secorvo
security consulting

Secorvo Security News

Januar 2012

So klug als wie zuvor

Studien sind beliebt. Häufig stützen sie die „Propheten im eigenen Haus“, deren Worte kein Gehör finden. Gelegentlich befreien sie Entscheider von der Last der Verantwortung. Und manchmal versachlichen sie eine Diskussion, indem sie den einen oder anderen Irrglauben widerlegen.

Weniger beliebt sind allerdings Studien, die nicht das vom Auftraggeber erwartete oder erwünschte Ergebnis liefern. Zwar werden die Verfasser vom Auftraggeber bezahlt („Wes' Geld ich nehm', des' Lied ich sing“), mit einer Tendenzstudie setzen sie aber ihre Glaubwürdigkeit aufs Spiel – und riskieren Ruf und künftige Geschäfte.

Bei überraschenden Resultaten ist zumindest in der Politik die Neigung zu beobachten, missliebige Ergebnisse zurückzuhalten – vielleicht in der so trügerischen wie verzweifelten Hoffnung, damit einer unerwünschten öffentlichen Debatte ausweichen zu können.

So geschehen mit dem vom Justizministerium beim Max Planck Institut in Freiburg in Auftrag gegebenen Gutachten zur Frage der Erforderlichkeit der Vorratsdatenspeicherung. Die Existenz der „2., erweiterten Fassung“ einer zwischen Mai und August 2010 (!) durchgeführten und im Juli 2011 abgeschlossenen Untersuchung machte erst eine Veröffentlichung von Auszügen in Spiegel Online am 27.01.2012 bekannt. Danach konnten die Autoren keine Hinweise dafür finden, dass der Wegfall der Vorratsdatenspeicherung negative Folgen für Strafverfolgung und Gefahrenabwehr habe: Wasser auf den Mühlen des Justiz- und Öl im Feuer des Innenministeriums.

Liest man die Schlussfolgerungen genau, so wird hinter dem tobenden öffentlichen Säbelrasseln deutlich, dass die Autoren mit einer „sehr unsichere(n) statistische(n) Datengrundlage“ und „sehr unterschiedlichen Einschätzungen bei den unmittelbar betroffenen Praktikern“ arbeiten mussten – sprich: keine belastbaren Erkenntnisse gewinnen konnten. Eines ist daher sicher: Die nächste Studie kommt bestimmt. Und in diesem Fall wäre das auch sehr zu begrüßen.

Inhalt

secorvo
security consulting

Security News

Ungemach für Surf-Tracker

Am 08.12.2011 hat die Art. 29 Gruppe, der beratende Zusammenschluss der europäischen und nationalen Datenschutzaufsichtsbehörden eine Stellungnahme zur künftigen Anwendung der so genannten Cookie-Richtlinie (RL 2009/136/EG) abgegeben. Sie bezieht sich auf Vorschläge der European Advertising Standards Alliance (EASA) sowie des Internet Advertising Bureau Europe (IAB), die ein Opt-out-Verfahren zum Gegenstand hatten.

Als unzureichend abgelehnt werden sowohl ein selbstregulativ von den Tracking-Netzwerken einzusetzendes Icon zur Information des Nutzers als auch das Angebot, über eine zentrale Seite Sperrcookies zu laden. Der geänderte Art. 5 Abs. 3 der E-Privacy Richtlinie (RL 2002/58/EG in der Fassung der RL 2009/136/EG) fordere eine klare und umfassende Information *vor* dem Setzen eines Cookies und ein Opt-In. Dabei sei unwesentlich, ob der Cookie personenbezogene Daten speichere. Tracking-Dienste setzten eindeutige Identifikatoren ein, die ein Erfassen einzelner Nutzer erlaubten und seien damit selbst ein personenbezogenes Datum.

Als zulässige und geeignete Varianten neben Pop-up Fenstern zur Information und Einwilligung werden vorgeschaltete Seiten, die von Heise vorgeschlagene 2-Klick Lösung, ein statisches Informationsbanner und Tracking verhindernde Browser-Voreinstellungen angesehen. Auch genüge eine einmalige Einwilligung für ein gesamtes Werbenetzwerk.

Damit rücken – aus berechtigten Gründen – statt der IP-Adresse die Tracking-Cookies als Identifizierungsmerkmal ins Zentrum der Regulierung. Mit der überfälligen Umsetzung der „Cookie-Richtlinie" werden daher die mühsam erreichten Übereinkünfte mit Tracking-Betreibern wie z. B. Google Makulatur: Der Einsatz von Google Analytics verstößt dann – ohne eine informierte Einwilligung des Seitenbesuchers – gegen geltendes europäisches Datenschutzrecht. Bei Verstößen wird mit Abmahnungen der deutschen Datenschutz-Aufsichtsbehörden zu rechnen sein.

Smartphone-Sicherheit

Vor etwa zehn Jahren hat die NSA mit SELinux eine Linux-Variante veröffentlicht, die dank starker Sicherheitsmechanismen erheblich widerstandsfähiger gegen Angriffe ist als ein „normales" Linux.

Am 06.01.2012 veröffentlichte die NSA die erste Version von SEAndroid, ein Projekt, in dem die SELinux-Architektur auf Android übertragen wurde. Derzeit steht noch keine fertige Firmware zur Verfügung; interessierte Nutzer müssen daher noch selber kräftig Hand anlegen.

Das hinter SELinux und SEAndroid stehende Sicherheitsmodell ist durchaus geeignet, verschiedenen Sicherheitsproblemen wirksam zu begegnen. Ob es sich durchsetzen kann, hängt jedoch stark vom Engagement der Smartphone-Hersteller ab.

Die größte Herausforderung bei der Umsetzung ist die Komplexität der Konfiguration. Dafür müssen die Hersteller einen gut durchdachten Ansatz wählen, bei dem die Sicherheitsmechanismen wirksam werden, ohne dass sich der Nutzer mehr als nur oberflächlich mit dem System beschäftigen muss. Gelingt das nicht, wird auch ein unter SEAndroid betriebenes Smartphone bestenfalls „gefühlt sicherer" sein.

Authentifikation systematisch

Am 12.12.2011 erschien, fünf Jahre nach der Erstfassung, die erheblich überarbeitete und erweiterte Revision 1 der Electronic Authentication Guideline (SP 800-63) des NIST. Darin wird das Thema Authentifikation über unsichere Netze von der initialen Registrierung der Teilnehmer bis hin zum Weiterreichen der Information über den authentifizierten Benutzer an nachgeordnete Anwendungen systematisch betrachtet. Vier aufeinander aufbauende Sicherheitsniveaus und konsistente Anforderungen an alle Nutzungsphasen eines Authentifikationsverfahrens werden definiert.

Auch wenn das Dokument primär für US-Behörden gedacht ist und daher auf Behördenstandards wie FIPS-140-2 oder PIV-Cards abhebt, so bietet es doch eine sehr gute Grundlage für eine angemessene Präzisierung des oft schwammig verwendeten Begriffs „starke Authentifikation".

Kuck mal, wer da...

Der am 28.11.2011 publizierte 20. Tätigkeitsbericht (2009-2010) des Landesbeauftragten für den Datenschutz Niedersachsen, Joachim Wahlbrink, legt einen Schwerpunkt auf das Thema Videoüberwachung. So wurden in einer großen Fastfood-Restaurantkette nicht nur ein hoher Anteil unzulässiger Überwachungen, sondern auch zahlreiche Datenschutzmängel bei der Installation, Dokumentation und der Erfüllung allgemeiner Datenschutzanforderungen festgestellt.

Einer Beschwerde folgend wurden vier Restaurants der Kette geprüft, die mit insgesamt 94 Kameras förmlich gespickt waren. Diese überwachten vielfach den Sitzbereich – unzulässig nach einem Urteil des AG Hamburg von 2008, denn in öffentlichen

Bereichen, in denen sich Personen typischerweise länger aufhalten, tritt das Beweis- und Präventionsinteresse des Betreibers hinter das Persönlichkeitsrecht der Betroffenen zurück. Nicht vom Personal einsehbare Bereiche dürfen nur noch für eine Übergangszeit weiter beobachtet werden; finden keine nennenswerten Vandalismus-Vorfälle statt, ist auch diese Überwachung mangels Erforderlichkeit einzustellen.

Das betroffene Unternehmen hat infolge der Prüfung seine gesamten einschlägigen Richtlinien überarbeitet, eine Löschfrist von 72 Stunden eingeführt und von den Franchisenehmern die Bestellung von Datenschutzbeauftragten eingefordert.

Auf die andauernde Ausweitung von Videoüberwachungen in Unternehmen reagieren die Aufsichtsbehörden mit einer Intensivierung der Prüfungen. Eine kritische Überprüfung der eigenen Prozesse und Löschfristen erscheint daher angeraten.

Verwirrungs-Taktik

Man stelle sich vor, für jedes Produkt, das man in einem Kaufhaus erwerben möchte, müsste man einen separaten Eingang zum Gebäude mit eigenem, individuellen Ladenschild nutzen. Bald wüssten viele Kunden nicht mehr, bei wem sie da eigentlich gerade einkaufen.

Vielleicht weil die Türen im Internet billiger sind, reservieren viele Marketing-Experten – zur Betonung der Wichtigkeit einer Aktion oder eines neuen Angebots – bei jeder sich bietenden Gelegenheit eine neue Second-Level-DNS-Domain, anstatt Subdomains des eingeführten Namens zu nutzen. So ist es nicht ungewöhnlich, wenn man bei der Online-Buchung eines Flugtickets von der Suche nach passenden Verbindungen über die Eingabe der Daten bis hin zu Zahlung und Buchungsbestätigung über drei oder vier verschiedene Domains geleitet wird.

Dabei bereitet gerade diese verbreitete Praxis Phishing und ähnlichem Trickbetrug den Boden – denn die Nutzer gewöhnen sich durch die alltägliche Verwirrung an ständige Domain-Wechsel und schöpfen im Angriffsfall keinen Verdacht.

Richtig bedenklich aber stimmt es, wenn auch im Sicherheitsbereich derartigen Unsitten Vorschub geleistet wird. So empfahl das BSI am 11.01.2012 einen durchaus sinnvollen Test auf Befall mit der DNSChanger-Malware. Allerdings nicht auf den eigenen amtlichen Webseiten, sondern unter der Domaine dns-ok.de. Wenig später tauchte unter dem homophonen Namen dns-okay.de eine (glücklicherweise harmlose) Verballhornung der Seite auf. Und auf der Webseite bka-trojaner.de wird unter der Titelzeile botfrei.de und den Logos von BSI und eco Hilfe gegen Ransomware angeboten – eine Webseite, die auf den ersten Blick keinen Deut seriöser wirkt als die Schadsoftware, vor der da gewarnt wird.

Kein Wunder also, wenn – wie am 12.01.2012 berichtet – zahlreiche Internetnutzer fürchten, sich auf derartigen Seiten eher mit einem Staatstrojaner zu infizieren als Hilfe zu finden.

Secorvo News

Neue Seminare

Die stetige Weiterentwicklung auf dem Gebiet der Informationstechnologie bringt auch neue Herausforderungen für die IT-Sicherheit mit sich. Ab dem Frühjahr 2012 erweitern wir daher unser Seminarangebot und bieten mit Aktuelle Herausforderungen der Informatinossicherheit vom 23.-24.05.2012 einen Überblick über neue Angriffsszenarien und Risiken sowie wirksame Schutzstrategien und Sicherheitslösungen.

Ihre IT-Security-Grundlagenkenntnisse können Sie vom 13.-15.03.2012 beim Seminar IT-Sicherheit heute auffrischen. Mehr über den Schutz von Web-Anwendungen erfahren Sie vom 21.-22.03.2012 beim Seminar Verlässliche Web-Anwendungs-Sicherheit. Und vom 26.-30.03.2012 bieten wir mit dem Certified Professional for Secure Software Engineering (CPSSE) eine praxisorientierte Einführung in die sichere Softwareentwicklung. Freie Plätze gibt es auch noch für das T.I.S.P.-Seminar vom 07.-12.05.2012 – bei frühzeitiger Anmeldung bekommen Sie Ihr Exemplar des T.I.S.P.-Buchs rechtzeitig vorab zugesandt (Programme und Online-Anmeldung).

Karlsruher IT-Sicherheitsinitiative

Einen fulminanten Start ins Jahr 2012 hatte die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si), die die Kooperation mit dem Kompetenzzentrum für Angewandte Sicherheits-Technologie (KASTEL) am 26.01.2012 mit einer gemeinsamen Veranstaltung einleitete: „Kryptographie zum Anfassen“ lautetet das Thema des Vortrags, der von einer einzigartigen Ausstellung historischer Kryptomaschinen aus zahlreichen Sammlungen begleitet wurde. Zum ersten Mal in der Geschichte der KA-IT-Si musste die Anmeldeliste zwei Tage vor der Veranstaltung wegen Überbuchung geschlossen werden.

Das nächste KA-IT-Si-Event zum Thema „Sichere Softwareentwicklung“ findet am 01.03.2012 im Schlosshotel Karlsruhe statt. Beginn ist um 18 Uhr. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

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

Februar 2012	
08.-09.02.	22. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	19. DFN Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2012	
01.03.	Sichere Software-Entwicklung (KA-IT-Si, Karlsruhe)
13.-15.03.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-16.03.	Black Hat Europe 2012 (Blackhat, Amsterdam/NL)
21.-22.03.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
26.-30.03.	CPSSE (Secorvo College, Karlsruhe)
April 2012	
15.-19.04.	Eurocrypt 2012 (IACR, Cambridge/UK)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
April 2012	
07.-12.05.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
09.-10.05.	BvD Verbandstag 2012 (BvD e.V., Berlin)

Fundsache

Am 20.12.2011 veröffentlichte die amerikanische Electronic Frontier Foundation (EFF) einen 24seitigen Guide for Travelers Carrying Digital Devices zum Grenzübertritt in die USA mit digitalen Daten – mit vielen hilfreichen Empfehlungen für US-Reisende.

Impressum

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

ISSN 1613-4311

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

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

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

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

secorvo
security consulting

Secorvo Security News

Februar 2012

Trau, schau, wem?

Nicht erst durch die jüngste Entdeckung identischer Primfaktoren in Public Key Zertifkaten durch die Krypto-Forscher der EPFL (siehe „PKI-Feldstudie“) wissen wir, dass es mit der Vertrauenswürdigkeit von „Trust Centern“ möglicherweise nicht immer so weit her ist, wie wir glaubten. Dabei ist schon der Begriff „Trust Center“ semantischer Nonsens – denn natürlich wird dort weder Vertrauen gesammelt noch erzeugt. Im Kontext von Technik ist „Vertrauen“ ohnehin irreführend. Denn der Begriff bezeichnet „die subjektive Überzeugung (auch Glaube) der Richtigkeit, Wahrheit bzw. Redlichkeit von Handlungen, Einsichten und Aussagen eines anderen oder von sich selbst“, so die Definition in Wikipedia. Vertrauen können wir daher einzig und allein Menschen entgegen bringen, denn Richtigkeit, Wahrheit und Redlichkeit sind keine Eigenschaften technischer Systeme. Wenn wir von „Vertrauen in Technik“ sprechen, meinen wir daher eigentlich etwas anderes: nämlich unser Vertrauen darauf, dass diejenigen, die ein technisches System entwarfen, entwickelten, betreiben und warten unser Vertrauen verdienen.

Menschen vertrauen anderen Menschen vor allem dann, wenn sie gute Erfahrungen damit gemacht haben, wenn ihnen keine Hinweise bekannt sind, die Misstrauen nahe legen, und wenn sie den Eindruck gewinnen, dass dem Gegenüber die Bestätigung des Vertrauens wichtig ist. Genau deshalb sind ein positives Markenimage und Prüf-Zertifkate unabhängiger Dritter vertrauensbildend, und Berichte über Vorfälle Gift für eine Vertrauensbeziehung.

Allerdings darf man Vertrauen nicht mit Sicherheit verwechseln. Vertrauen „überbrückt“ Unsicherheit und (Rest-)Risiken: Es greift da, wo Technik nicht weiterhilft. Denn dass RSA-Schlüssel nicht faktorisiert werden können, dass die Identität des Schlüsselinhabers sorgfältig geprüft wurde und dass die zugehörigen Private Keys Dritten unzugänglich sind, lässt sich durch Technik nicht garantieren. Daran müssen wir glauben. Oder auch nicht, wie Aesop schon wusste.

Inhalt

secorvo
security consulting

Security News

PKI-Feldstudie

Krypto-Forscher der EPFL Lausanne haben in einer am 17.02.2012 veröffentlichten Studie mehrere Millionen Public Keys untersucht, die u. a. vom SSL-Observatory der EFF gesammelt worden waren. Dabei traten einige Fakten zutage, die bei Fachleuten nur Kopfschütteln ernten können: U. a. wurden zu ein und demselben RSA-Schlüsselpaar über 16.000 verschiedene X.509-Zertifikate entdeckt – unklar bleibt, für wie viele unterschiedliche Inhaber. Und etwa 0,2 % der untersuchten RSA-Moduli haben einen ihrer beiden Primfaktoren mit anderen Public Keys gemeinsam, d. h. sie können trivial per GGT-Berechnung gebrochen werden. Dazu kommen noch vereinzelte RSA-„Schlüssel", bei denen einer der beiden Primfaktoren 2 ist, oder bei denen als öffentlicher Exponent 1 verwendet wird – in beiden Fällen ist auch ein 2048-Bit-RSA-Key nicht sicherer als Doppel-ROT13. Daneben gibt die Studie Aufschluss auf die Verbreitung verschiedener Algorithmen und Schlüssellängen: Nur einer von über 11 Mio. Public Keys nutzte elliptische Kurven (ECDSA).

Um die Betroffenen zu schützen, wurde nicht veröffentlicht, ob die betreffenden Schlüssel in PGP-Keys, in selbstsignierten Zertifikaten von Billig-Routern oder in durch öffentliche Trustcenter erstellten Zertifikaten gefunden wurden. Letzteres würde ein weiteres Schlaglicht auf die unterentwickelte Qualitäts- und Risikomanagement-Kultur der Branche werfen – genau wie der am 04.02.2012 publik gewordene Fall, dass bewusst ein CA-Zertifikat zum „Aufbrechen" von SSL verkauft wurde. Merke: Die Schlüssellänge allein garantiert keine unknackbaren Schlüssel – und ein Zertifikat offenbar auch nicht.

Grenzen staatlicher Auskunftsrechte

Das Bundesverfassungsgericht hat mit Beschluss vom 24.02.2012 die Auskunftsbefugnisse von Geheimdienst-, Ermittlungs- und Polizeibehörden eingeschränkt. Überprüft wurden die Auskunftsverfahren über Telekommunikationsbestandsdaten nach den §§ 111 ff. Telekommunikationsgesetz (TKG). Die Preisgabe von PIN, PUK und weiteren Zugangscodes zu den Endgeräten und die Zuordnung von dynamischen IP-Adressen über diese Auskunftsansprüche sind danach verfassungswidrig.

Zwar wurde das automatisierte Auskunftsverfahren und die grundsätzliche Speicherpflicht der TK-Provider in weiten Teilen bestätigt. Der Grundrechtseingriff sei vergleichsweise gering und gerechtfertigt. Die Auskunftserteilung über die Zuordnung von dynamischen IP-Adressen sei jedoch ein Eingriff in das Telekommunikationsgeheimnis (Art. 10 GG) und von den Auskunftsnormen nicht umfasst. Zudem stellen die Auskunftspflichten keine Erhebungsgrundlage für die abfragenden Behörden dar. Diese benötigen fachspezifische Befugnisnormen. Im Fall von § 113 Abs. 1 S. 2 TKG, der Auskunft über Zugangscodes, fehle der Regelung zudem eine ausreichende Bindung an die Zwecke der Codeverwendung.

Bemerkenswert sind die Ausführungen zur bevorstehenden Einführung von IPv6 mit flächendeckend statischen IP-Adressen. Sollte es hierdurch zu einer umfassenden Deanonymisierung der Internetnutzung kommen, wird dem Gesetzgeber die Pflicht zur Neubetrachtung der Eingriffsbeschränkung aufgegeben. Damit bleibt das Bundesverfassungsgericht seiner Rolle als Bollwerk gegen ausufernde staatliche Überwachung treu.

Taschendiebstahl 2.0

Mit der zunehmenden Verbreitung von Smartcard-Chips, die neben den Kontaktflächen auch eine RFID-Schnittstelle besitzen, sprießen auch deren Anwendungen: Nach dem nPA hat am 11.01.2012 die Deutsche Kreditwirtschaft angekündigt, dass die GeldKarte bald unter dem Namen „girogo" auch berührungslos nutzbar sein wird.

Das weckt Befürchtungen über einen berührungslosen Taschendiebstahl. Prompt wurde auf der Shmoocon am 29.01.2012 demonstriert, wie einfach sich eine RFID-fähige Kreditkarte „im Vorbeigehen" kopieren lässt. Glücklicherweise muss der Cyber-Taschendieb bei sicheren Verfahren als „Händler" auftreten und riskiert so seine Entdeckung. Und gegen eine Weiterleitung als Man-in-the-Middle an einen realen Händler helfen Protokolle, die mittels Kryptographie und Signallaufzeiten den Radius eines möglichen Missbrauchs beschränken. Eher ist jedoch zu erwarten, dass elektromagnetische Abschirmung für Portemonnaies bald genauso üblich sein wird wie eingewebte Metallfäden in Winterhandschuhen.

Bauen am IT-Grundschutz

Am 19.02.2012 hat das BSI auf den Webseiten zum IT-Grundschutz die Entwürfe für drei neue Bausteine (Webanwendungen, MacOSx und OpenLDAP) zur Kommentierung bereitgestellt. Da die Weiterentwicklung der IT-Grundschutz-Kataloge zur Zeit etwas stagniert – die 11. Ergänzungslieferung aus 2009 ist immer noch die aktuelle zertifizierungsrelevante Version – ist die Fortschreibung von Bausteinen zu begrüßen. Eine Kommentierung der Entwürfe legen wir allen Interessierten ans Herz.

Die Bereitstellung der bereits im Juni 2011 zunächst nur als pdf publizierten 12. Ergänzungslieferung mit anderen wichtigen Bausteinen als Meta-Daten für das Grundschutz-Tool sowie als html-Version wird dennoch sehnlich erwartet.

Multimedialer Overflow

Der Titel "Spiel mir das Lied vom Rootkit" im Heise-Newsticker vom 30.01.2012 gefiel auch uns – die darin vorgestellte Angriffsmethode allerdings weniger: Eine präparierte Midi-Datei auf einer Webseite kann via Internet-Explorer und Windows-Media Player über eine Heap Spray Attacke einen Buffer Overflow in der Bibliothek winmm.dll auslösen. Anschließend kann beliebiger Code ausgeführt und das System übernommen werden. Trojaner, die die Schwachstelle ausnutzen, sind bereits im Umlauf. Mit einem Patch von Microsoft wurde die Schwachstelle, von der zahlreiche Windows-Systeme betroffen sind, im Januar behoben.

Soweit so vertraut: Richtig neu sind Buffer Overflows in Multimediaanwendungen nicht. Im Gegenteil: Darüber sollten Softwareentwickler inzwischen hinaus sein. Zu befürchten ist aber wohl, dass auch weiterhin derartige Schwachstellen aufgedeckt werden. Dagegen helfen nur Ansätze wie das Sandboxing von IE9, dedizierte Lösungen wie Bitbox oder Surf-VMs à la c't Surfix. Oder eine komplette Trennung des Internetzugangs vom Client-PC über eine virtuelle Maschine wie ReCoBS. Btw.: Haben Sie auf den ersten Link des Beitrags geklickt?

Wer zweimal klaut...

Zum Schutz gegen Urheberrechtsverletzungen im Internet werden derzeit Warnhinweismodelle diskutiert. Danach sollen Zugangsprovider auf Veranlassung von Rechteinhabern Anschlussinhabern, die eine Urheberrechtsverletzung begehen, eine Warnung zusenden sowie eine Liste der gewarnten Anschlussinhaber führen. Nach einer festzulegenden Zahl von Verstößen sollen die Rechteinhaber informiert werden; sie können dann entscheiden, ob sie eine Auskunft über den Anschlussinhaber zur Rechtsverfolgung einholen möchten.

Das Bundeswirtschaftsministerium (BMWi) hat nun am 01.02.2012 eine 2011 in Auftrag gegebene vergleichende Studie über Warnhinweismodelle und die Umsetzbarkeit eines solchen Modells in Deutschland veröffentlicht. Die knapp 350seitige Studie (zzgl. 50 Seiten Anhang) bewertet die Modelle grundsätzlich positiv, unter der Voraussetzung, dass bei Missachtung der Warnungen eine konsequente Rechtsverfolgung erfolgt.

Voraussetzung für das Modell ist jedoch eine Vorratsdatenspeicherung der Zugangsanbieter. Die Studie geht von der grundsätzlichen Zulässigkeit der Verwendung dieser Daten aus. Das Datenschutzrecht wird jedoch nur oberflächlich und fehlerhaft berücksichtigt: So verwechseln die Autoren bezüglich der zu führenden Liste Anonymität und Pseudonymität; auch wird die Erforderlichkeit außer Acht gelassen, bei der Übermittlung von Mehrfachverstößen nach Rechteinhabern zu differenzieren.

Nebenbei liefert die Studie außer dem Vergleich der verschiedenen europäischen Ansätze einen Einblick in die derzeitigen Planspiele der Bundesregierung.

Secorvo News

Bildungszeit

Vom 13.-15.03.2012 haben Sie die Möglichkeit, Ihre IT-Security-Grundlagenkenntnisse beim Seminar IT-Sicherheit heute aufzufrischen. Sichern Sie sich kurzfristig noch einen der freien Plätze. Wir freuen uns auf Ihre Teilnahme!

Die nächste Schulung mit anschließender Zertifikatsprüfung zum TeleTrusT Information Security Professional (T.I.S.P.) findet vom 07.-11.05.2012 statt. Bei frühzeitiger Anmeldung bekommen Sie Ihr Exemplar des T.I.S.P.-Buchs rechtzeitig vorab zugesandt.

Ebenfalls im Mai, vom 23.-24.05.2012, können Sie sich beim Seminar Aktuelle Herausforderungen der Informationssicherheit einen Überblick über neue Angriffsszenarien und Risiken sowie wirksame Schutzstrategien und Sicherheitstechnologien verschaffen.

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

Rolltor für den Online-Shop

Die Entwicklung sicherer Online-Plattformen, die potentiell jedem Angreifer ausgesetzt sind, stellt aus Sicherheitssicht eine ganz besondere Herausforderung dar. Sie stellen gänzlich neue Anforderungen an die Qualifikation der Entwickler, die Sicherheitskultur des Unternehmens und die Qualität und Verfügbarkeit von Sicherheitswerkzeugen.

Matthias Honka (asknet AG) beleuchtet in seinem Vortrag auf dem kommenden KA-IT-Si-Event am **01.03.2012** die Gratwanderung zwischen agiler Softwareentwicklung und schneller Reaktion auf Kundenwünsche einerseits und Kontrollmaßnahmen zum Schutz digitaler Güter andererseits. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

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

März 2012	
01.03.	Rolltor für den Online-Shop (KA-IT-Si, Karlsruhe)
13.-15.03.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-16.03.	Black Hat Europe 2012 (Blackhat, Amsterdam/NL)
21.-22.03.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
26.-30.03.	CPSSE (Secorvo College, Karlsruhe)
April 2012	
15.-19.04.	Eurocrypt 2012 (IACR, Cambridge/UK)
16.-17.04.	a-i3/BSI-Symposium 2012 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
Mai 2012	
07.-12.05.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
23.-24.05.	Aktuelle Herausforderungen der Informations-sicherheit (Secorvo College, Karlsruhe)

Fundsache

Der Branchenverband BITKOM hat am 03.02.2012 die digitale Fassung einer Broschüre mit Sicherheitstipps für Smartphone-Nutzer publiziert, die für den IT-Gipfel 2011 erstellt worden war. Ein hilfreiches Handout auch für Unternehmen – wenn die wesentliche Nachricht auch ist: Wenn Ihr Sicherheit wollt, müsst Ihr Zeit investieren.

Impressum

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

ISSN 1613-4311

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

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

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

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

secorvo
security consulting

Secorvo Security News

März 2012

Wer hat Angst vorm Murmeltier?

Wir schreiben das Jahr 1990. Vor wenigen Jahren hat Apple den Macintosh vorgestellt und damit die IT-Landschaft nachhaltig geprägt. Da stellt Microsoft ein ähnliches Betriebssystem für die Geräte anderer Hersteller vor – und rollt damit den Markt auf. Kurz darauf breitet sich Schadsoftware für diese Systeme aus.

Zurück im Jahr 2012. Vor wenigen Jahren hat Apple das iPhone vorgestellt und damit die IT-Landschaft nachhaltig geprägt. Da stellt Google ein ähnliches Betriebssystem für die Geräte anderer Hersteller vor – und rollt damit den Markt auf. Kurz darauf breitet sich Schadsoftware für diese Systeme aus.

Einmal mehr scheint das Murmeltier zu grüßen. Allerdings dieses Mal ein Murmeltier mit Reißzähnen und auf Steroiden: Wir sind „always on" und per Netz angreifbar, Angreifer bewegen sich nicht mehr nur neugierig in fremden Gefilden, sondern haben sich längst ziel- und profitorientiert organisiert und können auf bewährte Angriffsmuster wie Drive-by-Infektionen, Phishing und Trojaner zurück greifen.

Auf Seiten der Verteidiger scheint die Zeit allerdings stehen geblieben zu sein: Anwender nutzen nur selten und widerstrebend ausreichend sichere Passcodes, Hersteller setzen auf die Stabilität ausgelieferter Software und haben die Notwendigkeit eines adäquaten Patch-Managements nicht erkannt, Sicherheitssoftware wird als Komforthindernis und unnützer Kostenfaktor wahrgenommen und nicht selten werden private Geräte an der Unternehmens-IT vorbei genutzt.

Höchste Zeit also, uns klar zu machen, dass das Smartphone von heute eben nicht der Computer von 1990 im Hosentaschenformat ist, auch wenn der Marktinnovator wie vor 28 Jahren noch immer Apple heißt. Sondern genau so sorgfältig geschützt werden muss, wie ein PC (oder Mac) anno 2012. Ehe das Murmeltier schmerzhaft zubeißt.

Inhalt

secorvo
security consulting

Security News

97 % vermeidbare Angriffe

Am 22.03.2012 hat Verizon mit dem 2012 Data Breach Investigations Report eine spannende Analyse publiziert. Auf 80 Seiten werden die Untersuchungsergebnisse von 855 Sicherheitsvorfällen des Jahres 2011 vorgestellt. Die Erkenntnisse sind erschreckend: So werden 96 % aller Angriffe als „nicht schwierig" eingestuft, und 97 % aller Vorfälle wären durch einfache Schutzmaßnahmen vermeidbar gewesen. Erkannt wurden die meisten der Vorfälle (85 %) erst nach Wochen, und in den seltensten Fällen von den Unternehmen selbst (8 %). In größeren Unternehmen konnte der Einfallsweg häufig nicht mehr rekonstruiert werden (31 %).

In den meisten Fällen gelang es einem Angreifer, Schadsoftware remote zu installieren (95 %). In größeren Unternehmen trugen in signifikantem Umfang *SQL-Injections* (12 %), Malware-Downloads (12 %), angeklickte E-Mail-Attachments (18 %) und *Drive-by-Infections* (18 %) zum Angriffserfolg bei: ein Beleg für unzureichende „Security Awareness" in den betroffenen Unternehmen.

Die Erkenntnisse der Studie erlauben den Schluss, dass isolierte Schutzmaßnahmen heute in der Regel zu kurz greifen und Unternehmen verstärkt auf ein umfassendes Schutzkonzept setzen und dabei vor allem ihre im Internet präsenten Anwendungen im Blick behalten müssen.

Dabei können offenbar Zertifizierungen – oder zumindest externe Auditierungen – helfen: Denn 96 % der von den analysierten Sicherheitsvorfällen betroffenen Unternehmen erfüllten nicht die Anforderungen von PCI DSS.

Smartphone-Security-Software

Android ist eines der Sicherheitsthemen, bei denen momentan viel Bewegung zu beobachten ist – im Guten wie im Schlechten. So präsentierte einerseits die NSA im Februar 2012 ein auf SELinux zurück gehendes, um zusätzliche Sicherheitsfunktionen erweitertes SE Android; in Deutschland wurden auf der CeBIT 2012 abhörsichere Handys auf Android-Basis vorgestellt.

Andererseits belegt eine am 07.02.2012 veröffentlichte Untersuchung der Universität North Carolina, dass ca. 0,02 % der Apps in Googles Market und etwa zehn bis 25mal so viele in unabhängigen Märkten Malware enthalten. Dabei behauptete Google am 02.02.2012, nach der Einführung eines automatisierten „Türstehers" bereits einen vierzigprozentigen Rückgang bösartiger Software im Market beobachtet zu haben.

Eine bösartige App zu laden ist jedoch nicht der einzige Weg, über den Schadsoftware auf ein Smartphone gelangen kann: Bei der RSA Konferenz präsentierten Forscher am 29.02.2012 eine funktionsfähige Drive-by-Infektion für Android-Geräte, deren „Marktwert" sie auf 15.000 US$ schätzten. Derweil berichtete die Intel-Tochter McAfee am 14.03.2012 von einem in Spanien gesichteten Android-Trojaner, der sich als vorgeblicher Generator von Sicherheitscodes tarnt, Online-Banking-PINs abphisht und auch gleich die zugehörigen mTANs umleitet – Online-Diebstahl ganz ohne Infektion des heimischen PC.

Dem am 15.03.2012 veröffentlichten Testbericht des unabhängigen Magdeburger Labors AV-Test zufolge erreichen hingegen nur zehn von 41 getesteten Virenscannern für Android eine Schadsoftware-Erkennungsrate von mehr als 90 %. Und auch für verlorene Geräte sieht die Statistik nicht gut aus: Am 09.03.2012 berichtete Symantec von den Resultaten eines Feldtests, bei dem nur etwa die Hälfte der als Köder „vergessenen" Smartphones zurückgegeben, aber die Daten fast aller Geräte vom Finder eingehend durchsucht wurden.

Derzeit sollten daher die Erwartungen an das bei Smartphones erreichbare Sicherheitsniveau generell nicht zu hoch angesetzt werden.

Neues iPad – neuer Crack...

Am 07.03.2012 hat Apple „The New iPad" samt iOS 5.1 vorgestellt. Es kommt mit neuem Prozessor und überarbeiteter Firmware daher und weckte bei Sicherheitsverantwortlichen in Unternehmen die Hoffnung, bestehende Sicherheitslücken, ob durch die Hard- oder die Software der iDevices bedingt, zu beheben. Doch dieser Traum währte nur kurz: Nach kaum einer Woche wurden erste Hinweise auf einen neuen Jailbreak publiziert und auch an älteren iDevices (iPhone 4S und iPad2) demonstriert.

Nicht nur die Geschwindigkeit war überraschend, mit der die Jailbreak Community agierte, sie stellte darüber hinaus auch noch gleich drei Ansätze vor, wie ein solcher Jailbreak in die Tat umgesetzt werden kann. Erstaunlich ist auch, dass einer dieser Ansätze auf einer bereits seit vier Monaten bekannten Schwachstelle beruht. Hier hat wohl die Qualitätssicherung für iOS 5.1 geschwächelt.

Den Sicherheitsverantwortlichen in den Unternehmen bleibt also auch weiterhin nur zu empfehlen, genau zu prüfen, welche Anwendungen und Informationen auf iDevices verwendet und gespeichert werden dürfen, und gegebenenfalls eine Sicherheitsüberprüfung der dienstlich eingesetzten iDevices durchzuführen.

Apple goes Datenschutz

Jedes iOS-Gerät verfügt über eine 40 Stellen lange Zeichenkette, mit der sich iPhone, iPad und iPod touch eindeutig identifizieren lassen: die so genannte UDID (*Unique Device Identifier*). Viele Apps benutzen diese UDID zur Erstellung detaillierter Nutzerprofile und zur Weitergabe an Werbetreibende. Datenschützern war dies schon lange ein Dorn im Auge und führte dazu, dass Apple bereits Mitte August 2011 ankündigte, dies zu ändern.

Nun ist es offenbar soweit: Apple verweigert zur Zulassung eingereichten Apps die Freigabe, wenn sie von der UDID Gebrauch machen. Entwickler, so Apple, sollen sich in ihren Apps zukünftig eigene Kennnummern erstellen und diese unabhängig voneinander verwalten. Eine Umstellung, die vor allem das Tracking individueller Geräte und ihrer Nutzer über mehrere Apps hinweg verhindern soll.

App-Entwickler müssen sich daher umstellen – für sie gibt es zukünftig keine zuverlässige Möglichkeit mehr, anhand der Hardware-ID festzustellen, dass eine App auf einem bestimmten, registrierten und zugelassenen Gerät läuft.

Schwachstellen-Hitliste

Das Forbes-Magazin hat nach eigenen Recherchen eine „Preisliste" für Schwachstellen einzelner Systeme und Anwendungen veröffentlicht. Sie wird derzeit von Apple angeführt: Für iOS-Schwachstellen werden angeblich bis zu 250.000 US$ bezahlt. Die Nachfrage scheint primär von „regierungsnahen Institutionen" zu kommen. Forbes nennt auch einige Kriterien, die erfüllt sein müssen, damit Höchstpreise bezahlt werden: Die Schwachstelle muss neuartig sein, muss dem Käufer exklusiv überlassen werden und darf auch dem Hersteller nicht mitgeteilt werden.

Dieses Interesse könnte aus den Strafverfolgungsbehörden stammen, die im Falle einer Beschlagnahme auch ohne Mitwirkung des Eigners auf die gespeicherten Daten zugreifen möchten, Oder aber es gibt noch Sicherheitsbehörden, deren Glaube an einen funktionierenden behördlichen „Online Trojaner", der sich in der Szene verbergen lässt, nach wie vor ungebrochen ist. Vielleicht arbeiten die Kollegen vom Nachrichtendienst aber auch schon an Stuxnet Mobile.

Secorvo News

Smartphones. Smartpads. Smartlecks.

Steve Jobs hat eine enorme Flutwelle ausgelöst, die Massen an Smartphones und Tablettcomputern in die Unternehmen schwemmt. Zwar können sich IT-Abteilungen eine Zeit lang „schützen", aber früher oder später muss sich auch der letzte standhafte CIO der Kraft der Mobile Device Welle ergeben – der Druck ist einfach zu hoch.

Doch was treibt die Anwender zum verstärkten Einsatz von Smartphones und Tablettcomputern? Was bedeutet der Einsatz solcher Geräte für die IT-Abteilungen, für die IT-Sicherheit und für das Unternehmen? Und welches Mobile Device Management System ist das Beste?

Diese Fragestellungen erörtert Christian Rückert (Netlution GmbH) in seinem Vortrag „Sicheres Mobile Device Management" auf dem nächsten KA-IT-Si Event am **26.04.2012.** Dabei werden neben den führenden Mobile Device Management Lösungen auch organisatorische Themen diskutiert. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Wir freuen uns auf Ihre Teilnahme!

Seminare in Q2

Das zweite Quartal 2012 startet bei Secorvo College mit dem Seminar PKI – Grundlagen, Vertiefung, Realisierung vom 23.-26.04.2012. Erfahren Sie mehr zu Konzeption, Implementierung und Nutzung von PKIs und sichern Sie sich kurzfristig noch Ihren Seminarplatz. Wir freuen uns auf Ihre Teilnahme.

Wenige freie Plätze gibt es auch noch für die nächste Schulung zum TeleTrusT Information Security Professional (T.I.S.P.) vom 07.-11.05.2012 mit anschließender Zertifikatsprüfung. Als Seminarteilnehmer bekommen Sie Ihr Exemplar des T.I.S.P.-Buchs zur Vorbereitung automatisch vorab zugesandt – Sie können das Buch natürlich auch unabhängig von einer Seminaranmeldung bestellen (ISBN: 978-3-942594-08-0).

Ebenfalls im Mai, vom 23.-24.05.2012, bieten wir mit dem zweitägigen Seminar Aktuelle Herausforderungen der Informationssicherheit einen kompakten Überblick zu wesentlichen Themen rund um die Weiterentwicklung der Informationssicherheit.

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

Veranstaltungshinweise

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

April 2012	
15.-19.04.	Eurocrypt 2012 (IACR, Cambridge/UK)
16.-17.04.	a-i3/BSI-Symposium 2012 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
Mai 2012	
07.-12.05.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
09.-10.05.	BvD Verbandstag 2012 (BvD e.V., Berlin)
23.-24.05.	Aktuelle Herausforderungen der Informations-sicherheit (Secorvo College, Karlsruhe)
Juni 2012	
11.-13.06.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
14.-15.06.	Datenschutzaudit (Secorvo College, Karlsruhe)
18.-19.06.	DuD 2012 (Computas, Berlin)

Fundsache

Wer hat nicht schon mal von den Sicherheitsprinzipien „Least privilege“ oder „Fail safe defaults“ gehört. Entgegen weit verbreiteter Annahmen handelt es sich hierbei um lang bekannte Prinzipien, die vor 37 Jahren von Saltzer und Schroeder in ihrem Aufsatz „The Protection of Information in Computer Systems“ vorgestellt wurden. Wem das Originalpapier zu trocken ist, dem könnte die Erklärung der Prinzipien anhand von Szenen aus Star Wars gefallen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Jörg Völker

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

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

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

secorvo
security consulting

Secorvo Security News

April 2012

Fluch der Vielfalt

Eigentlich ist es der Kern seines Erfolgs: Das „Multi-Purpose"-Konzept des Personal Computers eröffnete Rechenmaschinen einen Multi-Milliardenmarkt. Unvorstellbar heute, dass ein Computer nur eine spezielle Nutzung erlaubt: ein „Word-Prozessor" als Schreibmaschinenersatz, ein „Adress-Manager" statt des Registers im Kalender oder ein Handy, das nur zum Telefonieren taugt. Überlebende Exemplare solcher „Spezial-PCs" (gleichwohl Traum jedes Herstellers, da sie besseren Kopierschutz und höhere Margen bieten) verlieren stetig Marktanteile – wie derzeit Spielkonsolen und mp3-Player.

Das war in der Frühzeit des Computers anders. Ken Olsen, Präsident der Digital Equipment Corp., meinte noch 1977: „Es gibt keinen Grund, warum irgendjemand einen Computer in seinem Haus wollen würde." Im gleichen Jahr erschien der PET von Commodore, und vier Jahre später der IBM-PC. Damit war der Geist aus der Flasche: Heute erwarten wir, dass ein Computer, und heiße er auch „Smartphone" oder „Tablet", via Apps und Internet-Verbindung ein schier grenzenloses Angebot an Funktionen in sich vereint.

Für diese Funktionsvielfalt zahlen wir jedoch einen Preis. Wenn „alles geht", gehen auch Dinge, die wir uns weniger wünschen. Denn Schadsoftware ist vor allem eines – nämlich Software. Und ein „Multi-Purpose"-Gerät kann nicht entscheiden, ob eine App als Nutz- oder als Schadsoftware einzustufen ist. Auch den Hersteller können wir kaum dafür in Haftung nehmen, dass er auf seinen Geräten (fast) alles zulässt – denn genau das haben wir ja gewollt.

So kommt es spätestens beim Online-Banking zum Schwur. Denn ohne ein „One-Purpose-Device" zur Abwicklung unserer Bank-Transaktionen bleibt immer ein Trojaner-Risiko – das wir streng genommen schwerlich der Bank anlasten können, denn wir sind ja die Betreiber des „Alles-Geht-PC". Auch wenn die Einsicht schwerfällt: Wenn wir Sicherheit wollen, müssen wir auf Vielfalt verzichten. Und wenn wir – aus funktionalen Gründen oder aus Bequemlichkeit – nicht verzichten wollen, akzeptieren wir unvermeidlich das Risiko.

Inhalt

Security News

Zielgerade oder Sackgasse?

Auf der Crypto-Konferenz Mitte August 2005 wurde ein Angriff gegen SHA-1 präsentiert, der zwar noch nicht praktikabel aber effizienter als Brute-Force-Angriffe war. Seither wurde dieser Angriff verbessert, MD-5 praktisch gebrochen und auch ein Angriff auf die SHA-2-Familie schien in Reichweite.

In dieser Situation, in der die Welt der Krypto-Hashfunktionen, unverzichtbar für Signaturen, Integritätsschutz oder Schlüsselableitung, in Flammen stand, rief das NIST 2007 – ähnlich wie bei der erfolgreichen Entwicklung des AES – einen Wettbewerb für das Nachfolge-Hashverfahren SHA-3 ins Leben.

Nun biegt der Wettbewerb auf die Zielgerade ein: Fünf Finalisten sind benannt, unter denen noch in diesem Quartal der Sieger gekürt werden soll. Anders als beim AES hält sich das NIST jedoch bedeckt. Denn der vermeintliche Flächenbrand entpuppte sich als Strohfeuer: der SHA-2 erscheint heute sicherer als vor sieben Jahren. Und wie NIST-Vertreter Tim Polk am Rande des 83. IETF-Meetings Ende März 2012 erläuterte, wird SHA-3 in den meisten Anwendungsfällen langsamer sein als SHA-2.

Viele Mitglieder des Standardisierungsgremiums schrecken daher davor zurück, eine Unterstützung von SHA-3 verbindlich zu fordern. Angesichts langer Produktzyklen, die dazu führen, dass selbst SHA-2 heute noch nicht durchgängig genutzt werden kann, könnte dies jedoch ein riskantes Spiel sein: ein anderes „Fall-Back"-Verfahren gibt es nicht. Anwender sollten daher in den kommenden Jahren bei ihren Lieferanten auf eine Unterstützung des SHA-3 drängen.

Hintertür

Nicht auszurotten ist offenbar die Neigung von Herstellern, einen permanenten Remote-Zugang in ihre Geräte oder Programme in Gestalt versteckter „Hintertüren" einzubauen. So warnte das US-CERT am 24.04.2012 vor hard-kodierten Accounts in Produkten der Siemens-Tochter RuggedCom, die auch zwölf Monate nach der ersten Warnung nicht behoben sind, und wurde am 26.04.2012 bekannt, dass Telekom-Router vom Typ Speedport einen trivialen Zugang zu privaten WLAN-Netzen via Backdoor ermöglichen.

Diese Vorfälle reihen sich ein in eine lange Liste ähnlicher Probleme. Prominente Beispiele sind eine Schwachstelle in Siemens S7-Geräten vom August 2011 und eine kritische Lücke in Apple Quicktime vom August 2010.

Die Implementierung undokumentierter Zugänge zu Systemen oder Anwendungen ist, wie der Hausschlüssel unter der Fußmatte, eine Einladung für ungebetene Gäste – und gehört auch zu Testzwecken untersagt. Unternehmen sollten sich zumindest für kritische, von außen erreichbare Systeme die Abwesenheit solcher Hintertüren vom Hersteller zusichern lassen.

Haftung bei Filesharing

Das Bundesverfassungsgericht hat mit Beschluss vom 21.03.2012 gegenüber dem OLG Köln deutlich gemacht, dass es die Frage der Überwachungspflichten der Inhaber eines Internetanschlusses noch nicht für abschließend entschieden hält.

Das OLG Köln hatte unter Berufung auf das sog. WLAN-Urteil des BGH („Sommer unseres Lebens") vom 12.05.2010 Prüfpflichten des Anschlussinhabers auch für den Fall angenommen, dass der wahre Störer bekannt ist. Im entschiedenen Fall handelte es sich um den Sohn der Lebensgefährtin. Trotz entgegenstehender Rechtsprechung bspw. des OLG Frankfurt ließ das OLG Köln die Revision nicht zu. Das Bundesverfassungsgericht bejahte dagegen die Uneinheitlichkeit der Rechtsprechung und hielt die Revision für offensichtlich zulässig.

In einer Nebenerwägung hat das Bundesverfassungsgericht außerdem bewusst die Frage offen gelassen, ob die anwaltlichen Massenabmahnungen überhaupt eine taugliche und zu vergütende anwaltliche Leistung darstellen. Für die Unternehmen der Musikindustrie und ihre anwaltlichen Vertretungen bedeutet diese Entscheidung, dass mit weiteren Beschränkungen der postulierten Sorgfaltspflichten der Anschlussinhaber gerechnet werden muss – und dass Massenabmahnungen vielleicht in naher Zukunft kein funktionierendes Geschäftsmodell mehr darstellen.

Steueridentifikationsnummer

Mit Urteil vom 18.01.2012 hat der Bundesfinanzhof über die Rechtmäßigkeit der Vergabe der steuerlichen Identifikationsnummer entschieden. Schwerpunkt des Urteils bildet die Prüfung eines möglichen Verstoßes gegen das Grundrecht auf informationelle Selbstbestimmung der Betroffenen. Anhand der Gesetzesbegründung werden die hier Zwecke der Einführung sowie die über die Steueridentifikationsnummer abgewickelten Übermittlungen untersucht. Die Nummer gelte der Verfahrensvereinfachung, der Durchsetzung der Belastungsgleichheit der Steuerzahler und dem Bürokratieabbau. Dabei kommt das Gericht zu der Einschätzung, dass der Eingriff in die informationelle Selbstbestimmung durch die überragende Bedeutung der verfolgten Schutzziele gerechtfertigt wird.

Mit den Gefährdungen, die mit dem Eingriff verbunden sind, setzt sich das Gericht jedoch kaum auseinander und kommt so zum Schluss, dass die jeweiligen rechtlich verankerten Zweckbindungen der übermittelten Daten den Eingriff ausreichend beschränken. Die Frage, inwieweit bereits die Nummer als Mittel der Datenzusammenführung einen Eingriff darstellt, bleibt unberücksichtigt. Überhaupt werden als Risiken lediglich die gesetzlich vorgesehenen Einsatzzwecke betrachtet und der Eingriff infolge dessen als gering eingestuft.

Ähnlich kurz verneint das Gericht mit Verweis auf die pauschale Forderung nach technischen und organisatorischen Sicherheitsmaßnahmen in § 5 StIdV das Bestehen von Sicherheitsrisiken durch den Einsatz der Steueridentifikationsnummer.

Tatsächlich stellt das Urteil keine ernsthafte Auseinandersetzung mit den Datenschutzrisiken der Steueridentifikationsnummer dar. Die Rechtfertigung des Grundrechtseingriffs wird allein durch den Nutzen begründet – eine beängstigende Argumentation in einem freiheitlichen Rechtsstaat.

Secorvo News

Cloud kommt von Klauen. Oder?

Die Frage nach Sicherheit und Datenschutz beim Cloud Computing wird derzeit intensiv diskutiert. Wie lassen sich sensible Daten in der Wolke wirksam vor Missbrauch schützen? Und wie kann es gelingen, Anforderungen des Datenschutzrechts an Cloud-Computing-Dienste effektiv umzusetzen? Können diese Anforderungen überhaupt rechtsgestaltend und durch technisch-organisatorische Maßnahmen erfüllt werden, oder sollte man als verantwortungsbewusstes Unternehmen auf Cloud Computing verzichten?

Diesen und weiteren Fragen gehen Dirk Achenbach (Karlsruher Institut für Technologie) und Michael Knopp (Secorvo) beim nächsten KA-IT-Si-Event "Cloud kommt von Klauen. Oder?" am **10.05.2012** im Rahmen der Cloudzone 2012 nach. Die Impuls-Vorträge der beiden Referenten bringen die Herausforderungen auf den Punkt und skizzieren Lösungsansätze – anschließend heißt es „Ring frei" für eine intensive Diskussion.

Das Event beginnt diesmal ausnahmsweise bereits um 17 Uhr – und findet im Konferenzbereich der Messe Karlsruhe statt, wie gewohnt mit anschließendem Buffet-Networking. Als KA-IT-Si-Teilnehmer haben Sie außerdem die Möglichkeit, vorab die Cloudzone 2012 kostenfrei zu besuchen. Wir freuen uns auf Ihre Anmeldung!

4. Tag der IT-Sicherheit

Nach der hervorragenden Resonanz der vergangen Jahre freuen wir uns, Sie auch 2012 wieder zum **Tag der IT-Sicherheit**, einer Gemeinschaftsveranstaltung der KA-IT-Si mit der IHK Karlsruhe, dem CyberForum e.V. und KASTEL, einladen zu können. Die Veranstaltung beginnt am **12.07.2012** um 14.00 Uhr im Saal Baden der IHK Karlsruhe. Auch in diesem Jahr erwarten Sie wieder spannende Vorträge rund um die IT-Sicherheit. Die Möglichkeit zur Online-Anmeldung finden Sie Kürze unter http://www.ka-it-si.de. Wir freuen uns auf Ihre Teilnahme!

Nächste Seminare

Das kommende T.I.S.P.-Seminar vom 7.-11.05.2012 ist ausgebucht – die nächste Gelegenheit zur Zertifizierung bieten wir am 17.-21.09.2012 sowie am 12.-16.11.2012.

Genug Zeit, um sich bis dahin den Sommerurlaub mit dem T.I.S.P.-Buch zu versüßen – oder eines der beiden folgenden Seminare zu besuchen, die Ihre besondere Aufmerksamkeit verdienen: Aktuelle Herausforderungen der Informationssicherheit (23.-24.05.2012) bietet eine kompakte Auseinandersetzung mit wesentlichen aktuellen Technologien und Trends. In zwei Tagen werden sechs Themenfelder und zugehörige Schutzmaßnahmen diskutiert. Das Seminar Datenschutzaudit: Best Practice (14.-15.06.2012) zeigt auf, wie es gelingt, auch ohne gesetzliche Maßgaben, sinnvolle und effiziente Datenschutzaudits zu planen und durchzuführen. Basis hierfür sind die umfassenden Erfahrungen des Referententeams.

Alle weiteren Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Veranstaltungshinweise

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

Mai 2012	
07.-12.05.	T.I.S.P.-Schulung und Prüfung (Secorvo College, Karlsruhe)
09.-10.05.	BvD Verbandstag 2012 (BvD e.V., Berlin)
10.05.	Cloud kommt von Klauen. Oder? (KA-IT-Si, Kalrsuruhe)
23.-24.05.	Aktuelle Herausforderungen der Informationssicherheit (Secorvo College, Karlsruhe)
Juni 2012	
11.-13.06.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
14.-15.06.	Datenschutzaudit (Secorvo College, Karlsruhe)
18.-19.06.	DuD 2012 (Computas, Berlin)
19.-21.06.	Forensik (Secorvo College, Karlsruhe)
Juli 2012	
12.07.	4. Tag der IT-Sicherheit (IHK Kalrsruhe, CyberForum und KA-IT-Si, Karlsruhe)
21.-26.07.	Blackhat USA 2012 (Las Vegas/US)
26.-29.07.	DEFCON 20 (Las Vegas/US)

Fundsache

Am 23.04.2012 erschien die 8. Ausgabe des Magazins „hack in the box“ als pdf. Darin werden unter anderem Angriffsmethoden wie die Nutzung von Browser Exploit Packs und gezielte Angriffe auf den Windows-Kernel anschaulich dargestellt.

Impressum

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

ISSN 1613-4311

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

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

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

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

secorvo
security consulting

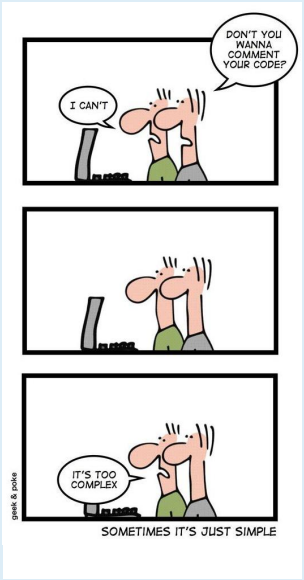
Secorvo Security News

Mai 2012

Die Geister, die ich rief...

Der Umgang mit unkontrollierter Komplexität wurde schon Goethes Zauberlehrling zum Verhängnis. Zunächst verlief alles nach Wunsch des Protagonisten: Er verschaffte sich durch Nutzung eines Reinigungstools eine Arbeitserleichterung. Leider wies dieses einige Schwachstellen auf und ließ sich durch den Lehrling nicht mehr kontrollieren – da wuchs dem Armen die Unbeherrschbarkeit seines Setups über den Kopf: "*Die ich rief, die Geister, werd ich nun nicht los.*"

Moderne Software-Entwicklung weist erschreckend viele Parallelen zu Goethes Lehrling auf. So verlässt sich heute die Mehrheit der Anwendungen auf externe Bibliotheken und Frameworks. Der eigene Code dient häufig nur noch der abstrakten Orchestrierung von wie durch Zauberhand bereit gestellter Funktionalität. Das tiefere Verständnis der genutzten Werkzeuge geht dabei verloren. Gerade die Sicherheit des Endprodukts aber hängt wesentlich von der Sicherheit der verwendeten Bibliotheken ab – und um die ist es nicht besonders gut bestellt: Aspect Security fand im März 2012 in jeder vierten Bibliothek bekannte Sicherheitsbugs. Der geregelte Umgang mit der Komplexität externer Komponenten muss zumindest die Kontrolle der genutzten Werkzeuge und den Überblick über Schwachstellen gewährleisten.



Der Weg zur Meisterschaft ist steinig. Aber nur die erlaubt den erlösenden Ruf: "*In die Ecke, Besen! Besen! Seids gewesen!*"

Inhalt

secorvo
security consulting

Security News

Puls des Internet

Das SSL Observatory der Electronic Frontier Foundation (vgl. SSN 12/2010 und 02/2012) widmet sich den SSL-Zertifikaten in „freier Wildbahn" samt den ausstellenden Trust Centern. Eine gute Ergänzung bietet SSL Pulse, eine am 25.04.2012 publizierte Statistik über die Sicherheit von SSL-Websites, bei der unter anderem die Konfiguration der angebotenen SSL/TLS-Protokollversionen und Cipher Suites geprüft wurde. In diese Übersicht flossen die Ergebnisse von ca. 200.000 SSL Server Tests der Qualys SSL Labs ein.

Beunruhigendes Ergebnis: ca. drei Viertel aller Sites sind anfällig gegen die im September 2011 publizierte BEAST Attacke, die es einem Angreifer unter bestimmten Umständen ermöglicht, SSL/TLS-geschützte Passwörter oder Cookies zu ermitteln. Die technische Analyse verrät naturgemäß nicht, ob die betroffenen Serverbetreiber diese Bedrohung als zu gering bewerten, um die mit einem Update oder Einschränkungen verbundenen Gegenmaßnahmen zu ergreifen, oder ob sie die Attacke schlicht nicht kennen. Betreibern öffentlicher SSL/TLS-Server ist jedenfalls sehr zu empfehlen, den eigenen Server dem (kostenfreien) SSL Server Test zu unterziehen – und sei es nur als Rückversicherung, dass die beabsichtigte Konfiguration korrekt umgesetzt ist – bevor andere feststellen, dass der Server doch nicht zum letzten Viertel zählt.

Warnung vor Hotspots

Am 08.05.2012 warnte das Internet Crime Complaint Center (IC3) des FBI, dass Laptops, die sich in öffentliche (Hotel-) WLANs einbuchen, eine Verseuchung durch Malware befürchten müssen. Diese Warnung reiht sich ein in ähnliche Hinweise auf versteckte Manipulationen von Betreibern öffentlicher Hotspots – und kann Techniker erstmal nicht überraschen.

Mit zunehmender Moblilität steigt jedoch die Gefahr, dass Nutzer öffentlichen Hotspots blind vertrauen. Verlässlichen Schutz bietet die Nutzung des VPN-Zugangs der eigenen Firma oder ein vertrauenswürdiges „Personal VPN". Mindestens aber sollte eine „Personal Firewall" Zugriffe von außen abblocken und jeder mobile Nutzer sicher stellen, dass er nicht über ungesicherte Verbindungen auf kritische Dienste zugreift oder vertrauliche Informationen übermittelt.

Vertrauenswürdiges Internet

Am 10.05.2012 kündigte die NCC Group an, das verlorene Vertrauen in das Internet durch die Schaffung einer neuen Top-Level-Domäne (TLD) *.secure* wieder zurück zu gewinnen. Zuteilungen für Domänen unterhalb der neuen TLD sollen nur Betreiber erhalten, die Mindestsicherheitsstandards für ihre Systeme vorweisen können.

Details hierzu werden zur Zeit abgestimmt. Es ist aber bereits bekannt, dass die durchgängige Verwendung von SSL/TLS für Webseiten, die Absicherung von DNS mit DNSSEC und die Verwendung von DKIM für E-Mails gefordert werden. Auf der FAQ-Seite wird angekündigt, dass die Dokumente von Antragstellern durch den Betreiber Artemis überprüft werden.

Aufschlussreich ist der Abschnitt über die Kosten einer *.secure*-Domäne: "*.SECURE domains provide premium value to registrants and their customers an will be priced accordingly.*" Die Erfindung einer Gelddruckmaschine? Auch wenn bereits begründete Zweifel am tatsächlichen Sicherheitsgewinn laut werden, ist eines definitiv sicher: Die indische Regierung wird mit ihrer Domäne kaum glücklich werden: https://in.secure

Neues TK-Recht

Am 04.05.2012 ist das Gesetz zur Änderung telekommunikationsrechtlicher Regelungen in Kraft getreten. Ziel des Gesetzes ist die Stärkung der Verbraucherrechte. Für die Nutzung von Standortdaten der Nutzer wurde in § 98 Abs. 1 TKG eine neue Informationspflicht eingeführt: Der Gerätenutzer – nicht der Anschlussinhaber – muss bei jeder Standortermittlung hierüber per Textmitteilung in Kenntnis gesetzt werden.

Wird der Schutz personenbezogener Daten verletzt, sind neben der BNetzA der Bundesdatenschutzbeauftragte, in schwer wiegenden Fällen die Betroffenen zu informieren. § 109a Abs. 3 TKG verpflichtet die Anbieter ein Verzeichnis über Datenschutzverletzungen zu führen. Die hierdurch entstehende Pflicht zur Selbstanzeige soll durch Verweis auf das Verwertungsverbot in § 42a Satz 6 BDSG rechtsstaatlich entschärft werden.

Die Verpflichtung zur Erstellung und Vorlage eines Sicherheitskonzepts (§ 109 TKG) wurde ausgedehnt auf die Anbieter von Telekommunikationsdiensten. Außerdem wurde entsprechend § 42a BDSG eine Meldepflicht bei Sicherheitsverletzungen in § 109 Abs. 5 und § 109a TKG eingeführt. Die Bundesnetzagentur kann daraufhin den Betreiber oder Dienstanbieter zu einem ausführlichen Bericht verpflichten. Außerdem kann sie nach Abs. 7 dem Betreiber oder Dienstanbieter eine Auditierung auferlegen.

Mit dem Änderungsgesetz zielt der Gesetzgeber darauf, den Datenschutz durch Transparenzpflichten zu stärken. Zwar ist dies zu begrüßen, allerdings muss befürchtet werden, dass gehäufte Transparenz irgendwann zu Abstumpfung der Adressaten führt und damit ihre Wirkung verlieren wird.

Nmap 6

Pünktlich zum nahenden World IPv6 Day hat Gordon „Fyodor" Lion am 21.05.2012 ein neues Release des Portscanners Nmap herausgebracht – passenderweise mit Versionsnummer 6. Eines der Hauptfeatures besteht denn auch in voller IPv6-Unterstützung. Neben den „üblichen" Verbesserungen (schnellere Scan-Engine, mehr und ausgefeiltere Skripte) zeichnet sich ab, dass die Grenzen zwischen Portscanner und Schwachstellenscanner immer mehr verwischen: auch das neue Release von Nmap setzt seinen Vormarsch in Richtung Webanwendungsscanner fort.

Mit dem Einsatz von IPv6 müssen sich Administratoren und Pentester von der beliebten Praxis verabschieden, ein Subnetz nach laufenden Diensten zu durchscannen – das verbietet die schiere Größe des Adressraums von IPv6-Subnetzen. Alternative Ansätze zum Auffinden von Hosts sind beispielsweise in RFC 5157 beschrieben.

Ein Tool, das dabei nützlich werden könnte, ist das neue Nping, das zur Familie der Nmap-Tools hinzugekommen ist; dessen IPv6-Unterstützung ist aber derzeit noch als „experimental" eingestuft.

Einer der Zukunftspläne für Nmap sieht vor, neue NSE-Scripte und OS-Fingerprints über einen Update-Service bereit zu stellen. Aber auch so bleibt Nmap in absehbarer Zukunft eines der wichtigeren Test-Tools für Admins und Pentester.

Neuer Ripper

Seit dem 06.05.2012 steht Version 2.5 des forensischen Werkzeugs RegRipper für Windows zur Verfügung. Bisherige Plugins funktionieren nicht nur weiterhin; mit ihnen können nun die Metadaten einzelner Dateien wie z. B. Benutzerprofilen (NTUSER.DATs) oder Dateigruppen wie Verknüpfungen (*.LNKs) direkt aus den schreibgeschützten Volume Shadow Copies (VSC) abgefragt werden. Dadurch kann auf das fehleranfällige Kopieren von Dateien aus VSCs verzichtet werden. Mit Unterstützung des neuen Dateisystems ReFS ist RegRipper bereits für Windows 8 gerüstet.

Secorvo News

Seminare für alle

Sie haben Verstärkung im Team bekommen? Herzlichen Glückwunsch! Als Steilkurs für die neue Kollegin oder den neuen Kollegen empfehlen wir unser Seminarpaket aus "Sicherheitsmanagement heute" und "IT-Sicherheit heute". Und falls an Ihrer Bürowand noch kein T.I.S.P.-Zertifikat prangen sollte: Das nächste Zertifizierungsseminar bieten wir vom **17.–21.09.2012**. Das T.I.S.P.-Buch erhalten Sie mit der Anmeldung vorab – als erbauliche Urlaubslektüre. Weitere Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

4. Tag der IT-Sicherheit

Gemeinsam mit der IHK Karlsruhe, dem Cyber-Forum e.V. und KASTEL veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **12.07.2012** bereits zum vierten Mal den "Tag der IT-Sicherheit". Die Veranstaltung beginnt um 14.00 Uhr im Saal Baden der IHK Karlsruhe. Auch in diesem Jahr erwartet Sie wieder ein spannendes Vortragsprogramm. Ausgewiesene Experten stellen den Stand der Entwicklung bei Hackerangriffen („Live Hacking") und Schutzstrategien in Theorie und Unternehmenspraxis vor. Gelegenheit zum fachlichen und persönlichen Austausch mit Referenten, Teilnehmern und Ausstellern bietet die „Networking-Pause".

Nach der positiven Ressonanz der vergangenen Jahre rechnen wir mit zahlreichen Teilnehmern und empfehlen daher eine frühzeitige Anmeldung. Wir freuen uns auf Ihre Teilnahme!

Sicher – sicherer – Android?

Besitzern von Smartphones bietet sich eine reiche, ständig größer werdende Auswahl von Apps. Aber wie sicher ist eine Mobile-Banking-App, wenn das neueste Tablet-Spiel "unerwünschte Nebenwirkungen" hat? Wie gut können sensitive Daten in Unternehmens-Apps geschützt werden, wenn die Smartphone-Besitzer daneben so viele Apps eigener Wahl installieren, wie der Speicher hergibt?

Mit diesen und anderen Fragen setzt sich Hans-Joachim Knobloch (Secorvo) beim nächsten KA-IT-Si Event am **21.06.2012** auseinander. Sein Vortrag "Apps - tickende Bomben im Bauch des Androiden?" gibt einen Überblick über die Sicherheitsarchitektur von Android, beleuchtet verschiedene Bedrohungsszenarien und stellt Mechanismen sowie Konzepte zur sicheren Gestaltung von Android-Apps vor.

Beginn der Veranstaltung ist um 18.00 Uhr im Panoramasaal der IHK Karlsruhe. Um Anmeldung wird gebeten.

Veranstaltungshinweise

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

Juni 2012	
18.-19.06.	DuD 2012 (Computas, Berlin)
19.-21.06.	Forensik (Secorvo College, Karlsruhe)
21.06.	Sicher – sicherer – Android? (KA-IT-Si, Karlsruhe)
Juli 2012	
12.07.	4. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
21.-26.07.	Blackhat USA 2012 (Las Vegas/US)
26.-29.07.	DEFCON 20 (Las Vegas/US)
August 2012	
06.-08.08.	DFRWS 2012 (DFRWS, Washington/US)
08.-10.08.	21th USENIX Security Symposium (Usenix, Bellevue/US)
19.-23.08.	Crypto 2012 (IACR, Santa Barbara/US)
20.-24.08.	SecSE 2012 (SINTEF, Prag/CZ)
27.08.	Sommerakademie 2012 (ULD Schleswig-Holstein, Kiel)

Fundsache

Kaum zu glauben: Die schier unausrottbare SQL-Injection – der „Buffer-Overflow der Web-Applikationen" – wird 2012 bereits 14 Jahre alt. Die Erstveröffentlichung erschien 1998 in Heft 54 des Phrack Magazine (Volume 8).

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Safuat Hamdy, Kai Jendrian (Editorial), Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting. Abdruck des Cartoons mit freundlicher Genehmigung von geek & poke.

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

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news"). Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Juni 2012

Süßes Gift

Mit Begriffen im schnörkellosen Suchfenster fing es an. Bald ersetzte ‚Googeln' mühsame Bibliotheksrecherchen. Es folgte der Online-Stadtplan: Statt unhandlicher Faltkarten ein Klick auf die Anschrift, und der Routenplaner von Google Maps zeigt uns den Weg. Vor dem nächsten Termin (abgerufen aus dem Google-Kalender) schnell ein Blick in die Nachrichten. Ohne Kleingeld und Kiosk, voluminöse Papierformate und druckschwarze Finger, bequem via Google News und Chrome-Browser auf dem Display des Android-Smartphones. Die Zeit reicht noch für ein Picasa-Upload des Enkel-Fotos für die Oma und eine Youtube-Recherche, da kommt via Gmail ein Vertragsentwurf herein – auf Portugiesisch. Schnell in den Google-Übersetzer geschoben, ein wenig Nachbearbeitung in Google-Docs, und schon liegt eine verständliche Fassung für die Google-Talk-Konferenz vor...

Geräuscharm hat sich Google in unser Leben geschlichen. Betört von der Verlockung unentgeltlicher, benutzerfreundlicher Online-Dienste opfern wir willig Zug um Zug unsere Unabhängigkeit: Nicht mehr lange, und Google wird auch unsere Online-Shops, Zahlungssysteme, Fernsehsender und Webseiten betreiben. Und wir werden uns fragen: Wie ging eigentlich Leben ohne Google?

38 Mrd. US-Dollar Umsatz erwirtschaftete Google 2011, das entspricht etwa 5,5 % des deutschen Steueraufkommens. Damit finanziert Google seine „Gratiskultur". Mitbewerber werden das nicht ewig durchhalten – und aufgeben. Und dann wird, Schritt für Schritt, auch Googles Gratiskultur zu Ende gehen. Aus Mangel an Alternativen werden wir – abhängig und betört – die Zeche zahlen.

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, (...) kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden", konstatierte das BVerfG im Volkszählungsurteil 1983. Der Preis der Bequemlichkeit ist manchmal – die Freiheit.

Inhalt

secorvo
security consulting

Security News

PKI ist schwierig

Wie Microsoft am 03.06.2012 einräumte, trug der Flame-Trojaner eine gültige Code-Signatur mit einem Zertifikat, das auf die Microsoft Root CA zurück geht und eigentlich von Microsoft für die Lizenzkontrolle von Terminal Servern erstellt wurde.

Kryptologen und Verschwörungstheoretiker wird interessieren, dass von den Flame-Autoren dafür eine MD5-Hashkollision genutzt wurde, die nicht nach dem bisher bekannten Schema konstruiert wurde. Noch frappierender ist das Eingeständnis, dass dies zumindest für Windows XP gar nicht nötig gewesen wäre – weil es auch Zertifikate ohne die Kennzeichnung „für Code-Signing" akzeptiert.

Immerhin ergriff Microsoft die Gelegenheit, im PKI-Bereich durchzugreifen: Künftig wird Windows (einschließlich XP) für die meisten Zwecke Zertifikate für RSA-Schlüssel kleiner 1024 Bit Schlüssellänge zurückweisen. Zudem werden – weil man der Sperrung mittels CRLs nicht recht traut – nicht nur neue CA-Zertifikate über eine Certificate Tust List in Windows nachgepflegt, sondern auch zu sperrende CAs per Windows Update als „nicht vertrauenswürdig" gekennzeichnet. Den Anfang machten die an den Terminal-Server-Lizenzen beteiligten MS-CAs. Der eigentliche Vertrauensanker in der PKI-Praxis sind also nicht die Root-CAs, sondern die Betriebssystem- und Browser-Hersteller.

Passwörter sind schwierig

Immer noch schützen hauptsächlich Passwörter digitale Identitäten im Web. Dabei droht die Gefahr weniger von Brute-Force-Angriffen auf Webanwendungen – denn dagegen helfen schon achtstellige Passwörter, die sich nicht in Wörterbüchern finden. Gravierender sind Sicherheitsvorfälle, bei denen die Passwort(hash)datenbanken von Anbietern kompromittiert werden – wie in diesem Monat bei LinkedIn, eHarmony und Last.fm geschehen. Offenbar wurden in allen Fällen bekannte Mechanismen zum Schutz von Passwortdatenbanken vor Offline-Angriffen nicht eingesetzt. Auch angesichts vereinzelter Kritik an diesen Mechanismen – Sicherheit erfordert immer einen Trade-Off.

Solange Entwickler Passwort-Datenbanken nicht angemessen schützen, sollten Sie für unterschiedliche Dienste auch unterschiedliche Passwörter verwenden. Und „Finger weg" von so genannten Passwort-Checkern: Probieren Sie mal The Passwort Security Checker aus – allerdings besser mit einem fiktiven Passwort...

Signatur-Harakiri

Am 04.06.2012 hat die Europäische Kommission den Entwurf einer Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vorgestellt. Der Entwurf soll die Signaturrichtlinie (RL 1999/93/EG) ersetzen, die als lückenhaft und überarbeitungsbedürftig gilt. Die Verordnung, die in den Mitgliedstaaten direkt anwendbares Gesetz wäre, soll die bislang nicht erreichte Harmonisierung herstellen und nimmt zudem beträchtliche Erweiterungen vor. Ziele sind die Entwicklung eines digitalen Binnenmarktes, die Förderung öffentlicher Dienste, die Anregung des Wettbewerbs und die Verbesserung der Benutzerfreundlichkeit.

Die Verordnung stellt „qualifizierte Siegel" an die Seite qualifizierter elektronischer Signaturen, führt qualifizierte Zertifikate zur Website-Authentifizierung und qualifizierte elektronische Zustelldienste ein und regelt die bereits bekannten Zeitstempel samt den zugehörigen Beweisvermutungen. Die Regelung der Zustellungsdienste fällt deutlich knapper aus als der deutsche De-Mail-Ansatz, ignoriert jedoch mit seiner Beweisvermutung auch eine Vielzahl wichtiger Detailfragen, wie etwa die der Empfangseröffnung. Die Kommission wird ermächtigt, Detailregelungen zu treffen.

Spätestens mit den direkt geltenden Beweisvermutungen greift die Verordnung tief in die nationalen Rechtsordnungen ein, ohne Rücksicht auf jegliche bestehende Systematik. Zu mehr Rechtssicherheit wird ein solches Vorgehen kaum führen.

Die Kommission geht offenbar von einer völlig verkürzten Problemanalyse aus. Während die Stellungnahme der Bundesregierung immerhin fehlende Nutzerakzeptanz und ein Auseinanderfallen von primären Nutznießern und Kostenträgern anspricht, fehlen in den Augen der Kommission lediglich europaweite Interoperabilität und die ergänzten weiteren Dienste für den Durchbruch der Signaturen. Bei dieser Förderung braucht das Konzept der elektronischen Signatur eigentlich keine Feinde mehr.

Safer Browsing

Am 21.05.2012 jährte sich die „Safe Browsing"-Initiative von Google zum fünften Mal. Nach eigenen Angaben identifiziert Google täglich knapp 10.000 Malware-verseuchte Webseiten und warnt deren Betreiber, ISPs und CERTs – sowie bis zu 14 Mio. Suchanfragen. 2012 summierten sich die entdeckten Phishing-Sites auf über 300.000 pro Monat. Das ist mehr als ein Tropfen auf dem heißen Stein – ein wichtiger Beitrag zur Eindämmung der zunehmenden Online-Kriminalität.

Große Fische

Angreifer, die Online-Banking-Nutzer ins Visier nehmen, haben seit Jahren mit heftiger Gegenwehr der Kreditinstitute zu kämpfen. Mit iTANs, mTANs und TAN-Generatoren, Überweisungslimits und hartem Vorgehen gegen „Geldboten", die – oft reichlich naiv – ihre Konten für die betrügerischen Überweisungen zur Verfügung stellen, halten die Banken die Schäden bislang in Grenzen.

Nun stehen offenbar erstmals Firmenkunden im Fokus der Angreifer, wie McAfee in einem am 26.06.2012 publizierten White Paper ausführt. Zwar ist das erfolgreiche Einschleusen von Trojanern in Unternehmen oft ungleich schwieriger; dafür ist der finanzielle Anreiz deutlich größer, schließlich weisen Geschäftskonten in der Regel eine erheblich höhere Liquidität auf. Zudem bleiben gut getarnte Transaktionen mit mittelgroßen Beträgen länger unentdeckt – und erleichtern es einem Angreifer, die Spuren zu verwischen.

Spätestens jetzt ist es an der Zeit, die Führung des Firmen-Online-Kontos, sofern noch nicht geschehen, auf einen separaten Rechner und Token-Nutzung umzustellen – denn iTANs bieten keinen ausreichenden Schutz vor Trojanern, die sich als „Man-in-the-Browser" im System einnisten.

IPv6 World Launch Day

Auf den World IPv6 Day 2011 folgte am 06.06.2012 der World IPv6 Launch Day: Seitdem sind diverse Internet-Sites dauerhaft über IPv6 erreichbar. Der IPv6-Support der Hersteller wird auch im Home-Bereich immer besser, und verschiedene ISPs planen, auch im Consumerbereich IPv6 anzubieten. Diesmal ist die „Drohung" IPv6 wohl ernst gemeint.

Eine übereilte Einführung kann jedoch fatale Folgen für Sicherheit und Betrieb der eigenen Netze haben. So wurde auf dem IPv6-Kongress am 10.-11.05. 2012 der Aufwand einer IPv6-Umstellung mit der Behandlung des Y2K-Problems verglichen. Die größte Gefahr bestehe darin, IPv6 wie IPv4 mit längeren Adressen zu betreiben, da IPv6 eine deutlich andere Architektur aufweist. Ein typischer Stolperstein ist beispielsweise NAT, das bei IPv6 so nicht vorgesehen ist. So langsam sollte die Beschäftigung mit der Umstellung daher auch bei Sicherheitsverantwortlichen oben auf der Agenda stehen.

Secorvo News

4. Tag der IT-Sicherheit

Bereits zum vierten Mal findet am **12.07.2012** der "Tag der IT-Sicherheit" statt - eine Gemeinschaftsveranstaltung der KA-IT-Si mit der IHK Karlsruhe, dem CyberForum e.V. und KASTEL.

Im Rahmen der diesjährigen Keynote „Hacking 2012" werden aktuelle Entwicklungen bei Angriffsmethoden aufgezeigt und einige Bedrohungen live vorgeführt. Anschließend erwarten Sie weitere spannende und praxisnahe Vorträge zu den Themen Hardware- und Softwaresicherheit, Verschlüsselung und Onlinebanking, begleitet von fachlichem und persönlichem Networking mit Referenten, Teilnehmern und Ausstellern. Beginn ist um 14.00 Uhr im Haus der Wirtschaft/Saal Baden der IHK Karlsruhe. Wir freuen uns auf Ihre Anmeldung!

Zertifiziertes Wissen

Wenn Sie planen, noch 2012 das T.I.S.P.-Zertifikat zu erwerben, empfehlen wir Ihnen, den Termin jetzt zu wählen: Für das Seminar vom **17.-21.09.2012** stehen noch wenige freie Plätze zur Verfügung; ein weiteres Seminar bieten wir vom **12.-16.11.2012** an. Die Autoren des T.I.S.P.-Buches (im Seminarpreis enthalten) bereiten Sie persönlich auf die Zertifikatsprüfung vor.

Sicherheitslöcher in Software sind meist die Ursache von Sicherheitsvorfällen. Damit Ihre Webanwendungen und Programme dagegen gefeit sind, sollten Sie Ihren Entwicklern das Seminar „Certified Professional for Secure Software Engineering (CPSSE)" vom **24.-27.09.2012** ans Herz legen. Dort erfahren sie, worauf es bei der Entwicklung sicherer Software ankommt. Das CPSSE-Zertifikat bestätigt ihre persönliche Qualifikation – und belegt den Qualitätsanspruch Ihres Unternehmens.

Alle weiteren Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Erfolgreiche KA-IT-Si

Die Events der KA-IT-Si verzeichnen in diesem Jahr einen besonders großen Zulauf – fast 300 Teilnehmer haben die Veranstaltungen in der ersten Jahreshälfte besucht. Mit der MF APP AG und der proRZ Rechnenzentrumsbau GmbH konnten außerdem zwei neue Partner für die Initiative gewonnen werden.

Wir danken Ihnen für Ihr Interesse an unseren Events und freuen uns auf ein Wiedersehen nach der Sommerpause. Am **13.09.2012** meldet sich die KA-IT-Si mit der nächsten Veranstaltung zurück.

Informationen zum Vortrag und die Möglichkeit zur Anmeldung gibt es demnächst auf http://www.ka-it-si.de.

Veranstaltungshinweise

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

Juli 2012	
12.07.	4. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
21.-26.07.	Blackhat USA 2012 (Las Vegas/US)
26.-29.07.	DEFCON 20 (Las Vegas/US)
August 2012	
06.-08.08.	DFRWS 2012 (DFRWS, Washington/US)
08.-10.08.	21th USENIX Security Symposium (Usenix, Bellevue/US)
19.-23.08.	Crypto 2012 (IACR, Santa Barbara/US)
20.-24.08.	SecSE 2012 (SINTEF, Prag/CZ)
27.08.	Sommerakademie 2012 (ULD Schleswig-Holstein, Kiel)
September 2012	
17.-21.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
18.09.	Anwendertag IT-Forensik 2012 (Fraunhofer SIT, Darmstadt)
24.-27.09.	CPSSE-Schulung (Secorvo College, Karlsruhe)
25.-26.09.	D·A·CH Security (GI/OCG/BITKOM/SI/TeleTrusT, Konstanz)

Fundsache

Am 12.06.2012 hat das US-amerikanische NIST eine Überarbeitung der Special Publication SP 800-121 „Bluetooth-Security“ veröffentlicht, die nun auch die Schutzmechanismen von Bluetooth v4.0 umfasst.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

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

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

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

secorvo
security consulting

Secorvo Security News

Juli 2012

Als gestern noch Zukunft war

Erinnern Sie sich noch? Bush ist neuer US-Präsident, Scharping tritt als Bundesverteidigungsminister zurück. Der Kanzler heißt Schröder, der Formel-1-Weltmeister wieder Schumacher und der gerade erst eingeführte Euro „Teuro“: wir schreiben das Jahr 2002. Noch immer gibt es kein betriebsbereites UMTS-Mobilfunknetz, obwohl die Lizenzen schon seit zwei Jahren versteigert sind. Gerade erst wurde der AES nach dreijährigem Auswahlverfahren zum Nachfolger des DES gekürt. Online-Banking-Transaktionen werden mit einfachen TAN-Listen autorisiert, Apple hat den ersten iPod vorgestellt. Niemand weiß, was ein ‚Smartphone' sein soll, Compaq wird von HP übernommen und Mannesmann Mobilfunk heißt nun Vodafone D2. Und im Juli erscheint die erste Ausgabe der „Secorvo Security News“.

Zehn Jahre, 480 Seiten und knapp 1.000 Nachrichten liegt dieses Ereignis nun zurück. Die Themen und Herausforderungen, die uns in den vergangenen zehn Jahren beschäftigt haben, werden uns zweifellos auch im kommenden SSN-Jahrzehnt begleiten.

Allerdings wird es nicht leichter für IT-Sicherheit und Datenschutz. Daten werden in wachsendem Umfang Cloud-Diensten anvertraut, die IT wird sich mehr und mehr von einer Infrastruktur- zu einer Service-Dienstleistung entwickeln. Die Endgeräte werden kleiner, leistungsfähiger und unabhängiger – und zukünftig, ob wir das wollen oder nicht, auch direkt mit anderen Endgeräten (POS-Terminals, Ticket-Kontrollgeräten, medizinischen Geräten, Zugangssystemen, SmartMetern etc.) kommunizieren. Immer mehr digitale Spuren werden unser Verhalten detailliert protokollieren; zugleich werden zentrale Konfiguration und Kontrolle der Endgeräte schwieriger – eine Entwicklung, der das geltende Datenschutzrecht und heutige IT-Sicherheitskonzepte nur begrenzt gewachsen sind.

Wir werden diese Entwicklung weiterhin kritisch begleiten. Wenn Sie uns anlässlich des zehnten Geburtstags der SSN dazu ermutigen möchten, freuen wir uns über einen Kommentar von Ihnen.

Inhalt

secorvo
security consulting

Security News (2002-2012)

Neuer SHA-Standard

Am 28.08.2002 gab das US-amerikanische NIST einen neuen Secure Hash Standard (SHS) bekannt, der den SHS (FIPS PUB 180) aus dem Jahr 1993 ab 01.02.2003 ersetzt. FIPS PUB 180-2 umfasst neben SHA-1 drei weitere Algorithmen, die jeweils einen 256 (SHA-256), 384 (SHA-384) und 512 (SHA-512) bit langen Ausgabewert erzeugen. Die neuen Hashfunktionen ermöglichen ein höheres Sicherheitsniveau für digitale Signaturen: Ab einer Schlüssellänge von 1.500 bit (RSA) bzw. 168 bit (DSS) ist bislang der Hashwert das kryptografisch schwächste Glied.

SSN 09/2002 – Selbst zehn Jahre später wird der Standard noch nicht durchgängig unterstützt.

Security Tools: „Top 75"

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

SSN 03/2003 – Diese auf heute 125 Tools erweiterte Liste bietet immer noch einen guten Überblick.

SigG-Novelle

Am 19.11.2004 hat der Bundestag in zweiter und dritter Lesung das deutsche Signaturgesetz (SigG) novelliert. Zentrale Änderung: Für die Beantragung eines qualifizierten Signaturschlüssel-Zertifikats genügt nunmehr ein PIN-TAN-basierter Prozess – der eigenhändig unterschriebene Antrag mit Vorlage des Personalausweises ist bei bestehenden Kunden nicht mehr erforderlich. Damit kommt die Novelle den deutschen Banken entgegen, die eine Vereinfachung der Prozesse gefordert hatten, um ihre Bankkarten zu Signaturkarten aufwerten zu können. Die Bundesregierung erhofft sich mit diesem Schritt eine erhebliche Ausweitung der nach wie vor nur marginalen Verbreitung qualifizierter Signaturen; freilich fehlen trotz dieser Verfahrensvereinfachung noch immer die seit vielen Jahren versprochenen Anwendungen für „Otto Normalsignierer", die für ihn einen erkennbaren Zusatznutzen darstellen und einen Technikwechsel rechtfertigen.

SSN 11/2004 – Auch 2012 sind SigG-Signaturen per Bankkarte und Anwendungen dafür Mangelware.

iTAN

Auf Phishing-Angriffe reagieren jetzt auch die deutschen Banken mit zusätzlichen Sicherheitsmerkmalen. Die Postbank meldete am 07.08.2005, dass sie ihr PIN-TAN-Verfahren um ein iTAN genanntes Merkmal ergänzt: Zukünftig sind die TAN auf der Liste indexiert. Bei jeder Transaktion schickt der Bankserver den Index, und nur die passende TAN ist gültig. Dieser einfache Challenge-Response-Mechanismus entwertet abge-"phishte" TAN. Die iTAN schützt nicht vor allen Angriffen, erhöht aber die Sicherheit des Online-Bankings deutlich.

SSN 08/2005 – Der Anfang vom Ende des PIN-TAN-Verfahrens. Die Jagd hat begonnen.

WAF-Auswahlhilfe

Das Web Application Security Consortium (WASC) hat die Version 1.0 der „Web Application Firewall Evaluation Criteria" vorgelegt. Dabei handelt es sich um eines der ersten Dokumente, in welchem Entscheidern und Firewall-Architekten ein ausführlicher Katalog wichtiger Anforderungen an eine Web Application Firewall (WAF) zur Verfügung gestellt wird. Diese Anforderungsliste erleichtert den Vergleich, die Bewertung und die Auswahl geeigneter WAF-Lösungsansätze und verfügbarer Produkte

SSN 01/2006 – Noch immer sind WAFs kein Standard-Schutzmechanismus von Web-Applikationen.

Der König ist tot ...

... es lebe der König: Am 01.07.2007 wurde der ISMS-Standard ISO/IEC 17799:2005 vom Technical Committee JTC 1/SC 27 in ISO/IEC 27002:2005 „Information technology – Security techniques – Code of practice for information security management" umbenannt. Inhaltlich blieb er unverändert. Mit der Umbenennung hat die ISO einen wichtigen Beitrag zur Bereinigung der babylonischen Namensverwirrung im Bereich der sicherheitsrelevanten Standards geleistet – nach ISO/IEC 27001:2005 und ISO/IEC 27006:2007 existiert jetzt der dritte Standard im Nummernkreis 270xx. Die Nummerierung verdeutlicht die „Verwandtschaft" zu ISO 9001 (Qualitäts-) und ISO 14001 (Umweltmanagement).

SSN 08/2007 – Mittlerweile ist die ISO-Reihe 270xx sechsteilig und nicht mehr weg zu denken.

Mifare-Cloning

Auf dem Jahreskongress des Chaos Computer Clubs stellten Karsten Nohl und Henryk Plötz am 28.12.2007 einen Angriff auf das Authentifikationsverfahren kontaktloser Mifare-Chipkarten vor. Dem vom Hersteller geheimgehaltenen, etwa 15 Jahre alten „CRYPTO1"-Algorithmus waren sie mit einer

Mikroskop-Analyse des Chip auf die Spur gekommen, um dann nach kryptographischen Schwächen (zu kleiner Zufallswert, lineares Schieberegister) darin zu suchen. Zu dieser Krypto-Schwachstelle gibt es nun den passenden „Mifare-Cloner“: Am 12.03. 2008 haben Forscher der Radboud Universiteit Nijmegen ein Video in YouTube veröffentlicht, auf dem sie zeigen, wie sie mit minimalem Aufwand Mifare-basierte Zugangskarten duplizieren. Von der Attacke betroffen sind Tausende von Anwendungen mit einer Milliarde ausgegebenen Karten, vom Betriebsausweis über die Kantinenkarte bis zum bargeldlosen Bezahlsystem im öffentlichen Nahverkehr, sofern sie Mifare-Chips des Typs MF1 IC S50 oder S70 verwenden. Fein raus ist, wer seine Anwendung bereits auf den neueren Mifare DESFire (MF3 IC D40) migriert hat – statt einer etwas ältlichen Stromchiffre verwendet er bei der Authentifikation wahlweise DES oder TripleDES.

SSN 03/2008 – Eingesetzt werden sie noch immer. Ende 2009 hat es auch Mitbewerber Legic erwischt.

SSL-Authentifikation für alle

SSL – seit zehn Jahren unter dem Namen Transport Layer Security (TLS) genormt – ist ein bekanntes, bewährtes und deshalb von seinem ursprünglichen Zweck, der Absicherung von Webzugriffen, auch auf andere Bereiche wie z. B. VPN oder WLAN übertragenes Sicherheitsprotokoll. Sollte man meinen. Auch sollte sich im Jahr 20 nach der Erstveröffentlichung des X.509 Standards herumgesprochen haben, dass Zertifikate naturgemäß öffentliche Daten sind und für sicherheitsrelevante Operationen das private Gegenstück des per Zertifikat bestätigten öffentlichen Schlüssels benötigt wird.

Umso größer die Verwunderung, als Microsoft am 10.03.2009 im Security Bulletin MS09-007 einräumte, dass die SSL-Komponente in Windows – vom Veteranen Windows 2000 bis zum neuesten 64-Bit-System – bei der Client-Authentifikation jahrelang patzte: Zwar wurde die Gültigkeit des vorgelegten Zertifikats geprüft; der im Standard vorgeschriebene Schritt, per Signatur der ausgetauschten Protokollnachrichten zu verifizieren, dass der Client auch den passenden privaten Schlüssel verwendet, wurde jedoch eingespart. Tatsächlich akzeptierte der Server also jeden Client mit irgend einem gültigen Zertifikat - ob nun dem eigenen oder einem fremden.

Durch das weite Einsatzspektrum von SSL/TLS sind wahrscheinlich nicht nur IIS-basierte Webanwendungen von diesem Bug betroffen, sondern jede zertifikatsbasierte VPN-, WLAN- und NAC-Anmeldung, sofern dabei der Microsoft-eigene RADIUS-Dienst IAS zum Einsatz kommt. Vielleicht haben sich die Microsoft-Entwickler bei der Implementierung auf das SSL-Diagramm in Wikipedia verlassen – das den wichtigen Verifikationsschritt ebenfalls fehlerhaft darstellt. Manchmal geht Studieren doch über Probieren.

SSN 03/2009 – Blindes Vertrauen in die Implementierung von Sicherheitsprotokollen ist gefährlich.

iPhone Security

In nicht wenigen Unternehmen hält derzeit Apples iPhone Einzug. Trotz seiner nach wie vor deutlichen Nachteile bei Business-Anwendungen gegenüber RIMs BlackBerry wiegen „Sex-Appeal“ und Nimbus des Geräts auch bei Führungskräften oft schwerer. Wie sicher aber sind Unternehmensdaten auf einem iPhone? Was ist von der Hardware-Verschlüsselung und anderen Schutzmechanismen zu halten? Lassen sich iPhones ohne Inkaufnahme zusätzlicher Risiken in die IT-Infrastruktur integrieren? Diesen Fragen ist Jörg Völker auf den Grund gegangen – und hat die Ergebnisse seiner Untersuchungen nun in der Fachzeitschrift „Datenschutz und Datensicherheit“ (DuD) veröffentlicht.

SSN 06/2010 – Die ungebrochene Popularität von Smartphones hält das Thema im Brennpunkt.

c = m

Kryptografie kann so einfach sein. Das dachen wohl auch die Programmierer der Entwicklerversion von Ruby bei der Implementierung des RSA-Verfahrens: Wenn $c = m^e \bmod n$ zu berechnen ist – dann geht das mit $e := 1$ am schnellsten. Damit folgt: $c = m \bmod n$, $m < n \Rightarrow c = m$. Falls Sie mit dieser Ruby-Version zwischen dem 01.09. und dem 04.11.2011 RSA-Schlüssel erzeugt haben, sollten Sie diese schnellstmöglich ersetzen.

SSN 11/2011 – Hoffentlich haben Rivest, Shamir und Adleman das nicht lesen müssen...

Secorvo News

Freie Plätze sichern

Die Schulung zum T.I.S.P.-Zertifikat mit den Autoren des T.I.S.P.-Buchs am **17.–21.09.2012** ist fast ausgebucht. Das nächste T.I.S.P.-Seminar (und letzte in 2012) findet vom **12.–16.11.2012** statt – frühzeitige Anmeldung wird empfohlen.

Security Awareness Symposium

Am **11.–12.09.2012** sind wir mit dem 8. Security Awareness Symposium wieder zu Gast in der Buhlschen Mühle in Ettlingen. Das Programm ist noch in Abstimmung – wer das Event auf keinen Fall verpassen möchte, kann sich aber bereits heute online anmelden. Wir freuen uns auf Ihr Kommen!

Veranstaltungshinweise

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

August 2012	
06.-08.08.	DFRWS 2012 (DFRWS, Washington/US)
08.-10.08.	21th USENIX Security Symposium (Usenix, Bellevue/US)
19.-23.08.	Crypto 2012 (IACR, Santa Barbara/US)
20.-24.08.	SecSE 2012 (SINTEF, Prag/CZ)
27.08.	Sommerakademie 2012 (ULD Schleswig-Holstein, Kiel)
September 2012	
11.-12.09.	8. Security Awareness Symposium (Secorvo, KA-Ettlingen)
17.-21.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
18.09.	Anwendertag IT-Forensik 2012 (Fraunhofer SIT, Darmstadt)
24.-27.09.	CPSSE-Schulung (Secorvo College, Karlsruhe)
25.-26.09.	D·A·CH Security (GI/OCG/BITKOM/SI/TeleTrusT, Konstanz)
Oktober 2012	
09.-11.10.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
12.10.	1. Freiburger Datenschutztag (vivaSoft/Datenschutz individuell, Freiburg)
23.-26.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)

Impressum

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

ISSN 1613-4311

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

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

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

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

secorvo
security consulting

Secorvo Security News

August 2012

Sprachmartialisierung

Erst verwirren sich die Worte.
Dann verwirren sich die Begriffe.
Und schließlich verwirren sich die Sachen.

Konfuzius (551-479 v.Chr.)

Schon immer ist der Fachjargon der IT-Sicherheit mit sprachlichen Anleihen aus dem Militärischen gespickt. Ein Einbruchsversuch in ein IT-System ist ein „Angriff", extern erreichbare Rechner isolieren wir in „demilitarisierten Zonen" (DMZ) und mögliche Bedrohungen beschreiben wir als „Angriffsvektoren". Das mag historische Gründe haben – inzwischen haben wir uns daran gewöhnt. Hilfreich war das allerdings nie. So ist es schwierig, Laien für Schutzmaßnahmen zu gewinnen, wenn man von drohenden „Angriffen" schwadroniert – das klingt maßlos überzogen. Überzeugender ist der Hinweis auf mögliche „Eindringlinge", die „Daten entwenden" – digitale Einbruchsszenarien liegen eher im Bereich des Vorstellbaren.

Sprache ist aber, wie wir nicht erst seit Orwells „Neusprech" wissen, nicht nur Ausdruck unserer Weltsicht. Sie beeinflusst auch unsere Wahrnehmung, mittelfristig unser Denken und langfristig unser Verhalten. Wie wirksam ein konsequentes Sprachuniversum sogar offensichtliche Unmenschlichkeit rechtfertigen kann, ließ sich in Deutschland wiederholt (zuletzt bei der RAF) beobachten.

Inzwischen hat die militärische Diktion auch die Politik erreicht. Ob sich Politiker die martialischen Bezeichnungen wegen ihrer Medienwirksamkeit zu Eigen gemacht haben oder das mediale Dauerfeuer die Ursache ist: Seit 2011 haben wir ein „Nationales Cyber-Abwehrzentrum". Wenn ein Staat eine solche Institution benötigt, rechnet er offenbar mit drohenden Cyber-Schlachten – auf gut Deutsch: dem Cyberkrieg, einem „organisierten und unter Einsatz erheblicher Mittel mit Waffen und Gewalt ausgetragenen Konflikt, dessen Handlungen auf die Verletzung und Tötung des Gegners zielen". Bei allem Respekt vor den Möglichkeiten digitaler Spionage und Sabotage – ist es wirklich „Krieg", was wir realistischer Weise befürchten müssen? Und wann fühlt sich da jemand zum „Erstschlag" genötigt?

Inhalt

secorvo
security consulting

Security News

Web-App-Krümel

Nur 3 % der Entwickler seien an Sicherheit von Software interessiert – zu diesem Schluss kommt SANS-Autor Frank Kim in seinem Blog-Eintrag vom 23.07.2012 nach Zählung der Security-Vorträge auf Entwicklerkonferenzen. Dem widersprechen die Ergebnisse der (inzwischen zwölften) WhiteHat-Studie zu sicherheitsrelevanten Schwachstellen in Webanwendungen vom 17.07.2012: Danach hat die Zahl schwerer Schwachstellen pro Anwendung in den vergangenen Jahren signifikant abgenommen. Allerdings werden im Schnitt noch immer zu viele Schwachstellen gefunden.

Zahlreiche neue Tools unterstützen die Entwicklung sicherer Software. Zur Integration von Sicherheit in die agile Software-Entwicklung hat SAFECode am 16.07.2012 das lesenswerte White-Paper „Practical Security Stories and Security Tasks for Agile Development Environments" veröffentlicht. Bezüglich der Überprüfung der Sicherheit von Software bietet die aktuelle Übersicht über 62 freie und kommerzielle Webanwendungsscanner aus dem Juli 2012 mit Benchmarks nach verschiedenen Kriterien eine Entscheidungshilfe. Für das virtuelle Patchen ist in vielen Apache-Webservern heute mod_security im Einsatz. Seit dem 26.07.2012 ist mod_security auch für die Webserver IIS und ngnix verfügbar.

Eingebettet in ein Gesamtkonzept eines erweiterten Software Development Life Cycle aus Entwicklerschulung und -sensibilisierung, Sicherheitsaudits, Monitoring und Blocking tragen solche Tools auch zu einer Reduktion von Sicherheits-Schwachstellen bei. Security-Vorträge auf Entwicklerkonferenzen könnten dann irgendwann obsolet werden.

Ende der Übergangsregelung

Am 31.08.2012 läuft die letzte Übergangsfrist der BDSG-Novelle von 2009 ab. Verschiedene Newsletter und Seiten aus dem Datenschutz- und E-Commerce-Spektrum fordern daher zum Durchforsten der zur Werbung genutzten Adressdatenbanken auf; viele Anbieter bitten ihre Mailing-Empfänger bereits um neue Einwilligungen.

Tatsächlich führt der Fristablauf nicht zu größeren Änderungen. Von § 47 Nr. 2 BDSG sind nur vor dem 01.09.2009 zum Zweck der Werbung (§ 28 Abs. 3-5 BDSG) erhobene Daten betroffen. Die Voraussetzungen für die Zulässigkeit der Versendung von E-Mail-Newslettern sind im Wesentlichen durch § 7 Abs. 2 und 3 UWG und die elektronische Einwilligung durch §§ 6 Abs. 2 und 13 Abs. 2 TMG geregelt.

Die Versendung von E-Mail-Werbung an Bestandskunden steht – vorbehaltlich eines Kundenwiderspruchs – auch zukünftig nicht unter einem Einwilligungsvorbehalt und darf auch weiterhin über einen „Opt-Out"-Mechanismus realisiert werden.

Die BDSG-Novelle von 2009 hat lediglich eine Angleichung an diese schon seit 2001 bzw. 2004 geltenden Vorschriften vorgenommen. Die vor 2009 bestehenden Erlaubnistatbestände sind zwar teils eingeschränkt, teils erweitert (und in der Verständlichkeit reduziert) worden; sie gelten jedoch im Wesentlichen fort. Eine neue Einwilligung ist nur erforderlich, wenn keiner der Erlaubnistatbestände ohne Betroffenenbeteiligung greift und keine dokumentierte Einwilligung vorliegt.

Wer bislang Datenschutzvorgaben eingehalten hat, muss nicht befürchten, dass er mit Ablauf der Übergangsfrist seine Kunden nicht mehr anschreiben darf.

Wer die Vergangenheit kontrolliert...

...kontrolliert die Zukunft, sagt die Ingsoc-Partei in George Orwells 1984. Für elektronische Geldgeschäfte gilt sinngemäß: Wer die Benutzerschnittstelle kontrolliert, kontrolliert den Benutzer. Beim Online-Banking manifestiert sich das Problem unter dem Schlagwort Man-in-the-Browser. Dass ca. 60% der Varianten des Zeus-Trojaners selbst von aktueller Antivirus-Software nicht erkannt werden, veranlasste die ENISA in einer Pressemeldung vom 05.07.2012 zur Warnung an die Banken, doch besser davon auszugehen, dass alle Kunden-PCs infiziert sind, so dass deren Browser-Anzeige und -Transaktionen von Angreifern beeinflusst werden können. Die ENISA empfiehlt daher, zur Prüfung durch den Benutzer Transaktionsdaten auf einem zweiten, vertrauenswürdigen Gerät anzuzeigen. Online-Banking mit TAN-Listen sollte man tunlichst nur noch auf frisch gebooteten, sauberen Systemen nutzen, wie z. B. Bankix.

Auch am Point-of-Sale muss man inzwischen mit solchen Angriffen rechnen – und dort helfen weder TAN-Generator noch Bankix: Am 12.07.2012 demonstrierten Forscher von SRLabs in einem ARD-Beitrag, wie sich die Firmware von weit verbreiteten POS-Terminals manipulieren lässt. Mehrere von SRLabs entdeckte Schwachstellen erlauben, über Netzwerk oder lokale Schnittstellen einen „Man-in-the-POS" einzuschleusen. Keine der Schwachstellen erlaubt es, das zertifizierte Sicherheitsmodul des Geräts zu manipulieren – aber das ist auch gar nicht nötig, da das Modul nur die Protokollschritte des Zahlungsverfahrens kontrolliert und nicht das Display und PIN-Pad. So können Angreifer direkt an der Quelle phishen – denn wer die Benutzerschnittstelle kontrolliert...

Datenschutz in der Cloud

Die Art. 29 Datenschutzgruppe hat am 01.07.2012 eine Stellungnahme zum Datenschutz bei Cloud Computing veröffentlicht. Neben einer Zusammenfassung der typischen Datenschutzrisiken und Empfehlungen zur Herstellung von Datenschutzkonformität hebt sie die Durchführung einer umfassenden Risikoanalyse durch den Cloud-Nutzer hervor. Bezüglich der meist komplexen Unterauftragnehmerstrukturen wird in Anlehnung an die Europäischen Standardvertragsklauseln empfohlen, eine Haftung des Cloud-Anbieters für Unterauftragnehmer, das Einholen des Einverständnisses des Auftraggebers zu Unterauftragnehmern und die obligatorische Weitergabe der Vertragspflichten an diese vertraglich zu verankern.

Darüber hinaus listet die Stellungnahme zu berücksichtigende Vertragsinhalte bei der Cloud-Beauftragung auf, die über die Liste in § 11 Abs. 2 BDSG zur Auftragsdatenverarbeitung hinausgehen, darunter bspw. eine Standortliste der Verarbeitungsorte. Ebenso findet sich eine Liste der Kategorien von zu verlangenden technisch-organisatorischen Maßnahmen. Es wird mehrfach hervorgehoben, dass ein starkes Verhandlungsungleichgewicht zwischen Nutzer und Anwender keine Rechtfertigung für den Verzicht auf Datenschutzanforderungen darstellt.

Interessant ist die Einschätzung der Safe Harbor Relevanz: Daneben wird in jedem Fall eine vertragliche Vereinbarung gefordert, die Datenschutzanforderungen konkretisiert. Außerdem sollen vom Dienstleister zusätzlich zur Selbstzertifizierung Nachweise über die Erfüllung der Datenschutzanforderungen erbracht werden. Damit enthält die Stellungnahme wichtige Hinweise und Mindestanforderungen an die Vertragsgestaltung.

Awareness wirkt

Im Juli berichtete The Register, dass bei der niederländischen Chemiefirma DSM die Aufmerksamkeit einiger Angestellten verhinderte, dass Schadsoftware in das Intranet des Unternehmens eingeschleust wurde. Die Mitarbeiter übergaben der IT-Abteilung auf dem Firmenparkplatz entdeckte USB-Sticks – auf denen sich, wie eine Analyse ergab, Malware befand, die zu einer Infektion geführt hätte.

Fokussierte Angriffe dieser Art sind inzwischen keine Seltenheit mehr. Nur Unternehmen, die es nicht dem Zufall überlassen, wie kompetent Mitarbeiter auf Gefährdungen und Eindringversuche reagieren, haben gegen solche Attacken eine realistische Chance.

Am **11.–12.09.2012** treffen sich Verantwortliche aus zahlreichen Unternehmen in der Buhlschen Mühle in Ettlingen auf dem von Secorvo organisierten "8. Security Awareness Symposium", um über erfolgreiche Sensibilisierungsmaßnahmen und ihre Erfahrungen aus eigenen Awareness-Kampagnen zu diskutieren.

Secorvo News

Vertieftes Know-How

Festigen Sie vorhandenes Wissen, schließen Sie Lücken, ergänzen Sie Ihre Erfahrungen und Kenntnisse um aktuelle Erkenntnisse der Informationssicherheit mit einer Schulung zum T.I.S.P. Lassen Sie sich von den Autoren des T.I.S.P.-Buchs vom **17.–21.09.** oder **12.–16.11.2012** auf die anschließende Zertifikatsprüfung vorbereiten.

Wie sich Sicherheit von Beginn an in den Softwareentwicklungsprozess integrieren lässt, erfahren Sie in der Zertifikatsschulung "Certified Professional for Secure Software Engineering (CPSSE)" am **24.–27.09.2012** in Karlsruhe.

Alles, was Sie für die Konzeption und den Betrieb einer Unternehmens-PKI wissen müssen, vermitteln wir Ihnen auf unserer PKI-Schulung am **23.–26.10.2012.**

Alle Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Teamverstärkung

Seit dem 01.08.2012 verstärkt Sven Köhler das Secorvo-Consulting-Team. Die Schwerpunkte des erfahrenen Sicherheitsspezialisten liegen im Risiko- und Notfallmanagement, bei Sicherheitsaudits sowie der Zertifizierung nach IT-Grundschutz und dem IDW Prüfungsstandard 980 für die Prüfung von Compliance Management Systemen.

Trutzburg für jeden

Mit steigendem Leistungsbedarf nehmen die Herausforderungen zu, die bei der Planung und Gestaltung eines sicheren Serverraums oder Rechenzentrums auch von kleinen und mittleren Unternehmen zu bewältigen sind.

Markus Schäfer (proRZ Rechenzentrumsbau GmbH) gibt mit seinem Vortrag auf dem kommenden KA-IT-Si Event am **13.09.2012** einen Überblick über die Anforderungen an eine moderne zentrale IT und stellt Best-Practice-Maßnahmen zu deren sicherer Realisierung vor. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

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

September 2012	
11.-12.09.	8. Security Awareness Symposium (Secorvo, KA-Ettlingen)
13.09.	Trutzburg für jeden (KA-IT-Si, Kalrsuruhe)
17.-21.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
18.09.	Anwendertag IT-Forensik 2012 (Fraunhofer SIT, Darmstadt)
24.-27.09.	CPSSE-Schulung (Secorvo College, Karlsruhe)
25.-26.09.	D·A·CH Security (GI/OCG/BITKOM/SI/TeleTrusT, Konstanz)
Oktober 2012	
09.-11.10.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
12.10.	1. Freiburger Datenschutztag (vivaSoft/Datenschutz individuell, Freiburg)
15.-17.10.	IDACON 2012, (WEKA-Akademie, Würzburg)
16.-18.10.	it-sa 2012, (SecuMedia Verlag, Nürnberg)
22.-26.10.	OWASP AppSec USA 2012, (OWASP Foundation, Austin/US)
23.-24.10.	ISSE 2012, (TeleTrusT/eema, Brüssel)
23.-26.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp.

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

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

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

secorvo
security consulting

Secorvo Security News

September 2012

Das „Einweg-Paradigma“

Wer mit aufmerksamem Blick bewährte Schutzmaßnahmen in Bereichen außerhalb der Informationstechnik verfolgt, kann ein Phänomen beobachten, dass ich das „Einweg-Paradigma“ nennen will.

Ein Sanitäter oder Arzt, der sich und seine Patienten vor Infektionen schützen will, verwendet Einweg-Handschuhe, eine Einweg-Spritze, Einweg-Spatel und desinfizierte Einweg-OP-Kittel. Spurensicherer verhindern mit Einweg-Überschuhen und Einweg-Overalls die Kontamination eines Tatorts. Mit Einweg-Taschentüchern versuchen wir bei einem Schnupfen die Ansteckungsgefahr zu bannen. Den Fahrradhelm tauschen wir nach einer heftigen Kollision, und im Fahrzeug schützt der Einweg-Airbag die Insassen. Einweg-Alkoholtester bewahren die Testperson vor Infektion und den Tester vor Manipulation. Einweg-Gläser und –Trinkbecher aus Kunststoff oder Karton verhindern Schnittverletzungen, Einweg-Kontaktlinsen Unfälle. Kleine Kinder wickeln wir in Einweg-Windeln. Einweg-Verpackungen sorgen für hygienisch einwandfreie Lebensmittel, und Einweg-Umschläge schützen unsere Briefe während des Transports vor unbefugter Kenntnisnahme und Beschädigung.

Zwar belastet der Erfolg dieses Einweg-Paradigmas unsere Umwelt. Dennoch ist der Sicherheitsgewinn meist erheblich. In der modernen Informationstechnik hingegen – dort, wo Einweg-Lösungen nicht einmal die Umwelt belasten würden – beschränken wir uns geradezu antiquarisch auf's Reparieren: Die Bugs im Betriebssystem werden *gefixt*, der Browser beim Auftauchen von Zero-Day-Exploits *gepatcht*, die Web-Applikation mit Schwachstelle bekommt ein *Update*. Man stelle sich einmal vor, die Löcher in OP-Handschuhen würden in ähnlicher Weise über Jahre mit Flicken gedichtet.

Ach, wie schön wäre doch ein Einweg-Betriebssystem mit Einweg-Browser: morgens gestartet und abends gelöscht – keine Chance für Exploits, und der Patch-Marathon hätte endlich ein Ende.

Inhalt

Security News

Nicht ganz zufällig

Forscher der Uni Cambridge veröffentlichten am 10.09.2012 eine Analyse, der zufolge Kriminelle an einem manipulierten POS-Terminal (vgl. SSN 08/2012) von einer eingelegten EMV-Bankkarte Transaktionsdaten abzapfen könnten, die sich später am Geldautomaten einspielen und in Bares umwandeln lassen. Die technische Ursache des Problems ist, dass manche Geldautomaten einen mehr oder minder vorhersagbaren (und damit unbrauchbaren) „Zufallswert" als Schutz gegen Replay-Angriffe verwenden. Bei der Lektüre des Papiers weiß man nicht, worüber man mehr den Kopf schütteln soll: Darüber, dass die Entwickler als „Unpredictable Number" (UN) einen fortlaufenden Zähler verwendeten, dass bei Abnahmetests nur geprüft wird, ob vier nacheinander erzeugte UN sich unterscheiden, oder dass man als Reverse-Engineer echte Geldautomaten günstig bei eBay erstehen kann.

Vielleicht ist es keine so gute Idee, wichtige Teile des Schutzes des Bankkunden in die Hand der Hersteller von POS-Terminals und Geldautomaten zu legen.

Kontrollierter Benutzer

Ein prägnantes Beispiel, wozu die in SSN 08/2012 thematisierte Kontrolle der Benutzerschnittstelle durch einen Angreifer missbraucht werden kann, wurde am 04.09.2012 aufgedeckt. Dabei klinkt sich ein Man-in-the-Browser-Trojaner in eine Online-Banking-Sitzung ein und verweist auf „technische Probleme", derentwegen zunächst eine „Testüberweisung" durchgeführt, mit dem ChipTAN-Generator geprüft (sic!) und freigegeben werden müsse. Die Transaktion ist allerdings echt. Noch perfider ist der Trojaner, vor dem das BKA bereits am 15.07.2011 warnte (vgl. SSN 07/2011) – er täuscht eine irrtümliche Gutschrift auf dem Konto des Opfers vor, die nun „zurücküberwiesen" werden müsse. Schließlich gibt es da noch den im Juli 2012 aufgetauchten Telefonbanking-Trojaner, der zum „Datenvergleich" Angaben zum Kontoinhaber abfragt – zuletzt auch die Telefonbanking-PIN.

„Technische Probleme" sind ein bei Trojanern beliebter Vorwand für seltsame Anweisungen. Ihnen sollten daher mit größter Skepsis begegnet werden.

Elektronische Rechnungen

Am 02.07.2012 hat das Bundesministerium für Finanzen in einem Schreiben an die obersten Finanzbehörden der Länder die Auswirkungen des nach längerer Verhandlung mit dem Bundesrat am 01.11.2011 verabschiedeten Steuervereinfachungsgesetzes 2011 (vgl. SSN 06/2011) auf elektronische Rechnungen präzisiert. Danach ist eine qualifizierte elektronische Signatur nicht mehr Voraussetzung für die umsatzsteuerrechtliche Anerkennung. Statt dessen muss lediglich ein „innerbetriebliches Kontrollverfahren" die korrekte Übermittlung der Rechnung sicherstellen. Stimmen die Angaben zu Leistung, Leistendem, Entgelt und Zahlungsempfänger dürfe davon ausgegangen werden, dass die Übermittlung fehlerfrei erfolgt ist. Dafür genügt zukünftig ein manueller Abgleich der Rechnung bspw. mit den zugehörigen Auftrags- oder Vertragsunterlagen. Die Zustimmung des Empfängers zum elektronischen Rechnungsversand kann nun auch durch Annahme der AGB oder konkludentes Handeln erfolgen.

Damit sind qualifizierte elektronische Signaturen wieder um eine „Killerapplikation" ärmer.

VoIP- und UC-Bedrohungen

Gebührenbetrug bleibt eine der zentralen Bedrohungen gegen IP-basierte Telefonie (VoIP) und Unified Communications (UC). Dies geht aus dem im August veröffentlichten Bericht der SecureLogix Corporation vom 12.06.2012 hervor. Dort wurden für verschiedene Szenarien die jeweils relevanten Bedrohungen auf Grundlage der berichteten Vorfälle der vergangenen sechs bis 12 Monate identifiziert. Danach sind Einzelschäden von 100.000 US$ und mehr nicht ungewöhnlich. Sie entstehen entweder durch massive Anwahl von Premium- und Mehrwertdiensten oder durch eingedrungene Angreifer, die Telefoniekapazitäten „vermieten". Bei letzteren sind zudem weitere illegale Aktivitäten wie Voice SPAM oder Social Engineering möglich. Auch moderne Smartphones – eher Kleinformatcomputer mit Telefonie-App und nicht ausgereiften Sicherheitskonzepten – sind inzwischen Quellen für Gebührenbetrug, wie der Lookout Mobile Security Report 2012 vom 05.09.2012 bestätigt.

Unternehmen, die VoIP- oder UC-Anlagen einführen, dürfen derzeit nicht davon ausgehen, dass sie bereits gehärtete Systeme erhalten – im Auslieferungszustand sind diese meist auf maximale Funktionalität, nicht aber auf Sicherheit konfiguriert. Und das kann teuer werden, wie die angeführten Studien eindrucksvoll belegen.

Mitarbeiterscreening

Der Bundesfinanzhof hat mit Urteil vom 19.06.2012 die Zulässigkeit von Mitarbeiterscreenings zur Erlangung eines AEO-Zertifikats „Zollrechtliche Vereinfachungen/Sicherheit" bestätigt. Die Erteilung des Zertifikats, das Erleichterungen bei der Abwicklung grenzüberschreitenden Warenverkehrs ermöglicht, ist abhängig von einer Überprüfung des Personals

des Antragstellers gegen die Listen der VO Nr. 2580/2001 und VO Nr. 881/2002.

Dabei handelt es sich um Antiterrorlisten, die durch den Europäischen Rat nach den Vorgaben des Gemeinsamen Standpunkts 2001/931/GASP erstellt werden. Sie unterliegen zwar einer halbjährigen Überprüfung, der Rechtsschutz der Betroffenen ist jedoch schwach ausgeprägt. Finanzielle Zuwendungen an die gelisteten Personen sind verboten.

Der Bundesfinanzhof sieht den Abgleich durch den Arbeitgeber durch § 32 Abs. 1 Satz 1 BDSG erfasst. Verwendet würden ohnehin nur Stammdaten der Beschäftigten. Dem Arbeitgeber stünde das Einholen einer Einwilligung der Beschäftigten oder der Verzicht auf das Zertifikat frei. Daher handele es sich auch nicht um einen staatlichen Eingriff. Den Abgleich als Bedingung für die Zertifikatserteilung zu verlangen, sei verhältnismäßig.

Während die Entscheidung für die betroffenen Unternehmen ein gewisses Maß an Rechtssicherheit schafft, ist die Begründung äußerst fragwürdig. Das Verlangen des Abgleichs ist weder durch den Zollkodex (ZK) noch durch dessen Durchführungsverordnung gefordert. Die Verhältnismäßigkeit des Abgleichs mit den konkreten Terrorlisten wäre daher unter Abwägung von Transparenzpflichten und Rechtsschutzmöglichkeiten der Beschäftigten zu prüfen gewesen. Die Ausführungen zur Möglichkeit der Einwilligungseinholung sind aus Datenschutzsicht mangels Freiwilligkeit zudem rechtlich falsch. Letztlich liegt das Problem jedoch bei der Praxis der Verdächtigenlisten, die im Hinblick auf Datenschutz und Rechtsstaatlichkeit berechtigt in der Kritik stehen.

Speicherforensik

Am 18.09.2012 wurde Version 2.2 RC2 des Open-Source-Forensik-Tools Volatility freigegeben, das seit August die Betriebssysteme Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 sowie alle verfügbaren Service Packs und 64bit-Architekturen unterstützt. Insgesamt 67 Windows-Plug-Ins ermöglichen seitdem beispielsweise die Auswertung von Eventlogs im Hauptspeicher unter Windows XP und Server 2003 oder der Historie der CMD-Kommandozeile. Sogar Interaktionen in der GUI sind über die Erzeugung von Pseudo-Screenshots aus Fensterpositionsdaten rekonstruierbar.

Nun unterstützen 34 weitere Plug-Ins auch forensische Speicher-Analysen unter allen Linux-Derivaten (Debian, Ubuntu, OpenSuSE, Fedora, CentOS, Mandriva) ab Kernel 2.6.11 bis 3.5.

Volatility hat damit – wieder einmal – die Meßlatte für kommerzielle Lösungen in diesem Bereich deutlich höher gelegt und sollte heute bei keiner forensischen Incident Response mehr fehlen.

Secorvo News

Heute schon gefacebookt?

Ende 2011 waren nach einer Studie des Bitkom 74 % der deutschen Internet-Nutzer in einem „Sozialen Netzwerk“ registriert. Inzwischen dürften es einige mehr sein. Und in vielen Unternehmen drängen Marketing- und Personalabteilung auf eine Unternehmenspräsenz bei Facebook & Co. Meist ist ein erheblicher Teil der Mitarbeiter bereits „drin".

In den zu einem erheblichen Teil (Google+, facebook) von amerikanischen Anbietern betriebenen Social Networks lauern jedoch zahlreiche Fallen: Copyrightverletzungen, unkontrollierte Informationspreisgabe und Verstöße gegen Datenschutzbestimmungen gehören dazu.

Beim nächsten KA-IT-Si-Event "Heute schon gefacebookt?" am **08.11.2012** gibt der Jurist Michael Knopp einen Überblick über die wichtigsten Stolpersteine – und praktische Tipps, wie sie sich vermeiden lassen. Für ein besonderes Ambiente ist gesorgt: Erstmals ist die KA-IT-Si mit ihrer Veranstaltungsreihe in den stilvollen Räumlichkeiten der Buhlschen Mühle in Ettlingen zu Gast. Das Tagungszentrum liegt ca. 10-15 Minuten Fahrzeit vom Karlsruher Hauptbahnhof entfernt. Beginn der Veranstaltung ist um 18 Uhr. Um Anmeldung wird gebeten. Wir freuen uns auf spannende Diskussionen und interessantes Networking!

Wissen auffrischen

Unsere Seminare vermitteln nicht nur Grundlagen der IT-Sicherheit für Einsteiger in dem Gebiet (wie IT-Sicherheit heute, **20.–22.11.**), sondern stellen auch die "aktuellen Herausforderungen der Informationssicherheit" vor (**07.–08.11.**).

Experten mit mindestens drei Jahren Berufserfahrung in der Informations- bzw. IT-Sicherheit können ihre Kenntnisse mit dem T.I.S.P.-Zertifikat krönen (**12.–16.11.**). Das von Secorvo verfasste 500seitige T.I.S.P.-Buch Zentrale Bausteine der IT-Sicherheit (siehe die Leser-Rezensionen) ist im Preis eingeschlossen und wird allen Teilnehmern frühzeitig vor Seminarbeginn zugesandt.

Alle weiteren Seminarangebote, das druckfrische Jahresprogramm 2013 und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Veranstaltungshinweise

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

Oktober 2012	
12.10.	1. Freiburger Datenschutztag (vivaSoft/Datenschutz individuell, Freiburg)
15.-17.10.	IDACON 2012, (WEKA-Akademie, Würzburg)
16.-18.10.	it-sa 2012 (SecuMedia Verlag, Nürnberg)
22.-26.10.	OWASP AppSec USA 2012 (OWASP Foundation, Austin/US)
23.-24.10.	ISSE 2012 (TeleTrusT/eema, Brüssel)
31.10.-03.11.	hashdays security & risk conference 2012 (DEFCON Switzerland, Luzern/CH)
November 2012	
07.11.	German OWASP Day 2012 (OWASP Germany, München)
08.11.	Heute schon gefacebookt? (KA-IT-Si, Ettlingen)
07.-08.11.	Aktuelle Herausforderungen der Informationssicherheit (Secorvo College, Karlsruhe)
12.-17.11.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
22.-23.11.	36. DAFTA (GDD, Köln)

Fundsache

Als Pendant zu diversen Top Ten der Smartphone-Risiken veröffentlichte die enisa am 25.11.2011 einen Leitfaden, der die zehn wichtigsten Sicherheitsmaßnahmen detailliert, an die App-Entwickler denken sollten – leider noch ohne Plattform spezifische Hinweise zu iOS, Android & Co.

Impressum

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

ISSN 1613-4311

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

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

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

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

secorvo
security consulting

Secorvo Security News

Oktober 2012

Grenzen der Kooperation

Im Februar 2004 wurde Facebook als Studentennetzwerk gegründet. Vier Jahre danach war Facebook bereits international, auch auf deutsch, verfügbar, und die Gründung von Facebook Ireland Ltd. wurde angekündigt. Weitere vier Jahre später ist Facebook die unumstrittene Nummer Eins der sozialen Netzwerke mit geschätzt einer Milliarde Mitglieder. Eine rasante Entwicklung.

Seit 2010 rücken jedoch vermehrt Datenschutzprobleme in den Fokus. Die Hamburgische und die Schleswig-Holsteinische Datenschutzaufsicht sind gegen Facebook bzw. Fanpage-Betreiber vorgegangen. Eine österreichische Studentengruppe hat eine Reihe von Beschwerdeverfahren bei der irischen Datenschutzaufsichtsbehörde DPC angestoßen. Sogar die US-amerikanische Federal Trade Commission (FTC), zuständig für das Safe Harbor-Abkommen, ist eingeschritten und hat jährliche Audits vereinbart. Hinzu kommen diverse Datenschutzpannen.

Dabei überwiegt ein kooperativer Ansatz, um dem neuen Phänomen „Soziale Netzwerke" Rechnung zu tragen. Ein solcher gestalterischer Ansatz hat den Vorteil, unter Nutzung gesetzlicher Auslegungsspielräume passende Regeln zu entwickeln, die das Geschäftsmodell nicht zerstören, aber Gemeinwohlinteressen durchsetzen.

Kooperation darf aber nicht zur Anbiederung werden, bei der staatliche Autoritäten sich lächerlich machen und ihre Autorität verlieren. Das Gutachten der DPC zu Facebook vollbringt dies jedoch schon im Vorwort: Facebook habe zur vollsten Zufriedenheit kooperiert, dabei Empfehlungen und Best Practices akzeptiert. Ein genauerer Blick zeigt, dass facebook vielen Empfehlungen gar nicht oder nur ungenügend nachgekommen ist. Hinweise auf die vorliegenden Rechtsverstöße fehlen völlig, Sanktionsandrohungen finden sich nicht.

Um Grenzen zu setzen, muss auch Kooperation Grenzen haben.

Inhalt

secorvo
security consulting

Security News

Unselbständig

Fast zwei Jahre nach Verabschiedung des unter Federführung des Bitkom entwickelten Datenschutzkodex für Geodatendienste am 01.12.2010 hat der Verein Selbstregulierung Informationswirtschaft e.V. Ende September die nach Abschnitt 6 des Kodex zu errichtende Website der zentralen Informations- und Widerspruchstelle vorgestellt. Sie bietet eine Suchmöglichkeit nach Geodaten anhand der Postanschrift und verweist auf die Widerspruchsverfahren der Anbieter (im Wesentlichen Google Streetview). Die gemeinsame telefonische Beratungsstelle (6.2) sucht man ebenso wie den Beschwerdeausschuss (8.2) und das Gremium zur Selbstkontrolle (7.2) vergeblich; dafür findet sich ein Einheits-Widerspruchformular.

Der Kodex selbst blieb bereits bezüglich der eingeräumten Betroffenenrechte hinter geltendem Datenschutzrecht zurück (Widerspruch erst nach Veröffentlichung). Und nennenswerte Bedeutung wird ihm offenbar seitens der Unterzeichner auch nicht eingeräumt – in den deutschsprachigen Datenschutzangaben zu Google Streetview wird er nicht einmal erwähnt.

Deutlicher als mit solcherlei Selbstregulierung kann man kaum nach einer Verschärfung des Datenschutzrechts rufen.

Ungebrochen

Am 02.10.2012 verkündete das NIST nach fünf Jahren den Gewinner des Wettbewerbs um den Hash-Standard SHA-3. Es ist der „Keccak"-Algorithmus, der sich vor allem durch zwei Eigenschaften gegenüber dem SHA-2 auszeichnet: Er beruht auf einem anderen Grundprinzip als die Familie der MD-Hashes bis einschließlich SHA-2, was zur Hoffnung berechtigt, dass sich mögliche künftige Angriffe auf SHA-2 nicht so einfach auf SHA-3 übertragen lassen. Und er lässt sich besonders effizient in Hardware realisieren – kaum verwunderlich, da die vier Keccak-Autoren, unter ihnen einer der Sieger des AES-Auswahlwettbewerbs, bei Halbleiterherstellern arbeiten, die beide Security-Chips im Portfolio haben.

Anders als beim AES ersetzt SHA-3 den Vorläufer nicht, sondern wird vom NIST als Ergänzung betrachtet, die für manche Einsatzfelder Vorteile bieten kann – und als Rückversicherung, falls SHA-2 eines Tages gebrochen werden sollte. Anwender des SHA-1 sollten nicht warten, bis SHA-3 in Produkten verfügbar ist: Der Sicherheitsgewinn durch den Wechsel zum SHA-2 (SSN 09/2002) ist deutlich größer als von SHA-2 zu SHA-3.

Unzufrieden

Auf Grundlage einer Rechtsprüfung der französischen Datenschutzaufsichtsbehörde (CNIL) hat die Art. 29 Gruppe (europäische Datenschutzaufsicht) Google am 16.10.2012 in einem offenen Schreiben zur Überarbeitung der Datenschutzerklärung und Nutzungsbedingungen vom 01.03.2012 aufgefordert. Im Anhang bescheinigen die Aufseher Google, dass die geltenden Richtlinien jegliche Begrenzung des Verarbeitungszwecks und des Gebrauchs personenbezogener Daten vermissen lassen.

Hauptkritikpunkte sind die mangelnde Transparenz Googles bezüglich der verarbeiteten Daten, die Verarbeitung und Zusammenführung von personenbezogenen Daten über Dienstgrenzen hinweg ohne Rechtsgrundlage oder Einwilligung, das Fehlen jeglicher Löschfristen und der Vorbehalt einer jederzeitigen Änderung der Richtlinien. Es folgen Empfehlungen zur besseren Gestaltung der Datenschutzrichtlinien, zur Einführung vereinfachter Opt-Out Mechanismen und zum Einholen von Einwilligungen in nicht offen ersichtliche Verarbeitungen. Die in Deutschland 2011 vereinbarten Regelungen zu Google Analytics (Ausschluss der dienstüberschreitenden Verwendung, Abschluss eines Auftragsdatenverarbeitungsvertrages und Anonymisierung der IP-Adressen) werden zur Nachahmung empfohlen – etwas voreilig vielleicht, tragen sie doch wenig zu mehr Transparenz der Verarbeitung bei. Sie stehen zudem unter dem Vorbehalt der Umsetzung der EU-Cookie-Richtlinie von 2009.

Unverändert

Das CA/Browser-Forum ist eine informelle Organisation von fünf Browser-Herstellern und ca. 30 kommerziellen CA-Betreibern, die u. a. das Prozedere festlegt, wie Root-Zertifikate in den Browsern vorinstalliert werden. Als eine Konsequenz aus den Trustcenter-Einbrüchen des vergangenen Jahres (SSN 09/2011) wurde diskutiert, das Forum zu reformieren und für interessierte Anwenderkreise zu öffnen, die darauf angewiesen sind, dass Vertrauensanker tatsächlich vertrauenswürdig sind. Wie am 05.10.2012 bekannt wurde, stimmten die Mitglieder jedoch für einen geschlossenen Club.

Die Browser-Hersteller haben die künftige Entwicklung ohnehin in der Hand: Im August 2012 trat der DANE/TLSA-RFC in Kraft, nach dem Serverbetreiber eigene SSL/TLS-Zertfikate im DNS publizieren und Clients sie per DNSSEC validieren können. Sobald die Browser- oder Plugin-Entwickler diese Alternative alltagstauglich umsetzen, dürften öffentliche Root-CAs an Stellenwert einbüßen.

Ungeeignet

Am 19.09.2012 beschloss die Bundesregierung einen Gesetzesentwurf zur Förderung der elektronischen Verwaltung, mit dem auf Bundesebene Hindernisse bei der Einführung elektronischer Verwaltungsverfahren beseitigt werden sollen. Neben der qualifizierten elektronischen Signatur sind nun auch De-Mail und elektronische Formulare unter Verwendung der eID-Funktion des Personalausweises als Ersatz für die Schriftform vorgesehen. Bundesbehörden werden verpflichtet, hierfür den Zugang zu eröffnen, und das De-Mail-Gesetz wird um die Möglichkeit ergänzt, über den Verzeichnisdienst die Zugangseröffnung gegenüber der Verwaltung zu erklären. Bundesbehörden sollen zudem zur elektronischen Aktenführung übergehen und Papierdokumente – wenn sie aus rechtlichen Gründen nicht weiter benötigt werden – entsorgen (sic!).

Es darf bezweifelt werden, dass dem E-Government auf diesem Weg messbare Impulse gegeben werden: fast jede Regelung des Gesetzes liefert den adressierten Behörden eine Ausnahme von der Umsetzungspflicht, die ergänzten Verfahren sind (wie die qualifizierte elektronische Signatur) wenig verbreitet, und ein Großteil der Regelungen hinkt bereits praktizierten Verfahren um Jahre hinterher. Da wirkt die Berechnung der Ersparnisse wie blanker Zweckoptimismus: In 82 Millionen Fällen pro Jahr soll die Bearbeitungszeit je Bürger um acht Minuten sinken – 10 Stunden in 75 Lebensjahren.

Unverzichtbar

Seit dem 02.10.2012 ist das automatisierte Sichtungs-Tool Forensic Scanner verfügbar. Es ist mit 44 Plugins für die Bereiche „System“ und „User“ vorkonfiguriert. Besonders bei Erstuntersuchungen von Windows-Domaincontrollern oder Terminalservern spielt dieses Werkzeug seine Stärken aus, da es sowohl einzelne als auch Gruppen von Benutzerkonten analysieren kann und die Ergebnisse in ASCII-Dateien ausgibt.

Die am 26.09.2012 stark erweiterten und überarbeiteten 243 Plugins des „großen Bruders“ RegRipper detaillieren die Bereiche „System“ (49) und „User“ (106) deutlich weiter, so dass die mit dem Forensic Scanner gelieferten Anhaltspunkte vertieft untersucht werden können. Doch Vorsicht – der korrekte Sicherheitskontext (psexec –s cmd.exe), in dem der Forensic Scanner zur Ausführung gebracht wird, entscheidet darüber, ob er auf die zu untersuchenden Daten zugreifen kann. (Das lässt sich einfach prüfen, indem man mit beiden Werkzeugen dasselbe Windows-Benutzerprofil analysiert und die Ergebnisse für identische Plugins vergleicht.)

Unumgänglich

Am 10.10.2012 ist auf THC die Version 2.0 des THC-IPv6-Toolkits veröffentlicht worden. Es enthält zahlreiche Tools, mit denen inhärente Schwachstellen von IPv6 demonstriert werden können, vor denen eine Personal Firewall für IPv4 nicht schützt. Für Administratoren ist es zugleich ein guter Werkzeugkasten, um die eigenen Netzwerke auf IPv6 zu untersuchen oder sie zu auditieren.

Das Toolkit belegt, dass die Hacker-Community ihre IPv6-Hausaufgaben gemacht hat: Zur Ausnutzung der inhärenten Schwachstellen von IPv6 stehen bereits alle Werkzeuge zur Verfügung. Zwar wird IPv6 nicht in einem „magischen Moment“ IPv4 ablösen. Dennoch: Selbst wenn die IPv6-Einführung im eigenen Netz noch nicht auf der Tagesordnung steht, wird es für Betreiber und Administratoren Zeit, sich mit IPv6 auseinanderzusetzen, um Angreifern im Verlauf einer Umstellung nicht blindlings ins Messer zu laufen – zumal in der Standard-Konfiguration von Windows IPv6 bereits aktiviert ist.

Secorvo News

… zum Dritten

Die dritte und letzte Gelegenheit für IT-Sicherheitsexperten, ihre Kenntnisse in diesem Jahr mit dem T.I.S.P.-Zertifikat zu krönen, bieten wir am **12.–16.11.** Allen Teilnehmern wird vor Seminarbeginn das von Secorvo verfasste 500seitige Begleitbuch zum T.I.S.P. (Zentrale Bausteine der IT-Sicherheit) zur Vorbereitung zugesandt.

Heute schon gefacebookt?

In vielen Unternehmen drängen Marketing- und Personalabteilung auf eine Unternehmenspräsenz bei Facebook & Co, und meist ist ein erheblicher Teil der Mitarbeiter bereits „drin". In den zum großen Teil von amerikanischen Anbietern betriebenen Social Networks lauern jedoch zahlreiche Fallen, wie Copyrightverletzungen, unkontrollierte Informationspreisgabe und Verstöße gegen Datenschutzbestimmungen.

Zu diesen Fragen gibt der Jurist Michael Knopp am **08.11.2012** beim letzten KA-IT-Si-Event dieses Jahres einen Überblick und praktische Tipps. Für ein besonderes Ambiente ist gesorgt: Erstmals ist die KA-IT-Si mit ihrer Veranstaltungsreihe in den stilvollen Räumlichkeiten der Buhlschen Mühle in Ettlingen zu Gast (Anfahrt; ca. 10-15 Minuten S-Bahn-Fahrt vom Karlsruher Hauptbahnhof). Beginn der Veranstaltung ist um 18 Uhr. Um Anmeldung wird gebeten. Wir freuen uns auf spannende Diskussionen und ein interessantes Networking!

Veranstaltungshinweise

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

Oktober 2012	
31.10.-03.11.	hashdays security & risk conference 2012 (DEFCON Switzerland, Luzern/CH)
November 2012	
05.-06.11.	TISP Community Meeting (TeleTrusT, Köln)
07.11.	German OWASP Day 2012 (OWASP Germany, München)
08.11.	Heute schon gefacebookt? (KA-IT-Si, Ettlingen)
09.11.	Zur Rolle des CISO/IT-Sicherheitsbeauftragten (GI-FG SECMGT, Frankfurt)
12.-17.11.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
22.-23.11.	36. DAFTA (GDD, Köln)
27.-30.11.	DeepSec 2012 (DeepSec, Wien)
Dezember 2012	
03.-04.12.	IsSec/ZertiFa 2012 (Computas, Berlin)

Fundsache

Am 30.07.2012 hat der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) die Ergebnisse einer Befragung von 1.000 Internet-Nutzern ab 14 Jahren und 800 IT-Leitern, CIOs, Datenschutzbeauftragten und Geschäftsführern zu Datenschutz und Informationssicherheit veröffentlicht. Die 30seitige Studie gibt nicht nur Einblick in Organisation, Kosten und Technik der Informationssicherheit in deutschen Unternehmen, sondern zeigt auch den großen Anteil von Internet-Nutzern, die aufgrund von Sicherheitsbedenken die Inanspruchnahme von Online-Diensten verweigern.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Knobloch, Michael Knopp (Editorial), Jochen Schlichting

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

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

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

secorvo
security consulting

Secorvo Security News

November 2012

Überflüssig

„Nachweisbar, sicher, zuverlässig“. Klingt gut, was die Deutsche Telekom ihren De-Mail-Kunden verspricht. Allein – heißt das, dass T-Online-E-Mails weder sicher noch zuverlässig sind? 1&1 bewirbt De-Mail mit „sicherem digitalen Briefversand“ – muss man daran bei web.de, gmx und den E-Mail-Postfächern von Geschäftskunden zweifeln?

Der tatsächliche Vorteil von De-Mail gegenüber einer herkömmlichen E-Mail ist schnell benannt: Die Identität des Senders und vor allem der Empfang sind wie bei einem Einschreiben nachweisbar. Nutznießer sind daher in erster Linie die Absender: Mit der Aktivierung eines De-Mail-Accounts ermöglicht der Empfänger jedem De-Mailer eine nicht abstreitbare Zustellung. Anders als beim Einschreiben gilt die De-Mail jedoch als zugestellt, sobald sie im Postfach liegt – auch im Urlaub. Und damit starten auch etwaige Fristen.

Die wahren Profiteure sind jedoch die Provider: Ihnen bietet sich die einmalige Chance, den (D)E-Mail-Versand wie SMS transaktionsbezogen abzurechnen – und so am Rückgang des Briefverkehrs der Unternehmen zu Gunsten von E-Mails mitzuverdienen.

Das Geschäftsmodell hat jedoch einen Haken, wie jetzt auch die Telekom und 1&1 erkannt haben: Da eine De-Mail wie ein eingeschriebener Brief dem Sender in Rechnung gestellt wird, profitiert vor allem der Anbieter, der die Großversender (Versicherungen, Banken, Behörden) für den Dienst gewinnen kann. Telekom und 1&1 fordern daher eine Umsatzbeteiligung von der Deutschen Post, die die De-Mail derzeit bei ihren Geschäftskunden bewirbt.

Die Interessen der Endnutzer bleiben dabei auf der Strecke – darüber kann auch das „Schutzversprechen“ der De-Mail-Anbieter nicht hinwegtäuschen. Denn „sicher und zuverlässig“ sind (ggf. verschlüsselte) E-Mails auch ohne De-Mail. Und in den extrem seltenen Fällen, in denen eine Nachweisbarkeit erforderlich ist, genügt das gute alte Einschreiben vollauf. Hoffen wir, dass der Markt es richtet.

Inhalt

secorvo
security consulting

Security News

Das Tracking und die Standards

Beim „Tracken“ von Internet-Benutzern stehen sich Datenschützer und Werbewirtschaft scheinbar unversöhnlich gegenüber. Umso erstaunlicher die jüngsten Fortschritte bei technischen Ansätzen zur Abwehr von Tracking: So hat am 06.11.2012 auch Google die sehr versteckte Implementierung von „Do Not Track“ (DNT) für Google Chrome 23 angekündigt. Deutlich offensiver geht Microsoft vor, die mit dem Internet Explorer 10 DNT als Standard aktivieren. Damit haben sie eine hitzige Diskussion ausgelöst, die in einem Apache-Patch gipfelt, der die DNT-Option von IE 10 ignoriert.

Ergänzend hat das W3C am 02.10.2012 die Working Drafts für die Standards Tracking Preference Expression und Tracking Compliance and Scope veröffentlicht. Angesichts technischer Entwicklung, Standards und öffentlichen Diskussionen wächst die Hoffnung, dass sich DNT zu einem Werkzeug entwickelt, mit dessen Hilfe Benutzer ihren Willen zukünftig unmissverständlich und durchsetzbar zum Ausdruck bringen können.

Die Eltern und das Filesharing

Die Entscheidungen zur Störerhaftung des Anschlussinhabers bei Urheberrechtsverstößen sind seit dem 15.11.2012 um ein höchstrichterliches Urteil reicher. Mit der Feststellung, dass Eltern ihre Kinder zwar über Verbote aufklären müssen, dann aber bei Urheberrechtsverletzungen nicht wegen einer Aufsichtspflichtverletzung haften, hat der BGH eine weitere Streitfrage geklärt.

In dem entschiedenen Fall hatte der 13jährige Sohn der Beklagten 147 Audiodateien über einen längeren Zeitraum via Tauschbörse zum Download angeboten; die Icons der verwendeten Tausch-Software waren sogar auf dem Desktop seines Rechners zu sehen. Die Vorinstanzen hatten aus § 832 Abs. 1 BGB Aufsichtspflichten abgeleitet, die über eine einfache monatliche Verlaufskontrolle auf dem Rechner sowie die Installation eines „Security-programms“, das die Installation weiterer Programme verhindern sollte, hinausgingen: Danach hätten die installierten Programme über die Systemsteuerung überprüft werden müssen. Der BGH hat diese Pflichten auf Aufklärung reduziert, sofern mit der Einsichtsfähigkeit des Kindes zu rechnen ist.

Damit gewichtet der BGH zugleich das Gefahrenpotential des Internetzugangs als Schädigungsinstrument niedriger. Daher könnte das Urteil auch bei zukünftigen Entscheidungen zu den Pflichten von Internetanschlussinhabern zu zurückhaltenderen Forderungen führen.

Das BSI und die Macs

Lange hat sich zum Thema Mac OS beim BSI nicht viel bewegt – die Vorabversion des IT-Grundschutz-Bausteins MacOSx datiert vom Januar 2012. Aktuelle Mechanismen wie die Vollverschlüsselung vor allem mobiler Geräte mit FileVault 2 sucht man vergeblich. Am 15.10.2012 hat das BSI nun Empfehlungen zur sicheren Nutzung von Macs unter Apple OS X Mountain Lion veröffentlicht. Leider bleiben die Hinweise überwiegend oberflächlich oder schaffen Verwirrung: So widerspricht das Dokument den Empfehlungen des BSI im Anti-Botnet Beratungszentrum zum Einsatz von Virenschutzprogrammen unter Mac OS.

Dabei sollte man sich als Mac OS User besser nicht in Sicherheit wiegen – das belegt schon eine kurze Suche in der CVE-Liste. So lange weder Apple noch die NSA oder CISecurity aktuelle Security Guidelines für OSx veröffentlicht haben, bieten die Empfehlungen des BSI immerhin einen ersten Einstieg in die Sicherheitskonfiguration eines Macs.

Die Biometrie und die Software

Zumindest in Business-Laptops sind Fingerabdrucksensoren zur Benutzerauthentifikation inzwischen weit verbreitet. Sie vereinfachen das Betriebssystem-Login – und hinterlassen das gute Gefühl, den Laptop „biometrisch“ gesichert zu haben.

Tatsächlich ist es mit dem Schutz nicht ganz so weit her, wie schon am 28.08.2012 bekannt wurde: Geräte, die mit Sensoren der Firma UPEK ausgestattet waren, speichern die Windows-Passwörter ihrer Benutzer AES-verschlüsselt in der Registry – durch einen Implementierungsfehler allerdings so, dass es Mitarbeitern von ElcomSoft gelang, die Passwörter auszulesen.

Das wäre wenig mehr als ein Bug unter vielen – wenn da nicht die (inzwischen von der Webseite des Anbieters gelöschte) Liste der Hersteller wäre, die den UPEK-Sensor einsetzen: Acer, Asus, Dell, Gateway, Lenovo, MSI, NEC, Samsung, Sony und Toshiba. Sucht man auf der Webseite der (erst im Juli 2012 für 356 Mio. USD erworbenen) Apple-Tochter AuthenTec, zu der UPEC seit 2010 gehört, nach näheren Informationen, stößt man auf den lapidaren Hinweis: „AuthenTec's Smart Sensor products are no longer available.“

Gelöst ist das Problem (anders lautenden Ankündigungen zum Trotz) offenbar bisher nicht. Daher können wir nur dringend dazu raten, die entspre-

chenden Treiber zu deinstallieren und den Sensor nicht für das Windows-Login zu nutzen – selbst wenn die Festplatte des Rechners verschlüsselt ist.

Das OWASP und die DuD

Die OWASP AppSecUSA 2012 lockte am 25. und 26.10.2012 ca. 800 Interessierte nach Austin, und am 07.11.2012 trafen sich über 200 Teilnehmer beim OWASP Day Germany 2012 in München zum Thema sichere Webanwendungen. Beide Veranstaltungen zeichneten sich durch eine durchgängig sehr hohe Qualität der Vorträge und (den Teilnehmerzahlen sei Dank) vielfältige Möglichkeiten zum Networking aus. Die Vorträge aus München stehen inzwischen zum Download bereit. Die steigenden Teilnehmerzahlen unterstreichen die wachsende Bedeutung der Anwendungssicherheit. Interessierte finden auf den Seiten des deutschen Chapters der OWASP sowie im Schwerpunktheft 11/2012 der DuD einen guten Einstieg in das Thema.

Das Online-Banking und die mTAN

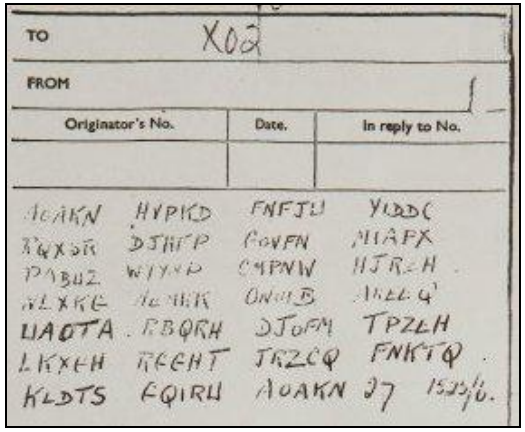
Am 13.11.2012 hat das Berliner Landeskriminalamt eine Warnung für Nutzer des mTAN- (oder SMS-TAN)-Verfahrens veröffentlicht. Diese Bedrohung ist nicht ganz neu – schon am 25.09.2010 hatte David Barroso in seinem Blog über Erweiterungen des Banking-Trojaners ZeuS zu einem „Man-in-the-Mobile"-Trojaner gewarnt (siehe auch Fundsache SSN 9/2010). Jetzt scheinen SMS-Trojaner deutsche Bankkunden im großen Stil ins Visier zu nehmen.

Der Angriff ist denkbar einfach – und hebelt den „getrennten Kanal" zur Übersendung der TAN vollständig aus. Der Trojaner fordert den Bankkunden am PC zum Download eines „Handy-Updates" auf – das anschließend dafür sorgt, dass jede SMS-TAN an den Angreifer weitergeleitet wird.

Gegen diesen Angriff ist nur ein einziges Kraut gewachsen: Die Geistesgegenwart des Nutzers. Denn strikte „Kanaltrennung" kann nur funktionieren, wenn niemals Software direkt oder indirekt über den (möglicherweise befallenen) PC auf das Smartphone übertragen wird.

Die Taube und die Nachricht

Die am 01.11.2012 von BBC News veröffentlichte verschlüsselte Nachricht, die in Südengland am Skelett einer Brieftaube gefunden wurde und wahrscheinlich von einem Sergeanten der Royal Air Force aus dem Ende des Zweiten Weltkriegs stammt, konnte bisher nicht entschlüsselt werden. Wer sich über Weihnachten daran versuchen möchte: Hier ist der Chiffretext.



Secorvo News

500 T.I.S.P.-Zertifkate

Jetzt ist es amtlich: Mitte November erhielt der 500ste T.I.S.P.-Absolvent sein Zertifikat. Das vom Bundesverband IT-Sicherheit (TeleTrusT) entwickelte Expertenzertifikat, das dreijährige Berufserfahrung in der IT-Sicherheit voraussetzt, hat sich damit als berufsqualifizierender Nachweis für Informationssicherheit durchgesetzt und genießt hohe Anerkennung.

Das von Secorvo verfasste, 500-seitige Begleitbuch zum T.I.S.P.-Seminar „Zentrale Bausteine der Informationssicherheit" (80 Euro) bietet eine Zusammenfassung des T.I.S.P.-Grundlagenwissens in 22 Kapiteln – eine unverzichtbare Lektüre für lange Winterabende. Wer sich zu einem T.I.S.P.-Seminar bei Secorvo anmeldet, erhält das Buch zur Vorbereitung übersandt. Nächster Termin: **15.–19.04.2013**.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Eröffnung des Kryptologikums

In das kommende Jahr startet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit einem Highlight: Am **31.01.2013** werden wir im Zentrum für Kunst und Medientechnologie (ZKM) das „Kryptologikum" des Karlsruher Institute of Technology (KIT) eröffnen. Ähnlich dem Mathematikum in Gießen, dem Dynamikum in Pirmasens und dem Technoseum in Mannheim bietet das Kryptologikum in einer zunächst dreitägigen Ausstellung (vom 01.-03.02. 2013) Kryptographie zum „Begreifen". Die Exponate veranschaulichen kryptographische Prinzipien, und es werden historische Verschlüsselungsmaschinen gezeigt, die Kriege entschieden haben.

Das Eröffnungsevent beginnt um 18 Uhr im Kubus des ZKM in Karlsruhe. Zur Einstimmung bieten wir um 16 und 17 Uhr eine Führung zur voll funktionsfähigen Zuse Z22 an, die im ZKM ausgestellt ist.

Wir freuen uns auf Ihre Teilnahme – und empfehlen Ihnen eine frühzeitige Anmeldung.

Veranstaltungshinweise

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

Dezember 2012	
03.-04.12.	IsSec/ZertiFa 2012 (Computas, Berlin)
27.-30.12.	29th Chaos Communication Congress (29C3) (Chaos Computer Club, Hamburg)
Januar 2013	
15.-17.01.	OMNICARD 2013 (in TIME berlin, Berlin)
31.01.	Eröffnung des Kryptologikum (KIT, ZKM & KA-IT-Si, Karlsruhe)
Februar 2013	
06.-07.02.	23. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
19.-20.02.	20. DFN Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2013	
05.-09.03.	CeBIT (Deutsche Messe, Hannover)
11.-14.03.	CPSSE-Schulung (Secorvo College, Karlsruhe)
12.-15.03.	Black Hat Europe 2013 (Blackhat, Amsterdam/NL)
18.-21.03.	Security Engineering (Secorvo College, Karlsruhe)

Fundsache

Jedes Kryptoverfahren ist immer nur so sicher wie seine Schlüssel – dieses Prinzip wird leider beim Design von Sicherheitslösungen allzu häufig missachtet. Am 16.11.2012 hat das US-amerikanische NIST als Special Publication SP 800-133 konkrete Empfehlungen zur Schlüsselgenerierung veröffentlicht – ein ‚Must Read' für jeden Systemdesigner.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Michael Knopp.

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

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

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

secorvo
security consulting

Secorvo Security News

Dezember 2012

Das Analoge im Digitalen

Es mutet manchmal eigenartig an, wie bereitwillig viele Menschen die Risiken der digitalen Welt ignorieren. Bruce Schneier zeichnet in seinem jüngsten Crypto-Gram diese „schöne neue Welt" sogar als eine Art „digitaler Leibeigenschaft" – mit Amazon, Apple, Facebook und Google in der Rolle der Feudalherren, denen ihre Vasallen alles anvertrauen. Aus der Fürstenperspektive gibt es natürlich wenig Grund, die Legitimität dieses einseitigen Vertrauensverhältnisses und der Möglichkeit absoluter Kontrolle in Zweifel zu ziehen. Merkwürdig stimmt allerdings, dass Milliarden Nutzer sich begeistert in diese Abhängigkeit begeben – und sogar zu glühenden Anhängern werden, die bereitwillig mithelfen, nicht nur das Mantra ihres Herrn zu verbreiten, sondern es eifernd gegen jeden Skeptiker oder Kritiker und gegen alle Anhänger anderer Fürsten zu verteidigen.

Einige bemühen zur Rechtfertigung immerhin Fatalismus: „Warum ich die iCloud benutze? Apple weiß doch ohnehin alles über mich...". Dabei kämen die meisten von ihnen im wirklichen Leben kaum auf ähnliche Ideen: „Warum sollte ich meinem Nachbarn nicht meine Kreditkarte und die EC-Karte mit PIN anvertrauen? Den Haustürschlüssel hat er doch auch schon..." Helfen könnten daher bewährte Strategien aus der analogen Welt auch in der digitalen:

- Vertraue Dritten nie blind – sondern immer nur so, dass du das Vertrauen auch jederzeit wieder entziehen kannst.
- Setze nie alles auf eine Karte.
- Vertraue nie unbegrenzt – behalte immer einen Rest Kontrolle.

Weder frühmittelalterliche Fürstenhuldigung noch Bequemlichkeit oder Kostenfokussierung sind eine angemessene Haltung für Risikobewertung und Schadensbegrenzung. Aber wie formulierte Marie Freifrau Ebner von Eschenbach (1830-1916) doch so treffend: „Die glücklichen Sklaven sind die erbittertsten Feinde der Freiheit."

Inhalt

secorvo
security consulting

Security News

Rechtsverstoß Double-Opt-In

Am 27.09.2012 hat das OLG München mit einer Entscheidung für große Verunsicherung gesorgt, nach der die Bestätigungsanfrage beim Double Opt-In-Verfahren zur E-Mail-Werbung als unzumutbare Belästigung zu betrachten ist, wenn sie nicht nachweislich vom Empfänger veranlasst wurde.

Dies wird von der Beratungsszene und Anbietern kontrovers diskutiert. Klar ist: § 7 Abs. 2 Nr. 3 UWG verbietet E-Mail-Werbung ohne ausdrückliche und nachweisbare Einwilligung. Das Double-Opt-In soll daher sicherstellen, dass keine werbliche Ansprache via E-Mail erfolgt, wenn die Einwilligung nicht vom Inhaber der dabei angegebenen E-Mail-Adresse auf Anforderung bestätigt wird. Der BGH hat 2004 in anderer Konstellation bereits entschieden, dass ein Double Opt-In den notwendigen Nachweis der elektronischen Einwilligung führen kann.

Nun kann ein Teil eines Authentifizierungs- und Schutzmechanismus ohne werbliche Inhalte naturgemäß eigentlich keine unzumutbare Belästigung sein, solange sie durch einen Webseiteneintrag veranlasst wurde. Dieser freilich muss genauso wie die spätere Bestätigung protokolliert und aufbewahrt werden. Allerdings kann bei einer Anmeldung über ein Webformular selbst bei Protokollierung kein personenbezogener Veranlassungsnachweis gelingen – es sei denn, der Nutzer würde sich auf andere Weise authentifizieren. Dann wäre jedoch eine Bestätigung (und damit auch die E-Mail-Benachrichtigung) überflüssig. Für die Versender von E-Mail-Newslettern und -Werbung bleibt jedoch bis zur höchstrichterlichen Klärung das Risiko, für das Double Opt-In-Verfahren abgemahnt zu werden.

Smart Meter Profiles

Das Weihnachtsgeschenk des BSI vom 21.12.2012 sind Version 1.1.7 der Protection Profiles für Smart Meter Gateways und Version 1.0 der Protection Profiles der in Smart Meter Gateways enthaltenen Security Modules. Die Funktionalitäts- und Interoperabilitätsanforderungen wurden in der Technischen Richtlinie TR-03109 (Version 1.0, Release Candidate) spezifiziert. Alle drei Dokumente sollen zusammen mit dem Referentenentwurf der Rechtsverordnung nach § 21i EnWG Anfang 2013 von der EU notifiziert und damit für die Entwicklung von Komponenten der so genannten „intelligenten Energienetze“ rechtlich bindend werden.

Zwar handeln die Spezifikationen alle wichtigen Sicherheitsaspekte von der Authentifikation bis zur verschlüsselten Übermittlung systematisch ab. Themen des Datenschutzes werden jedoch – trotz Mitwirkung des BfDI – auf gerade einer der 90 Seiten behandelt, beschränkt auf Pseudonyme und Übertragungsschutz. Fragen nach Erforderlichkeit, Zweckbindung oder Datensparsamkeit bleiben ausgeklammert: die Protection Profiles sorgen also auch bei unzulässiger Erhebung für einen guten Schutz. Die Frage der Rechtmäßigkeit der mit Smart Meter Gateways geplanten und möglichen Verarbeitung von Verbraucherdaten bleibt damit dem politischen Diskurs vorbehalten.

Löschen nach Regeln

Die Festlegung von Regellöschfristen für verarbeitete personenbezogene Daten ist eine der größten praktischen Herausforderungen des Datenschutzrechts. Ausgelöst durch Veröffentlichungen der Toll Collect GmbH über ihr Datenschutz-Löschkonzept schrieb der DIN Anfang 2012 ein vom BMWI gefördertes Projekt im Programm „Innovation mit Normen und Standards“ aus, um die Möglichkeit einer standardisierten Vorgehensweise für die Entwicklung von Löschkonzepten zu untersuchen.

Am 10.12.2012 wurde nun die in intensiver Diskussion mit Datenschützern aus Industrie und Aufsichtsbehörden von Secorvo erarbeitete Leitlinie zur Entwicklung eines Löschkonzepts (Dr. Volker Hammer, Karin Schuler) vorgestellt. Die zuständige ISO/IEC-Arbeitsgruppe hat Interesse an einer Fortsetzung der Standardisierungsarbeiten signalisiert; sofern die Finanzierung der Arbeiten durch Förderunternehmen gesichert werden kann, könnte nun unter deutscher Federführung ein internationaler Lösch-Standard für personenbezogene Daten entstehen. Bei Interesse stellen wir gerne einen Kontakt her – E-Mail an redaktion-security-news@secorvo.de genügt.

Cyberentschlossenheit

Das Europäische Parlament hat am 22.11.2012 eine Entschließung zur Cybersicherheit und Verteidigung angenommen. Darin werden EU-Institutionen und Mitgliedstaaten aufgefordert, unter Einbindung privater Unternehmen Maßnahmen zu ergreifen. Die Zustandsfeststellungen dokumentieren vor allem ein EU-weit uneinheitliches Vorgehen gegen Cyberattacken – trotz gewachsener Bedrohung. Insbesondere sähen nur wenige Staaten bislang den Schutz ihrer IT-Infrastrukturen als Teil ihrer Sorgfaltspflichten, nur zehn Mitgliedstaaten besäßen eine nationale Strategie, und mangels Meldungen bestünde eine hohe Dunkelziffer an Angriffen.

Gefordert werden ein gemeinsames Weißbuch, eine gründliche Erfassung der Angriffe und Bewertung der Gefahren, eine koordinierte Reaktion auf EU-Ebene und die Erarbeitung von Notfallplänen in Kooperation mit der ENISA. Schließlich wird sogar

die Anerkennung eines schweren Cyber-Angriffs als Solidaritätsfall und Kriegsgrund postuliert.

Die Entschließung signalisiert zwar Entschlossenheit; die Maßnahmenvorschläge erscheinen jedoch als ein willkürliches Sammelsurium von Ausbildungsförderung bis Kriegserklärung. Der Weg zu einer geschlossenen Strategie ist noch weit.

Neues vom Bundestrojaner

Am 17.10.2012 hatte die SPD-Fraktion der Bundesregierung in einer kleinen Anfrage 55 spannende Fragen zum Bundestrojaner gestellt – unter anderem zur Weigerung der Fa. DigiTask, dem BfDI Einsicht in den Quellcode zu gewähren. Am 10.12.2012 wurden nun die Antworten der Bundesregierung vom 21.11.2012 veröffentlicht. Einige sind durch einen Hinweis auf die Vertraulichkeitsstufe (VS-NfD) ersetzt. Dennoch enthält das Dokument interessante Details – u. a. den Hinweis, dass Skype-Telefonate nicht abhörbar seien und mit einer vom BKA selbst entwickelten Überwachungssoftware erst Ende 2014 gerechnet werden könne.

Keylogger

Heutige Hardware-Keylogger sind günstig (ca. 60$), bescheren Aufmerksamkeit (wie im Fall vom 23.10.2012), arbeiten beinahe transparent und speichern mehrere GB Tastendrücke. Sofortmaßnahmen für den Finder sind Passwortwechsel, polizeiliche Spurensicherung, Sicherung der Gebäude-Zutrittsprotokolle und ggf. in Abstimmung mit Datenschutz und Betriebsrat eine Raumüberwachung oder die Hinterlegung der Adresse eines Honeypots auf dem Logger.

Ähnlich hässlich ist die am 25.10.2012 von Ryan Barnett auf der AppSecUSA präsentierte Idee: Dabei infiziert eine Web Application Firewall ausgewählte „Besucher“ mit dem Browser Exploitation Framework (kurz BeEF) per Angriff auf Web Browser-Schwachstellen, um dann z. B. einen Software-Keylogger zu platzieren.

Manchmal kommt ein Keylogger auch nicht allein: Scannen Sie daher nicht nur regelmäßig Ihr System, sondern prüfen Sie auch von Zeit zu Zeit Ihre Schnittstellen – oder sorgen Sie mit Klebstoff für eine feste Verbindung von Tastaturstecker und PC.

Neujahrsputz

Wer gleich zu Beginn des neuen Jahres die Angriffsfläche seines PCs reduzieren möchte, sollte Java in seinen Browsern deaktivieren. Denn während es kaum noch einen guten Grund gibt, mit aktiviertem Java im Browser zu surfen, öffnen unsichere Java-Versionen Angreifern Tür und Tor: Von lediglich drei im Jahr 2011 stieg die Zahl der 2012 veröffentlichten Security Vulnerabilities des JRE auf beeindruckende 58 – stattliche 23 davon mit der höchsten Gefährdungsstufe 10.

Hilfreiche Anleitungen um Java mit wenig Aufwand wirksam aus dem Browser zu verbannen finden Sie bei Andrew Tech Help, Brian Krebs oder OSXDaily.

Secorvo News

Eröffnung des Kryptologikums

In das Jahr 2013 startet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit einem besonderen Highlight: Am **31.01.2013** werden wir im Zentrum für Kunst und Medientechnologie (ZKM) das „Kryptologikum“ des Karlsruher Institute of Technology (KIT) eröffnen. Ähnlich dem Mathematikum in Gießen, dem Dynamikum in Pirmasens und dem Technoseum in Mannheim bietet das Kryptologikum in einer zunächst dreitägigen Ausstellung (vom 01.-03.02. 2013) Kryptographie zum „Begreifen“. Die Exponate veranschaulichen kryptographische Prinzipien und es werden historische Verschlüsselungsmaschinen gezeigt, die Kriege entschieden haben.

Das Eröffnungsevent beginnt um 18 Uhr im Kubus des ZKM in Karlsruhe. Wir freuen uns auf Ihre Teilnahme – und empfehlen Ihnen eine schnelle Anmeldung.

Sichere Systeme

Technisch verursachte Sicherheitsvorfälle können in der Regel auf eine von drei Ursachen zurückgeführt werden: Konfigurationsfehler, Programmierfehler oder ein fehlerhaftes Systemkonzept. Die letzte dieser Ursachen ist oft besonders heikel: Sie entsteht durch das Zusammenspiel komplexer Einzelkomponenten und lässt sich zumeist nur durch einen teuren Systemwechsel beseitigen.

Um dieses Problem an der Wurzel zu packen, haben wir gemeinsam mit dem Institut für Kryptographie und Sicherheit (IKS) am Karlsruhe Institute of Technology (KIT) ein Seminar für Systementwickler konzipiert, in dem wir in das Konzept des „Security by Design“ einführen: Security Engineering – Anleitung zur Entwicklung sicherer Systeme am 18.-21.03.2012.

Im April folgt die nächste Schulungen zum T.I.S.P. Zertifikat – von den Autoren des T.I.S.P.-Buchs. Nutzen Sie die Gelegenheit, Ihre Qualifikation abzurunden und zertifizieren zu lassen. Alle weiteren Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter
http://www.secorvo.de/college

Veranstaltungshinweise

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

Januar 2013	
15.-17.01.	OMNICARD 2013 (in TIME berlin, Berlin)
31.01.	Eröffnung des Kryptologikums (KIT, ZKM & KA-IT-Si, Karlsruhe)
Februar 2013	
06.-07.02.	23. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
19.-20.02.	20. DFN-Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2013	
05.-09.03.	CeBIT (Deutsche Messe, Hannover)
11.-14.03.	CPSSE-Schulung (Secorvo College, Karlsruhe)
12.-15.03.	Black Hat Europe 2013 (Blackhat, Amsterdam/NL)
18.-21.03.	Security Engineering (Secorvo College, Karlsruhe)
April 2013	
09.-11.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
15.-19.04.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
16.-17.04.	Datenschutztage 2012 (Forum für Datenschutz, Wiesbaden)
23.-26.04.	PKI (Secorvo College, Karlsruhe)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Volker Hammer, Kai Jendrian, Michael Knopp, Sven Köhler.

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

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

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