mit der Schrotflinte...

Hase ./ Igel

Same procedure ...

ShellBag Forensik

Secorvo News

TISP und mehr

Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

Security News

Böse Schnittstelle

USB-Sticks haben nicht erst seit Stuxnet ([SSN 10/2010](#)) anderen Speichermedien den Rang als verbreitetste „Gefährder“ abgelaufen. Nach [Dumper, HackSaw und SwitchBlade](#) hat nun die Firma [Netragard](#) dies im Rahmen eines Penetrationstests in besonders kreativer Weise unter Beweis gestellt: Sie verschickte eine „trojanisierte“ USB-Maus als Werbegeschenk getarnt an einen Mitarbeiter des Unternehmens.

Darin befanden sich zusätzlich ein USB-Hub, ein USB-Flash-Drive sowie ein Mikrocontroller, der nach dem Anstecken eine Tastatur emulieren und Tastatureingaben an den PC senden konnte – die [Herstellung dieser Spezialmaus](#) wurde detailliert beschrieben. Mit einer Standard-Remote-Shell aus dem [Metasploit-Framework](#) konnte damit der PC übernommen und in das Netzwerk eingedrungen werden.

Ein ähnlich kreativer Ansatz, per USB und einem [Teensy Controller](#) Systeme anzugreifen, wurde am 13.07.2011 von [Didier Stevens](#) vorgestellt: Mit vorprogrammierten Tastatureingaben wird ein Editor geöffnet, binärer Code eingetippt und dieser als PDF gespeichert. Wird das PDF geöffnet, führt das befallene System den Code aus.

In beiden Fällen rettet kein Virenschutz – höchstens eine Kontrollsoftware für angeschlossene USB-Geräte, die die Maus als Datenspeicher entlarvt hätte. Aber es geht auch nicht ohne Benutzersensibilisierung, denn bei allen unbekanntem USB-Geräten ist Vorsicht geboten – auch Lautsprecher, Tassenwärmer oder Spaß-Geräte aus externer Quelle können solche Erweiterungen in sich bergen.

Secorvo Security News 07/2011, 10. Jahrgang, Stand 29.07.2011

IMSI-Catcher für jedermann

In Großbritannien verkauft Vodafone als [Femtozelle](#) ein [Gerät](#), das für UMTS eine ähnliche Funktion wie ein WLAN Access Point bietet: Das Handy des Kunden funkt zur Femtozelle, die über den heimischen Internet-Anschluss an das Vodafone Mobilfunknetz angebunden ist. Am 13.07.2011 [publizierte](#) nun die Gruppe [THC Untersuchungen](#) aus 2009/10, denen zufolge es gelang, dank eines schwachen Root-Passworts mittels Reverse-Engineering die Kontrolle über die Linux-basierten Zellen zu übernehmen. Nach [Ausbau bzw. Deaktivieren](#) einiger Sicherheitseinrichtungen konnten die Forscher dann – wie auch von [anderen Experten](#) erwartet – Gespräche abhören und auf fremde Kosten telefonieren.

Das gelang, weil die Femtozelle große Teile der Funktion eines UMTS Radio Network Controllers (RNC) wahrnimmt, darunter die Verschlüsselung der Funkstrecke, und die erforderlichen Schlüssel über die Internet-Anbindung aus dem Kern-Netz des Providers bezieht. In der ursprünglichen [UMTS-Architektur](#) ist der RNC eine Komponente des Providernetzes – nur autorisiertem Personal zugänglich und kein kleines Gerät im Kunststoffgehäuse, an das der zahlende Kunde Anschlüsse anlöten und „Man-in-the-Middle“ spielen kann.

Auch hier zeigt sich wieder wie wichtig es ist, zuerst die zu Grunde liegenden Sicherheitsannahmen zu hinterfragen, ehe man ein bewährtes Verfahren auf neue Szenarien überträgt.

Mit der Schrotflinte...

Auf Initiative Hessens hat der Bundesrat am 17.06.2011 einen [Entwurf zur Überarbeitung des Telemediengesetzes](#) (TMG-E) vorgelegt. Darin findet sich in § 13 Abs. 8 – entsprechend Art. 2 Abs. 5 der [Richt-](#)

[linie 2009/136/EG](#), die eine entsprechende Regelung in die [Datenschutzrichtlinie für elektronische Kommunikation](#) einfügte und bis Mai 2011 umzusetzen war – die Festlegung, dass die Speicherung und der Abruf von Daten im Endgerät des Nutzers künftig nur mit Unterrichtung und vorheriger Einwilligung zulässig sein werden.

Betroffen hiervon sind sämtliche Cookies und automatischen Abfragen, bspw. durch Apps. Praktisch würde damit der Einsatz von Cookies unhandlich bis unmöglich. Die Ausnahme der „unbedingten Erforderlichkeit zur Dienstnutzung“ ist ungeeignet, diese Wirkung zu entschärfen, denn wie viel Bequemlichkeit ist unbedingt erforderlich?

In § 13a TMG-E werden Anbieter von Foren, Blogs, Social Networks und ähnlichen Diensten verpflichtet ihre – nicht näher definierten – höchsten Sicherheitseinstellungen als Default anzubieten. Einzige materielle Vorgabe ist die Unauffindbarkeit durch Suchmaschinen. Eine Herabsetzung der Einstellungen soll nur Nutzern über 16 Jahren möglich sein.

In beiden Fällen ist die Absicht zu begrüßen, Transparenz, Nutzerkontrolle und Nutzerschutz im Internet zu stärken – die derzeitige Fassung des Gesetzentwurfs erscheint jedoch wenig durchdacht und praxisuntauglich.

Hase ./ Igel

Der Wettlauf zwischen IT-Sicherheit und organisierter IT-Kriminalität geht in die nächste Runde. Da Nutzer der [DHL Packstation](#) als potentielle Zieladresse für online ergaunerte Waren ein beliebtes [Phishing-Ziel](#) darstellen, ist seit März 2011 eine [Kunden-Magnetkarte erforderlich](#), um eine Sendung abzuholen. Am 25.06.2011 wurde nun [gezeigt](#), wie

man sich zu jeder Packstation-Adresse eine passende Magnetstreifenkarte selbst kodieren kann.

Magnetstreifenkarten haben auch am Geldautomaten bald ausgedient. Die Schadensfälle durch [Skimming](#) nehmen dermaßen überhand, dass viele Banken, wie am 05.07.2011 [bekannt wurde](#), die außereuropäische Nutzung der EC-Karte drastisch einschränken. Und beim Online-Banking schließlich [wechseln](#) viele Institute mittlerweile von der [iTAN](#) zu Verfahren mit Handheld-Kartenlesern ([chipTAN](#) oder [SmartTAN](#) genannt). Derweil [warnte](#) das BKA am 15.07.2011 vor Trojanern, die ihre Opfer ganz offen zu einer Überweisung auffordern – unter dem Vorwand, eine versehentliche Gutschrift rückgängig zu machen. Da hilft leichtgläubigen Kontoinhabern auch kein chipTAN-Verfahren mehr.

Es sieht also so aus, als ob uns dieser Wettlauf noch eine Weile erhalten bleibt. Noch ist allerdings unentschieden, welche Seite im Ziel der Igel ist.

Same procedure ...

Bei der Durchsicht der am 27.06.2011 veröffentlichten [CWE/SANS TOP 25 Most Dangerous Software Errors](#) – ermittelt anhand des [CWSS](#)-Bewertungssystems, reduziert auf [Tragweite, Verbreitung und Ausnutzbarkeit](#) der Schwachstellen – fühlt man sich wie [Miss Sophie](#) an Sylvester: Seit Jahren finden sich dieselben Schwachstellen auf den Top-Positionen der Liste, darunter [SQL-Injection](#), [Command Injection](#) und [Cross-Site Scripting](#), obwohl seit längerem wirksame Ansätze zu deren [Bekämpfung](#) bekannt sind.

Die Liste findet ihre praktische Bestätigung in [aktuellen Schwachstellenübersichten](#) und Berichten über erfolgreiche Hacks ([Citibank](#), [MySQL](#), [Barra-](#)

[cuda](#), [REWE](#), [Schufa](#), ...) und deckt sich größtenteils mit den weithin bekannten [OWASP Top 10](#).

Sofern die Entwicklung sicherer Software nicht bald durchgängig ernster genommen wird, müssen wir uns wohl auch im nächsten Jahr auf eine ganz ähnliche Übersicht einstellen. „Cheerio, Sophie, mee girl!“

ShellBag Forensik

Seit dem 29.05.2011 liegt der [Windows ShellBag Parser](#) von TZ Works als stabile und skriptfähige 64-bit-Version vor, die auch mit den [ShellBags von Windows 7](#) problemlos arbeitet – anders als etwa kommerzielle, forensische Suites, bei denen die Auswertung von ShellBags z. T. noch in den Kinderschuhen steckt.

Damit kann aus vorliegenden benutzerspezifischen Profil-Dateien von Windows (NTUSER.DAT, UsrClass.DAT) eine Vielzahl von Informationen über das Laufzeitverhalten eines Windows-Benutzerkontos gewonnen werden. Mit diesen Informationen wird die Erstellung von aussagefähigen Zeitlinien und Nutzungsabfolgen aus Metadaten des NTFS-Dateisystems, gecarvten Dateifragmenten und Benutzerkonteninteraktionen deutlich besser interpretierbar.

Da die Aufrufreihenfolge der jeweils letzten Aktionen in den ShellBags von Windows automatisch festgehalten wird, können so z. B. auch Malwareaktivitäten identifiziert werden, die im Benutzerkontext gestartet wurden – oder auch versehentlich gelöschte Verlaufshistorien zurück gewonnen werden.

Secorvo News

TISP und mehr

Nach der Sommerpause startet Secorvo College zunächst mit dem Seminar [„Sicherheitsmanagement heute“](#) vom 27.-29.09.2011. Es folgen die Seminare [„Verlässliche Web-Anwendungs-Sicherheit“](#) (05.-06.10.2011), [„IT-Sicherheitsaudit in der Praxis“](#) (10.-12.10.2011) und [„Datenschutzaudit: Best Practice“](#) (13.-14.10.2011).

Die nächste Gelegenheit zur TISP-Zertifizierung bietet Secorvo College mit der [T.I.S.P.-Schulung](#) vom 17.-22.10.2011 (einschließlich Prüfung).

Die Programme aller Seminare und die Möglichkeit zur Online-Anmeldung finden Sie unter <http://www.secorvo.de/college>.

Tag der IT-Sicherheit

Wer am 14.07.2011 den mit ca. 100 Besuchern hervorragend besuchten 3. Tag der IT-Sicherheit in der IHK Karlsruhe verpasst hat, findet die Unterlagen der Referenten auf den [Webseiten der IHK](#) unter der Dokumentennummer 83415 und eine [Pressemitteilung der KA-IT-Si](#) zum Download.

Zum Vormerken: Das [nächste KA-IT-Si-Event](#) findet am 22.09.2011 im Panoramasaal der IHK-Karlsruhe statt ([Anmeldung](#)).

Veranstaltungshinweise

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

August 2011	
04.-07.08.	DEFCON 19 (DEFCON, Las Vegas/US)
10.-12.08.	20th USENIX Security Symposium (Usenix, San Francisco/US)
14.-18.08.	Crypto 2011 (IACR, Santa Barbara/US)
September 2011	
13.-14.09.	Cybersecurity 2011 (Handelsblatt, EUROFORUM, Berlin)
19.-23.09.	OWASP Global AppSec North America (OWASP Foundation, Minneapolis/US)
27.-29.09.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Oktober 2011	
05.-06.10.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
24.-27.10.	it-sa (SecuMedia Verlag, Nürnberg)
26.-29.10.	hashdays security & risk conference 2011 (DEFCON Switzerland, Luzern/CH)

Fundsache

Das [German Chapter des Berufsverbands ISACA](#) hat am 17.05.2011 einen [Prüfleitfaden zur Auftragsdatenverarbeitung](#) (§ 11 BDSG) publiziert. Der knapp 40seitige Leitfaden enthält Prüffragen zu den acht in der Anlage zu § 9 BDSG geforderten Maßnahmenbereichen mit Bezügen zu COBIT (4.1), ISO 27xxx und BSI IT-Grundschutz.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

August 2011



Risiko-Awareness

Bruce Schneier – ein verlässlicher Garant für originelle und scharfsinnige Einschätzungen – veröffentlichte im Februar 2007 ein bemerkenswertes Essay zur „[Psychologie der Sicherheit](#)“ (aktualisiert im Januar 2008). Darin fasst er zahlreiche Erkenntnisse der Psychologie zur Risiko-Wahrnehmung zusammen, die vor allem eines deutlich machen: Menschen schätzen Risiken immer wieder falsch ein –

selbst dann, wenn sie über genügend Informationen verfügen.

Zwar geben wir vor (und bemühen uns bisweilen), Risiken nüchtern zu analysieren. Tatsächlich aber dominieren intuitive Bewertungen unser Handeln. So neigen wir dazu, spektakuläre, plötzliche und extern verursachte Risiken – wie die Gefahr einer Atomkatastrophe nach den Ereignissen in Fukushima – überzubewerten, während wir unerwünschte Risiken, die zudem nicht uns, sondern andere betreffen, unterschätzen (wie die Gefahr einer Massenpanik bei der Loveparade durch die Verantwortlichen in Duisburg).

Auch „gewohnte“ Risiken (wie die ca. 4.000 Verkehrstoten pro Jahr) werden meist unterbewertet – niemand lässt deshalb sein Auto stehen –, während bei neuen Risiken, über die gesprochen wird und die uns oder unsere Kinder direkt bedrohen – wie die EHEC/HUS-Infektion mit 50 Toten – gleich die halbe Nation den Verzehr von Gemüse einstellt.

So ergeht es uns auch mit Unternehmensrisiken. Weder ein Mehr an Information noch die Etablierung von Risikoanalyseverfahren wird daran etwas ändern – denn, wie Bruce Schneier zutreffend folgert, werden wir nur dann zu zutreffenden Risikobewertungen und angemessenen Reaktionen kommen, wenn „unser Sicherheitsgefühl mit der Sicherheitswirklichkeit übereinstimmt“.

Um das zu erreichen helfen intensive Risikodiskussionen wohl eher als trockene Analysen – und Awareness-Maßnahmen, die diffuse, anonyme, schleichende, verschwiegene und unerwünschte Risiken in unsere und die Wahrnehmung der Verantwortlichen rücken.



Inhalt

Risiko-Awareness

Security News

Mobile Keylogger

Kai su teknon, Facebook

Siemens S7 Hack

HTML 5 Security

Tracking-Tool der IVW

SIFT 2.1

Secorvo News

T.I.S.P. - Das Buch

Budenzauber

Security-Update 2011

2. Smart Grid Symposium

Veranstaltungshinweise

Fundsache

Security News

Mobile Keylogger

Keylogger, die Tastatureingaben protokollieren, wären auch auf Smartphones keine Überraschung – ließen sich aber auch dort recht leicht erkennen. Am 09.08.2011 [zeigten](#) jedoch zwei Forscher der University of California auf dem [6. USENIX Workshop HotSec](#), wie man in Android-Handys aus den Bewegungssensoren einen Keylogger macht.

Zwar verfügt Android über eine Instanz, die den Zugriff auf bestimmte Ressourcen (Adressbuch, Telefon, Netzwerk ...) regelt. Möchte ein Programm eine dieser Ressourcen nutzen, muss der Entwickler dies „anmelden“. Bei der Installation der „App“ erhält der Benutzer eine Liste der Ressourcen, die das Programm nutzen möchte. Erscheint die Liste dem Nutzer nicht angemessen – etwa weil ein Kartenspiel Zugriff auf das Netzwerk, das Adressbuch usw. haben möchte – kann er sich gegen eine Installation entscheiden. Die Nutzung des Bewegungssensors dürfte allerdings den meisten Nutzern unverdächtig erscheinen.

Auch bei Smartphones ist spätestens jetzt die Zeit der „erkennbar harmlosen Anwendungen“ vorbei. Ohne Personal Firewalls mit cleveren Heuristiken kann man nicht davon ausgehen, dass nur der Nutzer auf Daten und Anwendungen zugreifen kann.

Kai su teknon, Facebook

Trackingdienste zur Reichweitenmessung von Websites beschäftigen bereits seit geraumer Weile die Datenschutzaufsichtsbehörden ([SSN 08/2010](#)). Nach einer nun [veröffentlichten eigenen Untersuchung](#) hat das [ULD Schleswig-Holstein](#) am 19.08.2011 eine

[Aufforderung](#) an sämtliche verantwortlichen Stellen des Landes gerichtet, die Verwendung der von Facebook angebotenen [Social Plugins](#) zu unterlassen.

Grund sind die von Facebook verwendeten Cookies sowie die nachweislich erfassten Daten und vorgenommenen Verknüpfungen: Beim Aufruf von Webseiten, die z. B. den Facebook „Like-me“-Button nutzen, werden sowohl angemeldete als auch nicht angemeldete Nutzer von Facebook erfasst. Das Zusammenführen dieser Nutzungsdaten mit Facebookprofilen ist dank der Cookies über die Dauer von zwei Jahren möglich. Eine solche Verknüpfung stellt einen Verstoß gegen § 15 Abs. 3 TMG dar.

Weder die Webseiten-Anbieter noch [Facebook](#) halten hierfür ausreichende [Erklärungen zum Zweck und Umfang](#) dieser Datenerhebungen bzw. -übermittlungen vor; ein klarer Verstoß gegen § 13 Abs. 1 TMG. Nach der seit dem 25.05.2011 direkt anwendbaren Änderung von Art. 5 Abs. 3 der europäischen Datenschutzrichtlinie für elektronische Kommunikation ([RL 2009/136/EG](#)) ist zudem die Einwilligung des Nutzers vor dem Setzen solcher Cookies erforderlich, was bislang allgemein missachtet wird.

Für den Fall der Zuwiderhandlung hat das ULD ab Oktober 2011 Untersagungsverfügungen nach § 38 Abs. 5 BDSG angekündigt. Vielleicht wird so die Beachtung des Datenschutzrechts zum Wettbewerbsfaktor zwischen Social Networks. Ein erster Schritt wäre eine ausreichende Transparenz der Anbieter über ihre Datenverarbeitung.

Siemens S7 Hack

Das [ICS-CERT](#) (Industrial Control Systems Cyber Emergency Response Team) warnte am 03.08.2011 vor Schwachstellen in S7-300 SPS-Systemen: Mit

auf der diesjährigen [Black Hat](#) vorgestellten [Exploits von Dillon Beresford](#) können über einen Remote-Zugang Abläufe in der Steuerung verändert werden. Auch wenn andere SPS-Systeme wie die S7-400 von dieser Schwachstelle nicht betroffen sind, ist sehr zu empfehlen, Steuerungssysteme grundsätzlich in eigenen Netz-Segmenten zu betreiben – und schon gar nicht mit dem Internet zu verbinden.

HTML 5 Security

Noch immer sorgen viele alte Sicherheitsprobleme mit Web-Anwendungen für Probleme (siehe [SSN 07/2011](#)), da kommt mit [HTML 5](#) neues Ungemach.

Viele der neuen Features von HTML 5 bringen gänzlich neue Angriffsvektoren ins Spiel. Mit [Veröffentlichung](#) der Studie „[A Security Analysis of Next Generation Web Standards](#)“ vom 01.08.2011 sorgt die [ENISA](#) hier auf 60 Seiten für eine gute Übersicht. Neue Funktionen von HTML 5 und damit verbundene Sicherheitsprobleme werden ausführlich erläutert – eine Leseempfehlung für alle, die verstehen wollen, welchen Sicherheitsherausforderungen die Entwickler von Web-Applikationen zukünftig gegenüber stehen werden.

Tracking-Tool der IVW

Mit dem Skalierbaren Zentralen Messsystem (SZM) der Fa. INFOline misst die Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) seit Ende 2008 die Reichweite von Online-Medien. Der Hamburger Datenschutzbeauftragte Prof. Dr. Caspar hat in einer [Presseerklärung vom 08.08.2011](#) die Bereitschaft der Beteiligten gewürdigt, das SZM, das auch von [www.hamburg.de](#) genutzt wurde ([SSN 01/2011](#)), hinsichtlich des Datenschutzes anzupassen. Das SZM orientiert sich nun an den [Vorgaben des Düsseldorfer Kreises](#) zur

Reichweitenmessung und kürzt das letzte Oktett der IP-Adresse. Außerdem wird ein Opt-Out für die Nutzer angeboten. Die [Musterdatenschutzerklärung](#) klärt umfassend über das IVW-Verfahren auf, bleibt allerdings bezüglich der eingesetzten Cookies vage.

Es darf jedoch bezweifelt werden, dass in dieser Sache bereits das letzte Wort gesprochen ist. Auch das SZM verwendet Cookies, die eine längerfristige Wiedererkennung ermöglichen. Es ist wahrscheinlich, dass diese durch das in Art. 5 Abs. 3 der EU-Datenschutzrichtlinie für elektronische Kommunikation ([RL 2009/136/EG](#)) geforderte Opt-In erfasst werden, da mindestens ein Identifikator dauerhaft auf dem Endgerät gespeichert wird. Zudem bleiben bislang sämtliche Lösungen der mit dem Nutzertracking verbundenen Probleme unbefriedigend, da sie entweder die meisten Nutzer nicht erreichen (Opt-Out-Cookie), zu Nutzerunfreundlichkeit führen (vorherige Einwilligung) oder die Personenbeziehung weiterer Daten neben der IP-Adresse außer acht lassen.

SIFT 2.1

Seit dem 04.08.2011 ist das generalüberholte [SANS Investigative Forensic Toolkit \(SIFT\)](#) für registrierte Nutzer verfügbar: ein sehr umfangreicher, hochaktueller forensischer Werkzeugkasten für Gegner einer „one click forensic“, der die wichtigsten forensischen Entwicklungen der vergangenen zwölf Monate vereint.

Hervorzuheben sind die weitere Automatisierung der Zeitlinienerstellung mit [log2timeline](#), die Vervollständigung der umfangreichen Sammlung von RegRipper-Plugins sowie die Aktualisierung des Speicheranalysewerkzeugs [Volatility 2.0](#). Bei letzterem ist zu beachten, dass [ältere Volatility-Scripts](#) noch zu portieren sind. Thematisch wurde der Secorvo Security News 08/2011, 10. Jahrgang, Stand 31.08.2011

Bereich Smartphones für die Analyse von iPhone, BlackBerry und Android ergänzt. Allerdings genügt SIFT hier nicht allein – gerade bei iPhones ist [viel Know-How](#) für die erste Sicherung erforderlich.

SIFT sollte in keinem forensischen Arsenal fehlen; es liegt als verlässliches VMware-Image vor.

Secorvo News

T.I.S.P. - Das Buch

Mitte September wird es endlich verfügbar sein: das [Begleitbuch zum T.I.S.P.](#) Es führt, strukturiert in Anlehnung an das T.I.S.P.-Seminar, in die „Zentralen Bausteine der Informationssicherheit“ ein. Neun der elf an der Erstellung beteiligten Autoren sind zugleich Referenten der nächsten [T.I.S.P.-Schulung](#) vom **17.-22.10.2011** (mit Prüfung) bei Secorvo College; alle Teilnehmer erhalten das Buch zur Vorbereitung vorab zugesandt. Es sind noch wenige Plätze verfügbar – bis zum **12.09.2011** sogar zum Frühbuche Preis.

Die Programme weiterer Seminare und die Möglichkeit zur [Online-Anmeldung](#) finden Sie unter <http://www.secorvo.de/college>.

Budenzauber

Ein wirkungsvoller Informationsschutz steht und fällt mit dem sicherheitsbewussten Verhalten aller Mitarbeiter eines Unternehmens. Doch wie sensibilisiert man die Mitarbeiter nachhaltig für Informationssicherheit? Dieser Frage geht Dirk Fox auf dem kommenden [KA-IT-Si-Event](#) am **22.09.2011** im Panoramasaal der IHK Karlsruhe nach. In seinem Vortrag „Security Awareness in der Praxis“ fasst er Erfahrungen aus zahlreichen Security Awareness Kampagnen großer und mittelgroßer Unternehmen

der vergangenen Jahre zusammen und gibt Empfehlungen für ein wirkungsvolles Vorgehen. Die Veranstaltung beginnt um 18:00 Uhr. Um [Anmeldung](#) wird gebeten.

Security-Update 2011

„Für Hacker gibt es kaum noch Grenzen“, titelte die WirtschaftsWoche am 01.08.2011. Tatsächlich kann sich heute kein erfolgreiches Unternehmen – und sei es noch so klein – vor Angriffen auf seine Infrastruktur sicher wähen. In einem Land, das seinen wirtschaftlichen Erfolg Ideenreichtum und Wissen verdankt, setzt ein nachlässiger Umgang mit Daten jedoch die eigene Zukunft aufs Spiel.

Geschäftsführer und Vorstände wissen um diese Risiken – allerdings ändern sich Bedrohungs- und Gesetzeslage ständig. Mit dem [„Sicherheits-Update 2011“](#), am 05.10.2011 wollen LEITWERK, Secorvo und Securiton Abhilfe schaffen: Drei Expertenvorträge geben Einblick in die wesentlichen Fragestellungen – und das anschließende Come Together die Gelegenheit zum Erfahrungsaustausch.

2. Smart Grid Symposium

Nach dem großen Erfolg des „Smart Grid Symposiums“ im Februar dieses Jahres freuen wir uns, Sie zu unserem [2. Smart Grid Symposium](#) am **29.-30.11.2011** in der [Buhlschen Mühle](#) in Ettligen einladen zu können. Es erwarten Sie spannende Vorträge rund um den Datenschutz und die Datensicherheit im Smart Grid, u. a. vom Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundesverband der Energie- und Wasserwirtschaft (BDEW) und der EnBW. Werfen Sie einen Blick auf das [Programm](#) – wir freuen uns auf Ihre [Teilnahme!](#)

Veranstaltungshinweise

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

September 2011	
13.-14.09.	Cybersecurity 2011 (Handelsblatt, EUROFORUM, Berlin)
19.-23.09.	OWASP Global AppSec North America (OWASP Foundation, Minneapolis/US)
27.-29.09.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Oktober 2011	
05.10.	Security-Update 2011 (Leitwerk/Secorvo/Securiton, Appenweier)
05.-06.10.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
11.-13.10.	it-sa (SecuMedia Verlag, Nürnberg)
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
26.-29.10.	hashdays security & risk conference 2011 (DEFCON Switzerland, Luzern/CH)
November 2011	
11.-13.11.	FifF Jahrestagung 2011 zur Dialektik der Informationssicherheit (FifF e.V., München)
29.-30.11.	2. Smart Grid Symposium (Secorvo, KA-Ettlingen)

Fundsache

Die Darstellung von Herausforderungen der Web-Anwendungssicherheit muss nicht trocken daher kommen. Die zur Zeit aus drei Videos bestehende [OWASP Appsec Tutorial Series](#) informiert verständlich und unterhaltsam über aktuelle Fragestellungen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Michael Knopp, Klaus J. Müller, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

September 2011



Wem ist noch zu trauen?

Kürzlich ließ sich eine Zertifizierung beobachten, die heftige Zweifel an der Praxis der Vergabe von Zertifikaten aufkommen lässt. Dabei handelte es sich nicht um den Commodo- oder DigiNotar-Hack, sondern um eine [irreführende TÜV-Zertifizierung einer Billig-Wetterstation](#).

Der Vorfall wäre wenig mehr als eine amüsante Anekdote, wären nicht zahlreiche deutsche Webseiten und IT-

Produkte mit ähnlichen TÜV-Siegeln verziert – so auch Version 9 des Internet Explorers ([SSN 05/2011](#)).

Zweifelhaft daran ist weniger die der Zertifizierung vorausgegangene Prüfung, denn diese ließe sich nur beurteilen, wenn bekannt wäre, *wofür genau* (IE9) oder *nach welchen Kriterien* (Wetterstation) die Prüfung erfolgte. In beiden Fällen schweigt der TÜV sich darüber jedoch aus: Betriebsgeheimnis. Und wie ist das mit den TÜV-Siegeln zahlreicher Webseiten? Welche Zusicherung ist mit einem solchen Siegel verbunden?

Transparenz ist gerade bei Prüfverfahren, die nicht nach internationalen Standards erfolgen, besonders wichtig, da ein Siegel andernfalls zu missbräuchlicher Verwendung einlädt – erst recht, wenn der Zertifizierer eigentlich im Ruf steht, sein Handwerk zu verstehen. Geheimniskrämerei oder Selbstgefälligkeit sind hier fehl am Platz – sie leisten nur Nachlässigkeit oder gar Betrug Vorschub.

Der Wert von Zertifikaten – ob vom TÜV oder von einer CA – beruht darauf, dass dem Aussteller vertraut wird, und dazu gehört, dass die Prüfung nach höchsten Maßstäben der Sorgfalt erfolgt. Fragwürdige oder gar irreführende Zertifizierungen können das Fundament jeder Vertrauensinfrastruktur ins Wanken bringen. Die TÜVs sind seit Jahrzehnten eine Institution, deren Name für Verlässlichkeit steht. Umso schlimmer ist es, wenn sich ausgerechnet der TÜV für zweifelhafte Siegel und Gutachten hergibt.

Wem soll man dann noch vertrauen?



Inhalt

Wem ist noch zu trauen?

Security News

Haftung bei Phishing

DisTrust-Center

Konformes Google Analytics?

Datenschutzkritik

Verkehr der Zukunft – eCall

Secorvo News

Secorvo College aktuell

Security-Update 2011

Zweites Smart Grid Symposium

Veranstaltungshinweise

Fundsache

Security News

Haftung bei Phishing

Das Landgericht Landshut hat am 14.07.2011 über die Haftung einer Bank nach einem erfolgreichen Phishing-Angriff auf das iTAN-Verfahren [entschieden](#). Das Verhalten des Klägers, der gegenüber den Angreifern 100 TAN-Nummern durch Eingabe auf deren Seite preisgegeben hatte, wurde als fahrlässig, nicht aber als grob fahrlässig gewertet.

Nach § 675v Abs. 2 BGB haftet die Bank bei einem unautorisierten Zahlungsvorgang nur dann nicht, wenn der Kunde diesen betrügerisch, absichtlich oder grob fahrlässig ermöglicht hat. Grobe Fahrlässigkeit liegt bei einer Missachtung allgemein einleuchtender Überlegungen und einem damit einhergehenden diesbezüglichen schweren Verschulden vor. Die Unerfahrenheit des Klägers im Umgang mit Computern und seine sprachlichen Defizite mussten im vorliegenden Fall berücksichtigt werden.

Die Bank hatte ihre Kunden darauf hingewiesen, TANs nur zu verwenden, wenn zuvor z. B. eine Überweisung erfasst worden sei. Das Landgericht sah diesen Hinweis vor allem durch das „z. B.“ als zu unpräzise an, zumal der Trojaner SpyEye den Kläger auf eine Website lenkte, die äußerlich der Originalseite entsprach und die die nach dem Login geforderte TAN-Eingabe ausdrücklich als besondere Ausnahme darstellte. Erst recht könne die Bank dem Kläger nicht die Wahl des unsicheren von mehreren angebotenen Authentisierungsverfahren vorwerfen.

Für die [Konstruktion von Trojanern](#) stehen schon lange Baukästen wie Zeus bereit. Auch Smartphone-Betriebssysteme sind längst im Visier. Die Frage, ab welcher Grenze der Nutzer eine gestellte

Secorvo Security News 09/2011, 10. Jahrgang, Stand 29.09.2011

Falle erkennen muss, bleibt von den Umständen des Einzelfalls abhängig, doch mit steigender Qualität der Attacken wird die Chance der Banken schwinden, dem Kunden grobe Fahrlässigkeit vorzuwerfen. Sowohl Rechtsprechung als auch Gesetzgebung sind offenbar geneigt, dem Kunden ein hohes Maß an Unbesonnenheit zuzugestehen.

DisTrust-Center

Über den [Einbruch](#) beim Trust-Center DigiNotar vom 17.06.-22.07.2011 (der ja [nicht der erste](#) Trust-Center-Einbruch war), den folgenden [Lizenzentzug](#) durch die niederländische Regierung am 14.09.2011 und die letztliche [Liquidation](#) des Unternehmens am 20.09.2011 wurde in [verschiedenen Medien](#) ausführlich [berichtet](#). Was lehrt uns dieser Fall?

- Die Trust-Center-Branche betreibt nicht annäherungsweise ein Fraud-Management, wie es bei Finanz- und Zahlungsdienstleistern üblich ist. Ein Zertifikatsantrag für eine der weltweiten [Top-Websites](#) darf einfach nicht automatisiert ohne manuelle Prüfung zu einem Zertifikat führen.
- Das Krisenmanagement von GlobalSign, die [angeblich](#) ebenfalls kompromittiert wurden, war – Im Vergleich etwa zu [RSA Security](#) – geradezu vorbildlich und Vertrauen erweckend: Der Betrieb wurde gestoppt und häufige Updates zu den sofort eingeleiteten Sicherheitsuntersuchungen [veröffentlicht](#). Eine seltene Ausnahme.
- Viele Trustcenter verschweigen schamhaft, wie viele ihrer qualifizierten Signaturzertifikate in Umlauf sind. In diesem Fall wurde es für DigiNotar öffentlich: [4.200](#).
- Der eigentliche Vertrauensanker für SSL/TLS sind nicht die Trust-Center, sondern die [Browser-](#)

[Hersteller](#), die deren Root-Zertifikate installieren oder [löschen](#) und jetzt schärfere [Kontrollen fordern](#). Kaum ein Anwender kann sich die Mühe machen, etliche Dutzend vorinstallierter Roots (von denen viele noch nicht einmal mehr dem Unternehmen gehören, das sich vor Jahren im Root-Zertifikat „verewigt“ hat) zu durchforsten.

Der letztgenannte Punkt könnte sich in den nächsten Jahren ändern, wenn TLS-Zertifikate per [DANE](#) über DNS verteilt werden. Dann würden die [DNS-SEC-Schlüssel der DNS-Root Zone](#) zum [Vertrauensanker](#) für TLS – die [Single Internet Root](#) 2.0.

Konformes Google Analytics?

Kurz nachdem Prof. Dr. Caspar, Landesdatenschutzbeauftragter Hamburgs, das Verfahren des Reichweitenmessdienstleisters INFOnline ([SSN 08/2011](#)) als rechtskonform anerkannt hat, ist einer [Pressemeldung](#) vom 16.09.2011 nun auch seine Anerkennung der Anpassungen von Google Analytics zu entnehmen. Danach habe Google die [Forderungen des Düsseldorfer Kreises](#) vom 26./27.11.2009 durch die Verkürzung der IP-Adresse, das Bereitstellen eines Opt-Out-Verfahrens und seine Datenschutzhinweise erfüllt. Auf die Notwendigkeit späterer Anpassungen, sollte das Erfordernis eines Opt-In für die verwendeten Cookies eingeführt werden, wird am Rande hingewiesen.

Dennoch dürfen diese Aussagen nicht als Freifahrtsschein für Webseitenanbieter verstanden werden. Jene werden zunächst die nach § 13 TMG geforderte Transparenz auf den Datenschutzerklärungen ihrer Webseiten herstellen müssen. Vor der Nutzung ist ein Auftragsdatenverarbeitungsvertrag abzuschließen und durch Löschung des alten Accounts für die Löschung der Altdateien zu sorgen.

Auch bei einer – vom Seitenanbieter zu veranlassenden – Kürzung der IP-Adressen bleibt die [Datenverarbeitung im EG-Ausland ein Problem](#), das der Rechtskonformität durch Auftragsdatenverarbeitung im Weg steht. Selbst wenn der Webseitenbetreiber also seine Pflichten erfüllt (was sich der Überprüfung durch den Nutzer entzieht), bleibt die Rechtskonformität zweifelhaft, daher ist von einer Nutzung von Google Analytics weiterhin abzuraten.

Datenschutzkritik

Mit ihrem Einschreiten gegen eine Reihe von Diensten der Branchenriesen Google und Facebook haben Datenschutzbehörden in jüngster Zeit Schlagzeilen gemacht. In der [Blogger-Szene](#) werden die zweifelhaften Erfolge bereits als „Datenschutztheater“ bezeichnet.

So sind das Verpixeln von einzelnen Häusern in Straßenzügen mit gleichartigen Reihenhäusern, die durchgesetzte Verkürzung von IP-Adressen unter gleichzeitiger Nutzung von mindestens gleichwertigen weiteren Identifikationsmerkmalen (Cookies) bei Tracking-Diensten oder die eher halbherzige Auseinandersetzung mit Facebooks Gesichtserkennung in der Tat Beispiele für „Datenschutzerfolge“, die bestenfalls einzelne Symptome behandeln, das dahinter stehende Problem jedoch ungelöst lassen. Gleichzeitige Bestrebungen des Staates, eigene Datenbanken oder Überwachungsmittel wie die [Vorratsdatenspeicherung](#) neu oder wieder einzuführen, schwächen die Glaubwürdigkeit weiter.

Die Ziele des Datenschutzes angesichts immer vielfältigerer Mittel zur Verknüpfung von Informationen und einer Zunahme von verfolgbarem Kommunikationsverhalten umzusetzen wird nicht leichter, weder für den Gesetzgeber noch für die Exekutivorgane und Anwender. Es ist jedoch – und Secorvo Security News 09/2011, 10. Jahrgang, Stand 29.09.2011

darin ist den Kritikern recht zu geben – dringend erforderlich, die vorhandenen Regeln konsequent umzusetzen. Auf der anderen Seite sind der Schutzbedarf und die angeordneten Mittel auf allen Ebenen zu überprüfen. Ansonsten droht eine substantielle Schwächung des Schutzzumfangs der informationellen Selbstbestimmung.

Verkehr der Zukunft – eCall

In einer [Empfehlung vom 08.09.2011](#) hat die EU-Kommission gefordert, anschließend an die europaweite Einführung der Notrufnummer 112 einen eCall als automatisierten Notruf aus Fahrzeugen einzuführen. Dieser Notruf mit einem standardisierten Minimaldatensatz soll von den Fahrzeugsystemen selbst erzeugt und genau wie ein 112-Notruf behandelt werden. Die Empfehlung gibt Definitionen und Standards vor, die eine europaweite Einheitlichkeit der Systeme sicherstellen sollen.

Eine Kommissionsempfehlung ist rechtlich unverbindlich, d. h. es ergibt sich hieraus keine Umsetzungsverpflichtung für die Mitgliedstaaten. Wird ein entsprechendes System eingeführt, sind die Maßgaben jedoch zu berücksichtigen. Die Einführung eines eCalls wird zur Einführung von eigenen Mobilkommunikationswegen in Fahrzeugen führen. Es ist absehbar, dass diese Entwicklung nicht beim eCall-Dienst stehen bleiben wird. Die entstehenden Datenschutz und Sicherheitsfragen werden daher künftig im Auge zu behalten sein.

Secorvo News

Secorvo College aktuell

Für die nächste [T.I.S.P.-Schulung](#) vom 17.-22.10.2011 (einschließlich Prüfung) bei Secorvo College

sind noch vier Plätze frei. Schnellentscheider erhalten unmittelbar nach Eingang der Anmeldung das [Begleitbuch zum T.I.S.P.](#) zur Prüfungsvorbereitung zugesandt (im Seminarpreis inbegriffen).

Im November folgen die Seminare PKI – [Grundlagen, Vertiefung, Realisierung](#) (08.-11.11.2011), [IT-Sicherheit heute](#) (15.-17.11.2011) und [Certified Professional for Secure Software Engineering \(CPSSE\)](#) mit anschließender Zertifikatsprüfung (22.-25.11.2011). Die Programme aller Seminare, die Bewertungen unserer Teilnehmer und die Möglichkeit zur [Online-Anmeldung](#) finden Sie [hier](#).

Security-Update 2011

Kein erfolgreiches Unternehmen kann sich mehr vor Angriffen auf seine Infrastruktur sicher wähnen. In einem Land, das seinen Erfolg Ideenreichtum und Wissen verdankt, setzt ein nachlässiger Umgang mit Daten jedoch die Zukunft aufs Spiel. Zwar wissen Unternehmen von diesen Risiken – allerdings ändern sich Bedrohungs- und Gesetzeslage ständig. Mit dem „[Sicherheits-Update 2011](#)“, am 05.10.2011 wollen LEITWERK, Secorvo und Securiton Abhilfe schaffen: Drei Expertenvorträge beleuchten die wesentlichen Fragestellungen – mit anschließender Gelegenheit zum Gedankenaustausch am Buffet.

Zweites Smart Grid Symposium

Vom 29. bis 30.11.2011 findet das "[2. Smart Grid Symposium](#)" in der [Buhlschen Mühle](#) in Ettlingen statt. Es erwarten Sie spannende Vorträge rund um Datenschutz und Datensicherheit im „intelligenten Stromnetz“, u. a. vom Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundesverband der Energie- und Wasserwirtschaft (BDEW) sowie der EnBW. Werfen Sie einen Blick in das [Programm](#) – wir freuen uns auf Ihre [Anmeldung!](#)

Veranstaltungshinweise

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

Oktober 2011	
05.10.	Security-Update 2011 (Leitwerk/Secorvo/Securiton, Appenweier)
11.-13.10.	it-sa (SecuMedia Verlag, Nürnberg)
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
26.-29.10.	hashdays security & risk conference 2011 (DEFCON Switzerland, Luzern/CH)
November 2011	
08.-11.11.	PKI (Secorvo College, Karlsruhe)
11.11.	Outsourcing und Vendor Security (Gesellschaft für Informatik/Fachgruppe SECMGT, Frankfurt)
11.-13.11.	FifF Jahrestagung 2011 zur Dialektik der Informationssicherheit (FifF e.V., München)
15.-17.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
22.-23.11.	ISSE 2011 (TeleTrusT, Prag/CZ)
22.-25.11.	CPSSE (Secorvo College, Karlsruhe)
29.-30.11.	2. Smart Grid Symposium (Secorvo, KA-Ettingen)
Dezember 2011	
05.-06.12.	IsSec/ZertiFA 2011 (Computas., Berlin)

Fundsache

Am 26.09.2011 hat das US-amerikanische NIST den Draft der Special Publication SP 800-153 "[Guideline for Securing Wireless Local Area Networks \(WLAN\)](#)" publiziert. Auf kompakten 12 Seiten gibt sie konkrete Empfehlungen zur Absicherung von WLANs – auch wertvoll für den privaten Router. Die Kommentierungsfrist endet am 28.10.2011.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

Oktober 2011



Untragbar unerträglich

Gelegentlich ist es unerfreulich, mit einer Prognose richtig gelegen zu haben. Die Erkenntnisse um die vom Chaos Computer Club mit der am 08.10.2011 publizierte [Analyse eines „Staatstrojaners“](#) ausgelösten Recherchen übertreffen jedoch die schlimmsten Befürchtungen. Da ist zunächst das [Unternehmen](#), das die Überwachungssoftware im Auftrag von LKAs und BND entwickelte: Dessen früherer

Geschäftsführer wurde [nach Erkenntnissen des Handelsblatts](#) 2002 wegen Bestechung zu 1,5 Mio. € Geldbuße und 21 Monaten auf Bewährung verurteilt, und zumindest von Web-Sicherheit versteht es [nicht allzu viel](#). Dann ist da die Software: Sie verschlüsselt die zu übermittelnden Daten mit einem immer gleichen AES-Schlüssel und kann über nachladbare Module sowohl zur [Quellen-TKÜ](#) als auch zur [Online-Durchsuchung](#) eingesetzt werden. Für letztere hat das BVerfG in seinem [Urteil vom 27.02.2008](#) sehr hohe materielle Zulässigkeitsvoraussetzungen formuliert: „Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.“ Anders als bei einer (Quellen-) TKÜ genügen z. B. Verstöße gegen das Betäubungsmittelgesetz diesem Kriterium nicht.

Dass es keine gute Idee ist, die Entscheidung über den Funktionsumfang in die Hand der Strafverfolgung zu legen, zeigt das [Urteil des LG Landshut](#) vom 20.01.2011: Bei der Umsetzung eines Quellen-TKÜ-Beschlusses des Amtsgerichts wurden von den bayerischen Strafverfolgungsbehörden mit der Software im 30-Sek.-Takt rechtswidrig 66.000 Screenshots erzeugt. Möglicherweise [kein Einzelfall](#).

In einem Rechtsstaat ist auch die Exekutive an Gesetz und Verfassung gebunden – vor allem das unterscheidet ihn von einer Willkürherrschaft. Ein Landesinnenminister, [der einen solchen Rechtsbruch verteidigt](#), ist daher nicht nur unerträglich, sondern untragbar.



Inhalt

Untragbar unerträglich

Security News

Bepper-Trojaner

Grundschutz EL 12

CAINE erneuert

Risiken der Überwachung

Immer wieder Facebook

Security Theatre in der Cloud

Secorvo News

Kaminlektüre

Seminare

Durch die Hintertür

Veranstaltungshinweise

Fundsache

Security News

Bepper-Trojaner

Immer häufiger werden [QR-Codes](#) (zweidimensionale Barcodes) als Link zu weiterführenden Informationen in Zeitschriften, auf Plakaten, Webseiten oder Eintrittskarten angegeben. Diese Grafik kann mit einem Handy oder Smartphone abfotografiert und weiterverarbeitet werden, so dass der interessierte Nutzer auf der darin angegebenen Website landet, ohne eine URL eintippen zu müssen.

Am 30.09.2011 berichtete Denis Maslennikov von Kaspersky Labs über [einen Angriff](#), bei dem auf über QR-Codes referenzierten Webseiten dem Smartphone-Benutzer – ähnlich wie bei einem SMS-Trojaner – eine mit Schadsoftware angereicherte Version eines mobilen ICQ-Clients untergeschoben wird. Theoretisch war ein solcher „Bepper-Trojaner“ (umgangssprachlich für „[Aufkleber](#)“) bereits einige Wochen zuvor [beschrieben worden](#).

Ein gutes Beispiel dafür, wie aus einem ergonomischen Feature eine Angriffsmöglichkeit wird. Wer QR-Codes nutzt, sollte auf keinen Fall Software oder Apps auf diesem Weg beziehen.

Grundschutz EL 12

Seit dem 11.10.2011 steht die aktualisierte und erweiterte Version der BSI-Grundschutzkataloge in der [12. Ergänzungslieferung](#) (EL) im PDF-Format mit dokumenteninternen Sprungmarken online zur Verfügung. Die HTML-Version, die von freien Werkzeugen wie z. B. [verinice](#) genutzt wird, bleibt vorerst jedoch auf dem Stand der 11. EL. Für das [GSTOOL 4.7](#) wurde indes bereits eine Aktualisierung (Servicepack 3 und zugehörige Metadaten) für November

und Dezember 2011 [angekündigt](#), [Version 5.0](#) soll im 2. Quartal 2012 verfügbar sein.

Zeitgleich mit der Ergänzungslieferung wurden auch eine aktualisierte „[Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz](#)“ sowie die [Formblätter](#) und [Kreuzreferenztabellen](#), die viele Unternehmen als Grundlage für eigene Arbeitswerkzeuge nutzen, vom BSI bereitgestellt. Neben neuen Bausteinen wie „Virtualisierung“ (B 3.304) und „Terminalserver“ (B 3.305) wird für ein produktunabhängiges Vorgehen bei Webservern in der 12. EL nur noch der generische Baustein „Webserver“ (B 5.4) genutzt. Ein richtiger Schritt angesichts der sich schnell ändernden Technologie. Ein Hinweis auf die [OWASP-Top 10](#) wäre dort allerdings sinnvoll gewesen.

CAINE erneuert

Seit dem 19.09.2011 ist die frei nutzbare Live-CD-Forensikdistribution [CAINE](#) (Computer Aided Investigative Environment), die auf Ubuntu basiert, in der überarbeiteten Version 2.5 verfügbar. Auch gibt es eine spezielle USB-Stick-Version.

Besonders hilfreich sind die stark erweiterten NAUTILUS-Scripts für das direkte Einsehen von Dateiinformationen von z. B. gelöschten Dateien und Bilddaten. Ein besonderes Schmankerl ist das unscheinbare Script „FileInfo“, welches über die Option „Metadatenextraktion“ die Inhalte von [SQLite](#)-Datenbanken ausliest, die z. B. von Firefox, Nokia OVI, Skype und Apples iPhones genutzt werden. Abgerundet wird der positive Eindruck durch das Werkzeug [frag_find](#), mit dem z. B. Dokumententeile über identische Sektoren-Hashwerte gefunden und nachgewiesen werden können, vorausgesetzt, dass bei einer Untersuchung das nachzuweisende Dokument digital vorliegt.

Risiken der Überwachung

Das Landgericht Lüneburg hatte am 28.3.2011 über die Rechtmäßigkeit der Beschlagnahme der GPS-Überwachungsanlage eines Privatdetektivs zu [entscheiden](#). Die Anlage wurde zur lückenlosen Verfolgung des Aufenthaltsortes u. a. von Arbeitnehmern beim Verdacht missbräuchlicher Krankschreibungen eingesetzt. Zu diesem Zweck wurde sie an den Fahrzeugen der Zielpersonen angebracht. Dagegen hatte der niedersächsische Landesdatenschutzbeauftragte Strafanzeige gestellt.

Das Landgericht sah darin den Anfangsverdacht einer entgeltlichen unbefugten Erhebung und Verarbeitung personenbezogener Daten (§ 44 i.V.m. § 43 Abs. 2 Nr. 1 BDSG). Sollte die Entscheidung eines anschließenden Strafverfahrens der des Landgerichts folgen, die [nicht die erste](#) mit ähnlicher Tendenz ist, dürfte dies sowohl dem Auskunftseigewebe als auch Auftraggebern privater Überwachungsmaßnahmen deutliche Grenzen setzen.

Immer wieder Facebook

Auf der [Entwicklerkonferenz f8](#) am 22.09.2011 stellte Facebook neue Funktionen vor. So ermöglicht [Facebook Timeline](#) dem Nutzer nun, zurückliegende Erlebnisse oder Ereignisse an einer übersichtlichen Zeitleiste – wie eine persönliche „Chronik“ – einzustellen. Und unter der Bezeichnung „frictionless sharing“ kann man durch einmalige Einverständniserklärung gegenüber Facebook Webdiensteanbietern und Smartphone-Apps erlauben, alle eigenen Aktivitäten an Facebook zu melden. Dieses „Tracking“ des gesamten digitalen Lebens (Welche Musik kaufe ich gerade? Auf welcher Seite surfe ich? Welches Online-Spiel habe ich eben gestartet?) kann dann mit Freunden geteilt werden.

In Europa sind mit diesen Diensten die nächsten Rechtsstreitigkeiten vorprogrammiert. Wie bislang wird es auch dabei nicht darum gehen, ob der Nutzer seine Daten in dieser Form der Welt oder Facebook preisgeben darf, sondern dass nach deutschem Datenschutzrecht die Diensteanbieter verantwortliche Stelle für die Übermittlung der Nutzungsdaten sind. Daher benötigen sie als Folge von [§ 15 TMG](#) jeweils separate Einwilligungen, bei denen sie – deutlich weitergehend als in den [Datenverwendungsregeln von Facebook](#) – über Zweck und Art der Nutzung dieser Daten werden aufklären müssen. Dies gilt zumindest für alle europäischen Diensteanbieter und solche, die gezielt in Deutschland anbieten.

Solange sich Facebook außerdem Zweckänderungen und umfangreiche eigene Verarbeitungen vorbehält, selbst nicht umfassend aufklärt und keine ausreichende Einwilligung einholt, ist zudem Facebooks eigene Verarbeitung der Nutzerdaten rechtswidrig. Der Aktivist [Max Schrems](#) hat daher gegen Facebooks europäische Niederlassung in Irland wegen 22 Verstößen gegen europäisches Datenschutzrecht Anzeige erstattet.

Der Streit um und mit Facebook steht exemplarisch für die zahlreichen grundsätzlichen Missachtungen der Persönlichkeitsrechte im Internet – und des geltenden deutschen und europäischen Rechts.

Security Theatre in der Cloud

Am 04.10.2011 [kündigte](#) Amazon an, dass ab sofort Daten im Amazon Web Service (AWS) [S3](#) durch eine serverseitige Verschlüsselung (SSE) [geschützt](#) werden können – eine Meldung, die in der deutschen Presse viel Resonanz gefunden hat. Diese Verschlüsselung erlaubt die „[transparente Absicherung](#)“ von Daten in der Cloud – durch Amazon, inklusive der Secorvo Security News 10/2011, 10. Jahrgang, Stand 25.10.2011

Erzeugung, Verwaltung und Vernichtung von Schlüsseln. Da stellt sich die Frage: Was genau wird hier eigentlich geschützt? SSE bewahrt die auf Amazon-Rechnern gespeicherten Daten vor Preisgabe bei einem Diebstahl der Datenträger aus dem Rechenzentrum. Damit schützt Amazon mit viel Wirbel gegen ein eher kleines Risiko.

Einen deutlich besseren Schutz bietet die [Client-seitige Verschlüsselung](#) mit dem [AWS JDK for Java](#). Vielleicht möchte Amazon diesen Mechanismus aber gar nicht so gerne bewerben – schließlich macht er die Anwendungsentwicklung aufwändiger. Und die amerikanischen Sicherheitsbehörden sind dabei auch ausgesperrt.

Secorvo News

Kaminlektüre

Über vier Jahre haben wir daran geschrieben, und nach nur sechs Wochen war es so weit: Die erste Auflage des Secorvo-Buchs „[Zentrale Bausteine der Informationssicherheit](#)“, auch als Begleitbuch zum [T.I.S.P.](#) geeignet, ist ausverkauft. Auflage zwei ist bereits im Druck und voraussichtlich ab der ersten Novemberwoche verfügbar. Wem also noch eine Kaminlektüre für die langen Winterabende fehlt, dem sei das Werk ans Herz gelegt. Bei einer [Anmeldung zum T.I.S.P.-Seminar](#) (nächster Termin: 07.-11.05.2012) ist das Buch inklusive und wird vorab zugesandt.

Seminare

Für alle Kurzsentschlossenen bietet Secorvo noch drei Weiterbildungschancen (mit garantierter Durchführung) im Jahr 2011:

- Das Seminar [PKI – Grundlagen, Vertiefung, Realisierung](#) vom 08.-11.11.2011 bietet Ihnen einen Einblick in die Konzeption, Implementierung und Nutzung von PKIs.
- Ihre IT-Security-Grundlagenkenntnisse können Sie beim Seminar [IT-Sicherheit heute](#) vom 15.-17.11.2011 auffrischen.
- Eine praxisorientierte Einführung in die sichere Softwareentwicklung bekommen Sie beim Seminar [ISECCO Certified Professional for Secure Software Engineering \(CPSSE\)](#) vom 22.-24.11.2011 mit anschließender Zertifikatsprüfung.

Sichern Sie sich jetzt einen der noch freien Plätze. Die Programme aller Seminare, die Möglichkeit zur [Online-Anmeldung](#) und das Jahresprogramm 2012 finden Sie unter <http://www.secorvo.de/college>. Wir freuen uns auf Ihre Anmeldung!

Durch die Hintertür

Die Erbringung von IT-Dienstleistungen erfordert in wachsendem Umfang den Fernzugriff auf IT-Systeme. Wie kann man sich dabei aber gegen Zugriffe unberechtigter Dritter und einen unkontrollierten Datenabfluss schützen? Was ist bei der Fernwartung heute „state-of-the-art“ – und von welchen Techniken sollte man besser die Finger lassen?

Diese und weitere Fragen rund um die Absicherung von Wartungszugriffen beantwortet Dr. Böttger (Leiter [CONNECT](#)-SupportCenter) in seinem Vortrag auf dem kommenden Event „Wer kommt da durch die Hintertür?“ der [Karlsruher IT-Sicherheitsinitiative \(KA-IT-Si\)](#) am 17.11.2011 um 18 Uhr im Schlosshotel Karlsruhe. Um [Anmeldung](#) wird gebeten.

Veranstaltungshinweise

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

November 2011	
08.-11.11.	PKI (Secorvo College, Karlsruhe)
11.11.	Outsourcing und Vendor Security (Gesellschaft für Informatik/Fachgruppe SECMGT, Frankfurt)
15.-17.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
17.11.	Wer kommt da durch die Hintertür? (KA-IT-SI)
22.-25.11.	CPSSE (Secorvo College, Karlsruhe)
Dezember 2011	
05.-06.12.	IsSec/ZertiFA 2011 (Computas, Berlin)
Januar 2012	
17.-19.01.	OMNICARD 2012 (in TIME berlin, Berlin)
24.-26.01.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Februar 2012	
08.-09.02.	22. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	19. DFN Workshop „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)

Fundsache

Das [NIST](#) veröffentlichte am 27.09.2011 den Draft einer überarbeiteten Fassung der [Special Publication SP 800-121](#) „Bluetooth Security“, die nun auch die Bluetooth-Standards 3.0 und 4.0 (Low Energy) berücksichtigt. Die Security-Checkliste ist auf 34 Empfehlungen angewachsen und ersetzt die Listen für Headsets und Smart Card Reader der Vorfassung.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

November 2011



Lest Märchen!

Kennen Sie Grimms Märchen? Nein, das ist *keine* iPhone-App. Es war einmal vor vielen, vielen Jahren, da las man den Kindern abends vor dem Kamin Märchen vor – bevorzugt die der Gebrüder Grimm von 1812. Mancher macht das noch heute – sei es aus Tradition, aus Nostalgie oder in Ermangelung anderer Kinderbücher. Oder auch, weil der Fernseher kaputt und der iPhone-Akku leer sind. Wie

dem auch sei: Beim Lesen werden Sie feststellen, dass jedes Märchen zahlreiche Lehren enthält – und nicht nur die, die ins Auge springen. Einige davon helfen sogar der Informationssicherheit.

Nehmen wir beispielsweise das Märchen vom [Wolf und den sieben Geißlein](#). Zur Erinnerung: Der Wolf will in Abwesenheit der Geiß deren Kinder zum Öffnen der Haustüre überreden – die aber erkennen ihn erst an der Stimme, dann an der Pfote. Als er beides tarnt, öffnen sie ihm – und er verschlingt alle bis auf das siebte, das sich im Uhrkasten versteckt hat. Weil er sich in der Nähe zum Schlafen legt, wird er später von der Geiß aufgeschlitzt – und die Geißlein befreit.

Was können wir daraus lernen?

1. Plausibilitäts-Checks sind kein wirksamer Schutzmechanismus. (Auch wer redet wie eine Geiß, kann ein Wolf sein.)
2. Die erfolgreiche Abwehr von Angriffen sollte ein Alarmsignal sein. (Der nächste Angriff ist sicher besser als der abgewehrte.)
3. Security Policies sind ohne Sensibilisierung und gesunde Skepsis wertlos. (Angreifer sind erfindungsreicher als Policy-Autoren.)
4. Das Fehlen interner Schutzwälle gibt dem erfolgreichen Eindringling alles preis. (Interne Schotts begrenzen den Angriffserfolg.)
5. Nur bei tierisch dummen Angreifern gibt es eine Chance, die erbeuteten Daten zurück zu erhalten.

Vielleicht darf man wenigstens hoffen, dass bei einem erfolgreichen Angriff 14,3 % der Informationen verschont bleiben. Verstecken Sie daher sicherheitshalber schon mal das Wichtigste im Uhrkasten.



Inhalt

Lest Märchen!

Security News

Ertappt

c = m

No, map!

OWASP.de gibt Gas

Europäischer Treibsand

Secorvo News

Secorvo College aktuell

Für den Weihnachtsmann

Krypto zum Anfassen

Veranstaltungshinweise

Fundsache

Security News

Ertappt

Am 02.11.2011 hat der Hamburgische Datenschutzbeauftragte einen [Bericht](#) vorgelegt, der der Nutzung von Cookies durch Facebook nachgeht. Die dem Bericht zugrunde liegende Prüfung orientiert sich an den Zweckangaben, die Facebook [unter anderem gegenüber dem ULD Schleswig-Holstein](#) angeführt hat. Zu den einzelnen Zweckangaben wurden für die Prüfung Szenarien gebildet, die dann in einer sicheren Umgebung dokumentiert durchgespielt wurden. Ziel war, festzustellen, ob die verschiedenen Cookies die angegebene Wirkung zeigen würden.

So soll etwa der „datr“-Cookie gemäß Facebook Hinweise auf Missbrauch liefern, indem er feststellt, ob über denselben Browser viele verschiedene Accounts genutzt werden. Bei den durchgeführten Versuchen konnte eine solche Wirkung nicht bestätigt werden. Ähnliches gilt für zahlreiche andere Zweckangaben.

Daraus kann zwar nicht geschlossen werden, dass die Cookies, wie vielfach vermutet, domainübergreifend für das Nutzertracking genutzt werden. Es indiziert jedoch, dass Facebook für einen Teil seiner Cookies keinen zulässigen Verwendungszweck angeben kann. So lassen sich jedenfalls nicht in rechtskonformer Weise Nutzertransparenz herstellen und die Erforderlichkeit der Datenerhebung nachweisen.

Zu Recht stellt der Bericht mindestens einen Verstoß gegen die jeweiligen nationalen Umsetzungen von Art. 5 Abs. 3 der [E-Privacy-Richtlinie](#) fest. Bei den Aufsichtsbehörden dürfte Facebook damit weiteres Vertrauen verspielt haben.

c = m

Kryptografie kann so einfach sein. Das dachen wohl auch die Programmierer der [Entwicklerversion](#) von [Ruby](#) bei der Implementierung des RSA-Verfahrens:

Wenn $c = m^e \bmod n$ zu berechnen ist – dann geht das mit $e := 1$ am schnellsten. Damit folgt:

$$c = m \bmod n, m < n \Rightarrow c = m$$

Sollten Sie mit dieser Ruby-Version zwischen dem 01.09.2011 und dem 04.11.2011 RSA-Schlüssel erzeugt haben, dann ersetzen Sie diese besser schnellstmöglich. Denn wenn man bei DES schon Schlüssel als [schwache Schlüssel](#) bezeichnet, die bei zweimaliger Verschlüsselung den Klartext liefern,

$$\text{DES}(k, \text{DES}(k, m)) = m$$

muss man hier wohl von einem überschwachen Schlüssel mit $\text{RSA}(k, m) = m$ reden.

No, map!

Um ein erneutes Marketing-Desaster wie die Diskussion um die Abbildung deutscher Hausfassaden in Street View zu vermeiden, geht Google bei der Lokalisierungsfunktion in die Offensive: Wie viele [Standort-basierenden Dienste](#) (*location-based services*) verfügt auch Google Maps seit einer Weile über einen Standortbestimmungsdienst, aktivierbar über den „Knopf“ oberhalb der Zoom-Einstellung.

Da Google – anders als ein Smartphone – keinen direkten Zugriff auf Dienste des Netzbetreibers zur Standortbestimmung hat, wertet Google u. a. die SSIDs erreichbarer WLANs aus. Deren Standort-Daten wurden beim Fotografieren der Hausfassaden gleich mit erhoben oder von Nachbarn gemeldet – und werden in einer zentralen Datenbank (*Google Location Server, GLS*) vorgehalten.

Am 15.11.2011 machte Google publik, dass jeder, der mit seinem SSID (*service set identifier*) nicht im GLS aufgenommen werden möchte, die Löschung mit einem [ungewöhnlichen „Opt-Out“-Mechanismus](#) veranlassen soll: durch die Ergänzung der eigenen SSID um die Endung „_nomap“.

Sieht man einmal von der Frage ab, wie vielen privaten WLAN-Nutzern wohl eine entsprechende Umkonfiguration des eigenen WLAN-Routers gelingt, ohne Schaden anzurichten, bleibt die Gefahr, dass das Beispiel Schule machen könnte: Weitere Endungen wie z. B. „_noiphone“ oder „_noandroid“ dürften die verfügbaren 32 Byte maximaler SSID-Länge schnell abschmelzen. Vielleicht sollten die Standardisierungsgremien besser schon mal mit Anpassungsarbeiten am IEEE 802.11 beginnen...

OWASP.de gibt Gas

Beim [deutschen Chapter von OWASP](#) hat sich im November viel getan. Am 16.11.2011 wurde die [deutsche Übersetzung](#) der [OWASP Top 10](#) unter der Projektleitung von Kai Jendrian fertig gestellt und publiziert. Damit steht der anerkannte Branchenstandard nun auch in Deutsch zur Verfügung, um das Sicherheitsbewusstsein bei der Entwicklung von Webanwendungen zu verbessern – besonders bei Entwicklern in mittelständischen Unternehmen.

Am 17.11.2011 folgte in München der [4. German OWASP Day](#), bei dem sich mehr als 160 Experten über Sicherheitsfragen von Webanwendungen diskutierten. [Zwei parallele Vortrags-Tracks](#) deckten ein breites Spektrum an Themen ab – von Secure Software Development Life Cycle, Statischer Code Analyse über Web-Service-Security, Mobile Security und Browser-Sicherheit hin zu aktuellen Cyber-Bedrohungen. Ein Highlight war der [Ausblick auf](#)

[bevorstehende Entwicklungen](#) von Thomas Roessler (W3C).

Schließlich wurde am 19.11.2011 das Portal [hacking-lab.com](#) der OWASP Academy [freigeschaltet](#), mit dem sich Entwickler und Sicherheitsfachleute an praktischen Anwendungen zur Sicherheit von Anwendungen fortbilden sollen.

Europäischer Treibsand

Der Europäische Gerichtshof hat [am 24.11.2011 in einer Vorabentscheidung](#) über die Auslegung von Art. 7 der [Europäischen Datenschutzrichtlinie](#) entschieden. Anlass war ein Rechtsstreit zwischen dem Verband spanischer Kreditinstitute (ASNEF), dem Verband für E-Commerce und Direktmarketing (FECEMD) und dem spanischen Staat. Nach der Entscheidung sind die nationalen Gesetzgeber auf die in Art. 7 aufgezählten Zulässigkeitstatbestände festgelegt und dürfen diese nicht weiter einschränken oder weitere Tatbestände einführen.

Nach Ansicht der Kläger geht Spanien in seinem Datenschutzgesetz über Art. 7 hinaus, indem es die Verarbeitung personenbezogener Daten für berechnete Interessen des Verarbeiters ohne Einwilligung des Betroffenen nur für veröffentlichte Daten eröffnet. Dem hat der EuGH zugestimmt.

Den Mitgliedstaaten steht zwar offen, Leitlinien für die Abwägung zwischen dem Grundrechtsschutz der Betroffenen und den berechtigten Interessen aufzustellen, die den Unterschied zwischen veröffentlichten und unveröffentlichten personenbezogenen Daten berücksichtigen, er darf jedoch nicht durch den völligen Ausschluss unveröffentlichter Daten Art. 7 überschreiten. Dieser Grundsatz gelte allgemein für die Auslegung von Art. 7, der gleichzeitig für direkt anwendbar erklärt wurde.

Das deutsche Datenschutzrecht ist von der Entscheidung nicht direkt betroffen, da es in [§ 28 Abs. 1 Nr. 2 und 3 BDSG](#) getrennte Tatbestände für die Wahrnehmung berechtigter Interessen und allgemein zugängliche Daten enthält. Die Entscheidung wirft jedoch die Frage auf, ob die zahlreichen Detailregelungen des Bundesdatenschutzgesetzes lediglich erlaubte Leitlinien innerhalb der Grenzen des Art. 7 darstellen oder Datenkategorien ausschließende neue Tatbestände außerhalb von Art. 7 sind. Die Diskussion um die Zukunft des Datenschutzrechts ist damit um eine europäische Dimension reicher geworden.

Secorvo News

Secorvo College aktuell

Das Jahr neigt sich langsam dem Ende zu und für die Planung Ihrer Weiterbildung im kommenden Jahr lohnt sich bereits jetzt ein Blick in unseren [Seminarkalender 2012](#). Auch im neuen Jahr bietet Secorvo College wieder zahlreiche Weiterbildungsgelegenheiten.

Los geht es gleich im Januar mit dem Grundlagen-seminar [Sicherheitsmanagement heute](#) (24.-26.01.2012). Im März folgen dann [IT-Sicherheit heute](#) (13.-15.03.2012) und [Verlässliche Web-Anwendungs-Sicherheit](#) (21.-22.03.2012). Die erste Gelegenheit zur Zertifizierung Ihrer persönlichen Qualifikation im Bereich sichere Softwareentwicklung bieten wir Ihnen am 26.-30.03.2012 beim Seminar [Certified Professional for Secure Software Engineering \(CPSSE\)](#). Das nächste [T.I.S.P.-Seminar](#) führen wir vom 07.-11.05.2012 durch – Ihr Exemplar des [T.I.S.P.-Buchs](#) erhalten Sie bei frühzeitiger Anmeldung vorab zugesandt.

Das vollständige Jahresprogramm 2012, die detaillierten Programme aller Seminare und die Möglichkeit zur [Online-Anmeldung](#) und finden Sie unter <http://www.secorvo.de/college>. Wir freuen uns auf Ihre Anmeldung!

Für den Weihnachtsmann

Sollten Sie noch Platz unterm Tannenbaum haben und Ihr Weihnachtsmann noch keine durchschlagende Geschenkidee, dann lohnt ein Hinweis auf das [T.I.S.P.-Buch](#): Kann man sich etwas Schöneres vorstellen, als bei Kaffee und Keksen im Kerzenschein vor dem knisternden Kamin zu sitzen und genussvoll in den „Zentralen Bausteinen der Informationssicherheit“ zu schmökern? Wer sich das nicht entgehen lassen möchte, möge [hier](#) klicken – oder den Bestellwunsch gleich an den Weihnachtsmann weiterleiten.

Krypto zum Anfassen

Die [Karlsruher IT-Sicherheitsinitiative](#) (kurz: KA-IT-Si) erfreute sich in diesem Jahr erneut wachsender Teilnehmerzahlen – zuletzt konnten wir auf der Veranstaltung im November über 50 Teilnehmer begrüßen. Ab 2012 wird eine Kooperation mit dem [Karlsruher Institute of Technology](#) (KIT) und dem am 17.10.2011 feierlich eröffneten [Kompetenzzentrum für angewandte Sicherheits-Technologie](#) (KASTEL) die KA-IT-Si inhaltlich bereichern.

Am 26.01.2012 startet die Zusammenarbeit mit einem Highlight: Mit Vorträgen und Vorführungen werden wir einen Blick in die Geschichte der Kryptografie werfen – unterstützt durch historische Verschlüsselungsmaschinen u. a. aus der Sammlung des Instituts für Kryptografie und Sicherheit (IKS). Eine frühzeitige [Anmeldung](#) wird empfohlen.

Veranstaltungshinweise

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

Dezember 2011	
05.-06.12.	IsSec/ZertiFA 2011 (Computas, Berlin)
Januar 2012	
17.-19.01.	OMNICARD 2012 (in TIME berlin, Berlin)
24.-26.01.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
26.01.	Krypto zum Anfassen (KA-IT-Si, Karlsruhe)
Februar 2012	
08.-09.02.	22. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	19. DFN Workshop „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2012	
13.-15.03.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-16.03.	Black Hat Europe 2012 (Blackhat, Amsterdam/NL)
21.-22.03.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
26.-30.03.	CPSSE (Secorvo College, Karlsruhe)

Fundsache

Seit August 2010 findet sich auf der Webseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) eine [Handreichung zu § 11 des Bundesdatenschutzgesetzes](#). Darin bezieht der BfDI auf drei Seiten zu wichtigen Fragen Stellung, wie der Anpassung von Altverträgen oder dem Verständnis von „sich überzeugen“.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



Secorvo Security News

Dezember 2011



Macht verpflichtet

Jede Führungskraft und jedes Staatsoberhaupt sollte es wissen: Mit Macht und Einfluss wachsen nicht nur die Rechte, sondern vor allem die Pflichten.

Die stehen aber oft auf keinem Papier, sondern sind Teil eines „ethischen Codex“, wurden durch Kollegen oder Vorgänger vorgelebt oder gehören zur allgemeinen Erwartungshaltung an die jeweilige Position. Das macht es den Betroffenen nicht

leicht: Was gestern noch zulässig, unanstößig oder tolerabel war, kann in einer neuen Rolle ein absolutes „No-Go“ sein. Ohne eine mentale Umstellung geht das schnell schief – enge, langjährige Freundschaften geraten in den Verdacht der Vorteilsnahme, und die „unbürokratische“ Durchsetzung von Entscheidungen riecht schnell nach Amtsmissbrauch. Der souveräne Umgang mit Macht erfordert Selbstdisziplin und vorbildliches Verhalten ebenso wie die Beachtung von Regeln und Kontrollen, und manchmal auch Verzicht.

Das gilt auch für Administratoren. Denn die für den IT-Betrieb Zuständigen sind mit großer Machtfülle ausgestattet: Sie besitzen weit gehende Zugriffsberechtigungen, haben Einblick in detaillierte Log-Protokolle und verfügen über mächtige Analyse-Tools. Mit der Selbstdisziplin ist es allerdings oft nicht weit her: Immer wieder existieren gemeinsame Admin-Passworte, werden aus unsicherer Quelle Programme geladen und ungeprüft installiert oder aus Neugierde Logdaten ausgewertet. Selbst vor dem Lesen vertraulicher Dokumente oder der E-Mails von Kollegen schrecken einige Administratoren nicht zurück. In dieselbe Richtung weist eine [Studie der Fa. Balabit](#) vom 15.11.2011: Danach gaben 74 % der anonym Befragten Administratoren zu, ihre Rechte bereits missbraucht zu haben.

Dabei sollten die Passwörter von Admins besonders lang, Logfiles und Daten im Normalbetrieb tabu, die Rechte auf das Erforderliche beschränkt und auf allen Rechnern nur lizenzierte und freigegebene Software installiert sein. Nicht nur Führungskräfte und Staatsoberhäupter, sondern auch „Admins“ haben eine Vorbildfunktion.



Inhalt

Macht verpflichtet

Security News

Advent, Advent, der Drucker brennt...

Und sie ist doch personenbezogen...

Content Security Standard

Datenschutz per Verordnung

Weihnachtsgeld

Bin schon da!

Secorvo News

Auf die letzte Minute...

Krypto live

Veranstaltungshinweise

Fundsache

Security News

Advent, Advent, der Drucker brennt...

Am 29.11.2011 wurden [Forschungsergebnisse](#) publik, nach denen HP-Druckern mittels eines manipulierten Druckauftrags ein Firmware-Update untergeschoben werden kann. Das von den Medien [begierig aufgegriffene](#) Detail, dass damit durch Überhitzung der Fixiereinheit möglicherweise ein Druckerbrand ausgelöst werden könnte, erwies sich jedoch als Falschmeldung: [Laut HP](#) verfügen die Drucker über einen Überhitzungsschutzschalter, der nicht per Firmware beeinflusst werden kann.

Ebenso als Falschmeldung erwies sich die Nachricht vom 18.11.2011, wonach Hacker eine Pumpe in einem amerikanischen [Wasserwerk zerstört](#) hätten: Am 30.11.2011 [erklärte ein Techniker](#), dass er aus seinem Russland-Urlaub versucht hatte, die defekte Pumpe per Remote-Wartung wieder in Gang zu bekommen.

Trotz dieser spektakulären [Advents-Enten](#) sollte man sich nicht in falscher Sicherheit wiegen, denn in beiden steckt ein wahrer Kern: Die [\(Un-\)Sicherheit von digitalen Prozessteueranlagen](#) ist bekannt, und spätestens seit [Woz!](#) trickreicher [Apple-II-Floppy](#) weiß man, dass es ein Wettbewerbsvorteil sein kann, Funktionen aus teurer Hardware in billige Firmware zu verlagern. Wenn das allerdings kritische Funktionalität betrifft, muss sich der Hersteller intensiv um die Firmware-Integrität kümmern.

Und sie ist doch personenbezogen...

Der [EuGH](#) hat am 24.11.2011 auch den Versuch einer belgischen Urheberrechtsverwertungsgesellschaft (SABAM) abgewiesen, einen Internet-Pro-

vider (Scarlet Extended SA) zur Implementierung eines P2P-Inhaltsfilters zu verpflichten.

Danach schränkt der Zwang, ein Filtersystem über sämtliche Inhalte auf eigene Kosten zu betreiben, die Provider in ihrem Recht auf unternehmerische Freiheit (Art. 16 der [Charta der Grundrechte der EU](#)) ein und schafft keinen angemessenen Ausgleich zwischen den betroffenen Grundrechten. Hierbei sei auch Art. 15 der [Richtlinie 2000/31/EG \(Richtlinie über den elektronischen Geschäftsverkehr\)](#) zu beachten, der es untersagt, Diensteanbietern eine allgemeine Überwachungspflicht aufzuerlegen. Zudem würden das Recht der Nutzer auf den Schutz personenbezogener Daten und auf Informationsfreiheit (Art. 8 und 11 der Charta) unzulässig eingeschränkt.

Bemerkenswert ist die uneingeschränkte Einstufung der IP-Adressen als personenbezogene Daten durch den EuGH – ein großer Schritt zur Klärung dieser wichtigen datenschutzrechtlichen Streitfrage.

Content Security Standard

Bereits in den [SSN 09/2010](#) hatten wir über das Mozilla-Konzept einer [Content-Security-Policy](#) (CSP) zur Server-gesteuerten Kontrolle aktiver Inhalte in Webseiten berichtet, das seit Version 4 von Firefox unterstützt wird.

Inzwischen wurde auch bei Google Chrome und dem Internet Explorer mit der Integration begonnen. Bei den Konkurrenzbrowsern dürfte wesentlich zur Motivation beigetragen haben, dass der Ansatz inzwischen durch das W3C gesteuert wird: Seit dem 12.12.2011 liegt ein überarbeiteter [CSP-Entwurf](#) für einen W3C-Standard vor. Es darf also erwartet werden, dass sich dieser wirksame Ansatz zum Schutz vor Cross-Site Scripting durchsetzen wird.

Datenschutz per Verordnung

Die Europäische Kommission hat am 29.11.2011 einen länger erwarteten [Entwurf einer Datenschutzverordnung](#) vorgelegt. Eine EU-Verordnung ist, anders als eine Richtlinie, unmittelbar geltendes Recht – kein unbedeutendes Dokument also.

In großen Teilen entspricht der knapp 80seitige Verordnungsentwurf bereits geltendem deutschem Datenschutzrecht oder greift Rechtsmeinungen der Aufsichtsbehörden auf. Allerdings schließt er auch Regelungslücken und verschärft die eine oder andere Bestimmung. So zählt die Verordnung alle Personen, die mit vernünftigerweise zu erwartenden Mitteln durch einen beliebigen Dritten identifiziert werden können, zu den Betroffenen (Art. 3). Zudem wird der Anwendungsbereich ausdrücklich auf das Veröffentlichende an einen unbestimmten Personenkreis erweitert (Art. 2).

Die Verschärfungen betreffen u. a. die Vorabkontrolle, die zu einer Risiko- und Folgenabschätzung ausgebaut wird (Art. 30). Die bisherigen Prinzipien (Verbot mit Erlaubnisvorbehalt, Erforderlichkeit, Zweckbindung und Transparenz) werden um das Recht auf Löschung und Vergessen ergänzt (Art. 15) – ein Prinzip, das ebenso wie die neue Forderung nach Datenschutz durch Technikgestaltung und datensparsame Grundeinstellungen (Art. 20) insbesondere auf Social Networks abzielt. Enttäuschend ist der Empfehlungscharakter der Bestimmung zu Datenschutz-Siegeln und Zertifikaten (Art. 36).

Gleichzeitig wird die geteilte Verantwortlichkeit für Datenverarbeitungen anerkannt (Art. 21). Die Pflicht zur Bestellung eines Datenschutzbeauftragten wird auf Unternehmen mit mehr als 250 Beschäftigten oder besonderen Verarbeitungen beschränkt (Art. 32-34). Eingeführt werden auch

verbindliche Unternehmensrichtlinien als Grundlage des Datenexports in Drittstaaten (Art. 40).

Die Durchsetzung wird durch ausführliche Vorgaben und erweiterte Befugnisse für die zu schaffende Aufsicht (Art. 43 ff) und Strafvorschriften (Art. 78 f) sowie Haftungsregeln (Art. 77) gestärkt.

Zwar ist zu erwarten, dass der Entwurf noch eine Reihe von Änderungen erfahren wird. Dennoch dürfte er endlich wieder Leben in die festgefahrene deutsche Diskussion um ein modernes Datenschutzrecht bringen.

Weihnachtsgeld

Weihnachtszeit ist Shopping-Zeit: Die Wochen vor Weihnachten sind nicht nur für Einzelhändler, sondern auch für Online-Shops die umsatzstärkste Jahreszeit. Dass wissen auch Black Hats – und drohen vermehrt mit DDoS-Attacken, die sie erst nach Zahlung eines Schutzgelds via Western Union aussetzen oder einstellen.

Am 20.12. erwischte es [Conrad Electronic](#), am 21.12. den Webhoster [Mittwald CMS](#), und am 22.12.2011 war der Werbemittelversand [schneider](#) nicht erreichbar. Nach Auskunft des [Bundesverbands des deutschen Versandhandels](#) (bvh) ergab eine Umfrage des britischen e-retailing-Verbands [imrg](#), dass bereits 20 % der E-Commerce-Unternehmen von dieser modernen Form der Schutzgelderpressung betroffen sind.

Kein Wunder, dass Analysten technischen Schutzmaßnahmen gegen gezielte DDoS-Angriffe ein erhebliches Marktwachstum prophezeihen – nach über 50% in 2011. Aber auch mit Bordmitteln kann man vielen DDoS-Angriffen etwas entgegensetzen – eine schöne [Übersicht solcher Maßnahmen](#) hat Moritz Jäger am 27.02.2011 publiziert.

Secorvo Security News 12/2011, 10. Jahrgang, Stand 23.12.2011

Bin schon da!

Alle Arten von Smartphones sind grundsätzlich durch Apps gefährdet, die Schadfunktionen enthalten – das ist nichts Neues. Neu ist, dass auch von vorinstallierten Tools eine Bedrohung ausgehen kann. Der Android-Entwickler Trevor Eckart veröffentlichte am 28.11.2011 ein [Youtube-Video](#), in dem er die von US-Providern und Herstellern auf über 141 Mio. Smartphones vorinstallierte App "[CarrierIQ](#)" analysierte. Die [Ergebnisse seiner Untersuchungen](#) publizierte er inzwischen auch auf seiner Webseite. Die Software, die ursprünglich zur Optimierung von Netzen gedacht war, erlaubt es, Benutzereingaben und weitere Informationen wie die aktuellen GPS-Koordinaten abzugreifen. Allerdings lässt sie sich nicht einfach deaktivieren – und ist zudem in der Lage, sich zu tarnen.

Auch können Android-Apps über vorinstallierte Anwendungen die zugewiesenen Berechtigungen (*permissions*) unterlaufen, wie Forscher der North Carolina State University herausfanden. Sie [stellten fest](#), dass viele vorinstallierte Apps von anderen Apps eingespannt werden können und so restriktiv eingestellte Berechtigungen erweitern (*permission leaks*). Wir empfehlen daher auch vorinstallierte Apps daraufhin zu prüfen, ob man sie wirklich benötigt, und – um die Angriffsmöglichkeiten zumindest etwas einzuschränken – nicht genutzte Apps zu deinstallieren. Auch sollte man die Dienste GPS und WLAN nur dann einschalten, wenn man sie benötigt. Das schafft nicht nur mehr Privatsphäre – sondern erhöht auch die Akku-Laufzeit.

Wir wünschen Ihnen erholsame und schöne Weihnachtsfeiertage – und einen guten Start in ein rundum sicheres Jahr 2012!

Secorvo News

Auf die letzte Minute...

Wer noch ein Plätzchen unter dem Baum zu füllen hat: Wenige Mausklicks genügen, und die „[Zentralen Bausteine der Informationssicherheit](#)“ gehören Ihnen – das Grundwissen des T.I.S.P. in 22 Kapiteln, als Nachschlagewerk oder zur Vorbereitung auf eine [T.I.S.P.-Zertifizierung](#) (79,95 Euro).

Krypto live

Ab 2012 wird eine Kooperation mit dem [Karlsruher Institute of Technology](#) (KIT) und dem am 17.10.2011 feierlich eröffneten [Kompetenzzentrum für angewandte Sicherheits-Technologie](#) (KASTEL) die [Karlsruher IT-Sicherheitsinitiative](#) (kurz: KA-IT-Si) bereichern.

So startet die KA-IT-Si gleich am 26.01.2012 mit einem Highlight: Verschlüsselungstechnik gestern und heute „zum Anfassen“ am [Institut für Kryptographie und Sicherheit \(IKS\)](#) des KIT. Die Veranstaltung beginnt um 18 Uhr im Informatik-Gebäude (50.34) des KIT-Campus Süd, Karlsruhe. Wir freuen uns auf Ihre [Teilnahme](#)!



Veranstaltungshinweise

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

Januar 2012	
17.-19.01.	OMNICARD 2012 (in TIME berlin, Berlin)
24.-26.01.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
26.01.	Krypto zum Anfassen (KA-IT-Si/KIT, Karlsruhe)
Februar 2012	
08.-09.02.	22. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	19. DFN Workshop „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2012	
13.-15.03.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-16.03.	Black Hat Europe 2012 (Blackhat, Amsterdam/NL)
21.-22.03.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
26.-30.03.	CPSSE (Secorvo College, Karlsruhe)
April 2012	
23.-26.04.	PKI (Secorvo College, Karlsruhe)
24.-25.04.	Datenschutztage 2012 (Forum für Datenschutz, Wiesbaden)

Fundsache

Der Virenschutzanbieter Kaspersky Lab hat einen „[Security-Adventskalender](#)“ herausgebracht – mit 24 kernigen Tipps für eine sichere Weihnachtszeit.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

