secorvo
security consulting

Secorvo Security News

Juni 2009

Riskante Mythen

Mythen erfreuen sich unausrottbarer Beliebtheit. Wie gerne glauben wir an einfache Erklärungen – besonders, wenn sie ein wohlfeiles Argument für vage Überzeugungen liefern, an unterschwellige Wünsche appellieren oder lieb gewonnene Vorurteile bestätigen.

1890 bestimmte der Physiologe Gustav von Bunge den Eisengehalt von 100 Gramm Spinat mit 35 Milligramm – von getrocknetem allerdings, dessen Eisengehalt zehnmal größer ist als der frischen Spinats. Das im Spinat enthaltene Eisen kann die menschliche Verdauung nicht einmal verwerten; dennoch glauben wir an dessen entwicklungsfördernde Kraft. Unzählige weitere Mythen bestimmen unsere Weltsicht: dass Lesen bei schlechtem Licht die Augen verdirbt oder wir nur einen Bruchteil der Kapazität unseres Gehirns nutzen. Alles Unsinn. Im Wochenmagazin DIE ZEIT geht Christoph Drösser seit 1997 in der Kolumne „Stimmt's?" verbreiteten Alltagsüberzeugungen auf den Grund und konnte viele als überlieferten Irrglauben entlarven.

Offenbar hat auch das Fachgebiet IT-Sicherheit ein Alter erreicht, in dem sich Glaubenssätze einnisten, die ohne weitere Prüfung übernommen und weitergegeben werden. Selbst die IT-Grundschutz-Kataloge sind davor nicht gefeit, wie sich am Beispiel der Passwort-Empfehlungen (M 2.11) zeigen lässt. Dort wird eine Sperrung des Zugangs nach drei Fehleingaben empfohlen – eine Maßnahme, die keinerlei Sicherheitsgewinn bewirkt, jedoch kostspielige Kennwortrücksetzungen nach Urlauben und erzwungenen Passwortwechseln. Schlimmer noch: Sie ermöglicht simple Denial-of-Service-Angriffe – durch absichtliche Fehleingaben bei fremden Accounts. Ähnlich die Forderung nach Passworten mit mindestens einem nicht-alphabetischen Zeichen: Da die meisten Benutzer Ziffer oder Sonderzeichen anhängen, verkleinert sich dadurch der Suchraum. Viel wirksamer wäre eine um ein Zeichen erhöhte Mindestlänge.

Auch diese Mythen werden, so ist zu befürchten, weiterleben: „Es ist schwieriger, eine vorgefasste Meinung zu zertrümmern, als ein Atom", wusste schon Albert Einstein.

Inhalt

secorvo
security consulting

Security News

Windows 7 Security

Windows 7 soll im Oktober 2009 auf den Markt kommen und gegenüber Windows Vista verbesserte und neue Sicherheitsfunktionen enthalten. Eine Einführung in diese Funktionen bietet Chris Corio in einem Technet-Artikel vom 24.04.2009.

Neben der verbesserten Integration biometrischer Authentifzierungsverfahren und Verfeinerungen bei Bitlocker zur Festplattenverschlüsselung ist vor allem die neue Funktion „Applocker" viel versprechend. Durch eine zentrale Steuerung der Anwendungen, die durch einen Benutzer ausgeführt werden können, kann die Sicherheit maßgeblich gesteigert werden. Im Vergleich zu den bereits in XP und Vista vorhandenen „Software Restriction Policies" wurden das Management verbessert und weitere Funktionen etabliert, die es beispielsweise ermöglichen, die Auswirkungen von Policies vorab zu testen und den Umgang mit aktualisierten Programmversionen und Updates erheblich zu vereinfachen.

Sofern im Unternehmen Prozesse zur Freigabe von Software für die Benutzer etabliert sind, können diese durch diese neuen Funktionen technisch durchgesetzt werden – ein Gewinn vor allem für Unternehmen, die bisher über keine Kontrollmöglichkeit des Softwareeinsatzes verfügen.

SHA-1 auf Kollisionskurs

Die Krypto-Hashfunktion SHA-1 steht bekanntlich schon seit längerem unter Beschuss, und der Nach-Nachfolger SHA-3 macht sich bereit, in die Startblöcke zu steigen (siehe SSN 10/2008). In der Rump-Session der Eurocrypt 2009 kündigten drei australische Forscher am 28.04.2009 in Köln den bisher besten Angriff auf SHA-1 an, den sie am 02.06.2009 veröffentlichten. Er soll den Aufwand zum Finden einer Kollision auf 2^{52} Operationen reduzieren. Auch wenn bezweifelt wird, dass alle Annahmen der Autoren haltbar sind, und der Aufwand realistisch auf 2^{57} Operationen geschätzt wird, sinkt die Sicherheit des SHA-1 damit auf die des überholten DES (2^{56}).

Allerdings spielen Kollisionsattacken in der Praxis erst dann eine Rolle, wenn der Angreifer die beiden zur Kollision führenden Texte bzw. Dateien selbst konstruieren kann. Die Kunst besteht dann darin, ein „Zwillingspärchen" aus einem unverfänglichen Datum (z. B. einem Webserver-Zertifikat oder einem einfachen „Hello World"-Programm, SSN 01/2009), das man legal signieren lässt, und einem bösartigen Alter Ego (z. B. einem Zertifizierungsstellen-Zertifikat oder einem Programm mit Schadcode) zu wählen, das denselben Hashwert und damit dieselbe Signatur besitzt. Eine Signaturprüfung wird sowohl Jekyll als auch Hyde als gültig (und vertrauenswürdig) akzeptieren.

Eine solche Kollisionskonstruktion gelingt mit dem vorgestellten Angriff nur, wenn es gelingt, zu einer mehr oder weniger sinnlosen Zeichenfolge eine legale Signatur zu erschleichen. Und auch der Einsatz von SHA-1 zum Integritätsschutz per HMAC ist glücklicherweise nicht betroffen.

Opera Unite(d)

Am 16.06.2009 wurde die Opera-Browser-Nachfolger Unite (V10b1) verfügbar gemacht; eine portable Version soll folgen. Als Update ist er vollständig im Benutzerkontext installier- und nutzbar. Neu in Opera Unite sind „Social Network"-Server-Komponenten („Services"), durch die innerhalb von Minuten nach Beantragung eines (auch pseudonymen) Accounts bei Opera auf dem lokalen Clientsystem u. a. Filesharing und ein Webserver gestartet werden. Der Webserver ist direkt von Extern über einen Fully Qualified Domain Name (FQDN) erreichbar, sobald der Einstiegspunkt in die Dateiverzeichnisstruktur gesetzt wurde. Unter Windows sind auch Server-Shares in Gestalt zugewiesener Laufwerksbuchstaben möglich. Mit einer einfachen Google-Suche werden die Shares sichtbar.

Das verwendete Proxykonzept tunnelt dazu bestehende Firewallstrukturen, sofern ein Zugriff auf den Unite Proxy bei Opera auf Port 16680/tcp zugelassen ist. Ist der Unite Proxy nicht erreichbar und die UPnP-Option in Opera Unite aktiviert, wird ein Multicast auf Netz 239/8 nach RFC 3171 durchgeführt. Immerhin: Port Punching-Techniken à la Skype werden bisher nicht unterstützt – allerdings befindet sich die Software auch erst im Beta-Stadium.

Opera's Zielsetzung, mit diesem Konzept Daten in Social Networks wieder unter die Kontrolle der Besitzer zu stellen, in Ehren – ein Blick in Kapitel 7 der EULA („Use of Service") zeigt jedoch, dass es wohl eher auf eine Wahl zwischen Teufel und Beelzebub hinausläuft.

Security-Check für Anwendungen

Am 03.06.2009 wurde die erste Version des Application Security Verification Standard (ASVS) des Open Web Application Security Projekts (OWASP) veröffentlicht. Der Standard enthält eine Vorgehensweise zur einheitlichen Durchführung von Sicherheitstests von (Web-) Anwendungen und will damit vergleichbare Aussagen über das Sicherheitsniveau erreichen. Eine Überprüfung kann dabei auf einem von vier Ebenen erfolgen: Automatisierte Prüfung (L1), manuelle Prüfung (L2), Design-Prüfung (L3) oder interne Prüfung (L4).

Zu begrüßen ist, dass der Schwerpunkt des Standards auf der Überprüfung des Vorhandenseins effektiver Sicherheitsmechanismen liegt. Auf 42 Seiten werden neben der generellen Vorgehensweise der vier Überprüfungs-Level auch detaillierte Prüfvorgaben für jedes Level vorgegeben. Diese unterfallen in 14 Themengebiete, darunter Security Architecture, Authentication, Session Management und Access Control, und neben weiteren auch Input Validation, Cryptography und HTTP Security. Schließlich legt der ASVS Anforderungen an die zu erstellenden Sicherheitsberichte fest.

Damit steht Entwicklern, Betreibern und Nutzern eine unabhängige Grundlage zur Überprüfung der Sicherheit von (Web-) Anwendungen zur Verfügung. Der Standard wird sich im Zusammenspiel mit weiteren OWASP-Projekten durchsetzen, die sich in der Praxis bewährt haben (wie z. B. dem Testing Guide oder Development Guide). Aber Vorsicht: Auch hier darf der Blick auf das Zertifikat nicht die Beschäftigung mit dem Testbericht ersetzen.

Regenbogenbrecher

Eine Passwort-Mindestlänge von acht Zeichen gilt selbst bei alphanumerischen Passwörtern noch immer als solide Empfehlung, auch in den IT-Grundschutz-Maßnahmenkatalogen des BSI.

Dabei werden die Entwicklung der Rechenleistung aktueller PCs, die Nutzung von Grafikkarten durch moderne Cracking-Tools sowie die Auswirkungen der von Philippe Oechslin (EPFL) bereits auf der Crypto 2003 publizierten Optimierungen für Rainbow Tables offenbar erheblich unterschätzt.

Ein schneller PC berechnet heute 800 Mio. NTLM-Hashwerte pro Sekunde – und hat in knapp 80 Stunden alle möglichen achtstelligen alphanumerischen Passwörter durchprobiert. Mit einer schnellen Grafikkarte (2 Mrd. Hashes/sec.) genügen 30 Stunden – und unter Verwendung von Oechslins Rainbow-Tables vom 12.02.2009 (74 Mrd. Hashes/sec.) sogar 50 Minuten. Wenn sie einem Cracking-Angriff auf die SAM-Datei zumindest einige Tage widerstehen sollen, müssen alphanumerische Passwörter heute eine Mindestlänge von 10 Zeichen aufweisen.

Phishing still alive

Am 12.05.2009 belegte die Anti-Phishing Working Group (APWG) mit Veröffentlichung ihres „Global Phishing Survey", dass Phishing noch lange nicht tot ist. Der 26 Seiten starke Bericht über die Trends im zweiten Halbjahr 2008 dokumentiert knapp 57.000 Phishing-Attacken unter Benutzung von 30.500 Domain-Namen – aus 170 Top Level Domains (TLDs). 81 % der Angriffe wurden von kompromittierten Webservern ausgeführt. Phishing ist weiterhin ein attraktiver Markt – und die Phisher passen sich aktuellen Verteidigungstrends an.

Erfreulich: Die APWG bietet eine Hilfestellung für den Fall, dass eine Webseite einem Hacking-Angriff durch Phisher zum Opfer gefallen ist. Und auch für den Endverbraucher werden gute Ratschläge erteilt – wenn auch nur in Englisch.

Folgt man einem Positionspapier von Microsoft Research vom 01.09.2008, ist Phishing ein „Profitless Endeavour": Danach weisen die hohen Aktivitätszahlen darauf hin, dass – größtenteils erfolglose – Kriminelle verzweifelt versuchen, sich doch noch ein Stück vom vermeintlich großen Kuchen der aus Online-Konten zu phishenden Beträge abzuschneiden. Allerdings geht das Papier nur von „einfachen" Phishing-Mails aus, die Anwender dazu auffordern, ihre Passwörter auf einer betrügerischen Webseite einzugeben. Das mag in den USA ausreichen, um ein Online-Konto zu plündern – in Deutschland gehört die iTAN mittlerweile zum Mindeststandard.

Allerdings ist auch die iTAN für Täter dank Trojanern und Man-in-the-Middle Attacken nicht unüberwindlich, wie ein Beitrag des BKA auf dem BSI Sicherheitskongress am 18.05.2009 belegt. Ob die Microsoft-Autoren bedacht haben, dass vermeintlich leergefegte Phishgründe wieder ergiebig werden, wenn man statt einer Angelrute einen Trawler mit Echolot benutzt?

Secorvo News

Sicherheitsregion Karlsruhe

Das Hightech.Unternehmer.Netzwerk CyberForum, die IHK Karlsruhe und die KA-IT-Si laden zum ersten Karlsruher „Tag der IT-Sicherheit" am **16.07.2009** ein. Im Saal Baden der IHK werden ausgewiesene Experten aus der „Sicherheitsregion Karlsruhe" ab 14 Uhr mit spannenden Vorträgen („Die sieben Todsünden der IT-Sicherheit") und preisgekrönten Beispielen aus der Praxis, u. a. von der Edelstahl Rosswag GmbH und der Fiducia IT AG, Einblicke in ihre Erfahrungen und Anregungen zur Diskussion geben. Beim anschließenden Buffet-Networking ab 18 Uhr bietet sich die Gelegenheit, Fragen zu Haftung, Datenschutz und IT-Sicherheit mit Referenten und Gästen zu vertiefen.

Nähere Informationen und Anmeldung unter www.ka-it-si.de. Teilnahmegebühr: 75 Euro.

Veranstaltungshinweise

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

Juli 2009	
06.-07.07.	SANS WhatWorks Summit in Forensics and Incident Response (SANS, Washington/US)
16.07.	Tag der IT-Sicherheit (IHK Karlsruhe/CyberForum e.V./KA-IT-Si, Karlsruhe)
August 2009	
12.-14.08.	USENIX Security '09 (Usenix, Montreal/CA)
16.-20.08.	Crypto 2009 (IACR, Santa Barbara/US)
17.-18.08.	Digital Forensic Research Workshop (DFRWS, Montreal/CA)
31.08.-04.09.	TRUSTBUS 09: 6th International Conference on Trust, Privacy & Security in Digital Business (University of the Aegean, Linz/AT)
September 2009	
07.-11.09.	TISP-Schulung (Secorvo College)
21.-23.09.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
24.09.	Pacta sunt servanda (KA-IT-Si, Karlsruhe)
29.09.-02.10.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)

Fundsache

Dass die Entwicklung einer modernen Passwort-Policy komplexer ist, als es auf den ersten Blick scheinen mag, belegt der am 21.04.2009 als Draft erschienene „Guide to Enterprise Password Management“ des NIST (Special Publication 800-118).

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, 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