secorvo
security consulting

Secorvo Security News

Januar 2010

O Elena, O mores...

Noch ist die Entscheidung über die verfassungsrechtliche Zulässigkeit einer Vorratsspeicherung von Telekommunikationsdaten nicht gefallen, da tritt das ELENA-Verfahren aus dem Windschatten in die öffentliche Wahrnehmung. Das überrascht etwas – wurde das Verfahren des „Elektronischen Entgeltnachweises" doch bereits am 22.09.2009 vom Bundestag beschlossen. Tatsächlich weist die Entstehungsgeschichte sogar sieben Jahre weit zurück – und ist ein Lehrstück regulativer Technikgestaltung in Deutschland.

Als Projekt „JobCard" erblickte Elena im August 2002 als ein Vorschlag der Hartz-Kommission das Licht der Welt. Signaturkartenverfechter witterten Morgenluft: War das endlich die „Killer-Applikation" der digitalen Signatur? Mit der Behauptung einer Entlastung der Unternehmen um 85,6 Mio. Euro jährlich – im Schnitt beeindruckende 29 Euro je Unternehmen – wurden die verfassungsrechtlichen Zweifel von Datenschützern an der für das Verfahren erforderlichen zentralen Speicherung von Arbeitnehmerdaten erstickt. Tatsächlich macht die Spezifikation der Datensätze vom 19.10.2009 (inzwischen von der Elena-Webseite gelöscht) sprachlos: Neben Entgeltinformationen werden Fehlzeiten mit Datum und Grund, Urlaubstage, Kündigungsgründe und vorausgegangene Abmahnungen inklusive einer Beschreibung des vertragswidrigen Verhaltens (Freitext) erhoben.

Wir erinnern uns: Datenschutz ist Teil des allgemeinen Persönlichkeitsrechts (Art. 2 GG). Eines der Prinzipien ist der Erforderlichkeitsgrundsatz („Datensparsamkeit") – keine Spur davon bei Elenas Vorratsdatenspeicherung. Aber mit dem Datenschutzrecht nimmt man es bei Elena sowieso nicht so genau: „Eine Auskunft ist vor 2012 (...) nicht realisierbar, da der Abruf durch die abrufenden Stellen erst ab 2012 möglich ist„, heißt es lapidar auf der Webseite. Ein klarer Rechtsverstoß, denn das Auskunftsrecht besteht nach § 34 BDSG uneingeschränkt. Wir empfehlen: Fordern Sie es ein (Vorlage). Und falls Sie keine Auskunft erhalten, wenden Sie sich an den Bundesdatenschutzbeauftragten.

Inhalt

secorvo
security consulting

Security News

768 bit faktorisiert

Schon am 12.12.2009 gelang einem internationalen Kryptologen-Team um Bos, Franke, Kleinjung, Lenstra und Montgomery die Lösung der 768-bit-RSA-Challenge – die Zerlegung eines 768-bit-Modulus in seine Primfaktoren. Details der Number Field Sieve-Faktorisierung veröffentlichten die Autoren am 06.01.2010. Danach benötigten sie 2^{37} Operationen (≈ 4,7 Mio. MIPS-Jahre) zur Bestimmung der Primfaktoren – nur ein Zehntel des von Silverman im Jahr 2000 geschätzten Aufwands. Für den aufwändigsten Teil der Berechnung, das „Aussieben", arbeiteten viele hundert Workstations über zwei Jahre – das entspricht etwa 1.500 Rechenjahren eines 2.2 GHz AMD Opteron-Prozessors.

Tatsächlich deckt sich dieser Erfolg fast exakt mit der im Jahr 2002 veröffentlichten Prognose von Secorvo (siehe Abb.): Darin hatten wir die Faktorisierung von 768 bit für Anfang 2010 vorausgesagt.

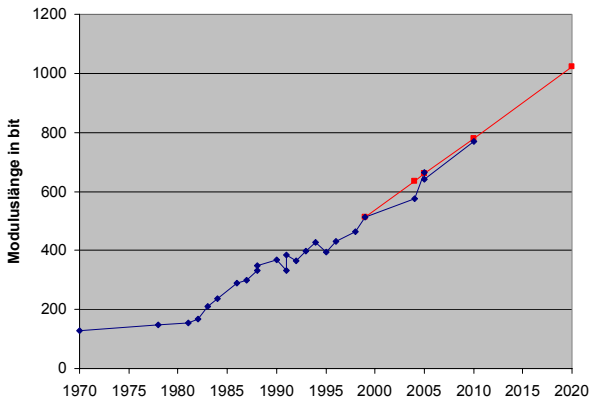


Abb.: Faktorisierungserfolge (blau), Prognose (rot)

Trotz dieses Faktorisierungserfolgs liegt die öffentliche NFS-Faktorisierung eines 1.024-bit-Modulus noch deutlich in der Zukunft – der dafür erforderliche Aufwand ist um den Faktor 1.000 größer. In den kommenden fünf Jahren sei daher auch unter Berücksichtigung des technischen Fortschritts nicht mit einer Faktorisierung zu rechnen. Die Secorvo-Prognose erwartet die Faktorisierung Anfang des Jahres 2020 – spätestens dann sollten 1.024-bit lange RSA-Schlüssel nicht mehr eingesetzt werden.

Legic gebrochen

Fast auf den Tag genau zwei Jahre nach dem spektakulären Brechen der Mifare-Classic-Chipkarten (siehe SSN 03/2008) haben Karsten Nohl und Henryk Plötz am 29.12.2009 auf dem 26. Chaos Computer Congress das Clonen von Legic Prime Chipkarten präsentiert. Da der Hersteller, wie sie feststellen mussten, komplett auf Kryptoverfahren verzichtet und lediglich ein simples 7-bit-Schieberegister für den „Schlüsselstrom" verwendet hatte, konnten sie sich eine aufwändige Chip-Analyse sparen – „Security by Obscurity" bricht man eleganter mit „Trial and Error".

Unternehmen, die vor zwei Jahren schadenfroh mit dem Finger auf die vom Mifare-Hack betroffenen Firmen gezeigt, sich aber bis heute auf ihre Legic Prime Chips verlassen haben, ohne auf das „Legic Advant"-Verfahren zu migrieren, droht nun ein böses Erwachen – den Passepartout in ihr Unternehmen gibt es jetzt zum Preis einer Taxifahrt.

WASC Threat Classification

Zum Jahresbeginn wurde am 01.01.2010 vom Web Application Security Consortium (WASC) die Version v2.0 der „WASC Threat Classification" veröffentlicht. Die Darstellung von 34 verschiedenen Angriffen (z. B. Buffer Overflow, XSS, SQL Injection) auf Web-Anwendungen und 15 Schwachstellen (z. B. Directory Indexing, Insufficient Authorization, Server Misconfiguration) ist sowohl online als auch als 171 Seiten starkes PDF-Dokument verfügbar. Sie gibt einen guten Überblick über aktuelle mögliche Probleme von Web-Anwendungen.

Jeremiah Grossman nimmt in seinem Blog eine Zuordnung zwischen der WASC Threat Classification und den OWASP Top Ten 2010 RC1 (siehe SSN 11/2009) vor – wobei sich der Eindruck aufdrängt, dass durch eine engere Zusammenarbeit und Abstimmung zwischen WASC und OWASP doppelte Arbeit vermieden werden könnte.

Empfohlene Kryptoverfahren

Das US-amerikanische National Institute of Standards and Technology (NIST) veröffentlichte am 14.01.2010 die jüngsten Empfehlung zu Krypto-Algorithmen und Schlüssellängen als Draft Special Publication 800-131. Danach steigt das vorgeschriebene Sicherheitsniveau ab 2011 auf mindestens 112 bit – nur noch Triple-DES mit drei Schlüsseln und AES-128, -192 und -256 dürfen dann noch von Bundesbehörden eingesetzt werden. Auch der SHA-1 darf ab 2011 nicht mehr für die Signaturerzeugung genutzt werden, DSA und RSA müssen Moduluslängen von mindestens 2.048 bit verwenden und Verfahren auf Elliptischen Kurven wie ECDSA Endliche Körper der Ordnung 224. Ab dem Jahr 2031 soll das Sicherheitsniveau auf mindestens 128 bit steigen – eine Anforderung, die die NSA bereits heute an „secret" klassifizierte Daten stellt.

Dem Entwurf des BSI zu Folge wird sich auch die Empfehlung geeigneter Algorithmen der BNetzA, die in Kürze im Bundesanzeiger publiziert werden wird, an die NIST-Empfehlung annähern: RIPEMD-

160 und SHA-1 dürfen danach nur noch bis Ende 2010 zur Signaturerzeugung eingesetzt werden, die Mindestlänge von RSA-Moduli steigt auf 1.976 bit.

DNSSEC livehaftig

Seit dem 05.01.2010 stellt die DENIC eG im DNSSEC Testbed für Deutschland auf zwei speziell eingerichteten Nameserverclustern einen Name Service für die Top Level Domain .de bereit, bei dem die autoritativen Auskünfte per DNSSEC signiert sind. Dies ist zwar noch kein regulärer DNSSEC Betrieb für .de, aber doch genau wie im richtigen Leben: Die DNS-Auskünfte des Testbeds sind ebenso vollständig und aktuell wie die der offiziellen Nameserver von a.nic.de bis z.nic.de.

Wer selbst schon DNSSEC für seine .de-domain einsetzt, muss sich noch bis zum März 2010 gedulden - ab dann wird die DENIC auch Key Signing Keys untergeordneter Domains registrieren und per DNSSEC zertifizieren.

Audit-Wundertüte runderneuert

Die am 11.01.2010 erschiene Auditing-Distribution Backtrack 4 Final wurde gegenüber Version 3 auf Ubuntu umgestellt, um ein zeitnahes Patchmanagement zu ermöglichen. Der revisionssicher nachvollziehbare Change der ca. 500 Prüfwerkzeuge – sowie zukünftiger Ergänzungen – kann anhand der Loginformationen der Installationsumgebung nachgewiesen werden. Wichtige Ergänzungen – neben der deutlich erweiterten Treiberunterstützung für Hardware – sind bekannte Programmpakete, wie OpenVAS 3.0, Nmap 5.2 und Metasploit 3.3.3. Die Sniffersuite lässt nun auch bei Bluetooth, RFID und Voice over IP kaum noch einen Wunsch offen.

Der Scanner OpenVAS wurde als freier Nessusersatz integriert und läuft stabil mit ca. 15.500 Prüfungen. Zeitsparend ist die integrierte Versionierung von bisherigen Scans und Scanergebnissen für deren Wiederholbarkeit. Für Prüfungen, die einen Proof-of-Concept erfordern, ist die Weiterführung von milw0rm in der exploit-db (mehr als 10.000 technische Schwachstellen) eine erfreuliche Ergänzung. Spannend wird es – die richtige Grafikkarte(n) vorausgesetzt – bei der Nutzung von Werkzeugen, die auf CUDA basieren. Hier sind u. a. Multiforcer (Passwort-Bruteforcer für MD5, FASTMD5, MD4, FASTMD4, NTLM, FASTNTLM, SHA1, FASTSHA1), der RAR-Archivbrecher cRARk und Pyrit (für WPA2-PSK) treue Helfer.

Insgesamt also ein unverzichtbares Werkzeug für den (technischen) Auditor mit zahlreichen sinnvollen „Aufrüstungen".

SOA-Kompendium

Am 05.01.2010 hat das BSI Version 2.0 des in erster Fassung vor zwei Jahren veröffentlichten „SOA-Security-Kompendium Sicherheit in Service-orientierten Architekturen" herausgegeben. In dem 371seitigen PDF-Dokument werden verschiedene Sicherheitsaspekte von SOA-Umgebungen ausführlich dargestellt. Aufgrund der Komplexität des Themas ist die Verfügbarkeit eines umfassenden Referenzwerks, das neben einer Einführung besonders die Themen Technologien (96 Seiten), Security Management (46 Seiten) und spezielle Sicherheitskonzepte (72 Seiten) behandelt, eine echte Arbeitshilfe.

Secorvo News

Secorvo College aktuell

Die Nachfrage nach einer TISP-Zertifizierung ist ungebrochen - seit 2004 haben 350 Sicherheitsexperten das Zertifikat erworben. Lassen auch Sie Ihre Qualifikation bei der nächsten TISP-Schulung mit anschließender Prüfung vom **22.–27.02.2010** zertifizieren. Dass Sicherheit auch in der Software Entwicklung eine immer wichtigere Rolle spielt, zeigt das wachsende Interesse am Certified Professional for Secure Software Engineering (CPSSE). Das Zertifikat können Sie vom **16.–19.03.2010** erwerben. Im März steht außerdem erstmals das neue Seminar „Sicherheitsmanagement heute" auf dem Programm. Verschaffen Sie sich vom **23.–25.03.2010** einen Überblick über die Grundlagen des Information Security Managements. Das gesamte Seminarangebot 2010 sowie die Möglichkeit zur Online-Anmeldung finden Sie hier.

SecurityCup 2009

Die Karlsruher IT-Sicherheitsinitiative beginnt ihre diesjährige Veranstaltungsreihe mit einem spannenden Thema: Die FIDUCIA IT AG führte 2009 ihre dritte Security-Awareness-Kampagne durch – auf höchstem konzeptionellen Niveau und mit einer aktiven Mitarbeiterbeteiligung von über 50 Prozent. Am 18.02.2010 stellen Lutz Bleyer, Leiter der Zentrale Security bei der FIDUCIA IT AG Karlsruhe, und Sven Kaun, Geschäftsführer der Dauth.Kaun Communication Group GmbH sowohl die Highlights des „SecurityCup 2009" als auch ihre „Lessons Learned" und „Do's and Dont's" vor. Anschließend gibt es Gelegenheit zum Networking am Buffet. Um Anmeldung wird gebeten.

Veranstaltungshinweise

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

Februar 2010	
02.-03.02.	20. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
03.-04.02.	ESSoS (DistriNet Research Group, Pisa/I)
04.-05.02.	COSADE 2010 (CASED, Darmstadt)
05.-07.02.	ShmooCon 2010 (Shmoo Group, Washington/USA)
09.-10.02.	17. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
11.02.	Infoveranstaltung Datenschutz (CyberForum/ORGA GmbH, Karlsruhe)
15.-18.02.	SecSE 2010: Fourth International Workshop on Secure Software Engineering (SINTEF, Krakau/PL)
18.02.	Wege zum Ruhm – „SecurityCup 2009“ (KA-IT-Si, Karlsruhe)
22.-26.02.	TISP-Schulung (Secorvo College)
23.02.	CASED-Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
März 2010	
16.-19.03.	ISSECO Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)
April 2010	
13.-16.04.	PKI (Secorvo College)
20.-21.04.	Security News Symposium 2010 (Secorvo, Ettlingen)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Jochen Schlichting

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

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

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

secorvo
security consulting

Secorvo Security News

Februar 2010

Editorial: Gotcha

Mit jedem Klick im Browser geben wir viele Informationen preis, die wir für sich genommen harmlos finden. Bei genauer Betrachtung zeigt sich aber, dass 33 bit Information ausreichen, um einen Menschen weltweit eindeutig zu identifizieren. Jeder Browser übermittelt in der Grundeinstellung zahlreiche Daten, die geeignet sind, einen digitalen Fingerabdruck des Surfers zu erstellen. Durch clevere Ergänzungen verraten Browser weitere Informationen wie die eingesetzten Add-Ons oder das Zeitverhalten bei der Passwort-Eingabe.

Damit nicht genug: Wie seit fast acht Jahren in der Mozilla-Community diskutiert, lassen sich den Browsern durch History-Stealing Informationen über vormals besuchte Seiten entlocken. Diese Technik wird von Internetseiten wie didyouwatchporn.com oder whattheinternetknowsaboutyou.com eindrucksvoll demonstriert. Mag man diese Seiten noch amüsant finden, vergeht einem das Lachen spätestens bei der Lektüre der Studie „A Practical Attack to de-Anonymize Social Network Users“, in der erläutert wird, wie durch History-Stealing die tatsächliche Identität eines Surfers über das Nutzerverhalten in Sozialen Netzwerken ermittelt werden kann – dies lässt sich im Selbstversuch leicht überprüfen.

Diese Techniken sind leider nicht nur von theoretischer Bedeutung, sondern werden teilweise schon zum Tracking von Surfern eingesetzt. Mit etwas Fantasie lässt sich ausmalen, was möglich wäre, wenn Dienste wie Google-Analytics oder etracker damit arbeiten würden. Die Tendenz, die Privatsphäre von Internet-Nutzern einzuschränken, ist – aus unterschiedlichen Motiven – weit verbreitet, das zeigen Initiativen wie die Vorratsdatenspeicherung, der Bundestrojaner oder die zahlreichen Datenschutzskandale in der Wirtschaft.

Kundige Nutzer können durch Selbstschutzmaßnahmen ihre Situation verbessern. Für den Schutz der Privatsphäre aller Internet-Nutzer ist es jedoch erforderlich, dass Browser diesen in der Grundkonfiguration respektieren.

Inhalt

secorvo
security consulting

Security News

Bitte einbrechen!

Einsichtsfähigkeit zählt im Allgemeinen nicht zu den menschlichen Stärken. Noch seltener gelingt es den meisten Menschen, die Kluft zwischen Einsicht und Umsetzung zu schließen. Ein Paradebeispiel dafür ist die wachsende Begeisterung, mit der Privates auf Portalen wie StudiVZ, Wer-kennt-wen, Facebook oder Xing preisgeben wird – und Hunderttausende ihren Tagesablauf via Twitter herauszwitschern.

Am 17.02.2010 ging die Webseite „Please rob me!“ online – eine Art „Awareness-Service“ für Uneinsichtige, betrieben von forthehack (Rijswijk). Eine automatische Twitter-Suche liefert alle aktuellen Nachrichten, aus denen die Abwesenheit von zu Hause erkennbar ist, und zeigt Namen, Foto und den aktuellen Aufenthaltsort an (via foursquare). Zugegebenermaßen eine drastische Methode – aber vielleicht wirksamer als Predigten. Wie wäre denn eine Webseite „Don't hire me!“ mit den heftigsten StudiVZ-Fotos vom vergangenen Wochenende?

25 MDPE

Am 17.02.2010 wurden die von Mitre und SANS zusammengestellten „2010 CWE/SANS Top 25 Most Dangerous Programming Errors“ als grundlegende Überarbeitung der vorjährigen Liste veröffentlicht. Wenig überraschend finden sich unter den schwerwiegendsten Schwachstellen Cross Site Scripting, SQL-Injection und Cross Site Request Forgery wieder auf den Plätzen eins, zwei und vier.

Bahnbrechend neue Erkenntnisse liefert die Liste nicht – Dokumente wie die OWASP Top Ten oder WASC Threat Classification (SSN 01/2010) weisen auf die gleichen Gefahren hin. Im Gegensatz zu diesen beiden Dokumenten adressiert die CWE/SANS-Liste die Probleme aus Entwicklersicht und bietet, auch durch Verweis auf die deutlich umfangreichere „Common Weakness Enumeration“-Datenbank, konkrete Hilfestellung zur Vermeidung oder Behebung der identifizierten Probleme. Softwareentwicklern sind alle drei Dokumente zur regelmäßigen Lektüre zu empfehlen.

Film-Tipps für Chipkartenfans

Im Januar machte ein RBB-Video Furore, das die Umsetzung des Angriffs auf Legic Prime (siehe SSN 01/2010) am Hamburger Flughafen zeigt. Im Februar sind gleich zwei spannende Videos zu empfehlen: Bei der Konferenz Blackhat DC präsentierte Chris Tarnovsky am 02.02.2010 das Ergebnis monatelanger Analysen: Mit einer Laborausstattung zum geschätzten Anschaffungspreis von US$ 200.000 und unter Verschleiß etlicher Testmuster gelang es ihm, geheime Daten aus dem Trusted Platform Module (TPM) einer XBox Spielekonsole auszulesen – einem TPM-Chip der Infineon SLE66 Smartcard-Chipfamilie. In einem Wired-Video vom 23.08.2008 hatte Tarnovsky bereits demonstriert, wie er einen Smartcard-Chip und seine Datenleitungen frei legt. Nun gibt es eine belegte Abschätzung des nötigen Aufwands an Geld und Zeit.

Den Sicherheitsforschern der Universität Cambridge um Ross Anderson gelang es derweil, mit einem am 11.02.2010 als Vorabdruck veröffentlichten Man-in-the-Middle Angriff das EMV-basierte „Chip & PIN“ Verfahren zu brechen, das in Großbritannien für Kartenzahlungen am Point of Sale (POS) eingesetzt wird. Dabei gaukelten sie der Karte vor, dass das Terminal eine Transaktion mit Unterschrift (statt PIN) angefordert hat, während sie dem Terminal signalisierten, dass eine (beliebige) Ziffernkombination von der Karte als gültige PIN akzeptiert wurde. Die zwischen der (gestohlenen) echten Karte und dem ins Terminal eingesteckten Kartenadapter eingeschobene Gerätschaft passt, wie in einem BBC-Video zum Bericht vom 11.02.2010 demonstriert, bequem in einen Rucksack.

Spektakulär an dem Angriff ist, dass er auch im Online-Modus des POS-Terminals funktioniert und der Kundenbeleg „PIN verified“ ausweist. Chip&PIN verstößt offenbar gegen die wichtige Design-Maxime für kryptografische Protokolle, dass in die errechneten Authentisierungs- oder Signaturdaten alle relevanten Statusinformationen eingehen müssen – in diesem Fall auch die Tatsache, ob eine PIN angefordert bzw. verwendet wurde.

Wert von Sicherheitsbeweisen

Quantenkryptografie wurde bisher von seinen Protagonisten als absolut sichere Verschlüsselungsmethode verkauft, da die Grundlagen des Quanten-Schlüsselaustauschs auf den ehernen Gesetzen der Quantenphysik basieren. Der Traum vom praktisch verwendbaren One-Time-Pad war in so greifbare Nähe gerückt, dass es schon erste kommerzielle Produkte dafür gibt. So bestechend der Sicherheitsbeweis für Quantenkryptografie ist – man muss auch auf die äußeren Umstände einer Implementierung achten, denn der Beweis setzt voraus, dass ein Angreifer den Austausch nicht beobachten kann, ohne bemerkt zu werden.

In einem Beitrag auf dem CCC-Kongress führte ein Team aus Singapur am 27.12.2009 vor, wie gängige Implementierungen ausgehebelt werden können, indem sie geblendet werden. Die Quantenphysik beschreibt Phänomene im mikroskopischen Bereich, was jedoch nicht bedeutet, dass es keine Wechsel-

wirkung mit der makroskopischen Welt gibt. Dies zeigt, dass die Quantenkryptografie noch am Anfang steht, und dass noch Jahre bis zur Entwicklung praxistauglicher Verfahren vergehen werden.

Es zeigt darüber hinaus, dass man die Annahmen, die einem Sicherheitsbeweis zugrunde liegen, sehr genau verstehen muss. Nicht umsonst hat die Forschung etwa zwanzig Jahre gebraucht, um ein brauchbares und allgemein anerkanntes Modell für die Sicherheit von Verschlüsselung zu finden. Dabei wurden viele Beweise und Modelle verworfen, weil die Annahmen zu stark oder implizite Annahmen unrealistisch waren. Es bedeutet jedoch nicht, dass man auf Sicherheitsbeweise verzichten kann, denn ad-hoc-Konstruktionen und intuitive Entwürfe taugen erst recht nicht – das immerhin ist gut belegt.

Learning Websecurity by Doing

Ausprobieren ist eine der besten Methoden, um komplexe Sachverhalte zu verstehen. Diesen Ansatz verfolgt das OWASP WebGoat Projekt. Bisher waren allerdings zu Beginn einige Hürden zu nehmen, wie die manuelle Installation der Anwendung. Seit dem 27.01.2010 ist das nicht mehr erforderlich: Das OWASP Broken Web Applications Projectwaspbwa (owaspbwa) bietet eine VMware-kompatible virtuelle Maschine zum Download an, die eine Vielzahl fertig installierter schwachstellenbehafteter Web-Anwendungen enthält. Dem Lernbegierigen stehen neben WebGoat Konzeptanwendungen wie Vicum, Multidae, Damn Vulnerable Web App und andere, auch ältere Versionen mit echten Bugs von phpBB, WordPress und Yazd zur Verfügung. Wir wünschen viel Erfolg beim „Hands on"-Training.

Brothers are Listening

Aufgrund des am 20.02.2010 auf CryptoMe.org veröffentlichten „Microsoft® Online Services Global Criminal Compliance Handbook" ließ Microsoft die Domäne am 25.02.2010 wegen Verstoßes gegen den Digital Millennium Copyright Act (DMCA) kurzzeitig sperren. Das Dokument vom 29.05.2008 zählt auf Seite 22 die im Rahmen von Auskunftsersuchen der US-Behörden zu liefernden Daten auf. Betroffen sind der Freemail-Dienst Hotmail, die Authentifizierung Windows Live ID, das Instant Messaging mit Windows Live Messenger und das Unterhaltungsportal Xbox. Bei anderen amerikanischen Online-Diensten wie Facebook, Skype, Paypal, MySpace oder Yahoo sieht es hinsichtlich der Kooperationsfreude mit Behörden ähnlich aus, wie die ca. 30 „Lawful Spy Guides" auf CryptoMe belegen.

Zwar haben Benutzer dieser Dienste im Rahmen der Registrierung einer solchen Weitergabe ihrer Daten zugestimmt. Vermutlich werden diese Nutzungsbedingungen aber ebenso genau und häufig gelesen wie kleingedruckte AGB – unterliegen nur nicht denselben Verbraucherschutzbestimmungen. Die Gestaltung der Dienste genügt zudem meist nicht den Anforderungen des Telemediengesetzes (TMG) vom 26.02.2007, das in § 13 wichtige datenschutzrechtliche Anforderungen stellt, darunter die Widerrufbarkeit von Einwilligungen, die Erstellung ausschließlich pseudonymer Nutzungsprofile und die Möglichkeit zur anonymen Nutzung.

Durchsetzbar sind diese Anforderungen bei amerikanischen Anbietern nicht. Zu denken gibt allerdings, dass inzwischen deutsche Anbieter den Amerikanern nacheifern. Angesichts der bekannt gewordenen Datenschutz-Skandale lässt diese Entwicklung für die Zukunft Böses befürchten.

Secorvo News

Secorvo College aktuell

Noch immer wartet das Ausführungsgesetz zum Datenschutzaudit auf seine Verabschiedung. Des ungeachtet sind Datenschutzaudits bereits gängige Praxis in vielen Unternehmen. Das Seminar „Datenschutzaudit: Best Practice" am **20.–21.05.2010** stellt vor, welche Vorgehensweisen sich in der Praxis bewährt haben.

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

Security News Symposium

Am **20.–21.04.2010** ist es so weit – wir laden Sie herzlich ein zum ersten „Security News Symposium". Zahlreiche aktuelle Themen, die uns immer wieder in den Security News beschäftigen, werden im Zentrum intensiver Diskussionen stehen: Von neuen Bedrohungen durch und Empfehlungen zum Umgang mit USB-Sticks über Erfahrungen mit Krisenmanagement-Übungen, die Herausforderung iPhone, die Zukunft von Mifare und digitalen Signaturen bis zu verwurzelten Passwort-Mythen. Wir freuen uns auf Ihre Teilnahme.

Tag der IT-Sicherheit

Den 15.07.2010 sollten Sie sich vormerken: Dann findet der zweite Karlsruher „Tag der IT-Sicherheit", eine Kooperationsveranstaltung der KA-IT-Si mit der IHK Karlsruhe und dem Cyberforum e.V., im Saal Baden der IHK Karlsruhe statt. Es erwarten Sie Praxisberichte u. a. zu den Themen Wirtschaftsspionage, PDA-Sicherheit und Awareness.

Veranstaltungshinweise

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

März 2010	
08.-11.03.	Audit Challenge 2010 (Frankfurt School of Finance & Management, Frankfurt/Main)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)
April 2010	
13.-16.04.	PKI (Secorvo College)
20.-21.04.	Security News Symposium 2010 (Secorvo, Ettlingen)
20.-22.04.	Datenschutztage 2010 (FFD Forum für Datenschutz, Frankfurt)
27.-28.04.	a-i3/BSI-Symposium 2010 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
27.-29.04.	Forensik – Verfahren, Tools, Praxis (Secorvo College)
Mai 2010	
04.-05.05.	11. Datenschutzkongress 2010 (EUROFORUM, Berlin)
17.-19.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
20.-21.05.	Datenschutzaudit – Best Practice (Secorvo College)
25.-28.05.	3rd Int. Workshop on Post Quantum Cryptography PQCrypto 2010 (Cased, Darmstadt)

Fundsache

Der bewährte Mustervertrag des Bitkom zur Auftragsdatenverarbeitung liegt seit dem 04.12.2009 in einer neuen, an die Änderungen des BDSG angepassten Fassung 3.0 (inkl. Erläuterungen in Englisch) vor.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Jochen Schlichting

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

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

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

secorvo
security consulting

Secorvo Security News

März 2010

Innovationsklima

Erfolgreiche Innovationen sind das Lebenselixier eines an Rohstoffen armes Landes. Kein Wunder, dass mit Initiativen wie „Land der Ideen“ oder „Partner für Innovation“ der Erfindergeist beschworen und mit Innovationsindikatoren die Innovationsfähigkeit gemessen wird. Viel wichtiger als die Höhe der Investitionen in Bildung, Forschung und Entwicklung oder die Zahl der Patentanmeldungen ist in der Praxis aber eine andere Frage: Woran lässt sich erkennen, dass aus einer Innovation ein erfolgreiches Produkt wird? Diese Frage stellen sich täglich unzählige Manager, Unternehmer, Analysten und Investoren. Meist liegen sie mit ihren Einschätzungen daneben: Obwohl nur ein Bruchteil aller Ideen Produktreife erlangt, liegt deren „Floprate“ bei 70-90%.

Viel Geld ließe sich sparen, gelänge es, die Trefferquote zu erhöhen. Die Geschichte zeigt jedoch, dass das nicht so einfach ist. „Das Telefon hat zu viele ernsthaft zu bedenkende Mängel für ein Kommunikationsmittel. Das Gerät ist von Natur aus von keinem Wert für uns“, hieß es 1876 in einer internen Meldung von Western Union. „Ich denke, es gibt weltweit einen Markt für vielleicht fünf Computer“, prognostizierte 1943 Thomas Watson, Vorsitzender von IBM. Und Ken Olson, Präsident von DEC, stellte 1977 fest: „Es gibt keinen Grund, warum irgend jemand einen Computer in seinem Haus wollen würde.“ Selbst Bill Gates lag daneben, als er 1981 konstatierte: „640 Kilobyte sind genug für jeden.“

Einfacher ist es, mit der Prognose bis zum kommerziellen Durchbruch der Innovation zu warten. So muss wohl auch Spam, Bot-Netzen, Zero Day Exploits und neuerdings Banking Trojanern wie insbesondere ZeuS der Status einer erfolgreichen Innovation zugebilligt werden. Offenbar herrscht im Bereich der Internetkriminalität ein äußerst fruchtbares Innovationsklima – ganz ohne F&E-Förderung und Innovationsindikatoren. Das sollte zu denken geben. Hoffen wir, dass es Auszeichnungen wie dem Deutschen IT-Sicherheitspreis gelingt, den Tüftlergeist der „White Hats“ zu beleben.

Inhalt

secorvo
security consulting

Security News

Fog Computing

Cloud Computing ist derzeit in aller Munde. Google, Amazon und Co. vermieten überschüssige Kapazität kostengünstig oder gar umsonst als virtualisierte Dienste. Mit der Frage, was dabei aus Sicherheitssicht zu beachten ist, beschäftigen sich u. a. der Report „Cloud Computing Security Risk Assessment“ der ENISA (Fundsache in SSN 11/09), die am 01.03.2010 erschienenen „Top Threats to Cloud Computing“ der gerade einmal ein Jahr alten Cloud Security Alliance und der seit 14.03.2010 elektronisch verfügbare Forschungsartikel „A 'cloud-free' security model for cloud computing“ von Manal Yunis.

Beim genaueren Hinschauen bestehen die Handlungsempfehlungen überwiegend darin, dass der Wolkenmieter seine Hausaufgaben machen sollte: Risikobewertung, Security Management und insbesondere umfangreiche Überwachung und Revision dessen, was da in der Cloud vor sich geht. Und wie immer beim Outsourcing sollte man sich vergegenwärtigen, dass die Verantwortung zur Kontrolle - ernst genommen - den eingesparten Betriebsaufwand zumindest relativiert.

Allerdings wird der Kunde beim standardisierten Angebot eines großen Cloud Computing Providers im Gegensatz zum herkömmlichen Outsourcing deutlich schlechtere Karten haben, ein individuelles Service Level Agreement mit weitreichenden Einblicks- und Kontrollmöglichkeiten auszuhandeln – Cloud Computing wird damit zum Fog Computing.

Werden in der Wolke personenbezogene Daten verarbeitet, entstehen damit auch Risiken für Dritte – schön zusammengefasst in dem Bericht „Privacy in the Cloud“ von Robert Gellmann vom 23.02.2009.

In Deutschland ist eine solche Verarbeitung schnell rechtswidrig, denn die erst im vergangenen Jahr präzisierten Anforderungen des § 11 BDSG zur Auftragsdatenverarbeitung stellen strikte Bedingungen an die Zulässigkeit einer Verarbeitung durch Dritte. Vor Vertragsabschluss ist daher besondere Sorgfalt geboten, denn die Verantwortung für den Schutz der durch Dritte verarbeiteten personenbezogenen Daten verbleibt nach BDSG beim Auftraggeber.

ISMS-Hilfe

Mit dem am 01.02.2010 veröffentlichten und nun auch erhältlichen Standard ISO/IEC 27003: 2010 „Informations technology - Security techniques – Information security management system implementation guidance" hat das JTC 1/SC 27 eine konkrete Implementierungshilfe für ein Informationssicherheitsmanagement nach ISO/IEC 27001: 2005 entwickelt.

Auf 68 Seiten werden in dem Standard Empfehlungen zur Anwendung des ISO/IEC 27001:2005 und zum Aufbau eines ISMS gegeben sowie einige unklare Anforderungen präzisiert. Wer einen einfach zu befolgenden Fahrplan zum ISMS-Aufbau erwartet hat, wird von dem Dokument enttäuscht. Einem erfahrenen Sicherheitsverantwortlichen wird das Dokument in der Praxis allerdings für das eine oder andere Detail eine echte Arbeitshilfe sein.

Ladegerät mit Trojaner

Nachrichten über Trojaner sind leider inzwischen nichts Besonderes mehr. Die Meldung des US CERT vom 02.03.2010, dass ein USB-Batterieladegerät mit einem Trojaner ausgeliefert wurde, zeigt jedoch, dass immer kreativere Wege zur Verbreitung schädlicher Software gewählt werden.

Daher sollte grundsätzlich auch Software aus vermeintlich vertrauenswürdiger Quelle mit gesunder Skepsis begegnet und diese vor einer Installation überprüft werden.

Digitale Wahlen

Im März 2010 führte die International Association for Cryptologic Research (IACR) einen Probelauf für digitale Wahlen durch. Lange Zeit gab es Vorbehalte gegen diese Form der Wahl, nicht zuletzt, weil dies als Werbung für ein bestimmtes Produkt missverstanden werden könnte. Aus Gründen der Benutzerbequemlichkeit entschloss man sich jedoch, digitale Wahlen auszuprobieren – in einer nicht bindenden Probeabstimmung fand das Verfahren große Zustimmung.

Da mittlerweile immer öfter digitale Wahlen zu allen denkbaren Anlässen durchgeführt werden, scheint die Zeit möglicherweise reif dafür zu sein. Die von der IACR genutzte Technologie Helios beruht auf einem Konzept, das von Ben Adida als Dissertation am MIT unter der Betreuung von Ron Rivest entwickelt wurde. Es handelt sich um ein Wahlsystem, bei dem die Stimme anonym abgegeben wird (die Wähler selbst sind nicht anonym und müssen aber zuvor registriert sein), und bei dem jeder Wähler im Nachhinein (wie bei Bingo Voting, SSN 3/2009) verifizieren kann, ob seine Stimme gezählt wurde. Die HeliosSoftware ist quelloffen. Wem Download und Installation zu kompliziert sind, kann seine Wahl auch im Web organisieren: Heliosvoting bietet dazu eine virtuelle Wahlkabine mit virtuellen Stimmzetteln. Sobald alle Wahlberechtigten registriert sind, steht einer Abstimmung nichts mehr im Wege.

secorvo
security consulting

Ach wie gut, dass niemand ...

Dass Kontrollfragen wie die nach dem Mädchennamen der Mutter nicht nur im spanischen Sprachraum eine einfache Hintertür für gut gesicherte Zugänge sind, sollte sich herumgesprochen haben, als im US-Wahlkampf persönliche E-Mails von Sarah Palin publiziert wurden. Das Problem: Durch persönliche Kontakte oder sogar Internet-Recherchen sind die richtigen Antworten auf derartige Fragen oft leicht herauszufinden.

Forscher aus Cambridge und Edinburgh haben nun den Blickwinkel gewechselt: Ein Angreifer könnte im Stil der Rasterfahndung bei allen Anwendern z. B. auf die Frage nach dem Vornamen des Lieblingslehrers einfach eine Handvoll der geläufigsten Namen ausprobieren. Ihrer am 04.03.2010 veröffentlichten Studie zufolge ist die zu erwartende Trefferquote erschreckend hoch. Neben Tabellen, denen man u. a. den beliebtesten weiblichen Vornamen in den USA der 60er Jahre (Lisa) entnehmen kann, enthält das Papier einen Vorschlag für ein passendes Komplexitätsmaß und eine Literaturliste, die gute Argumente für den sicheren Einsatz resp. Verzicht bestimmter Kontrollfragen liefert.

SSL am Ende?

Die Sicherheit einer SSL/TLS-Verbindung steht und fällt mit der Vertrauenswürdigkeit des Server-Zertifikats. Soweit die Theorie. In der Praxis ist die jedoch gar nicht so einfach zu überprüfen: Viele der mehr als 250 von verbreiteten Browsern anerkannten Zertifizierungsstellen wurden inzwischen übernommen oder haben umfirmiert: Aus Baltimore wurde Cybertrust wurde Verizon, aus SecureTrust und XRamp wurde TrustWave – die alten Zertifikate haben jedoch noch bis zu 30 Jahre Gültigkeit. Wie vertrauenswürdig ist da das zugehörige CA-Zertifikat? Ist auf die Identitätsverifikation der Zertifizierungsstelle noch Verlass? Warnt der Browser, wenn eine oft besuchte Webseite ein neues Zertifikat von einer anderen Zertifizierungsstelle erhält?

Am 24.03.2010 stellten Christopher Soghoian und Sid Stamm in ihrem Papier „Certified Lies“ eine neue Angriffsklasse vor: Stellt eine CA z. B. einer Strafverfolgungsbehörde oder einem Nachrichtendienst ein „Intermediate CA“-Zertifikat aus, lassen sich gefälschte Zertifikate erzeugen und damit „man-in-the-middle“-Abhörangriffe durchführen. Die Firma Packet Forensics bietet dafür sogar eine fertige Appliance namens „5 Series“ mit einem Durchsatz von mehreren Gb/s an.

Als Gegenmaßnahme entwickeln sie ein Firefox-PlugIn namens CertLock, das in Kürze verfügbar sein soll. Es folgt einem „Trust-On-First-Use“-Prinzip und warnt, wenn der Zertifikatsaussteller wechselt oder die Länderkennungen von CA, besuchter Webseite oder Besucher sich unterscheiden.

Das ursächliche Problem – die Schwierigkeit, die Vertrauenswürdigkeit von SSL-Zertifikaten zu beurteilen – ist damit nicht gelöst. Folgt man Matt Blaze, so brauchen wir ein gänzlich neues Konzept.

Samurai gegen Web-Apps

Der Umfang der Tool-Sammlung „Samurai“ zur Analyse der Sicherheit von Web-Anwendungen hat sich mit Veröffentlichung der Version 0.8 vom 15.03.2010 auf ca. 1,7 GB mehr als verdoppelt. Die Installation der herunterladbaren ISO-Datei basiert immer noch auf der Ubuntu-Version 9.04, bietet aber einen zur Vorgängerversion deutlich erweiterten Werkzeugumfang. Sehr hilfreich ist die Möglichkeit, diese einfach aus den Code-Repositories der Entwickler zu aktualisieren.

Secorvo News

Security News Symposium 2010

Wie übt man einen Krisenfall? Sollte man iPhones verbieten? Welche verborgenen Risiken schlummern in USB-Sticks? Was kommt nach dem Mifare-Hack? Hängen wir an Passwort-Mythen? Diesen und weiteren aktuellen Fragen werden wir am **20.–21.04.2010** auf dem ersten „Security News Symposium“ in Karlsruhe/Ettlingen auf den Grund gehen. Wir freuen uns auf Ihre Teilnahme.

Teamverstärkung

Ab dem 01.04.2010 wird Michael Knopp das Secorvo-Team mit juristischer Kompetenz verstärken. Als Mitarbeiter der „Projektgruppe Verfassungsverträgliche Technikgestaltung“ (provet) und des „Instituts für Europäisches Medienrecht“ (EMR) hat er sich unter anderem mit rechtlichen Fragen der Langzeitarchivierung elektronischer Dokumente, mit Bürgerportalen und eGovernment-Lösungen auseinander gesetzt und sich als „Mittler zwischen den Welten“ von Recht und Technik bewegt.

Die guten ins Töpfchen

IT-Grundschutz-Zertifikate sind nach wie vor rar: Wenige Unternehmen schafften bisher eine Zertifizierung ihres Sicherheitsmanagements und der Umsetzung der in den Grundschutzkatalogen definierten Maßnahmen. Auf dem KA-IT-Si-Event am **29.04.2010** wird der DE-CIX, dem größten europäischen Internet-Knoten, im Panoramasaal der IHK Karlsruhe das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz verliehen. Begleitet wird die Prämierung von einem Erfahrungsbericht - und einem Sektempfang zum Büfett-Networken (Anmeldung).

Veranstaltungshinweise

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

April 2010	
19.-20.04.	Datenschutz kompakt (Gesellschaft für Datenschutz und Datensicherung e.V., Köln)
20.-21.04.	Security News Symposium 2010 (Secorvo, Ettlingen)
20.-22.04.	Datenschutztage 2010 (FFD Forum für Datenschutz, Frankfurt)
23.04.	Verbandstagung des Berufsverbandes der Datenschutzbeauftragten (BvD e.V., Berlin)
27.-28.04.	a-i3/BSI-Symposium 2010 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
29.04.	Die guten ins Töpfchen... (KA-IT-Si, IHK Karlsruhe)
Mai 2010	
04.-05.05.	11. Datenschutzkongress 2010 (EUROFORUM, Berlin)
17.-19.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
20.-21.05.	Datenschutzaudit – Best Practice (Secorvo College)
25.-28.05.	3rd Int. Workshop on Post Quantum Cryptography PQCrypto 2010 (Cased, Darmstadt)
Juni 2010	
07.-11.06.	TISP-Schulung (Secorvo College)

Fundsache

Am 17.03.2010 wurde die Studie „Know-How-Schutz in Baden-Württemberg 2009/2010“ des Sicherheitsforums BW und des Steinbeis-Instituts Stuttgart vorgestellt, für die 239 Unternehmen befragt wurden. Sie gibt ein detailliertes Bild der Einschätzung der Bedrohung durch Wirtschaftsspionage und der ergriffenen Schutzmaßnahmen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Kobloch, Kai Jendrian

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

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

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

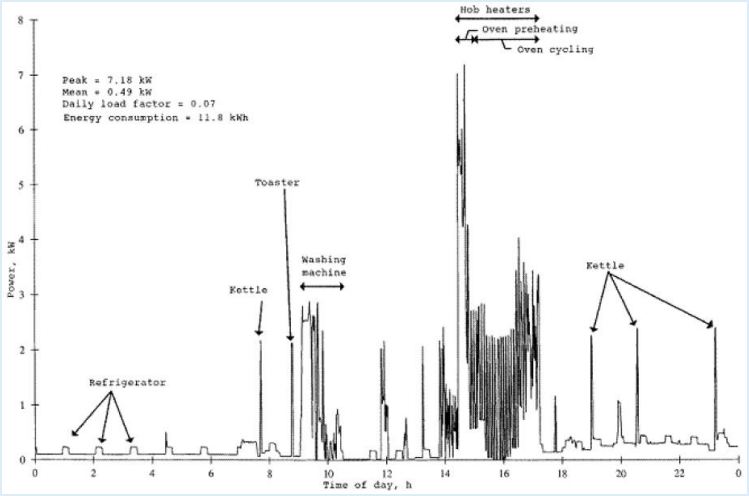
secorvo
security consulting

Secorvo Security News

April 2010

Der Feind in meiner Steckdose

Seit Januar müssen in Neubauten und bei Renovierungen „intelligente Stromzähler" verbaut werden, die Verbrauchswerte elektronisch übermitteln und eine Abrechnung nach wechselnden Tarifen erlauben. Damit sollen den Energieversorgungsunternehmen eine verbrauchsabhängige Energiebereitstellung ermöglicht und durch lastabhängige Tarife das Verbraucherverhalten gesteuert werden. Dass die vermeintlich unkritische Erfassung des Stromverbrauchs in 15'-Intervallen einen erheblichen Eingriff in den vom Bundesverfassungsgericht im Urteil zum „Großen Lauschangriff" vom 03.03.2004 definierten „Kernbereich privater Lebensgestaltung" darstellt, wird erst auf den zweiten Blick deutlich. Abgesehen von einem Gutachten des ULD vom 11.09.2009 und Kapitel 4 eines NIST-Drafts vom 02.02.2010 blieb selbst die fachöffentliche Diskussion weitgehend aus. Das ist, wie die Abbildung zeigt, wohl dringend nachzuholen.



Quelle: Elias Leake Quinn, Smart Metering & Privacy: Existing Law and Competing Policies, Frühjahr 2009, S. 3.

Inhalt

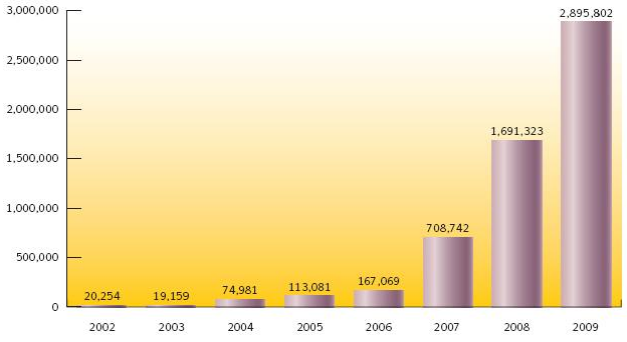
secorvo
security consulting

Security News

Symantec Report

Am 14.04.2010 erschien der immer wieder lesenswerte halbjährliche Internet Security Thread Report von Symantec. Einige der Ergebnisse, die Symantec über 240.000 eigene „Sensoren“ gewinnt, sind auch für Experten überraschend: So stürmten Angriffe mit bösartigen PDF-Dateien die Top-Ten; sie waren für 49% aller Web-basierten Attacken verantwortlich. Daher sollte dem Patchen des Acrobat-Readers eine mindestens ebenso hohe Priorität eingeräumt werden wie den Betriebssystem-Updates.

Während das „Window of Exposure“ trotz zahlreicher kritischer Bugs 2009 bei den meisten Browsern auf unter einen Tag schrumpfte, stieg die Zahl der neue Viren, Würmer und Trojaner 2009 auf durchschnittlich fast 8.000 – je Kalendertag.



Neue Viren, Würmer, Trojaner (Symantec)

Auch der Handel mit ergaunerten „Credentials“ floriert, wenn auch die Preise sinken: Kreditkartendaten gibt es schon ab 0,85 US$, E-Mail-Adressen ab 1,70 US$ je MB und Kontendaten bereits ab 15 US$. Offenbar überwiegt hier das Angebot die Nachfrage (bzw. die Zahl der „nützlichen Idioten“, die ihr Bankkonto für die Geldwäsche hergeben).

Internet zertifiziert

Am 29.04.2010 erfolgte im Rahmen eines Events der Karlsruher IT-Sicherheitsinitiative die offizielle Übergabe des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz an den deutschen Internet-Knoten DE-CIX – mit einem Durchsatz von mehr als 600 GBit/s der größte Knoten Europas und der zweitgrößte weltweit. Gute drei Jahre dauerte das von der Karlsruher Connect GmbH begleitete Projekt von der Idee bis zum von Secorvo durchgeführten erfolgreichen Audit. Die Erfahrungsberichte finden sich auf der Webseite der KA-IT-Si.

Der Aufwand hat sich nach Überzeugung von Arnold Nipper (CTO des DE-CIX) gelohnt: Das Projekt habe konsequente Sicherheitsprozesse und ein durchgängiges, hohes Sicherheitsniveau erzwungen – wichtige Voraussetzung für die Vertrauenswürdigkeit eines Internet-Knotens. Bei der Übergabe scherzte Bernd Kowalski, Abteilungsleiter Zertifizierung beim BSI, daher auch: „Jetzt ist das deutsche Internet Grundschutz-zertifiziert.“

Leitfaden IS-Revision

Am 19.03.2010 wurde vom BSI Version 2.0 des Leitfadens IS-Revision auf Basis von IT-Grundschutz veröffentlicht. Die Vorgehensweise wird umfänglich beschrieben und enthält wenig Überraschendes. Interessant sind die Aufwandschätzungen für eine „Querschnitts-Revision“, die mit 30-60 Personentagen bei normaler und bis zu 60-100 Personentagen bei sehr hoher Komplexität angesetzt werden. Für eine „IS-Kurzrevision“ werden 8-10 Tage geschätzt, eine Methode, um einen ersten definierten Eindruck zum Stand der Informationssicherheit zu erhalten.

Ein als Hilfsmittel zur Verfügung gestelltes Dokument Prüfthemen für die IS-Kurzrevision soll diese Kurzrevision unterstützen. Der Titel „verbindliche Prüfthemen“ klingt vielversprechend; bei genauerer Betrachtung werden aber nur Themen aufgelistet. Wie diese konkret zu prüfen sind, ist nicht geregelt. Lediglich stichpunktartig werden Beispiele angeführt, die einen großen Interpretationsspielraum lassen.

Es bleibt zu hoffen, dass im Rahmen der Überarbeitung der IT-Grundschutzkataloge bei den jeweiligen Maßnahmen auch verbindliche Prüffragen definiert werden, die dann als Grundlage für die Erstellung von Informationssicherheitskonzepten bzw. einer ISO 27001-Zertifizierung auf Basis von IT-Grundschutz sowie für die IT-Revision verwendet werden können.

Diffie + Murphy = Lenin

Gut 33 Jahre ist die Epoche machende Veröffentlichung von Whit Diffie und Marty Hellman zur Public Key Kryptographie inzwischen alt. Und selbst die bekannte und oft genutzte PKI-Bibliothek OpenSSL liegt nach mehr als einem Jahrzehnt Anlauf seit dem 29.03.2010 offiziell in Version 1.0 vor.

Eigentlich ist also alles ganz einfach mit einer PKI, sollte man meinen: CAs als vertrauenswürdige Zertifizierungsinstanzen stellen nach eingehender Prüfung der Antragsteller Zertifikate aus und PKI-Anwendungen nutzen diese Zertifikate, um mit den zugehörigen Schlüsseln alle relevanten Daten zu signieren oder für den beabsichtigten Empfänger zu verschlüsseln. In der Praxis scheint aber immer noch eher Murphys Gesetz zu regieren, wie die folgenden aktuellen Ereignisse zeigen.

Am 02.04.2010 wurde bei einer Kontrolle unter den bei der Mozilla Foundation geführten vertrauenswürdigen Stammzertifikaten ein herrenloses Root-CA-Zertifikat entdeckt. Erst vier Tage später konnte geklärt werden, dass der Schlüssel dieser CA zwar nicht kompromittiert ist, aber weder verwendet noch auditiert wird; daraufhin wurde das Zertifikat – für künftig neu installierte Firefox-Browser – aus der vorgegebenen Stammzertifikatsliste entfernt.

Am 01.04.2010 wurde gemeldet (leider kein Aprilscherz), dass es ausreicht, als Kunde eines Free-Mail- oder Web-Mail-Providers die E-Mail-Adresse „ssladministrator@…“ zu belegen, um hochoffizielle SSL-Zertifikate für Server unter der Domäne des jeweiligen Providers zu beziehen.

Am 13.04.2010 erschien ein Microsoft-Patch für Authenticode, der dafür sorgt, dass jetzt tatsächlich der gesamte in einem Cabinet oder Portable Executable Container enthaltene Code in die Prüfung der Code-Signatur einbezogen wird. Bis dato konnte ein Angreifer diesen Containern Code anfügen, ohne dass deshalb die Signatur des ursprünglichen Herausgebers als ungültig gewertet wurde.

Und ebenfalls am 13.04.2010 wurde ein Bug bestätigt, der dazu führt, dass Thunderbird ausgehende E-Mails u. U. nicht mit dem Zertifikat des adressierten Empfängers, sondern mit einem ganz anderen verschlüsselt.

Auch nach 33 Jahren sollte man es bei der PKI-Nutzung also immer noch mit der (fälschlich) Wladimir Iljitsch Uljanow (vulgo: Lenin) zugeschriebenen Maxime halten: Vertrauen ist gut. Kontrolle ist besser.

OWASP Top 10 – 2010,5

In den SSN 11/2009 haben wir bereits auf die Entwurfsversion der überarbeiteten OWASP Top 10 hingewiesen. Seitdem verstrichen fast sechs Monate intensiven Feinschliffs, bevor am 19.04.2010 die endgültige Version veröffentlicht wurde.

Das 22-seitige Dokument, an dem noch die Reihenfolge einiger Risiken im Tabellenkeller verändert wurde, zeigt anschaulich allen Verantwortlichen und an der Entwicklung von Web-Anwendungen Beteiligten die gravierendsten Risiken auf. Zusätzlich wird das notwendige Handwerkszeug zur Risikoreduzierung vorgestellt. Das halbe Jahr bis zur Veröffentlichung hat geholfen, den Entwurf zu einem rundum gelungenen Arbeitswerkzeug reifen zu lassen.

Secorvo News

Secorvo College aktuell

Die Nachfrage nach dem T.I.S.P.-Zertifikat ist ungebrochen: Schon weit über 300 deutsche Security Professionals dürfen sich mit diesem Titel schmücken, und 2010 werden voraussichtlich weitere 100 Absolventen das Zertifikat erwerben. Freie Plätze gibt es noch auf dem T.I.S.P.-Seminar am **07.–11.06.2010** (mit anschließender Prüfung). Die nächste Gelegenheit zur T.I.S.P.-Zertifizierung bietet Secorvo College nach der Sommerpause vom 20.-25.09.2010.

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

Lesestoff

In der März-Ausgabe der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“ (Schwerpunktthema „Softwaresicherheit“) hat sich Kai Jendrian ausführlich zur Überprüfung von Webanwendungen mit dem „OWASP Application Security Verification Standard 2009“ geäußert (S. 138-142).

Nachlese

Unser erstes „Security News Symposium“ am 20.-21.04.2010, auf dem wir zahlreiche aktuelle Themen der IT-Sicherheit und des Datenschutzes vertieften, wurde von den Teilnehmern überschwänglich gelobt – nicht nur für das hervorragende Essen. Wer es verpasst hat, kann eine CD mit den Vortragsunterlagen zum Preis von 50 Euro per E-Mail an security-news-symposium@secorvo.de bestellen. Das Essen lässt sich allerdings erst auf dem nächsten Symposium nachholen.

Vorschau

Am **07.–08.06.2010** findet die diesjährige 12. Fachkonferenz „DuD 2010“ in Berlin statt – mit einem spannenden und aktuellen Programm (von Cloud Computing über Elena, Auftragsdatenverarbeitung und den neuen Personalausweis bis zum Intelligenten Stromzähler) und Rekordbeteiligung: Schon jetzt gibt es mehr als 100 Anmeldungen. Wer noch dabei sein möchte, sollte sich zügig anmelden.

Ebenfalls vormerken sollten Sie den **15.07.2010** – den zweiten Karlsruher „Tag der IT-Sicherheit“, der in Kooperation von KA-IT-Si, IHK Karlsruhe und dem Cyberforum e.V. veranstaltet wird. Es erwarten Sie Praxisberichte u. a. zu den Themen Wirtschaftsspionage, iPhone-Sicherheit und Security Awareness.

Veranstaltungshinweise

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

Mai 2010	
04.-05.05.	11. Datenschutzkongress 2010 (EUROFORUM, Berlin)
20.-21.05.	Datenschutzaudit – Best Practice (Secorvo College)
20.-21.05.	International Secure Systems Development Conference (Enabled Security Limited, London/UK)
25.-28.05.	3rd Int. Workshop on Post Quantum Cryptography PQCrypto 2010 (Cased, Darmstadt)
30.05.-03.06.	Eurocrypt 2010 (IACR, Nizza/F)
Juni 2010	
07.-08.06.	DuD 2010 (Computas, Berlin)
07.-11.06.	TISP-Schulung (Secorvo College)
22.-25.06.	Certified Professional for Secure Software Engineering (CPSSE) (Secorvo College)
Juli 2010	
15.07.	2. Karlsruher „Tag der IT-Sicherheit“ (KA-IT-Si/IHK/Cyberforum, IHK Karlsruhe)
24.-29.07.	Black Hat (Las Vegas/US)

Fundsache

Eine ausführliche Auseinandersetzung mit Sicherheits- und Datenschutzaspekten von Smart Metern (= „Intelligenten Stromzählern“) im Smart Grid hat das NIST am 02.02.2010 als zweiten Draft zur Kommentierung veröffentlicht: *Smart Grid Cyber Security Strategy and Requirements* (NIST IR 7628, 305 Seiten).

Impressum

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

ISSN 1613-4311

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

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

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

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

secorvo
security consulting

Secorvo Security News

Mai 2010

Die Vernunft stirbt nie

Wiederholt gerieten in den vergangenen Monaten „Social Networks“ wie Xing, StudiVZ und Facebook aufgrund von Datenschutzvorfällen in die Schlagzeilen. Aber keineswegs allen lagen Gesetzesverstöße zu Grunde.

Die meisten Fälle gründeten auf einem sehr grundsätzlichen Missverständnis. Denn anders als die Betreiber Glauben machen möchten, sind „Social Networks“ keineswegs ein digitales Abbild sozialer Netze. Sie entsprechen nicht den fein gewobenen sozialen Beziehungen, die Menschen knüpfen, und in denen sie in unterschiedlichen Rollen auftreten: als Partner, Geschwister, Gönner, Kumpel, Mitbewerber, Kollegen, Bekannte, Freunde. Selbst ähnliche Rollenbeziehungen unterschieden sich im Detail erheblich: Denn Freund ist nicht gleich Freund, und Kollege nicht gleich Kollege.

In echten sozialen Beziehungen werden Informationen und Gerüchte, Tipps und Erlebnisse sehr selektiv und kontextabhängig getauscht – keine zwei Personen aus dem sozialen Beziehungsgeflecht eines Menschen verfügen über dieselben persönlichen Kenntnisse. Auch Sprache, Stil und Ton der Kommunikation unterscheiden sich.

„Social Networks“ sind hingegen große Verflacher: Jeder „Freund“ („Kontakt“) kann auf dieselben Daten und Informationen zugreifen – jederzeit und fast überall. Jede Person erscheint allen „Freunden“ gegenüber in derselben undifferenzierten Rolle. Und wer „twittert“, spricht im selben Ton und Wortlaut zu allen „Followern“. Im „echten Leben“ käme kein Mensch auf die Idee, jedem, den er kennenlernt, gleich seinen Geburtstag in den Kalender einzutragen, seine bisherige berufliche Laufbahn und alle Qualifikationen lückenlos zu offenbaren, unbegrenzten Zugriff auf sein Fotoalbum einzuräumen und gleich noch die Liste aller Freunde und Bekannten vorzulegen.

Der Irrsinn wird wohl immer mehr Menschen bewusst: Angeblich planen 60 % der deutschen Facebook-Nutzer eine Kontolöschung. Offenbar ist ein Hype doch nicht das Ende aller Vernunft.

Inhalt

secorvo
security consulting

Security News

DECT-Verschlüsselung gebrochen

Die Liste der gebrochenen proprietären Krypto-Verfahren ist erneut um eines angewachsen: Auf dem diesjährigen Fast Software Encryption Workshop (FSE 2010) vom 07.-10.02.2010 in Korea war das DECT-Verschlüsselungsverfahren an der Reihe.

Karsten Nohl, Erik Tews und Ralf-Philipp Weinmann gelang eine vollständige Rekonstruktion und die Feststellung ernsthafter Schwachstellen der DECT Standard Cipher (DSC). Dabei handelt es sich um eine 64-Bit Stromchiffre, die strukturell der GSM-Chiffre A5/1 ähnelt. Das Design beruht auf irregulär getakteten, linear rückgekoppelten Schieberegistern, einer Konstruktion, die typisch für Umgebungen ist, bei denen es auf eine möglichst einfache Implementierung und hohe Performanz ankommt.

Der Angriff ermöglicht es, den geheimen Schlüssel mit Hilfe leistungsstarker Hardware innerhalb weniger Stunden zu finden. Seit dem 04.04.2010 sind die Ergebnisse der Kryptoanalyse verfügbar.

Der Vorgang zeigt wieder einmal, dass von der Verwendung Hersteller eigener Kryptoverfahren dringend abzuraten ist – insbesondere, wenn das Verfahren (wie DSC) in zig-Millionen Endgeräten implementiert wird. Selbst wenn bald ein sicherer Nachfolger für DSC zur Verfügung stehen sollte, so wird DSC wegen seiner enormen Verbreitung noch auf Jahre in Gebrauch bleiben. Auch wenn es vom Standpunkt der Alcatel aus verständlich erscheint, mit einem geheim gehaltenen Verfahren Patentgebühren einnehmen zu wollen, so rechtfertigt dies nicht den Einsatz minderwertiger Algorithmen auf Kosten der Sicherheit der Verbraucher.

Das BDSG ist nicht genug

Während die Unternehmen noch an der Umsetzung der jüngsten Novellierung des BDSG arbeiten, leitete der Hamburger Senat, veranlasst durch Google Streetview, am 07.05.2010 dem Bundesrat einen Gesetzesentwurf zur Ergänzung des BDSG (BR-Drs. 259/10) zu. Schon am 01.04.2010 hatte das Bundesinnenministerium (BMI) Eckpunkte zum Arbeitnehmerdatenschutz vorgestellt, die ebenfalls auf eine Gesetzesänderung zielen.

Beiden Vorschlägen ist eine überbordende Einzelfallorientierung gemein. Der Hamburger Entwurf sieht zahlreiche Ergänzungen des ohnehin wuchernden § 28 vor, darunter eine eingeschränkte Erlaubnis für georeferenzierte Straßenansichten und ein Widerspruchsrecht, sowie eine Benachrichtigungspflicht in einem neuen § 33a. Die Eckpunkte des BMI greifen insgesamt elf Beispiele auf, wie Videoüberwachung, Datenerhebung im Bewerbungsverfahren und private Kommunikationsmittelnutzung. Sie sollen in einem neuen Kapitel „Arbeitnehmerdatenschutz" zusammengefasst werden.

Aber beide Entwürfe springen zu kurz: Weder lösen sie grundsätzliche Fragen des Datenschutzrechts, noch bieten sie angesichts des zu erwartenden ständigen Anpassungsbedarfs Rechtssicherheit.

iPhone der ID-Karten?

Zum 01.11.2010 wird der elektronische Personalausweis eingeführt. Das Bundesinnenministerium hat den Informationsbedarf angesichts des optionalen Charakters vieler Neuerungen erkannt und präsentiert nun eine eigene Website. Dort wird der ePersonalausweis als multifunktionaler Problemlöser angepriesen – quasi als iPhone der ID-Karten.

Die Informationen insbesondere über den elektronischen Identitätsnachweis sind sehr einfach gehalten. Es stehen eine Reihe von zum Teil fehlerhaften Formularen bereit. Vergeblich sucht man überzeugende Argumente für die Nutzung der neuen Funktionen, Hinweise zu dem für den elektronischen Identitätsnachweis erforderlichen Lesegerät oder die zu erwartenden Kosten. Auch über die benötigte Software schweigt sich das Portal aus.

Auf dem versteckt verlinkten Informationsangebot des BSI zu elektronischen Ausweisen finden sich die technischen und organisatorischen Einzelheiten – in Gestalt von fast 20 Technischen Richtlinien. Die schiere Menge und das Ausblenden kritischer Aspekte dürfte selbst dem professionell interessierten Publikum den Zugang erschweren. Dass der ePersonalausweis so zum Kultobjekt wird, darf bezweifelt werden.

Fish and Cheese

Am 04.05.2010 erweiterte Google seine Sammlung von Tools zur Sicherheit von Web-Anwendungen um Jarlsberg – eine Microblogging-Anwendung, löchrig wie dänischer Käse. Sie soll wie z. B. auch OWASP WebGoat (siehe SSN 2/2010) zum Experimentieren mit Web-Schwachstellen einladen. Erst kurz zuvor hatte Google am 19.03.2010 als Pendant den Application-Scanner skipfish veröffentlicht. Nun vergnügen sich Fisch und Käse in unserem Labor miteinander ...

Zeitläufte

Seit dem 08.04.2010 ist die stark überarbeitete Version 2 des SANS Investigative Forensics Toolkit (SIFT) als VMware mit über 350 Werkzeugen verfügbar. Wesentliche Neuerung ist der Logparser log2timeline, der mit Hilfe von timescanner alle Zeitinforma-

tionen aus über 23 Logformaten in 13 Artefaktklassen (u. a. EXIF, PCAP, Flash Cookies) automatisiert extrahiert. Nutzt man weitere in SIFT enthaltene Werkzeuge wie TSK (aktualisierte V 3.12 vom 23.05.2010) und RegRipper (modifizierte Windows-Version vom 10.05.2010), lässt sich die Menge korrelierbarer Zeitquellen vervollständigen. Durch eine abschließende chronologische Sortierung werden Aktivitäten eines untersuchten Systems oder interaktiven Benutzers im Zeitverlauf nachvollziehbar.

Da der überwiegende Teil der auswertbaren Informationen aus Verlaufsdaten besteht, die während der Systemnutzung automatisch anfallen, lässt sich so auf jedem länger genutzten (und unmanipuliertem) Linux- bzw. Windows-System das Nutzungsverhalten im Zeitverlauf rekonstruieren. Nicht nur Google und Facebook machen gläsern – auch das eigene System vergisst nie.

MoPS 2010

Gut drei Jahre nach dem Month of PhP Bugs (MoPB 2007, siehe SSN 3/2007) wurde der Mai 2010 zum Month of PHP Security (MoPS 2010) umgewidmet. Bisher veröffentlichte das vierköpfige Initiatoren-Komitee neun Artikel und vierzig neue Bugs – ein weiterer Beleg, dass eine konzertierte Aktion zur Verbesserung der Sicherheit von Software auch kurzfristig enorme Fortschritte bewirken kann.

Ein Quentchen Trost

„Das kann doch jedem mal passieren…“ – so wirkte die Bewertung des gefühlten Komplettausfalls des deutschen Internets am 12.05.2010 durch den Verursacher, die DENIC eG. Eine sehr knappe Stellungnahme trug zu zahlreichen Spekulationen über mögliche Ausfallursachen bei. Ein wenig gemildert wurde die Verunsicherung durch eine etwas ausführlichere Stellungnahme zu Hintergründen, zwei Tage nach dem Vorfall.

Vorbildlich dagegen der Blog-Eintrag, mit dem die ASF auf einen erfolgreichen Angriff auf das Apache Projekt vom 05.04.2010 reagiert hatte: Darin wurde der Angriff analysiert und sowohl technische als auch organisatorische Maßnahmen als Konsequenzen präsentiert. Auf diesem Niveau hätte man sich die Kommunikation des DENIC gewünscht – das hätte die verunsicherungsbedingten Folgeschäden des Ausfalls begrenzt. Auch Krisenkommunikation will gelernt sein.

Secorvo News

Alles auf eine Karte

Der Traum jedes Sicherheitsbeauftragten ist ein durchgängiges Identitätsmanagement, das Betriebsausweis, Gebäude- und Rechnerzugang integriert. Die KIT-Card, die mit der Gründung des „Karlsruher Instituts für Technologie“ (KIT) entstand, führt an diesen traumhaften Zustand heran – sie organisiert die Wege von über 8.000 Mitarbeitern der im Rahmen der Exzellenzinitiative ausgezeichneten Spitzenforschungseinrichtung.

Wie die technisch-organisatorische Umsetzung erfolgte, welche Klippen dabei zu umschiffen waren und was er aus dem Projekt gelernt hat, stellt Projektleiter Michael Gehle auf dem KA-IT-Si-Event am **24.06.2010** im Schlosshotel vor (Anmeldung).

Lizenz zum Prüfen

Seit dem 01.05.2010 verstärkt Jochen Schlichting als BSI-lizensierter ISO 27001-Auditor auf der Basis von IT-Grundschutz das Secorvo-Grundschutz-Team.

Best of Consulting

Ein leichter Anfall von Hybris, gewürzt mit einer Prise Chuzpe, ließ uns im vergangenen Jahr als kleiner David bei dem von der WirtschaftsWoche ausgelobten Beratungsranking „Best of Consulting 2010“ in der Kategorie „IT-Strategie“ antreten.

Nach drei Qualifikationsrunden, in denen die Qualität der Beratungsleistung aus der Sicht von zehn verschiedenen Kunden und ein ausgewähltes Referenzprojekt von einem wissenschaftlichen Fachbeirat analysiert und bewertet wurden, erreichte Secorvo im Februar 2010 das Finale.

Am 27.05.2010 wurde die Jury-Entscheidung über die Platzierung der Finalisten in Berlin bekannt gegeben – und Secorvo als Zweitplatzierter in der Kategorie IT-Strategie ausgezeichnet. Ein dritter Preis wurde wegen des großen qualitativen Abstands zu den weiteren Kandidaten nicht vergeben.

Veranstaltungshinweise

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

Mai 2010	
30.05.-03.06.	Eurocrypt 2010 (IACR, Nizza/F)
Juni 2010	
07.-08.06.	DuD 2010 (Computas, Berlin)
07.-11.06.	TISP-Schulung (Secorvo College)
Juli 2010	
15.07.	2. Karlsruher „Tag der IT-Sicherheit“ (KA-IT-Si/IHK/Cyberforum, IHK Karlsruhe)
24.-29.07.	Black Hat (Las Vegas/US)
29.07.-01.08.	DEFCON 18 (Las Vegas/US)
August 2010	
02.-04.08.	DFRWS 2010: Digital Forensic Research Workshop (Portland/US)
09.-13.08.	19th USENIX Security Symposium (Washington/US)
15.-09.08.	Crypto 2010 (IACR, Santa Barbara/US)
September 2010	
28.-29.09.	7. Security Awareness Symposium (Secorvo, Ettlingen)

Fundsache

Zahlreiche Datenschutz-Verstöße haben in den vergangenen Jahren die Sensibilität für den Schutzbedarf personenbezogener Daten geschärft. Seit September 2009 sammelt das „Projekt Datenschutz“ Berichte über Datenschutzpannen – gute Munition gegen hartnäckige Verweigerer.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Michael Knopp, Jochen Schlichting

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

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

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

secorvo
security consulting

Secorvo Security News

Juni 2010

Unqualifiziert qualifiziert

Damit eine elektronische Signatur als „qualifizierte“ gilt, muss sie bekanntlich etliche Voraussetzungen erfüllen. Eine davon ist, dass sie mit technischen Komponenten erstellt wurde, deren Sicherheit durch eine von der Bundesnetzagentur (BNetzA) anerkannte Stelle überprüft und bestätigt wurde.

Seit dem 19.12.2008 besitzt der Chipkartenleser „Kobil KAAN TriB@nk“ eine solche Bestätigung. Am 17.04.2010 veröffentlichte ein Unbekannter unter dem Pseudonym ‚Colibri’ eine Dokumentation, die zeigt, wie eine manipulierte Firmware in diesen Leser geladen werden kann. Damit ließen sich zumindest theoretisch nicht nur die PINs von Karteninhabern abfangen, sondern auch heimlich weitere Signaturen erzeugen.

Der Fehler: Der Leser validierte beim Update zwar die Signatur des Herstellers über die übertragenen Datenblöcke, prüfte jedoch nicht, ob die Blöcke auch in der richtigen Reihenfolge an der beabsichtigten Stelle im Speicher landen. Dass diese (inzwischen gepatchte) Lücke bei der Prüfung des Geräts übersehen wurde, zeigt, wie auch Prof. Dr. Rainer W. Gerling von der Max-Planck-Gesellschaft kommentierte, dass selbst eine standardisierte Zertifizierungsprüfung letztlich auf individuellem Geschick und Erfahrung des Prüfers basiert.

Am 07.06.2010 erklärte die BNetzA die Sicherheitsbestätigung des Geräts für ungültig – mit Wirkung zum Veröffentlichungstag des Angriffs. Damit schuf sie unvermeidlich zwei neue Klassen von elektronischen Signaturen (vgl. SSN 04/2009): Alle zwischen dem 17.04. und 07.06.2010 mit dem TriB@nk-Leser erstellten Signaturen wurden rückwirkend zu „dann doch nicht ganz so qualifizierten Signaturen“, alle zwischen dem 19.12.2008 und dem 17.04.2010 erstellten zu „qualifizierten, die möglicherweise gefälscht sein könnten“.

Bleibt ein profanes Problem: Woran erkennt man, sofern man möchte, bei der Prüfung einer Signatur, mit welchem Chipkartenleser sie erstellt wurde?

Inhalt

secorvo
security consulting

Security News

WLAN-Haftung

Anspruch auf Unterlassung, aber kein Schadensersatz – das ist das Ergebnis der mit Spannung erwarteten BGH-Entscheidung vom 12.05.2010 zur Haftung von Anschlussinhabern für von Dritten verübte Schädigungen über unbefugt genutzte WLANs.

Nach der seit dem 07.06.2010 vorliegenden Begründung treffen den Anschlussinhaber Prüfpflichten hinsichtlich der von ihm ergriffenen Sicherheitsmaßnahmen. So sind mindestens die zum Zeitpunkt des Routerkaufs marktüblichen Sicherungen zu ergreifen; ein kontinuierliches Aktualisieren der Maßnahmen sei allerdings nicht zumutbar.

In dem aus dem Jahr 2006 datierenden Fall erwartete der BGH eine aktivierte WPA-Verschlüsselung. Jedoch habe der Beklagte seine Sorgfaltspflicht verletzt, indem er für den Routerzugang kein eigenes, ausreichend langes Passwort vergeben, sondern es bei dem voreingestellten Passwort belassen habe – eine merkwürdige Einschätzung, sofern das Herstellerpasswort individuell und zufällig gewählt war.

Zur Klärung der bestehenden Rechtsunsicherheit wird diese Entscheidung wenig beitragen. Zu lückenhaft waren die weitgehend auf Annahmen und Unterstellungen beruhenden Sachverhaltsfeststellungen der Instanzgerichte; zu viele Fragen waren nicht Gegenstand der Revision. Offen bleibt bspw. die Anwendbarkeit der Deckelung der Abmahnkosten aus § 97a UrhG. Auch hätten dem Urteil Ausführungen zur Handhabung der Beweislastverteilung gut getan. Sowohl unschuldig Abgemahnte als auch Opfer einer Urheberrechtsverletzung werden es weiterhin schwer haben, ihre jeweiligen Rechtsansprüche durchzusetzen.

„Grundschutzscanner“

Seit dem Linuxtag (09.-12.06.2010) ist Version 3.0 der BOSS-Scanner-Live CD des BSI verfügbar. Sie basiert nun auf einer komfortabel startbaren Version des Scannerframeworks OpenVAS 3.0. Damit bleibt das BSI seiner Open-Source-Philosophie treu. Mit der Förderung der Entwicklung von Plugins (ca. 17.000) wurden auch die Anwender in Unternehmen und Behörden nicht vergessen: Aktuelle Plugins sind über den kommerziellen Greenbone Security Feed (GSF) beziehbar.

Der GSF in BOSS 3.0 liefert bei einigen Plugin-Ergebnissen genauere und weiter gehendere Ergebnisse als Nessus. Der GSF wurde im Kontext der als Open Source verfügbaren Security Management Suite OSSIM sogar mit Scan-Konfigurationen für die 10. und 11. Ergänzungslieferung der IT-Grundschutz-Kataloge ausgestattet. Aber Achtung: Ein „fehlerfreier“ Scan bedeutet nicht, dass ein IT-Verbund IT-Grundschutz-konform ist – naturgemäß werden z. B. organisatorische Maßnahmen nicht geprüft.

Erfreulich ist, dass mit BOSS 3.0 bewährte und neue Werkzeuge nun wieder „amtlich“ für Auditoren verfügbar sind, darunter amap, nmap, ldapsearch, snmpwalk, strobe, portbunny und w3af – ein wichtiges Signal zur Klärung der immer noch verbreiteten Unsicherheiten im Umgang mit dem „Hackerparagrafen“ § 202c StGB.

Sammelwütig

Nach Mahnungen diverser Gerichte und des Bundesdatenschutzbeauftragten (22. Tb., S. 58) hat das Bundesinnenministerium mit Zustimmung des Bundesrats am 04.06.2010 im Schatten der WM die konstituierende Verordnung zur „Verbunddatei Gewalttäter Sport“ und zahlreichen weiteren zentralen Dateien des Bundeskriminalamts erlassen.

Die Verordnung legt die Art der zu speichernden Daten für ca. 80 präventive Verbunddateien fest, die zwischen 100 und 6 Millionen Datensätze über verdächtige Bürger enthalten.

Für die „Hooligan-Datenbank“ mit 11.245 gespeicherten Personen (Stand 2009) dürfen neben Adress- und Identifizierungsdaten etwa Schulabschluss, frühere Staatsangehörigkeit, Volkszugehörigkeit, Angaben zu Personalausweis oder Reisepass, Angaben zu Kommunikationsmitteln, Konten- und Vermögensinformationen, Beziehungen zu Orten, Gruppen, Ereignissen oder Einzelpersonen sowie Referenzen auf weitere gespeicherte Vorgänge gesammelt und gespeichert werden. Zur Aufnahme in die Datei genügen eingeleitete Ermittlungen; beschränkt auf umfassende Kontaktdaten sogar die bloße Begleitung von Verdächtigen. Gelöscht werden müssen die Daten dagegen nur, wenn bei einer Einstellung des Verfahrens ausdrücklich das Fehlgehen des Verdachts festgestellt wurde.

Mit rekordverdächtiger Reaktionszeit hat das Bundesverwaltungsgericht am folgenden Tag einen anhängigen Löschantrag mit Verweis auf die Verordnung zurückgewiesen.

Ein Lerneffekt aus der gerade erst drei Monate alten Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung ist nicht feststellbar – das betrifft bereits die Rechtsgrundlagen im BKA-Gesetz: Es fehlen konkrete Vorgaben zur Datensicherheit, die Transparenz der Erhebung und Speicherung ist ebenso wie die diesbezüglichen Kriterien zur Zulässigkeit ungenügend – ein weiterer Fall für das Bundesverfassungsgericht?

Mythen sterben langsam

Am 28.06.2010 publizierte der Branchenverband BITKOM die Ergebnisse einer Forsa-Studie – mit vermeintlich erschütternden Ergebnissen: 41 % der Befragten ändern ihre Passworte nie. „Die wichtigsten Passwörter sollten alle drei Monate geändert werden“, fordert Prof. Dieter Kempf vom Präsidium des BITKOM.

Dabei sind erzwungene Passwortwechsel in der Praxis meist nutzlos: Sie verleiten Benutzer dazu, sich „Bildungsregeln“ zu überlegen – und damit den Sinn von Passwortwechseln zu konterkarieren. Denn Wechsel sollen im Falle einer Kompromittierung den Schaden begrenzen – erkennt der Angreifer aber die Bildungsregel, kann er aus jedem geknackten Passwort das nächste ableiten.

Zielführender als die Verbreitung von Passwort-Mythen (siehe SSN 6/2009) wäre die Forderung nach längeren Passwörtern. Das Projekt RainbowCrack publizierte am 17.06.2010 Version 1.41 des Software-Crackers, der mit einer schnellen Grafikkarte als Co-Prozessor und einer 576 GB großen Rainbow-Tabelle acht Zeichen lange Passwörter in 30 Minuten (!) findet. Kürzer als 10 Zeichen dürfen Passwörter (zumindest unter Windows) heute nicht mehr sein, wenn sie einem solchen Cracker wenigstens 90 Tage standhalten sollen – zum Schutz vor einer parallelisierten Berechnung sind 12 Zeichen das Minimum.

Nur ein Zeichen mehr, und der Aufwand, ein gutes Passwort zu Cracken, steigt um den Faktor 84 – das sollte für ein halbes Berufsleben reichen.

Schauen, was läuft

Am 15.06.2010 wurde Version 10 von Autoruns veröffentlicht. Ursprünglich von Sysinternals entwickelt und später von Microsoft übernommen zeigt es unter anderem an, welche Programme und Dienste unter Windows gestartet werden. Damit lassen sich nicht nur unnötig gestartete Programme, Dienste und Prozesse erkennen und deaktivieren, sondern auch eingenistete Schadsoftware und Spyware identifizieren.

Ähnliches leistet das Programm Starter; es bietet sogar die Möglichkeit, Dienste direkt zu konfigurieren oder eine Recherche zu den „Fundsachen“ in verschiedenen Internet-Suchmaschinen zu starten.

Allerdings sollten derartige Tools generell vor der produktiven Nutzung in einer Testumgebung überprüft werden – nicht selten wird beliebte Freeware in mit Schadcode infizierten Varianten verbreitet.

Löchrige Pen-Tests

Unter dem Titel “Why Johnny Can’t Pentest” veröffentlichten drei Forscher von der University of California am 27.04.2010 einen ausführlichen Vergleich aktueller Schwachstellenscanner für Web-Anwendungen. Dafür analysierten sie die Ergebnisse der Pen-Tests eigens entwickelter Web-Anwendungen mit bekannten Schwachstellen.

Die 21seitige Studie liefert nicht nur ein “Ranking” der getesteten Produkte – besonders interessant sind die Dokumentation der Vorgehensweise und die Erkenntnis, dass sich mit heutiger Technik einige Schwachstellen, wie beispielsweise Fehler in der Anwendungslogik, gar nicht und andere nur sehr schwer automatisiert erkennen lassen.

Das Fazit ist wenig überraschend: Der Einsatz von automatisierten Scannern sollte grundsätzlich durch händische Prüfungen ergänzt werden. Ausführlich werden die Ergebnisse der Studie auf der DIMVA 2010 in Bonn am 08.-09.07.2010 vorgestellt.

Secorvo News

iPhone Security

In nicht wenigen Unternehmen hält derzeit Apples iPhone Einzug. Trotz seiner nach wie vor deutlichen Nachteile bei Business-Anwendungen gegenüber RIMs BlackBerry wiegen „Sex-Appeal“ und Nimbus des Geräts auch bei Führungskräften oft schwerer.

Wie sicher aber sind Unternehmensdaten auf einem iPhone aufgehoben? Was ist von der Hardware-Verschlüsselung und anderen Schutzmechanismen zu halten? Lassen sich iPhones ohne Inkaufnahme zusätzlicher Risiken in die IT-Infrastruktur integrieren? Diesen und weiteren Fragen ist Jörg Völker auf den Grund gegangen – und hat die Ergebnisse seiner Untersuchungen nun in der Fachzeitschrift „Datenschutz und Datensicherheit“ (DuD) veröffentlicht.

„Tag der IT-Sicherheit"

Zum zweiten Mal findet am **15.07.2010** der Karlsruher „Tag der IT-Sicherheit“ statt – eine Kooperationsveranstaltung der IHK Karlsruhe, des Cyber-Forum e. V. und der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si). Die Vorträge behandeln aktuelle Themen der IT-Sicherheit und Best-Practice-Beispiele, darunter ein Lagebericht des Landesamts für Verfassungsschutz Baden-Württemberg zur Wirtschaftsspionage in deutschen Unternehmen, eine kritische Analyse der Sicherheit von iPhones und die erfolgreiche Awareness-Kampagne der EnBW AG.

Die Veranstaltung beginnt um 14 Uhr und richtet sich an Geschäftsführer und IT-Leiter unabhängig von Branche und Unternehmensgröße. Hier finden Sie das vollständige Programm und die Möglichkeit zur Anmeldung.

Veranstaltungshinweise

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

Juli 2010	
08.-09.07.	DIMVA 2010 (Bonn)
15.07.	2. Karlsruher „Tag der IT-Sicherheit“ (KA-IT-Si/IHK/Cyberforum, IHK Karlsruhe)
24.-29.07.	Black Hat (Las Vegas/US)
29.07.-01.08.	DEFCON 18 (DEFCON, Las Vegas/US)
August 2010	
02.-04.08.	DFRWS 2010: Digital Forensic Research Workshop (DFRWS, Portland/US)
09.-13.08.	19th USENIX Security Symposium (Washington/US)
15.-09.08.	Crypto 2010 (IACR, Santa Barbara/US)
September 2010	
20.-23.09.	SEC 2010 (IFIP, Brisbande/AUS)
20.-24.09.	TISP-Schulung (Secorvo College)
28.-30.09.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
28.-29.09.	7. Security Awareness Symposium (Secorvo, Ettlingen)

Fundsache

Die Skulptur „Kryptos“ des Künstlers James Sandborn vor dem Hauptsitz der CIA von 1991 enthält vier Kryptogramme, von denen drei 1998 von einem Mitarbeiter der CIA dechiffriert wurden. Das vierte, 97 Zeichen lange Kryptogramm ist bis heute ungelöst.

Impressum

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

ISSN 1613-4311

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

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

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

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

secorvo
security consulting

Secorvo Security News

Juli 2010

Makellose Bürger

Für den Staatsphilosophen Thomas Hobbes (1588-1679), aufgewachsen im von Bürgerkriegen geprägten England des 17. Jahrhunderts, legitimiert sich das Gewaltmonopol des Staates aus einem (fiktiven) Gesellschaftsvertrag, mit dem die Bürger alle Macht uneingeschränkt dem Souverän übertragen. Sie gewinnen damit Sicherheit vor äußeren Feinden und ihrer eigenen „wölfischen" Natur – zum Preis eines weitgehenden Verzichts auf freie Entfaltung.

Nun sind wir in den westlichen Industrieländern heute zum Glück weit von bürgerkriegsähnlichen Verhältnissen entfernt – aller organisierten Kriminalität und terroristischen Bedrohungen zum Trotz. Dennoch erfreut sich der Kerngedanke der Hobbes'schen Lehre auch in repräsentativen Demokratien zahlreicher Anhänger. Bürgerliche Freiheiten, wie sie sich in allen Verfassungen der Aufklärung als Abwehrrecht des souveränen Bürgers gegenüber einem übermächtigen Staat finden, werden in wachsendem Umfang Sicherheitsbedürfnissen geopfert – selbst dann, wenn es sich um nachweislich wirkungslose Symbolik handelt: „Nacktscanner" und Internet-Sperren lassen grüßen.

Nun sind innere und äußere Sicherheit zweifellos von hohem Wert – ohne sie können sich weder Freiheit noch Wohlstand entfalten. Man beachte jedoch die Kausalität: Sicherheit dient dem Schutz der freien Entfaltung. Tastet sie deren Substanz an, gefährdet sie das zu schützende Gut – und verfehlt ihren Zweck. Selbstmord ist eben keine angemessene Reaktion auf die Angst vor dem Tod.

Wie weit dieser Werterahmen bereits aus dem Blick geraten ist, zeigt die schamlos zynische Namenswahl der NSA für ein Überwachungsprojekt kritischer Infrastrukturen im Volumen von 100 Mio. US$, das das Wall Street Journal am 08.07.2010 öffentlich machte: „Perfect Citizen". Von der „Anomalie-Erkennung" ist es dann nicht mehr weit bis zu deren präventiver Beseitigung. Noch einfacher ginge es allerdings gleich ganz ohne Bürger.

Inhalt

secorvo
security consulting

Security News

Whitelisting am Ende?

Der Stoßseufzer „Wem kann man eigentlich noch trauen?“ ist leider eben so abgedroschen wie berechtigt. Anfang Februar 2010 wurde auf der Konferenz Black Hat DC demonstriert, dass sich Malware für iPhones sogar über Apples offiziellen App Store verteilen lässt – wie zuvor schon bei Stores anderer Hersteller. Am 17.06.2010 wies Marissa Vicario (Symantec) in ihrem Blog darauf hin, dass über 90% aller Malware-infizierten Webseiten von seriösen Anbietern stammen. Sie wurde am 28.06.2010 vom tschechischen Antiviren-Hersteller Avast bestätigt: Auf eine „Schmuddelkram“-Webseite kämen mittlerweile 99 seriöse Seiten, über die man sich beim Browsen infizieren kann. Dann wurde im offiziellen Download-Bereich für Firefox-Addons am 13.07.2010 die Schadsoftware „Mozilla-Sniffer“ entdeckt. Und schließlich musste Dell am 20.07.2010 Austausch-Motherboards zurückrufen, die ab Werk mit Malware bestückt waren.

Die Häufung derartiger Meldungen legt nahe, dass man sich immer weniger auf vermeintlich zuverlässige Quellen verlassen kann, von denen man Daten, Anwendungen oder Systeme bezieht. Der Whitelisting-Ansatz „Erlaube seriöse Quellen und behandle alle anderen restriktiv“ dürfte mittelfristig ins Leere laufen. Solange noch Zeit ist, sollten sich Unternehmen, die sich darauf stützen, Gedanken über einen Plan B machen.

Microsoft is evil, ...

... so die allgemeine Wahrnehmung, wenn es um die Sicherheit von PCs geht. Eine der wichtigsten Erkenntnisse im „Secunia Half Year Report 2010“ vom 13.07.2010 zeigt, dass diese Wahrnehmung nicht mehr der Realität entspricht: Von den 50 meist installierten Programmen auf PCs sind 24 Programme nicht von Microsoft – und weisen im Untersuchungszeitraum 3,5-mal so viele entdeckte Schwachstellen auf. Berücksichtigt man, dass die Zahl der „Bug-Searcher“ bei Microsoft deutlich höher sein dürfte, könnte das Verhältnis der tatsächlichen Schwachstellen noch größer sein. Diese Entwicklung sollte Anlass sein, auch für Programme von „Drittherstellern“ ein funktionierendes Patch-Management zu etablieren.

Viel Rauch um Skype

Seit dem 07.07.2010 geistern Meldungen durch die Presse, nach denen Sean O'Neil die Skype-Verschlüsselung „geknackt“ habe (siehe z. B. Spiegel Online oder Chip Online). Tatsächlich wurde ein von Skype verwendetes Verschlüsselungsverfahren *aufgedeckt*, auf dessen Geheimhaltung Skype sehr viel Mühe verwendet hat. So enthält der Code der Skype-Clients verschiedene Reverse-Engineering-Gegenmaßnahmen. Durch die Publikation des Codes sind diese *Gegenmaßnahmen* als gebrochen anzusehen.

Eine erste Begutachtung des Quellcodes hat ergeben, dass Skype als Stromchiffre eine Variante von RC4 nutzt – mit dem Ziel einer beabsichtigten Inkompatibilität. Da der Code nun offenliegt, wird sich bald zeigen, ob das modifizierte Verfahren ebenso sicher ist wie RC4, oder ob demnächst Millionen Nutzer unter den Folgen schlechter Kryptographie zu leiden haben werden.

Rückzug von der Signatur?

Der Rat der Europäischen Gemeinschaft hat am 13.07.2010 Vereinfachungen der Richtlinie über das gemeinsame Mehrwertsteuersystem (2006/112/EG) erlassen. Diese betreffen auch die vereinheitlichten Anforderungen an die elektronische Rechnungsstellung. Entscheidend ist die Änderung des Art. 233 Abs. 1, der bislang die Verwendung einer qualifizierten elektronischen Signatur oder die Nutzung des EDI-Verfahrens vorgab. Nun stellt sie dem einzelnen Steuerpflichtigen frei, mit welchen Mitteln er Authentizität, Integrität und Lesbarkeit der Rechnung vom Ausstellungszeitpunkt bis zum Ende der Aufbewahrungsfrist sicherstellt. Auch der Einsatz organisatorischer Kontrollmittel soll zulässig sein, solange eine verlässliche Buchungskontrolle zwischen dem Waren- oder Dienstleistungsbezug und der Rechnung gewährleistet wird. § 14 Abs. 3 UStG, der das Signaturerfordernis im deutschen Recht festschreibt, wird nun bis zum 31.12.2012 angepasst und gelockert werden müssen.

Unternehmen werden diese Entwicklung vermutlich mit Erleichterung zur Kenntnis nehmen. Die Bundesregierung hat die Signaturpflicht des § 14 Abs. 3 UStG ohnehin auf die Streichliste zum Bürokratieabbau gesetzt (dort lfd. Nr. 14) und plant eine Befassung mit der Thematik noch in diesem Jahr. Allerdings geht die Erleichterung auf Kosten der Rechtssicherheit, denn während sie die Mittel freigibt, bleibt die Verpflichtung zur Sicherung von Authentizität und Integrität erhalten. Ob allein organisatorische Maßnahmen hierfür ausreichen, wird für den Gesetzgeber, die Steuerpflichtigen und die Rechtsprechung schwer bestimmbar sein. So wird der Zwang zur ungeliebten Signatur durch ein erhöhtes Eigenrisiko der Unternehmen ersetzt.

CC-BS-Schutzprofil

Schutzprofile ermöglichen für eine definierte Produktkategorie von IT-Systemen eine standardisierte Beschreibung der Bedrohungen, Sicherheitsziele,

Annahmen über die Betriebsumgebung und daraus resultierenden Sicherheitsanforderungen. Sie legen die Mindeststandards für eine Zertifizierung nach den international vereinheitlichten „Common Criteria for Information Technology Security Evaluation“ fest.

Am 24.06.2010 veröffentlichte das BSI ein neues Schutzprofil für moderne verteilte Betriebssysteme. Das „Operating System Protection Profile (OSPP)“ wurde von einem Konsortium bestehend aus BSI, Vertretern des amerikanischen Zertifizierungsschemas (NIAP) und namhaften Betriebssystemherstellern entwickelt. Die aktuelle Version 2.0 der OSPP definiert die Anforderungen an ein sicheres Betriebssystem und fordert die Evaluierungsstufe EAL 4, die nicht nur formale Anforderungen an die Entwicklung stellt, sondern auch die Analyse von Design und Quellcode verlangt.

Dabei bezieht sich ein Schutzprofil wie auch eine CC-Zertifizierung immer auf eine definierte Einsatzumgebung. OSPP setzt voraus, dass die Plattform (Hardware, Geräte, Firmware), auf der das Betriebssystem ausgeführt wird, gegen physische Angriffe und Manipulationen geschützt ist und alle Managementaktivitäten von vertrauenswürdigen und geschulten Anwendern durchgeführt werden. Immerhin: Eine Abkoppelung des PCs vom Netz ist keine Voraussetzung für den sicheren Betrieb.

State of the Crypto-Art

Als Referenz dafür, welche Kryptoalgorithmen und Schlüssellänge dem Stand der Technik entsprechen, wird – zumindest hierzulande – gerne die vom BSI erarbeitete und von der BNetzA jährlich aktualisierte Übersicht über geeignete Algorithmen heran gezogen. Da sie sich auf das Signaturgesetz bezieht, berücksichtigt sie zwar nur Verfahren, die für Signaturen nötig sind. Allerdings lassen sich daraus die Anforderungen an ein entsprechendes Schutzniveau von Verschlüsselungsverfahren ableiten.

Am 16.07.2010 endete die Kommentarfrist für den Draft der NIST Special Publication 800-131, der Empfehlungen für Algorithmen und Schlüssellängen in allen wichtigen Anwendungsgebieten von Verschlüsselung über Signatur und Schlüsselableitung bis zu Message Authentication Codes geben wird. Er fordert für Verfahren der amerikanischen Bundesbehörden ab 2011 ein Sicherheitsniveau von mindestens 112 bit – das Doppelte dessen, was der (einfache) DES bot, und 32 bit mehr als die bis Ende 2010 verlangten 80 bit. An dieser Empfehlung werden auch nationale Standards künftig nicht vorbei kommen, die für sich reklamieren, kryptografisch „State of the Art“ zu sein.

Sichere Virtualisierung

Ein „Guide to Security for Full Virtualization Technologies“ wurde am 07.07.2010 vom NIST in einer Draft-Version veröffentlicht. Auf 35 Seiten werden anschaulich Begriffe und prinzipielle Sicherheitsmaßnahmen beim Einsatz von Server- und Desktop-Virtualisierung beschrieben. Der Guide eignet sich gut für einen systematischen Einstieg in die Thematik; konkrete technische Empfehlungen für bestimmte Virtualisierungslösungen bleibt er allerdings schuldig.

Deadlines

Zahlreiche Konferenzen zur IT-Sicherheit werfen ihre Schatten voraus – und werben noch um Beiträge. Schnell Entschlossene können bis zum **01.08.2010** einen Vorschlag für den 18. DFN Workshop „Sicherheit in vernetzten Systemen“ (15.-16.02.2011) einreichen.

Ebenfalls bis zum **01.08.2010** werden spannende Vorträge für die OWASP-Konferenz Appsec Germany 2010 (20.10.2010) gesucht. Und das Bundesamt für Sicherheit in der Informationstechnik (BSI) freut sich bis zum **10.10.2010** auf Einreichungen für den 12. Deutschen IT-Sicherheitskongress (10.-12.05.2011).

Secorvo News

Secorvo College

Gleich nach Ende der Sommerferien bietet Secorvo College die nächste Gelegenheit zur Zertifizierung als Information Security Professional mit dem TISP-Seminar am **20.–24.09.2010**. Nähere Informationen zu den Zulassungsvoraussetzungen, den Inhalten und der unabhängigen Zertifikatsprüfung finden Sie unter www.tisp.de (Online-Anmeldung).

Alle weiteren Seminarangebote im Oktober und November mit ausführlichem Programm unter http://www.secorvo.de/college

Security Awareness Symposium

Am **28.–29.09.2010** findet das von Secorvo, dem Berliner eLearning-Spezialisten digital spirit und der Karlsruher Agentur DauthKaun initiierte siebte „Security Awareness Symposium“ in Ettlingen statt. Auch diesmal erwartet Sie ein „Erfahrungsfeuerwerk“ von Projektleitern zahlreicher Awareness-Kampagnen, die ihre Ideen, Erfolge und „Lessons Learned“ präsentieren – ein Treffen, das Sie sich nicht entgehen lassen sollten, wenn die Sensibilisierung Ihrer Kollegen für IT-Sicherheit oder Datenschutz auch auf Ihrer Agenda steht (Anmeldung).

Veranstaltungshinweise

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

Juli 2010	
29.07.-01.08.	DEFCON 18 (DEFCON, Las Vegas/US)
August 2010	
02.-04.08.	DFRWS 2010: Digital Forensic Research Workshop (DFRWS, Portland/US)
09.-13.08.	19th USENIX Security Symposium (Washington/US)
15.-19.08.	Crypto 2010 (IACR, Santa Barbara/US)
30.08.	Sommerakademie 2010 (ULD, Kiel)
September 2010	
07.-10.09.	OWASP AppSec US (Irvine/US)
20.-24.09.	TISP-Schulung (Secorvo College)
28.-29.09.	7. Security Awareness Symposium (Secorvo, Ettlingen)
28.-30.09.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
Oktober 2010	
21.10.	it-sa Datenschutztag 2010 (Computas, Nürnberg)

Fundsache

Grundlegende praktische Regeln für die Informations- und IT-Sicherheit in kleinen und mittelständischen Unternehmen wurden im Interagency Report „Small Business Information Security: The Fundamentals“ (NISTIR 76121) der Computer Security Division des NIST vom Oktober 2009 zusammengefasst – prägnant auf 20 Seiten die wichtigsten Sicherheitsaspekte für Mensch und Technik.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Petra Barzin, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

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

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

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

secorvo
security consulting

Secorvo Security News

August 2010

Editorial: Todesmut

Urlaube überraschen gelegentlich mit neuen Erfahrungen. So fand ich mich kürzlich unversehens auf einem Baum wieder: unter mir zwölf Meter gähnendes Nichts, vor mir zwei nicht einmal fingerdicke, zehn Meter lange Drahtschnürchen zum nächsten Stamm, und dort, auf einer weniger als 1 qm großen hölzernen Plattform, meine feixenden Söhne. Vor meinem inneren Auge spulten sich, von inbrünstiger Reue begleitet, zwar nicht mein bisheriges Leben, aber doch die Ereignisse des vergangenen Abends ab: In geradezu jugendlichem Leichtsinn hatte ich meinen Söhnen zugesagt, mit ihnen einen nahen Hochseilgarten zu besuchen. Nun ja, welcher Vater mag sich schon von seinen Halbwüchsigen als Hasenfuß verlachen lassen... Jetzt aber gab es kein zurück mehr, und mit zittrigen Fingern klinkte ich meine beiden Karabiner ins Seil.

Als ich nach langen 60 Minuten endlich wieder festen Boden unter den Füßen hatte und mein Hirn wieder an etwas anderes als „Todesmut" denken konnte, machte ich eine überraschende Beobachtung: Kein einziger Besucher rutschte von einem der an Seilen baumelnden Balken, federnden Feuerwehrschläuche oder schaukelnden Saftkisten, über die man sich von Baum zu Baum hangeln musste. Und schon beim zweiten Parcours, auf den mich meine Söhne zwangen, wuchs meine Zuversicht, die andere Seite wohlbehalten zu erreichen, und gewann schließlich sogar die Oberhand.

Bei nüchterner Betrachtung war das kein Wunder, denn die soliden Sicherungen begrenzen das tatsächliche Risiko auf eine Falltiefe von 20 cm (und lachende Söhne).

Kaum zurück aus dem Urlaub konfrontierte mich das echte Leben mit einem völligen Kontrasterlebnis: ein CIO, der die Risiken unverschlüsselter mobiler Geräte mit einem „Bei uns ist noch nie etwas passiert" beiseite wischte. Da beschlich mich die ketzerische Idee, ihn in den Hochseilgarten einzuladen. Ob er sich dort oben wohl auch ausklinken würde?

Inhalt

secorvo
security consulting

Security News

Rechtswidrige Webseitenanalyse

Die Aufsichtsbehörde Baden-Württembergs für den Datenschutz im nicht-öffentlichen Bereich hat auf der Grundlage des Entschlusses des Düsseldorfer Kreises vom 26./27.11.2009 am 01.07.2010 eigene Hinweise zum Einsatz von Web-Analysediensten veröffentlicht. Insbesondere der Einsatz von Google Analytics wird als rechtswidrig eingestuft.

Die Datenschutzaufsichtbehörden betrachten IP-Adressen als grundsätzlich personenbezogene Daten. Daher erfordert ihre Erhebung und Verarbeitung zu Analysezwecken gemäß §§ 12, 15 TMG eine (praktisch nicht realisierbare) Einwilligung des Website-Nutzers. Weitere Gründe für die Einstufung liegen in der Datenübertragung in das außereuropäische Ausland, den Nutzungsbedingungen, in denen sich Google die Verarbeitung der Daten auch zu eigenen Zwecken vorbehält, die unzureichende Widerspruchsmöglichkeit und die ungewisse Löschsituation bei Vertragsende.

Fehl geht das Innenministerium allerdings, wenn es eine Auftragsdatenverarbeitung annimmt: Hierzu fehlen Kontrollmöglichkeiten und Weisungsrechte der Verwender sowie ein entsprechender Vertrag nach § 11 BDSG. Vor allem aber beschränkt sich Google nicht auf ein auftragsgebundenes Verarbeiten, sondern handelt eigenständig.

Damit riskieren die Nutzer von Google Analytics, die sich über Webseiten wie OnTraxx leicht identifizieren lassen, Bußgelder nach § 16 TMG. Zwar bietet Google in Reaktion auf den Düsseldorfer Kreis bereits Zusatzcode zur Verkürzung von IP-Adressen. Aber auch damit werden die Probleme des Widerspruchs gegen eine Profilbildung und der Auslandsübertragung nicht gelöst. Die Widerspruchslösung von Google – Sperrung von Cockies – ist unzureichend. In Baden-Württemberg sind nun verstärkte Kontrollen angekündigt; weitere Bundesländer dürften dem Beispiel folgen.

iPhone Jailbreak via Safari

Seit längerem ist bekannt, dass auch für das iPhone 4 und iOS 4.0.1 sowohl ein Jailbreak als auch ein Unlock möglich sein sollen (siehe SSN 11/2009). Dennoch war die Überraschung groß, als am 02.08.2010 das Dev Team den Jailbreak für das iPhone 4 veröffentlichte. So stand der Jailbreak nun nicht nur für alle iOS-Geräte von Apple (iPod, iPad, iPhone) und alle iOS-Versionen zur Verfügung, sondern nutzte eine Lücke im PDF-Reader des mobilen Safari-Browsers aus, der es PDF-Dateien erlaubt, unsignierten Code auf dem iPhone auszuführen.

Diese Lücke kann natürlich auch durch andere Angreifer ausgenutzt werden, um beliebige Anwendungen auf dem Gerät zu installieren. Einen wirksamen Schutz gegen diese Schwachstelle bietet derzeit nur das Update für iOS 4.0.2 vom 11.08.2010. Auf Geräten, die bereits einen Jailbreak durchgeführt haben, lässt sich ein Tool installieren, dass vor dem Öffnen von PDFs warnt. Ansonsten bleibt nur die Empfehlung, auf dem iPhone vorläufig lieber keine PDF-Dateien unbekannter oder zweifelhafter Herkunft zu öffnen.

RainbowCrack 1.5

Fast exakt ein Jahr nach Veröffentlichung der Version 1.4 (siehe SSN 08/2009) stellte das Projekt RainbowCrack am 26.08.2010 mit Version 1.5 eine für 64bit-Betriebssysteme optimierte Fassung ihres Passwort-Crackers zum Download bereit. Mit über 320 Milliarden (MD5-) Hashwerten pro Sekunde erreicht diese Version auf der Referenzhardware mehr als die vierfache Geschwindigkeit der Vorversion – selbst alpha-numerische 10-Zeichen-Passwörter lassen sich damit auf einem Standard-PC mit schneller Grafikkarte in wenigen Tagen finden.

I Can Stalk You...

Erst Mitte Februar hatte der Dienst „PleaseRobMe“ für Aufregung gesorgt, der aktuelle Twitter-Nachrichten anzeigte, in denen die Autoren ihren Aufenthaltsort fern von zu Hause preisgaben (siehe SSN 02/2010). Offenbar genügte das nicht, um Millionen naiver Tweeter die Gefährlichkeit ihrer öffentlichen Mitteilungsfreude vor Augen zu führen. Daher startete Myhemic Labs mit „ICanStalkU“ am 05.05.2010 eine Webseite, die den aktuellen Aufenthaltsort aus den Metadaten von auf Twitter veröffentlichten SmartPhone-Fotos gewinnt – die inzwischen häufig Geodaten enthalten.

Dabei ist Abhilfe simpel: Wie man iPhone, Android und Blackberry dazu überredet, keine Geodaten zu speichern, erläutern die Autoren bereitwillig. Wer eine solche Vorsicht pathologisch (oder zumindest übertrieben) findet, dem sei der Aufsatz von Blumberg und Eckersley über Locational Privacy vom August 2009 dringend zur Lektüre empfohlen.

Cryptool 1.4.30

Am 04.08.2010 wurde Version 1.4.30 der Lernsoftware Cryptool veröffentlicht. Wir haben dies zum Anlass genommen, die Software unter didaktischen Gesichtspunkten unter die Lupe zu nehmen. Nach der Installation stellt die Anwendung ein Hauptfenster zur Verfügung, innerhalb dessen allerlei Experimente angestellt werden können, d. h. der Anwender kann eine große Vielfalt von kryptografischen Verfahren auf beliebige Textdateien anwen-

den lassen, etwa zur Verschlüsselung oder zur Signaturerzeugung. Der Punkt, der Cryptool dabei so interessant macht, ist die Visualisierung der Verfahren. Die ist allerdings unterschiedlich gelungen ausgefallen; bei manchen Verfahren werden nur Zwischenergebnisse angezeigt, bei anderen wird der Anwender im Detail durch den Algorithmus geführt. Andere Experimentierfelder ergeben sich bei der Analyse klassischer Kryptoverfahren oder bei der Durchführung zahlentheoretischer Experimente.

Da es viele Mitwirkende an dem Projekt gibt, ist das Erscheinungsbild der Software insgesamt recht inhomogen. Das ist kein Schaden; etwas störend fielen aber unterschiedliche didaktische Herangehensweisen auf. So kommt die Zahlentheorie mit dem Charme einer Vorlesung daher, während etwa die Demonstration des AES-Verfahrens sehr lebendig und greifbar wirkt. Für zukünftige Versionen wäre es schön, wenn der didaktische Ansatz sowie die Visualisierung an verschiedenen Stellen poliert und vereinheitlicht würde. Auch wenn Cryptool aus einem Anwender keinen Kryptologen macht, hat es zweifellos einen hohen Lernwert – mit Spaßfaktor.

EU-Verfahrensverzeichnis

Die EU-Kommission hat am 26.07.2010 einen „Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht“ veröffentlicht. Das Papier soll den EU-Bürgern Transparenz darüber verschaffen, wer auf europäischer Ebene welche Daten zu welchem Zweck speichert und welche Stellen Zugriff erhalten. Erläutert werden 18 bestehende, in Umsetzung befindliche oder geplante Datensammlungen vom Schengener Informationssystem (SIS) über die Vorratsdatenspeicherungsrichtlinie bis zu dem geplanten Passenger Name Records (PNR) System für Europa.

Im Stil eines Verfahrensverzeichnisses werden zu jedem Instrument Hintergrund, Zweck, zentraler oder dezentraler Aufbau, die Art der gespeicherten personenbezogenen Daten, die Zugriffsberechtigungen, Regelungen zum Datenschutz, Speicherdauer, Umsetzungsstand und Überprüfungsverfahren angegeben. Zu einigen Datensammlungen, darunter zur Vorratsdatenspeicherungsrichtlinie, zur schwedischen Initiative zum Austausch von Ermittlungsdaten und zum Prüm-Beschluss (grenzüberschreitender DNA-Abgleich) werden Beispiele erfolgreicher Straftataufklärungen oder Statistiken angeführt. Zur Vorratsdatenspeicherung fehlt eine Erfolgsstatistik; es werden lediglich zwei Beispiele aufgeklärter Tötungsdelikte, eine Einbruchsserie und eine bandenmäßige Raubserie benannt.

Die Mitteilung ist gerade auch im Zusammenhang der Rechtsprechung des Bundesverfassungsgerichts zur TK-Vorratsdatenspeicherung zu begrüßen, die angesichts der sehr umfassenden Speicherung in diesem Bereich zur Zurückhaltung in weiteren Bereichen mahnt. Sie könnte Ausgangspunkt für die überfällige Diskussion sein, wie viel Kontrolle wir uns angesichts der tatsächlichen Aufklärungserfolge leisten wollen.

Secorvo News

Secorvo College aktuell

Sichern Sie sich einen Platz auf einem unserer Herbst-Seminare. Los geht es im September mit der Möglichkeit, Ihr Fachwissen durch das anerkannte T.I.S.P.-Zertifikat belegen zu lassen: Vom 20. bis 24.09.2010 findet die nächste T.I.S.P.-Schulung mit anschließender Zertifikatsprüfung statt. Für den „Doppelpack Grundlagen“ empfehlen wir eine baldige Anmeldung: Sicherheitsmanagement heute – Prozesse, Steuerung, Organisation vom 05. bis 07.10.2010 und der „Klassiker“ IT-Sicherheit heute vom 26. bis 28.10.2010 beleuchten neben den aktuellen Standards die wichtigsten Trends im IT-Sicherheitsbereich.

Xdr3$gFa*9z

Eine zentrale Verschlüsselungslösung für die größte Bank im Südwesten Deutschlands – diese Aufgabe haben die IT-Security-Experten Joachim Seeger und Volker Kölz von der Landesbank Baden-Württemberg (LBBW) gemeistert. Die Anforderungen umfassten nicht nur technische Herausforderungen: So sollte die Lösung für den Anwender so unauffällig wie möglich sein, weitestgehend automatisiert laufen und keinen Einfluss auf die Betriebsführung haben. Schließlich mussten die Daten bei einer Störung einfach wiederherstellbar sein. Wie die Experten der LBBW die Datei- und Ordnerverschlüsselung und die Verschlüsselung der Endgeräte heute organisieren, verraten sie am **23.09.2010** bei der nächsten Veranstaltung der KA-IT-Si im Schlosshotel Karlsruhe (Anmeldung).

Security Awareness 7.0

Auf dem siebten „Security Awareness Symposium“ am **28.–29.09.2010** in Ettlingen, das Secorvo zusammen mit dem Berliner eLearning-Spezialisten digital spirit und der Karlsruher Agentur DauthKaun initiierte, erwarten Sie wieder spannende Erfahrungsberichte von Projektleitern zahlreicher Awareness-Kampagnen, die ihre Ideen, Erfolge und „Lessons Learned“ präsentieren – ein Treffen, das Sie sich nicht entgehen lassen sollten, wenn die Sensibilisierung Ihrer Kollegen für IT-Sicherheit oder Datenschutz auf Ihrer Agenda steht (Anmeldung).

Veranstaltungshinweise

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

September 2010	
07.-10.09.	OWASP AppSec US (Irvine/US)
20.-24.09.	TISP-Schulung (Secorvo College)
21.-22.09.	D·A·CH Security (GI/OCG/BITKOM/SI/TeleTrusT, Wien)
28.-29.09.	7. Security Awareness Symposium (Secorvo, Ettlingen)
28.-30.09.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
Oktober 2010	
04.-07.10.	ISSE 2010 (Teletrust, Berlin)
04.-07.10.	Sicherheitsmanagement heute (Secorvo College)
19.-21.10.	ISSECO Certified Professional for Secure Software Engineering (Secorvo College)
19.-21.10.	it-sa (SecuMedia Verlag, Nürnberg)
21.10.	it-sa Datenschutztag 2010 (Computas, Nürnberg)
November 2010	
18.-19.11.	34. DAFTA (GDD e.V., Köln)

Fundsache

Der jüngste IBM X-Force-Halbjahresbericht vom 24.08.2010 belegt einige beunruhigende Tendenzen: Ein deutlicher Anstieg von pdf-Angriffen, die Zunahme von mit Schadsoftware „versetzten" Webseiten und die meisten innerhalb von sechs Monaten gezählten Sicherheitsschwachstellen. Für Interessierte bietet der 112seitige Bericht zahlreiche wertvolle Detailanalysen aktueller Bedrohungen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Michael Knopp, Jörg Völker

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

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

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

secorvo
security consulting

Secorvo Security News

September 2010

Laufzeitverlängerung

In Deutschland wurde im vergangen Jahrhundert eine Technologie eingeführt, die man für so sicherheitskritisch hielt, dass ihre Rahmenbedingungen gesetzlich geregelt wurden und der Bund eine Aufsichtsbehörde etablierte, um die Unternehmen zu überwachen, die die kritischen Anlagen zur Nutzung dieser Technologie betreiben. Die Begeisterung der Bürger über diese Technologie hielt sich stark in Grenzen – nun aber wird aus Gründen der Wirtschaftlichkeit diskutiert, ob die Bundesregierung nicht deren Laufzeit verlängern sollte.

Nein, die Rede ist nicht von der Nutzung der Kernenergie – sondern von der „qualifizierten elektronischen Signatur" (QES).

In einem Gutachten zu den Auswirkungen des ELENA-Verfahrens auf Wirtschaft, Bürger und Verwaltung vom 13.09.2010 stellte der Nationale Normenkontrollrat kürzlich fest, dass der mit Abstand größte Kostenfaktor auf Verwaltungsseite die Erstattung für die QES an die Antragsteller ist, die damit ihr Einverständnis zum Abruf ihrer Daten geben müssen – und das, obwohl die Beträge sehr optimistisch geschätzt wurden. Zur Kostensenkung wird nun vorgeschlagen, die Gültigkeit des QES-Zertifikats von fünf auf zehn Jahre zu verdoppeln oder aber gleich einen QES-fähigen Dritten „stellvertretend" schriftlich (sic!) zur Abruf-Autorisierung zu ermächtigen.

Nun ist aus Sicherheitsgründen die Gültigkeit der QES-Zertifikate per Rechtsverordnung auf fünf Jahre begrenzt, und auch die Sicherheit der Kryptoalgorithmen wird derzeit nur für sieben Jahre prognostiziert. Daraus lässt sich nun zweierlei folgern: Entweder wurden die durch ELENA möglichen Einsparungen deutlich zu optimistisch dargestellt. Oder aber die Nutzung der QES wird seit mehr als einem Jahrzehnt mit übertriebenen Sicherheitsrestriktionen gegängelt – und so unnötig verteuert.

Zum Glück ist es nur die qualifizierte Signatur, über deren Nutzung so munter spekuliert wird. Und nicht die Atomkraft.

Inhalt

secorvo
security consulting

Security News

Auslaufmodell Passwort

Seit 2003 ist es dank der von P. Oechslin entwickelten Rainbow-Tables heute für Passwort-Cracker um ein Vielfaches leichter, ein einwegverschlüsseltes Passwort zu rekonstruieren. Besonders betroffen von solchen Angriffen sind die Passwort-Hashes des Windows (LM) und des NT LAN Managers (NTLM), die kein „Salz" beim Hashen verwenden.

Oechslins Unternehmen stellt eine Webseite zur Verfügung, über die sich in Sekundenschnelle praktisch alle bis zu 14-stelligen Windows-Passwörter aus dem LM-Hash rekonstruieren lassen. Und im Projekt RainbowCrack (siehe SSN 8/2010) wurden inzwischen die NTLM-Hashes für fast alle achtstelligen Passwörter aus Großbuchstaben, Kleinbuchstaben und Ziffern tabelliert – auch für alle kürzeren Passwörter mit Sonderzeichen, und für alle neunstelligen aus Kleinbuchstaben und Ziffern.

Wenn irgend möglich sollten Windows XP-Administratoren daher LM-Hashes deaktivieren – bei Windows Vista ist dies ohnehin die Grundeinstellung, und Windows-Passwörter unter neun Zeichen Länge sollten grundsätzlich tabu sein.

Zehnstellige und längere Passwörter, die inzwischen zu fordern sind, sind für Anwender eine Zumutung – es scheint nun endgültig an der Zeit, über Alternativen wie Smartcard Logon nachzudenken.

Smartes Energienetz

Am 22.09.2010 veröffentlichte das amerikanische Marktforschungsunternehmen PikeResearch eine Studie, die für das intelligente Stromnetz (vulgo „Smart Grid") ein Marktwachstum von 75% für die kommenden Jahre vorhersagt – auf einen mehrstelligen Milliardenbetrag in 2015. Kein Wunder, dass sich Unternehmen wie Cisco bereits in Stellung bringen und Miele auf der IFA die ersten Smart-Grid-fähigen Haushaltsgeräte vorgestellt hat. Dass sich aus der Verbindung von Stromnetz, Haushaltsgeräten und Internet neue Schwachstellen ergeben, ist leicht auszumalen: Verhaltensprofile beim Messstellenbetreiber und ferngesteuerte Waschmaschinen bieten viel Stoff für Phantasien.

Auf diese Gefahren reagierte das US-amerikanische NIST am 02.09.2010 mit der Publikation der 600 Seiten starken Richtlinie „Guidelines for Smart Grid Cyber Security". Teil 2 des dreibändigen Werks ist dem Thema Datenschutz gewidmet. An ausgewählten Beispielen wird darin deutlich, welche Begehrlichkeiten der Zugriff auf Stromverbrauchsdaten wecken dürfte: So lokalisierte eine amerikanische Regierungsbehörde anhand des Energieverbrauchs pro Wohnfläche eine Marihuanazucht.

Auch in Deutschland werden datenschutzrechtliche Einwände gegen die Datenerhebung der derzeit ausgerollten Smart Metern laut. Denn aus dem Gebot in § 21b Abs. 3a EnWG, Messeinrichtungen bereitzustellen, die „den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegeln", lässt sich kein Erfordernis zur zeitnahen Übermittlung der Messdaten an den Messstellenbetreiber ableiten – zur Abrechnung reicht die Übermittlung der zeitlich aggregierten Daten.

Auch zur Bereitstellung der in § 40 Abs. 3 EnWG geforderten „lastvariable[n] Tarife" ist eine alternative Gestaltung denkbar: die Daten können z. B. so übertragen werden, dass eine Zuordnung einzelner Datensätze zu einem konkreten Zähler nicht möglich ist – und somit auch keine Erstellung haushaltsbezogener Profile.

Die derzeitigen Implementierungen, bei denen die Verbrauchsdaten im 15-Minuten-Intervall an den Energieversorger übermittelt werden, ist zur Vertragserfüllung nicht erforderlich – und mit dem Prinzip der Datensparsamkeit unvereinbar. Eine datensparsame Realisierung käme hingegen ganz ohne Profile außerhalb des Haushaltes aus.

Traurige Nachricht

Am 23.09.2010 ist im Alter von 52 Jahren überraschend Andreas Pfitzmann verstorben. Mitte der 80er Jahre hatte er mit seinen Arbeiten an der Universität Karlsruhe den „technischen Datenschutz" begründet und war seitdem ein einflussreicher Mahner und Mittler zwischen den Welten des Rechts, der Informatik und gesellschaftlicher Fragestellungen. Andreas Pfitzmann hat nicht nur durch seine mehr als 250 Veröffentlichungen und Stellungnahmen wichtige Weichenstellung der Technikgestaltung beeinflusst, auch als Gutachter des Bundesverfassungsgerichts (Vorratsdatenspeicherung, Online-Durchsuchung) und vieler Bundesbehörden, sondern auch als Hochschullehrer hunderte Studenten für das Thema begeistert. Er wird uns fehlen.

Datenschutz-Informationsquelle

Am 17.09.2010 hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) offiziell ein neues Datenschutz-Wiki als Nachschlagewerk für Datenschutz-Laien und Fachleute eröffnet. Das zum Start verständlicherweise noch recht überschaubare Angebot ist nicht amtlich und offen für jeden Interessierten. Auch die im Internetauftritt des BfDI enthaltenen Materialien sollen übernommen werden, vielleicht auch Texte der Luchterhand-Loseblatt-Sammlung.

Hervorgegangen ist das neue Angebot aus dem Datenschutz-Forum, einem Diskussionsforum zu Datenschutzfragen. Es reiht sich ein in weitere Informationsangebote wie das virtuelle Datenschutzbüro des ULD, das Berichtsarchiv ZAfTDa der FH Gießen-Friedberg, das thematisch engere Wiki des AK-Vorratsdatenspeicherung, die Dokumentation von Datenschutzvorfällen des Projekts Datenschutz und das stärker Material orientierte DuD-Wiki.

Für eine faire Bewertung der Qualität ist es noch zu früh, und verschiedene Bereiche wie die Kategorienbildung, bereitgestellte Artikelvorlagen und die Hilfe bedürfen noch der Entwicklung. Grundsätzlich ist die Initiative jedenfalls zu begrüßen. Es ist zu hoffen, dass durch die Beteiligung vieler Experten eine Wissenssammlung entsteht, die auch Hilfestellung in Zweifelsfällen und Auslegungsfragen bietet.

Servergesteuertes NoScript

In sicherheitsbewussten Kreisen sind die Firefox-Erweiterungen NoScript und RequestPolicy, durch die sich Nutzer vor Cross-Site-Scripting (XSS) schützen können, inzwischen fester Bestandteil des Browsers. Die Freude daran wird jedoch dadurch getrübt, dass ein Nutzer ständig entscheiden muss, welche Webseite er für hinreichend vertrauenswürdig hält, um aktive Elemente zuzulassen.

Mit einem Konzept für serverbasierte Vorgaben, "Content Security Policy" (CSP) genannt, gibt Mozilla nun Anbietern die Möglichkeit festzulegen, welchen Dritt-Anbietern von Inhalten mit aktiven Komponenten vertraut werden soll. Damit wird ein Teil der Funktionalität von NoScript und RequestPolicy fest in der kommenden Version 4 des Firefox-Browsers verankert. Die Gefahr eines XSS-Angriffs wird damit signifikant beschränkt, sofern CSP auch von Web-Anbietern genutzt wird. Bis dahin wird es sicher noch etwas dauern – das Interview mit dem Chefentwickler Brandan Sterne mag die Wartezeit ein wenig verkürzen.

Schweigendes Orakel

Eine spezielle Klasse von kryptologischen Angriffen nutzt das angegriffene System als „Orakel", indem diese aus unterschiedlichen Reaktionen (sprich: differenzierten Fehlermeldungen) ableiten, bis zu welchem Punkt der Angriff erfolgreich verlaufen ist.

Nach SSL und WPA (vgl. SSN 11/2008) hat ein solcher Orakel-Angriff nun die Cookies und Sitzungsdaten von ASP.NET-Webservern getroffen, wie Microsoft am 17.09.2010 einräumte: Mit einer auf das Jahr 2002 zurückgehenden Technik können diese Daten ohne Kenntnis des Schlüssels Bit für Bit entschlüsselt werden, solange der Server jedes Mal zurückmeldet, ob bei seinem Entschlüsselungsversuch korrekte Padding-Bits entstanden oder nicht.

Der zunächst von Microsoft empfohlene Workaround entbehrte nicht einer gewissen Ironie: Man nutze die „customErrors" Funktionalität, um die Fehlermeldungen unspezifisch umzugestalten...

OWASP lebt

Am 09. und 10.09.2010 fand die diesjährige weltweite OWASP Konferenz „AppSec 2010" im kalifornischen Irvine statt. Die von etwa 300 internationalen Experten besuchte und mit herausragenden Referenten besetzte Veranstaltung zeichnete sich durch spannende Fachdiskussionen über den Status und die Entwicklung der Web-Sicherheit aus. Zu den Highlights zählte die Keynote von David Rice, der Parallelen zwischen der Regulierung im Umweltschutz und der Web-Sicherheit aufzeigte. Alle Vorträge sollen in Kürze online verfügbar sein.

Interessierte sollten sich den 20.10.2010 vormerkten – an diesem Tag findet in Nürnberg die OWASP AppSec Germany 2010 mit einem ähnlich spannenden Programm statt.

Secorvo News

Secorvo College aktuell

Experten unter sich: Die kommenden Seminare von Secorvo College bieten dank der sehr guten Nachfrage eine ganz besondere Gelegenheit für einen intensiven fachlichen Erfahrungsaustausch, sei es über das Thema PKI, Audit, ISM oder Datenschutz.

Wissensvermittlung durch Secorvo gepaart mit fruchtbaren Diskussionen und viel Praxiserfahrung – noch gibt es freie Plätze bei den Oktober- und Novemberveranstaltungen.

Teamverstärkung

Mit Klaus J. Müller hat das Secorvo-Team am 01.09.2010 erneut Zuwachs bekommen – und damit unsere gesammelte Erfahrung im Gebiet Informationssicherheit und Datenschutz um 10 auf exakt 200 Jahre angehoben. Neben „klassischen" Themen der IT-Sicherheit hat sich Klaus Müller intensiv mit Smart Metern beschäftigt, nachzulesen unter anderem in der Fachzeitschrift DuD („Gewinnung von Verhaltensprofilen am intelligenten Stromzähler", DuD 6/2010).

Veranstaltungshinweise

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

Oktober 2010	
04.-07.10.	ISSE 2010 (Teletrust, Berlin)
04.-07.10.	Sicherheitsmanagement heute (Secorvo College)
09.-15.10.	Hacker Halted 2010 (Hacker Halted USA, Miami/US)
19.-21.10.	it-sa (SecuMedia Verlag, Nürnberg)
21.10.	it-sa Datenschutztag 2010 (Computas, Nürnberg)
26.-28.10.	IT-Sicherheit heute (Secorvo College)
November 2010	
03.-04.11.	#days Workshops: Exploit Laboratory / Protecting from GSM attacks (DEFCON, Luzern/CH)
05.-06.11.	#days Conference (DEFCON, Luzern/CH)
09.-12.11.	PKI (Secorvo College)
15.-17.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
18.-19.11.	34. DAFTA (GDD e.V., Köln)
22.-26.11.	T.I.S.P.-Schulung (Secorvo College)
Dezember 2010	
06.-07.12.	IsSec/ZertiFA 2010 (Computas, Berlin)

Fundsache

Am 20.09.2010 veröffentlichte Chintan Shah in seinem Blog bei McAfee eine lesenswerte Analyse eines der derzeit leistungsfähigsten (und damit gefährlichsten) „Crimeware"-Werkzeuge: Zeus. Über Konfigurationseinträge lässt sich Zeus zu einem individualisierten Banking-Trojaner umgestalten – der inzwischen sogar Angriffsmuster gegen das mTAN-Verfahren beherrscht.

Impressum

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

ISSN 1613-4311

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

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

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

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

secorvo
security consulting

Secorvo Security News

Oktober 2010

Stuxnet - mythenfrei

Auch wenn dem sich über USB-Sticks und Netze verbreitenden Wurm „Stuxnet“ technische Raffinesse und den Autoren viel Know-how zugestanden werden muss, ist sein Erscheinen wenig erstaunlich. Sowohl USB-Würmer als auch Zero-Day-Exploits (noch nicht veröffentlichte Schwachstellen) gab es bereits. Neu ist, dass industrielle Regelungs- und Steuerungssysteme befallen wurden, hier Siemens PCS 7 und WinCC. Was lässt sich aber, ohne über Auftraggeber und Zielsetzung zu spekulieren, aus dem Vorfall lernen?

Fakt 1: Virenschutz hat Grenzen. Stuxnet verbreitete sich unerkannt über einen Zeitraum von einem Jahr. Verlässlichen Schutz vor neuartigen Viren und Trojanern können Scanner nicht bieten. Ein wirksamer Schutz kritischer Systeme benötigt umfassendere Konzepte.

Fakt 2: Datenträger sind Gefahrenquellen. Die verbreitete Nutzung von USB-Sticks über Systemgrenzen (privat/dienstlich, intern/extern, Office/Produktionssystem) hinweg ist leichtsinnig – und Bequemlichkeit keine Rechtfertigung. Hier sollte im Detail geregelt werden.

Fakt 3: Vertrauen ist gut, Kontrolle besser. Sie trauen Ihrem Dienstleister oder Lieferanten. Aber haben Sie sich auch davon überzeugt, dass er ebenso auf Sicherheit achtet wie Ihr Unternehmen?

Fakt 4: Netzsegmentierung und Firewalls helfen. Viel zu häufig werden kritische Systeme nicht von weniger kritischen entkoppelt und Verbindungswünsche von innen ins Internet großzügig zugelassen. Einmal eingedrungen, haben Trojaner so leichtes Spiel.

Fakt 5: Schutzbedarfsanalysen identifizieren das Wesentliche. Erst anhand einer Klassifikation kritischer und weniger kritischer Systeme ist es möglich, geeignete Maßnahmen zur Vorsorge auszuwählen – und bei einem Vorfall angemessen und zeitnah zu reagieren.

Unsere Empfehlung: Rechnen Sie mit weiteren derartigen „Neuheiten“ bei Schadsoftware. Beugen Sie möglichen Schäden wirksam vor – durch Schutzmaßnahmen und definierte Sicherheitsprozesse.

Inhalt

secorvo
security consulting

Security News

Autoritätsfrage

Im Jahr 1906 schlüpfte der Schuster Wilhelm Voigt in die Uniform eines preußischen Hauptmanns. Die verlieh ihm so viel Autorität, dass er ohne Rückfrage die Stadtkasse von Köpenick ausgehändigt bekam. Heutige Betrüger nutzen ausgefeilte Trojaner, um in den Browser ihrer Opfer zu schlüpfen und deren Online-Konten zu übernehmen. Gegen derartige „Man-in-the-Browser"-Angriffe bietet es sich an, zusätzlich zum möglicherweise infizierten PC ein weiteres, vertrauenswürdiges Gerät einzusetzen – so etwa bei der mobileTAN das eigene Handy.

Allein: Mit der Autorität der angezeigten Original-Webseite der Bank oder des Online-Anbieters kann der (Haupt-)Mann im Browser dem Anwender nahe legen, die Warnungen seines externen Geräts zu ignorieren – oder sogar es selbst zu manipulieren. Dass dies nicht bloße Theorie ist, wurde am 25.09. 2010 bekannt: Eine Variante des Trojaners ZeuS drängt ihren Opfern ein Update des Sicherheits-Zertifikats (sic!) für ihr Handy auf – und installiert tatsächlich einen Trojaner, der zusammen mit seinem „Partner" auf dem PC die mobileTAN aushebelt.

Hosentaschenforensik

Mit dem FTK-Imager ist seit dem 08.10.2010 die grundlegend überarbeitete Windows-Version 3.0 des bewährten und kostenfreien forensischen Werkzeugs verfügbar. Neu ist die Unterstützung für Images mit den Dateisystemen VxFS, exFAT und Ext4 sowie des forensischen Festplattenabbildformats AFF. Damit ist eine Einbindung der Formate AFF, DD, RAW, E01 und S01 als schreibgeschützte physische Laufwerke unter Windows möglich. Für FAT und NTFS kann bei Bedarf auch eine Schreibemulation genutzt werden, ohne dass die Integrität der Abbilddatei beeinträchtigt wird. Besonders die unkomplizierte Einbindung der Dateisysteme unter Ext3, Ext4 und HFS+ (iPhone) spart Zeit. Ein kleiner Wermutstropfen bleibt: verschlüsselte Abbildformate sind derzeit nicht nutzbar.

Firefox als Vorratsdatenspeicher

Eines der Argumente gegen insbesondere staatliche Vorratsdatenspeicherung ist, dass niemand sicher sein kann, dass nicht eines Tages die angehäuften Daten von weniger wohlmeinender Seite missbraucht werden. Wie einfach das geht, führt gerade der Trojaner Trojan-PWS-Nslog vor: Wie am 06.10. 2010 gemeldet schaltet er kurzerhand in der Firefox-Konfiguration das Speichern eingegebener Passwörter ein und die Rückfrage dazu ab, um sich später der kompletten Sammlung zu bemächtigen.

Cyber Security Month

Den Oktober 2010 erklärte das Internet Storm Center ISC am 01.10.2010 zum "Cyber Security Month". Täglich erschien seitdem ein Tagebucheintrag mit praktischen Hinweisen zur IT-Sicherheit. Die Einträge der ersten Woche wendeten sich an Familien, die der nächsten an Kinder, danach wurden im Bereich "Bosses" Führungskräfte angesprochen und im letzten Teil die Mitarbeiter von Unternehmen. Die Einträge (sowie die zahlreichen Kommentare) enthalten viele hilfreiche Empfehlungen.

De-Mail ... zum Zweiten

Das Bundeskabinett hat am 13.10.2010 den zweiten Gesetzentwurf für De-Mail-Dienste beschlossen – eingestuft als „besonders eilbedürftig", denn Umsetzungsziel ist das Jahr 2011. Das schon im April 2009 von der Großen Koalition initiierte Gesetzgebungsverfahren wurde Ende der Legislaturperiode mit einem Appell des Bundestages an die neue Regierung zur Weiterführung des Projekts abgebrochen.

In dem neuen Entwurf sind weitere Regelungen enthalten. So ist die Verpflichtung des Anbieters, die Verbindung des Nutzers zu seinem Konto zu verschlüsseln, jetzt ausdrücklich geregelt, dafür ist die Verpflichtung zur Bereitstellung pseudonymer Adressen für natürliche Personen entfallen. Neu ist auch die Abholbestätigung einer E-Mail durch den Dienstanbieter des Empfängers gegenüber öffentlichen Stellen und die Verpflichtung der Anbieter, eine automatische Weiterleitung zu ermöglichen.

Zu besserer Verständlichkeit haben die Überarbeitungen nicht geführt. Einige Regelungen, wie die automatische Weiterleitung oder das Streichen der Verpflichtung zum Pseudonymangebot, konterkarieren gar den ursprünglichen Gesetzeszweck.

Perlen sicherer Softwareentwicklung

Sicherheit genießt meist nicht höchste Priorität bei Softwareentwicklern. Dabei gibt es praktikable Vorgehensweisen, die – nach Absolvieren der Lernkurve – nachweislich zu signifikant sichererem Code führen, wie z. B. Design by Contract, ein Ansatz, für den mittlerweile Unterstützung für viele gängige Programmiersprachen existiert.

Ein anderer, vom NIST am 06.10.2010 als SP 800-142 veröffentlichter Ansatz beschäftigt sich mit dem Problem, wie man der Masse an Testfällen effektiv Herr werden kann. Bekanntlich explodiert die Zahl der Testfälle mit der Anzahl der zu testenden Parameter und der Zahl der Werte, die diese annehmen können. Die Autoren präsentieren

Untersuchungsergebnisse, nach denen Programmierfehler selbst in komplexen Systemen sehr oft durch die Interaktion von nur drei bis vier Parametern ausgelöst wird, aber praktisch nie von mehr als sechs. Es ist daher nicht nötig, alle Kombinationen von Parametern durchzuprobieren, um alle Fehler aufzuspüren.

Erfreulicherweise haben die Autoren auch gleich ein frei verfügbares Werkzeug geschrieben, welches einen (fast) minimalen Satz an Kombinationen von Parametern erzeugt, dessen Umfang ganz erheblich geringer ist, als die Zahl sämtlicher Kombinationen. Weder das Werkzeug noch die Vorgehensweise wird Sicherheits-Wunder bewirken, jedoch gibt es nun - bei angemessener Anwendung - ein gutes Argument mehr gegen Ausflüchte, Systeme nicht sicher zu entwerfen und zu implementieren.

HTTPS soll HTTPS bleiben

Die Veröffentlichung des Firefox-Add-On Firesheep am 24.10.2010 auf der Toorcon in San Diego hat einem altbekannten Problem, der unsicheren Übertragung von Cookies als Session-IDs, neue Aufmerksamkeit zu teil werden lassen.

Mit dem Add-On ist es möglich, Netzwerkverkehr mitzuschneiden und automatisiert unverschlüsselt übertragene Session-IDs zu sammeln. Die durch diese IDs authentifizierten Accounts werden direkt in Firesheep angezeigt; ein Anmelden unter fremdem Account ist durch Doppelklick möglich.

Da viele populäre Seiten, u. a. auch Facebook, nach der Anmeldung über eine mit SSL geschützte Seite wieder auf unverschlüsseltes HTTP zurückschalten, geben sie die im Cookie gespeicherte Session-ID jedem preis, der den Netzverkehr mitlesen kann.

So lange dieses Problem nicht von Anwendungsseite durch konsequente Verschlüsselung, beispielsweise durch die Verwendung von HSTS, aus der Welt geschafft ist, bleibt nur, sich mit Werkzeugen wie Force TLS oder NoScript zu behelfen.

Neue Jagdreviere

Die Entfernung von SIM-Locks bei Mobiltelefonen ruft die Strafverfolgungsbehörden inzwischen nicht mehr nur bei gewerblichem Handeln auf den Plan. Nach Auskunft der Polizeiinspektion Göttingen vom 12.10.2010 sind im Zusammenhang mit solchen Entsperrungen nun auch Ermittlungsverfahren gegen 600 Kunden eingeleitet worden.

Zwar ist die Verletzung von Markenrechten durch die gewerbliche Entsperrung schon vor sechs Jahren höchstrichterlich festgestellt worden; ob es sich für die Endanwender dabei um einen Straftatbestand handelt, ist jedoch bislang ungeklärt. Daher ist eine Anklageerhebung in diesen Verfahren eher unwahrscheinlich, zumal die Einschlägigkeit der meisten geprüften Straf-, Urheber- und Wettbewerbsrechtsvorschriften gegenüber privaten Endkunden zweifelhaft ist.

Sollte aus dieser Initiative jedoch eine generelle Strafverfolgung resultieren, könnte sich dies schnell auf weitere Bereiche auswirken, in denen die Funktionsfähigkeit von Software oder Hardware durch das Entfernen von Sperren erweitert werden kann. Dabei wird es für private Nutzer auch auf die Haltung der Hersteller und Rechteinhaber ankommen, denn die Verfolgung vieler der in Erwägung gezogenen Straftatbestände, wie etwa Computerbetrug, setzt einen Strafantrag des Geschädigten voraus.

Secorvo News

Unser Seminarangebot 2011

Zum Jahresende geben wir Ihnen mit der TISP-Schulung vom 22.-26.11.2010 noch einmal die Gelegenheit, Ihr Wissen im Bereich IT-Sicherheit zu zertifizieren. Auch 2011 bietet unser Seminarangebot (jetzt mit Teilnehmer-Rating) Rahmen, Referenten und Teilnehmer für einen intensiven Erfahrungsaustausch unter Experten. Wir freuen uns auf Sie!

Kronjuwelen-Hacking

SAP-Systeme sind das Rückgrat unserer hochautomatisierten Wirtschaft. In den meisten größeren Unternehmen steuern SAP-Anwendungen die kritischen Unternehmensprozesse: Fertigung, CRM, Lieferantenmanagement, Personalplanung, Finanzen, Controlling. Sie verarbeiten sensitivste Daten – die Kronjuwelen des Unternehmens. Auf der nächsten Veranstaltung der Karlsruher IT-Sicherheitsinitiative beleuchtet Dr. Markus Schumacher (Virtual Forge) in seinem Vortrag „SAP Anwendungen im Visier von Hackern“ am **11.11.2010** (18 Uhr im Schlosshotel Karlsruhe) typische Angriffsmöglichkeiten, erläutert deren Ursachen und gibt Handlungsempfehlungen zum Schutz (Anmeldung).

Secorvo hören und sehen

Auf dem kommenden 18. DFN-Workshop „Sicherheit in vernetzten Systemen“ vom 15.-16.02.2011 in Hamburg wird Secorvo gleich mit zwei Vorträgen zu aktuellen Themen der IT-Sicherheit zu hören sein: Klaus J. Müller wird zu „Datenschutz und Datensicherheit in Smart Grids“ vortragen, und Jörg Völker aktuelle Erkenntnisse zur „Sicherheit von iPhones“ vorstellen.

Veranstaltungshinweise

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

November 2010	
03.-04.11.	#days Workshops: Exploit Laboratory / Protecting from GSM attacks (DEFCON, Luzern/CH)
05.-06.11.	#days Conference (DEFCON, Luzern/CH)
09.-12.11.	PKI (Secorvo College)
15.-17.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
18.-19.11.	Datenschutzsaudit: Best Practice (Secorvo College)
18.-19.11.	34. DAFTA (GDD e.V., Köln)
22.-26.11.	T.I.S.P.-Schulung (Secorvo College)
23.-26.11.	ISDC 2010 Europe (DeepSec GmbH, Wien/AT)
Dezember 2010	
05.-09.12.	AsiaCrypt 2010 (IACR, Singapur/SGP)
06.-07.12.	IsSec/ZertiFA 2010 (Computas, Berlin)
27.-30.12.	27th Chaos Communication Congress (27C3) (Chaos Computer Club, Berlin)
Januar 2011	
18.-20.01.	Omnicard 2011 (inTIME, Berlin)

Fundsache

Eine technisch tiefer gehende Analyse des Stuxnet-Wurms bietet ein am 12.10.2010 erschienenes 50seitiges Dossier der Firma Symantec, verfasst von Nicolas Falliere, Liam O Murchu und Eric Chien. Unter anderem zeigt es die wahrscheinliche Verbreitung – die mindestens von Juni 2009 bis Juni 2010 unbemerkt blieb.

Impressum

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

ISSN 1613-4311

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

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

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

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

secorvo
security consulting

Secorvo Security News

November 2010

Hybris kommt vor dem Fall

Seit dem 01.11.2010 gibt es den neuen „elektronischen" Personalausweis, der mit seinem kontaktlosen (Krypto-) Chip nicht nur die Speicherung zweier Fingerabdrücke sondern auch die Nutzung als Online-Ausweis und Signaturkarte ermöglichen soll. Dazu werden ein Kartenlesegerät sowie eine „AusweisApp" benötigt, die unter dem sperrigen Arbeitstitel „Bürger-Client" im Auftrag des BMI durch ein von Siemens geführtes Konsortium entwickelt wurde (SSN 12/2009).

Bereits am 21.09.2010 hatte der Chaos Computer Club medienwirksam demonstriert, dass die PIN durch einen Trojaner ausgespäht werden kann, sofern ein Kartenleser ohne eigene PIN-Tastatur verwendet wird. Das war in der Sache wenig überraschend; beim Online-Banking ist dieser Trojaner-Angriff lange bekannt. Der PC ist schließlich immer das schwache Glied in der Kette. Überraschend war allerdings die Reaktion der Bundesregierung: In einem Interview der FAZ versicherte die IT-Beauftragte der Bundesregierung Cornelia Rogall-Grothe („Bundes-CIO") am 01.11.2010: „Es gibt keine Sicherheitslücke. Vor Schadsoftware am PC kann sich jeder wirksam schützen, indem er Virenschutzprogramme benutzt und eine Firewall installiert. (...) Es ist die sicherste Technik, die es gibt."

Acht Tage später stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die AusweisApp zum Download bereit. Und keine 24 Stunden später publizierte Jan Schejbal in seinem Blog ein fatales Sicherheitsleck: Die Update-Funktion der AusweisApp prüft nicht, ob das SSL-Zertifikat auch zu dem Server gehört, von dem das Update geladen wird, und entpackt es, ohne zuvor die Signatur zu prüfen. Seit dem 10.11.2010 findet man auf der AusweisApp-Seite nun einen Verweis auf eine Pressemitteilung des BSI, in der es heißt, dass in Kürze eine neue Version der AusweisApp verfügbar sein wird – nach „umfangreichen Tests".

Etwas spät für „die sicherste Technik, die es gibt".

Inhalt

Security News

Deep links am Ende?

Bereits am 29.04.2010 hat der Bundesgerichtshof ein wichtiges Urteil zur Frage der Verlinkung von Website-Inhalten unter Umgehung der Startseite (*deep link*) verkündet. Danach liegt ein Urheberrechtsverstoß vor, wenn Schutzmaßnahmen der verlinkten Seite den Willen erkennen lassen, keine Direktverlinkung gestatten zu wollen. Auf die Wirksamkeit der Maßnahmen kommt es dabei nicht an. Seit dem 10.11.2010 liegt nun die Urteilsbegründung vor. Mit der „Session-ID" genannten Entscheidung fällt der BGH hinter die sieben Jahre alte Paperboy-Entscheidung zurück, die *deep links* auf ungeschützte Inhalte für zulässig erklärt hatte.

In dem zu entscheidenden Sachverhalt bot die Klägerin im Internet Stadtpläne an. Einmalige Zugriffe über die Startseite waren kostenlos, die Nutzung durch Einbindung der Karte jedoch lizenzpflichtig. Zum Schutz wurden Session-IDs verwendet, die als Teil der weiterführenden URL beim Besuch der Startseite vergeben wurden. Die Beklagte überwand diese Maßnahme, indem sie via Skript eine Session-ID abholte und diese in die URL einband. Trotz der offensichtlichen Unwirksamkeit dieser Schutzmaßnahme sah der BGH hierin eine urheberrechtswidrige Umgehung.

Das Urteil wirft jedoch Fragen auf. Da nach der Begründung des BGH allein die Erkennbarkeit des Urheberwillens (unabhängig von der Wirksamkeit des Schutzmechanismus und der Umgehungsabsicht des „Verlinkers") für den Urheberrechtsverstoß wesentlich ist, bleibt offen, wie mit *deep links* rechtssicher umgegangen werden kann. Schließlich kann ein Urheber auch seinen Willen ändern und zunächst frei zugängliche Dokumente nur noch nach gebührenpflichtiger Anmeldung preisgeben – ist daher vom Verlinker zu fordern, dass er regelmäßig prüft, ob der Urheber seinen Willen geändert hat? Sollte er vor Einrichtung eines *deep link* zu Nachweiszwecken einen Snapshot der Startseite speichern, oder sich lieber gleich vertraglich mit dem Urheber einigen? Oder vielleicht sogar mit Blick auf mögliche Abmahn-Wellen ganz auf *deep links* verzichten? Letzteres wäre zweifellos nicht nur das Ende der Links in den SSN, sondern das Ende des Internet, wie wir es heute kennen.

Rundum sorgenreich

Am 15.11.2010 kündigte Facebook einen Unified-Messaging-Dienst für alle Benutzer an, der E-Mail, Chat und SMS vereinen soll. Keine ganz neue Idee – vor allem aber eine Kriegserklärung an die Freemailer Gmail, Yahoo, Hotmail, GMX und Web.de. Immerhin signalisierten über 28 Mio. Facebook-Nutzer, dass ihnen diese Ankündigung gefällt. Darunter dürften auch zahlreiche Deutsche User sein, deren Zahl sich im Jahresverlauf von etwa vier auf über acht Mio. täglich mehr als verdoppelt hat – jeder zehnte hierzulande verbringt im Schnitt 18 Minuten am Tag bei Facebook.

Dabei ist Vorsicht angeraten: Wie Google analysiert auch Facebook alle Nutzerdaten zur Erstellung von Profilen, um zielgruppenscharfe Werbung schalten zu können. Zudem kann bei einem Webmailer nicht ausgeschlossen werden, dass es der eine oder andere Administrator mit der Privatsphäre nicht so genau nimmt: Erst am 14.09.2010 hatte ein Blogger bekannt gemacht, dass ein (inzwischen ehemaliger) Google-Mitarbeiter offenbar mehrfach Gmail-Accounts von Teenagern mitgelesen und sich in deren Kommunikation eingeschaltet hatte.

Vor allem die Vielzahl der Dienste (Maps, News, Kalender, Textverarbeitung und Tabellenkalkulation, Fotoalbum, Kontaktnetzwerk und Messaging) versorgt den Anbieter mit einem präzisen Bild der Interessen, Neigungen, Vorlieben und sozialen Beziehungen seiner Nutzer, sowie inzwischen sogar deren Standort – besonders interessant, wenn die Dienste auf Smartphones genutzt werden. Die Informationen zu Facebooks neuem Messaging-Dienst, zum Datenschutz, zur Konfiguration der Privatsphäre und zur Sicherheit sollte man sich daher genau anschauen – vor der Anmeldung.

Geschütztes Smart Metering

Auf ihrer 80. Konferenz am 03./04.11.2010 forderten die Datenschutzbeauftragten des Bundes und der Länder Verbesserungen beim Datenschutz der Smart Meter (SSN 09/2010). So sollen bei der Messung des Stromverbrauchs anfallende Daten „unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit [...] Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren" – denn technisch ist eine Übermittlung der Zählerstände dafür nicht erforderlich.

Gängige Praxis ist hingegen eine Übermittlung des Zählerstandes in 15-min-Intervallen mit schriftlicher Einwilligung des Kunden. Diese setzt jedoch Freiwilligkeit und Widerruflichkeit voraus – er kann sich also weigern oder die Einwilligung später zurückziehen. Aus Sicht des Investitionsschutzes sind EVUs also gut beraten, auf datenschutzfreundliche statt einwilligungsbasierte Lösungen zu setzen. Zur Verbrauchsminimierung sind „Vor-Ort-Analysen" ohnehin kostengünstiger realisierbar.

Märchen von Übermorgen

Während sich die Praktiker freuen, dass mit der zunehmenden Verbreitung von Windows Vista/7 der Umstieg vom suspekt gewordenen SHA-1 auf den SHA-2 endlich in greifbare Nähe rückt, läuft bereits der Wettbewerb um den Ende 2012 zu kürenden SHA-3 (SSN 06/2009). Zwei der beteiligten Forscher gingen nun in Aufsätzen vom 04.10. und 12.11.2010 der Frage nach, wie sicher die SHA-3-Kandidaten vor Quanten-Computern sind, da sich dort mit dem Algorithmus von Grover der Brute-Force-Aufwand bei vielen Verschlüsselungs- und Einwegfunktionen von 2^n auf $2^{n/2}$ Operationen senken lässt.

Für Kryptologen ist das ein gewaltiger Unterschied – für die praktische Anwendung des künftigen SHA-3 allerdings etwa so relevant wie die Frage, ob ein neuer Sattel auch für das Reiten toter Pferde taugt: Falls es eines Tages Quanten-Computer gibt, sind dank Shors Algorithmus auch RSA und fast alle anderen Signaturverfahren sofort zu brechen.

Safe Harbor am Ende?

Der Düsseldorfer Kreis, die informelle Zusammenkunft der Datenschutzaufsichtsbehörden im nichtöffentlichen Bereich, hat sich am 28./29.04.2010 auf eine Prüfungspflicht für übermittelnde Stellen gegenüber Safe Harbor-Unternehmen in den USA geeinigt und dies am 23.08.2010 bestätigt. Da sich diese Unternehmen gegenüber der Federal Trade Commission (FTC) und europäischen Behörden lediglich selbst zertifizieren, findet eine Prüfung, ob die Safe Harbor-Grundsätze und ein angemessenes Datenschutzniveau eingehalten werden, nicht statt. Daher hat nach Auffassung des Düsseldorfer Kreises das übermittelnde Unternehmen die Pflicht, z.B. die Aktualität der Zertifizierung, die Erfüllung von Informationspflichten gegenüber Betroffenen und die ergriffenen Maßnahmen zur Einhaltung der Safe Harbor-Grundsätze selbst zu prüfen. Dies ist zu dokumentieren und auf Nachfrage den Aufsichtsbehörden nachzuweisen. Bestehen Zweifel an der Einhaltung der Grundsätze, wird die Verwendung der EU-Standardvertragsklauseln empfohlen.

Für deutsche Unternehmen gehen damit der Nutzen des Safe Harbor-Abkommens und die Rechtssicherheit bei der Übermittlung verloren. Die Forderung der Aufsichtsbehörden nach einer institutionellen Kontrolle der Selbstverpflichtungen ist berechtigt, sollte aber besser in eine Änderung des Abkommens statt in neue Prüfpflichten münden.

Happy Birthday Phrack!

Das Hacker-Magazin Phrack, nach Fyodor (Autor von Nmap) "the best, and by far the longest running hacker zine", feierte am 17.11.2010 seinen 25. Geburtstag. Pünktlich zum Termin erschien Heft Nr. 67 – knapp 1,5 Jahre nach Heft 66. Es enthält gewohnt unterhaltsames Material und technisch fundierte Artikel wie "Dynamic Program Analysis and Software Exploitation" oder eine detaillierte Schwachstellenanalyse im ProFTP-Server. Wir freuen uns auf die nächsten 25 Jahre – Thank you, Phrack Staff, and keep up the good work!

Bundesrat zum Datenschutz

Mit seinen umfassenden Änderungsvorschlägen zum Entwurf eines Gesetzes zum Beschäftigtendatenschutz hat der Bundesrat am 05.11.2010 eine erneute Überarbeitung des Gesetzesentwurfs eingefordert. So sollen Beschäftigtendaten enger definiert, auf europäischer Ebene Regelungen zum Konzerndatenschutz angestrebt, durch Verzicht auf ein Übermaß an Verweisen die Lesbarkeit verbessert, eine Löschfrist für die Daten abgelehnter Bewerber eingeführt und ein allgemeines Beschäftigten-Screening nur bei Vorliegen tatsächlicher Anhaltspunkte für das Vorliegen von Straftaten gestattet werden. Eine Änderung der Definition von Dritten soll die Auftragsdatenverarbeitung in EG-Drittstaaten ermöglichen. Die von Datenschützern und den Bundesratsausschüssen geforderte grundsätzliche Einschränkung der dauerhaften Videoüberwachung und der Möglichkeiten zur Abweichung in Tarifverträgen oder Betriebsvereinbarungen zu Ungunsten der Beschäftigten fanden zwar keine Mehrheit. Dennoch wird deutlich, dass der Gesetzentwurf noch einen weiten Weg vor sich hat.

Secorvo News

100 mal Security News

Sie lesen gerade die 100. Ausgabe der Secorvo Security News: 400 Seiten mit fast 1.000 Nachrichten, für Sie selektiert, recherchiert und formuliert, liegen damit hinter uns. Über 6.500 Abonnenten haben die News bis heute gewonnen – mehr als die meisten deutschsprachigen Fachzeitschriften im Gebiet Informationssicherheit und Datenschutz.

Wir würden uns freuen, wenn Sie das Jubiläum zum Anlass nähmen und uns in einem kurzen Kommentar verraten, was Sie uns schon immer einmal sagen wollten. Unter allen Einsendern verlosen wir am 31.01.2011 einen Teilnahme-Gutschein für ein Secorvo-College-Seminar nach Wahl.

Smart Grid Symposium

Am 01.-02.02.2011 sind wir mit einem Symposium zu Datenschutz- und Datensicherheit rund um das „Intelligente Stromnetz“ wieder in der Buhlschen Mühle zu Gast. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

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

Dezember 2010	
05.-09.12.	AsiaCrypt 2010 (IACR, Singapur/SGP)
06.-07.12.	IsSec/ZertiFA 2010 (Computas, Berlin)
27.-30.12.	27th Chaos Communication Congress (27C3) (Chaos Computer Club, Berlin)
Januar 2011	
18.-20.01.	Omnicard 2011 (inTIME, Berlin)
Februar 2011	
01.-02.02.	Smart Grid Symposium (Secorvo, Ettlingen/KA)
02.-03.02.	21. SIT-SmartCard Workshop (SIT, Darmstadt)
08.-10.02.	CPSSE-Schulung (Secorvo College)
15.-16.02.	18. DFN-Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
März 2011	
01.-05.03.	CeBIT (Deutsche Messe, Hannover)
22.-24.03.	Sicherheitsmanagement heute (Secorvo College)
28.03.-01.04.	T.I.S.P.-Schulung (Secorvo College)

Fundsache

Am 05.02.2010 hat die EU-Kommission eine überarbeitete Fassung der Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (gemäß der EU-Datenschutzrichtlinie) verabschiedet (Amtsblatt der EU L 39/5 vom 12.02.2010), die seit dem 15.05.2010 in Neuverträgen sowie bei Vertragsänderungen zu berücksichtigen sind.

Impressum

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

ISSN 1613-4311

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

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

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

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

secorvo
security consulting

Secorvo Security News

Dezember 2010

Lehren aus Wikigate

Was ist WikiLeaks? Ein Ventil der Entrechteten? Eine Klagemauer der Gutmenschen? Das Fünkchen Hoffnung im universellen Wahnsinn? Oder ein Racheportal für Wichtigtuer? WikiLeaks mag als der Beweisversuch durchgehen, dass sich im Zeitalter des Internet nur wenig auf Dauer vertuschen lässt. Der Zorn des „Establishments" jedenfalls lässt sich kaum mit der Veröffentlichung der Botschaftsdepeschen erklären, sondern eher durch Publikationen wie der Videoaufnahme aus einem US-Hubschrauber am 05.04.2010, die das Niedermähen von 12 offensichtlich unbewaffneten Zivilisten, darunter zwei Mitarbeiter der Nachrichtenagentur Reuter, am 12.07.2007 in Bagdad zeigt. Unstreitig ist, dass Publikationen dieser Art einseitige Darstellungen korrigieren, dabei aber selbst Gefahr laufen, eine einseitige Sicht hervorzubringen – schließlich kommen diejenigen (Staaten) am besten davon, die besonders gut vertuschen. Dennoch sind solche Internet-Enthüllungen das demokratische Prinzip der „öffentlichen Kontrolle" in Reinkultur: Müssen Unternehmen und Behörden damit rechnen, dass Fehlverhalten publik wird, werden sie sich konsequenter um die Einhaltung ethischer Standards und rechtlicher Rahmenbedingungen kümmern.

Das eigentliche Wikigate hinter der öffentlichen Aufregung betrifft jedoch einen anderen Punkt: Offenbar hatten mehr als eine Million Personen regulär Zugriff auf die 250.000 Depeschen – sie waren damit schon vorher semi-öffentlich. Sehr viele WikiLeaks-Dokumente wurden von Zugriffsberechtigten enthüllt – die keine Entdeckung fürchten mussten, weil es so viele davon gab. Das ist der wahre Skandal: Wer das „need-to-know"-Prinzip derart großzügig auslegt, sollte sich besser vor (Wirtschafts-) Spionage ängstigen, als nach Whistleblowern zu fahnden. Denn, wie der Politikwissenschaftler Herfried Münkler so treffend in einem Spiegel Essay formulierte: „In der sozialen Welt ist Vertrauen an die Möglichkeit des Geheimnisses gebunden." Bevor das Vertrauen weg (und die Kontrolle total) ist, sollten wir wohl lieber erstmal die Zugriffsrechte begrenzen...

Inhalt

secorvo
security consulting

Security News

RossLeaks

Während sich die Welt mit der Sichtung und Sortierung von 250.000 überwiegend irrelevanten Diplomaten-Äußerungen beschäftigt, sucht sich die Wahrheit andere Kanäle. So publizierte Ross Anderson am 24.12.2010 sein Antwortschreiben an die UK Cards Association, die versucht hatte, unliebsame Veröffentlichungen über Schwachstellen des EMV-Verfahrens von der Webseite der Universität Cambridge entfernen zu lassen.

Mit akademischer Eloquenz klärt er in seinem Schreiben zunächst einmal über das Verständnis der Freiheit der Wissenschaft an der „Universität von Erasmus, Newton und Darwin" auf – und schließt mit dem Hinweis, dass das Vertrauen in Kreditkarten wohl weniger durch die Veröffentlichung, als vielmehr durch die Vertuschung bekannter Schwachstellen unterminiert werde. Eine erquickliche Lektüre zum Jahreswechsel.

Nach dem Ende des Internet

Nicht nur wegen inhaltlicher Regulierungsbestrebungen wie dem Jugendmedienschutz-Staatsvertrag, sondern auch aus technischen Gründen naht das Ende des Internet: Am 30.11.2010 vergab das Internet-Koordinationsgremium IANA vier der letzten elf /8-Blöcke mit je gut 16 Mio. IPv4-Adressen zur Unterverteilung an regionale Adressverwaltungen. Hochrechnungen zufolge werden die restlichen Blöcke bis März 2011 vergeben sein. Dann ist das Internet „voll".

Es wird also Zeit, den Umstieg auf IP Version 6 vorzubereiten, deren 128-Bit-Adressraum das Internet für die absehbare Zukunft am Leben erhalten dürfte. Eine am 01.12.2010 veröffentlichte Studie von RIPE NCC zeigt jedoch, dass die Übertragung von IPv6 über IPv4-Netze schon rein funktional noch mit erheblichen Kinderkrankheiten zu kämpfen hat. Das lässt Schlimmes für die Sicherheitseigenschaften von IPv6 befürchten. Am 27.12.2010 stellte der Autor des IPv6-Sicherheitstest-Toolkits thc-ipv6 beim CCC-Kongress 27C3 neue Erkenntnisse zu Sicherheitsproblemen von IPv6 vor – trotz der Neuerungen in den Bereichen Multicasts und Source Routing keine guten Nachrichten.

Nicht in Wittenberg

Auf ihrer Webseite hat die Gesellschaft für Informatik (GI) am 01.12.2010 ihre Zehn Thesen zu Sicherheit und Datenschutz im Cloud Computing angeschlagen. Darin werden die Hauptrisiken bei der Nutzung von Cloud Computing kompakt auf den Punkt gebracht. In knapper Form werden viele Baustellen angerissen, die vor einem Einsatz von Cloud Computing sorgfältig bearbeitet werden sollten. Denn die Ausrichtung der IT auf die Cloud erfordert auch in Sicherheitsfragen ein radikales Umdenken. Ergänzt werden die zehn Thesen der GI durch eine umfangreiche Literaturliste zum Thema Sicherheit und Datenschutz beim Cloud Computing.

Umfangreicher werden die relevanten Fragestellungen im 34seitigen Leitfaden für sicheres Cloud Computing des Verbands der deutschen Internetwirtschaft (eco) behandelt, der fast zeitgleich am 02.12.2010 veröffentlicht wurde. Dieser Leitfaden ist auf Anfrage erhältlich. Lediglich der Bitkom schwächelt: Der bereits am 18.09.2009 veröffentlichte, 84seitige Leitfaden Cloud Computing behandelt Datenschutzaspekte auf drei und Sicherheitsfragen auf einer halben Seite – kein rühmliches Bild.

SSLiversum – (Un)bekannte Welten

Nicht erst seit dem Erscheinen von Tools wie Firesheep (SSN 10/2010) ist es empfehlenswert, für den Zugriff auf Internet-Dienste soweit möglich HTTPS zu verwenden. Aber wie vertrauenswürdig sind „blaue" und „grüne" TLS-Zertifikate (SSN 06/2007) in den Weiten des Internet wirklich?

Dieser Frage widmet sich das SSL-Observatorium der EFF. Dessen Mitarbeiter stellten am 30.07.2010 auf der Defcon 18 einen Überblick ihrer Beobachtungen vor, den sie am 28.12.2010 beim CCC-Kongress 27C3 aktualisieren werden. Neben dem einer Protonen-Kollision nicht unähnlichen Graphen der ca. 650 (!) CAs, denen gängige Browser vertrauen, findet man im „SSLiversum" einige Perlen für PKI-Spötter, so etwa CAs in Manchester und New Jersey, die sich ein Schlüsselpaar teilen, Tausende von offiziellen Zertifikaten für „localhost" oder das Generalschlüssel-Zertifikat für vier Dutzend verschiedene Hosts.

Another one bites the dust

Alle Welt redet bei passender Gelegenheit gern und viel über Sicherheit. Den Worten folgen allerdings oft keine Taten; wenn doch, dann oft solche, auf die man besser verzichtet hätte. Das lässt sich regelmäßig nicht nur beim Gesetzgeber beobachten, sondern auch in der Industrie.

Was die Sache erstaunlich macht, ist, dass dies auch für die Großen gilt – die es eigentlich besser können oder wissen müssten. Unlängst war Canon an der Reihe: Bekanntermaßen lassen sich Digitalbilder heute mittels moderner Bildbearbeitungswerkzeuge so manipulieren, dass gute Collagen kaum noch als solche zu erkennen sind. Canon hatte daher die – an sich gute – Idee, Bilder so zu

authentifizieren, dass ein Fotograf die Echtheit einer Aufnahme nachweisen kann. Die Authentifizierung übernimmt ein (teures) Security-Kit (OSK-E3), das man an die Kamera anschließen kann. Die Funktionsweise des Kits hält Canon geheim – zur Erhöhung der Sicherheit.

Es kam, wie es kommen musste (Mifair lässt grüßen, SSN 3/2008): Das Verfahren wurde analysiert – und am 28.11.2010 von Dmitry Sklyarov öffentlich gebrochen. Die Details sind peinlich: Der Authentifizierungsmechanismus ist keine Signatur, sondern ein „keyed hash", der HMAC-Key ist für alle Kameras eines Modells identisch und in der Kamera gespeichert, und der Hashwert verwendet kein „Salz" – da hält sich das Mitleid in Grenzen. Wie formulierte Bruce Schneier einmal so schön: Geheime Verfahren sind meist solche, deren sich die Hersteller eigentlich schämen müssten... Dmitry Sklyarow meinte launig, Canon sollte vielleicht Leute einstellen, die etwas von Sicherheit verstehen. Kein schlechter Vorschlag – auch für zahlreiche andere Unternehmen (und gelegentlich den Gesetzgeber).

Aufschub für die Bilanzübermittlung

Mit dem Steuerbürokratieabbaugesetz wurde am 20.12.2008 in Gestalt des § 5b EStG eine Verpflichtung buchführender Unternehmen zur elektronischen Übermittlung ihrer Bilanzen und Gewinn- und Verlustrechnungen eingeführt, die bereits für das kommende Wirtschaftsjahr gegolten hätte. Mit Schreiben vom 16.12.2010 hat das Bundesfinanzministerium nun die Pflicht zur elektronischen Bilanz- sowie Gewinn- und Verlustrechnungsübermittlung um ein Jahr auf die ab dem 01.01.2012 beginnenden Wirtschaftsjahre verschoben.

Zunächst sollen ausgewählte Unternehmen freiwillig an einer Pilotphase zum Test des Verfahrens und des amtlich vorgeschriebenen Datensatzes (Taxonomie) teilnehmen.

Die Übermittlung sollte ursprünglich durch einen den Unternehmen zur Verfügung gestellten Client erfolgen, an den diese ihre Schnittstellen anzupassen hätten. Da weder der auf eXtensible Business Reporting Language beruhende Datensatz noch die Client-Spezifikationen bisher abgeschlossen vorliegen und die Entwürfe umfassender Kritik begegneten, wurde nun die Reißleine gezogen. Auch für den um ein Jahr verschobenen Start ist zu befürchten, dass er in großer Eile erfolgen muss; darunter dürfte auch die Sicherheit des Verfahrens leiden.

Vielleicht aber ist von dem Verfahren bis dahin ähnlich wenig übrig, wie heute von der 2002 eingeführten „Elektronischen Steuererklärung mit digitaler Signatur" – im Wesentlichen der Name „Elster".

Hintertüren überall

Gleich drei schwer wiegende Bugs und Hintertüren wurden Mitte Dezember aufgedeckt: Am 14.12. 2010 wurde öffentlich, dass eine Netzwerkspeicherlösung von Hewlett Packard ein nicht dokumentiertes Benutzerkonto mit vollen Zugriffsrechten und Standardpasswort („!admin") besitzt. Am 13.12. 2010 wurde bekannt, dass in der freien SmartCard-Bibliothek OpenSC über einen Pufferüberlauf im Treiber durch bestimmte Seriennummern Code auf dem Zielsystem ausgeführt werden kann.

Schließlich beschuldigte der Gründer des OpenBSD-Projektes, Theo de Raadt, am 14.12.2010 in einer E-Mail ehemalige OpenBSD-Entwickler, im Auftrag des FBI Hintertüren in die VPN-Komponente eingebaut zu haben – vor etwa 10 Jahren. Man könnte sich nun fragen, ob eine Hintertür in einem Open-Source-Projekt tatsächlich so lange unentdeckt bleiben kann – genau das aber hat das Debian-OpenSSL-Debakel (SSN 5/2008) schon vor über zwei Jahren gezeigt. Vor Hintertüren kann man nie sicher sein – weder bei kommerziellen Produkten noch bei freien Projekten.

Secorvo News

T.I.S.P. wird Standard

Seit der Entwicklung des T.I.S.P.-Zertifikats (TeleTrusT Information Security Professional) wurden über 400 Security-Experten mit diesem Qualifikationsnachweis ausgezeichnet. Immer häufiger wird der T.I.S.P. in Unternehmen zum Qualifikationsstandard für alle Mitarbeiter, die mit Aufgaben der Informationssicherheit betraut sind. Mehr als 50 T.I.S.P.-Absolventen, die sich Anfang November in Köln zum diesjährigen T.I.S.P. Community Meeting trafen, bestätigten diesen Trend. Auch 2011 bietet Secorvo College wieder mehrere Gelegenheiten zur Schulung und unabhängigen T.I.S.P.-Zertifizierung.

Smart Grid Symposium

Am 01.-02.02.2011 sind wir mit einem spannenden Symposium zu Datenschutz- und Datensicherheit rund um das „Intelligente Stromnetz" wieder in der Buhlschen Mühle zu Gast. Werfen Sie einen Blick in das Programm – wir freuen uns auf Ihre Teilnahme!

Last Call for Feedback

Noch bis zum 31.01.2011 nehmen Sie anlässlich der 100. Ausgabe der Secorvo Security News mit Ihrem Kommentar zu unseren News automatisch an der Verlosung einer Teilnahme an einem Secorvo College-Seminar Ihrer Wahl teil. Wir freuen uns auf Ihr Feedback – und drücken die Daumen!

Veranstaltungshinweise

Januar 2011	
18.-20.01.	Omnicard 2011 (inTIME, Berlin)
Februar 2011	
01.-02.02.	Smart Grid Symposium (Secorvo, Ettlingen/KA)
02.-03.02.	21. SIT-SmartCard Workshop (SIT, Darmstadt)
08.-10.02.	CPSSE-Schulung (Secorvo College)
15.-16.02.	18. DFN-Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
März 2011	
01.-05.03.	CeBIT (Deutsche Messe, Hannover)
22.-24.03.	Sicherheitsmanagement heute (Secorvo College)
28.03.-01.04.	T.I.S.P.-Schulung (Secorvo College)
April 2011	
04.-06.04.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
07.-08.04.	Datenschutzaudit: Best Practice (Secorvo College)

Fundsache

Erstmals haben sich die Datenschutz-Aufsichtsbehörden mit einem Beschluss des Düsseldorfer Kreises (vom 24./25.11.2010) auf Mindestanforderungen an den Datenschutzbeauftragten festgelegt. Darin werden schon bei Bestellung „umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung" des relevanten Datenschutzrechts erwartet, dazu „Kenntnisse der Informations- und Kommunikationstechnologie und der Datensicherheit". Bei externen DSB wird eine Mindestvertragslaufzeit von vier Jahren, bei Erstverträgen von 1-2 Jahren empfohlen.

Impressum

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

ISSN 1613-4311

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

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

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

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