secorvo
security consulting

Secorvo Security News

Juni 2012

Süßes Gift

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

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

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

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

Inhalt

secorvo
security consulting

Security News

PKI ist schwierig

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

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

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

Passwörter sind schwierig

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

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

Signatur-Harakiri

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

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

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

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

Safer Browsing

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

Große Fische

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

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

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

IPv6 World Launch Day

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

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

Secorvo News

4. Tag der IT-Sicherheit

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

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

Zertifiziertes Wissen

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

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

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

Erfolgreiche KA-IT-Si

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

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

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

Veranstaltungshinweise

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

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

Fundsache

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

Impressum

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

ISSN 1613-4311

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

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

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

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