Secorvo Security News

Dezember 2004

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 12, 3. Jhrg. 2004
Stand 22. Dezember 2004

ISSN 1613-4311

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

Inhalt

Editorial: Bekenntnis

Ohne Sicherheit ist keine Freiheit.
Wilhelm von Humboldt (1767-1835)

Seit mehr als zwei Jahren ziert dieses Zitat unsere Webseite. Warum? Eine berechtigte Frage, ist doch der Zusammenhang nicht ganz offensichtlich.

Sicherheit als Vorbedingung von Freiheit? Das klingt befremdlich, schränken Sicherheitsmaßnahmen doch meist unseren persönlichen Freiraum ein, wie Gepäckkontrollen am Flughafen, videoüberwachte öffentliche Räume oder Ausweiskontrollen an der Grenze. Über die Verhältnismäßigkeit solcher Maßnahmen muss selbstverständlich politisch gestritten werden – unbestritten ist allerdings, dass erst ein durch die „innere Sicherheit“ geschütztes friedliches Zusammenleben eine freie Entfaltung ermöglicht.

Eine ähnliche Entwicklung lässt sich im Internet beobachten. So lange das Netz nur ausgewählten Nutzergruppen zugänglich war, funktionierte diese neuartige offene Kommunikation durch Selbstregulierung – sogar ein wenig über das Geburtsjahr des WWW hinaus. Mit der wachsenden Verbreitung und der Entdeckung immer neuer Nutzungsmöglichkeiten war es jedoch vorbei mit der friedlichen Kommunikation. Viren, Würmer, Trojaner, Angriffsprogramme und Spam konterkarierten den Nutzwert des neuen Mediums. Inzwischen ist die Nutzung des Internet ohne wirksame Sicherheitsmechanismen praktisch nicht mehr möglich. Nur wer Viren scannt, Angriffe an der Firewall abfängt und Spam filtert, kann die kommunikativen Freiheiten eines Daten- und Dokumentenaustauschs frei von Verzögerung, Qualitätsverlust und Medienbruch genießen.

Ohne Sicherheit ist keine Freiheit. Ob man für diese Erkenntnis den Hauptvertreter des deutschen Humanismus bemühen sollte, sei dahingestellt. Tatsächlich geht es vielleicht gar nicht passender. Im Zweifel sollten Sie es mit Johannes Rau halten: „Trau keinem Zitat, dass Du nicht selbst aus dem Zusammenhang gerissen hast.“

1 Security News

1.1 Immer wieder MD5

Am 06.12.2004 geriet der Hash-Algorithmus MD5 wieder einmal in die Schlagzeilen, als der Wissenschaftler Dan Kaminsky ein Papier („MD5 To Be Considered Harmful Some Day“) veröffentlichte, in dem er praktische Angriffe auf den Algorithmus dokumentiert – durch die Konstruktion geeigneter „Kollisionen“ sei es möglich, zu verschiedenen Bitfolgen (u.a. auch Binärcode) denselben MD5-Hash zu generieren. Ein von ihm gleichzeitig veröffentlichtes Tool untermauert seine Behauptungen.

Dieser Report hat die schon vor Jahren geführten Diskussionen um MD5 wieder belebt: Prinzipielle Schwachstellen sind seit Anfang der 90er Jahre bekannt, das RSA Labs Bulletin vom 12.11.1996 riet bereits von der weiteren Verwendung ab, und die erste Algorithmenempfehlung des BSI zum Signaturgesetz von 1998 enthielt MD5 gar nicht erst. Viele der veröffentlichten Angriffe hatten aber lange eher akademischen Wert. Auch Kaminiskys Veröffentlichung musste sich diesen Vorwurf gefallen lassen – Fakt bleibt jedoch, dass MD5 schon längst nicht mehr eingesetzt werden sollte.

1.2 WLAN-Schnorrer erwischt

Wie die Zeitung Die Welt am 11.11.2004 berichtete, wurde in Bielefeld ein „WLAN-Schnorrer“ verhaftet. Der Mann fiel der Polizei dadurch auf, dass er in seinem geparkten Auto offensichtlich im Internet surfte. Tatsächlich bediente er sich eines ungesicherten WLAN-Access-Points. Der Laptop wurde beschlagnahmt, zusätzlich erfolgte eine Anzeige wegen Verdachts auf Ausspähen von Daten. Sollte es sich um ein ungeschütztes WLAN gehandelt haben, dürfte die Strafbarkeit fraglich sein – nach § 202a StGB liegt der Tatbestand des Ausspähens nur vor, wenn die Daten „gegen unberechtigten Zugang besonders gesichert sind“.

1.3 Neues ISIS-MTT-Profil

Am 01.12.2004 verabschiedete das ISIS-MTT Board Version 1.0 des Profils für Zertifikate zu Authentifikationszwecken. Dieses u.a. mit Unterstützung von Microsoft und Sun entstandene Profil fasst die Anforderungen zusammen, die in verschiedenen Systemumgebungen – von SSL-gesicherten Web-Anwendungen bis zur Anmeldung an Linux-Rechner – an ISIS-MTT konforme Zertifikate zur Authentifikation gestellt werden.

1.4 NSA-Guide zu MacOS X

Bereits am 15.10.2004 aktualisierte das Systems and Network Attack Center (sic!) der National Security Agency (NSA) seinen Security Configuration Guide für Apples Betriebssystem MacOS X. Neben Suns Solaris 8 ist MacOS derzeit das einzige Nicht-Windows-Betriebssystem, für das die NSA einen entsprechenden Security Guide veröffentlicht. Für die Anwender von Apple-Systemen sicher ein hilfreiches Dokument – denn auch Systeme, die nicht wie Windows im „Bull’s Eye“ der Hacker stehen, erfordern die gleiche Sorgfalt bei Konfiguration und Betrieb.

1.5 PGP Global Directory

Bereits seit vielen Jahren existiert ein mehr oder weniger gut funktionierendes globales Netz von öffentlichen Keyservern zum Austausch von PGP-Schlüsseln. Die Server synchronisieren sich dabei in der Regel untereinander, um ihre Datenbestände abzugleichen. Auch die Firma PGP, Inc. betreibt einen solchen Verzeichnisdienst, hat sich aber in der Vergangenheit nur unregelmäßig an der Synchronisation mit den anderen Keyservern beteiligt.

Jetzt geht PGP mit dem „PGP Global Directory“ einen Schritt weiter: Jeder PGP-Key, der über ein Web-Interface an den Server übermittelt wird, muss vom Schlüsselinhaber authentisiert werden. Hierfür wird dem Inhaber automatisch eine E-Mail geschickt, die er beantworten muss, bevor

sein Key in die Datenbank aufgenommen wird; dies wird alle sechs Monate wiederholt. Die E-Mail-Adresse wird dabei aus dem PGP-Key extrahiert, bei dem es sich jedoch nicht um einen älteren („v3“) Schlüssel handeln darf.

Grundsätzlich handelt es sich hierbei um einen sinnvollen Mechanismus, da er verhindert, dass (wie auf anderen Keyservern leider der Fall) unzählige Schlüssel hochgeladen werden, hinter denen kein „echter“ Benutzer steckt. Andererseits hat es bereits Beschwerden von PGP-Nutzern gegeben, deren Keys von Dritten an den Server übermittelt wurden – jene erhielten anschließend E-Mails des Keyservers, die sie als Spam einstuften...

1.6 Trojanisierte Fahrräder

Unter dem Stichwort Hack a Bike haben findige Hacker die Miet-Fahrräder des Call a Bike-Angebots der Deutschen Bahn manipuliert. Dazu wurde die Firmware der elektronischen Fahrradschlösser bei etwa 200 Rädern in Berlin durch eine eigene Version mit Hintertür-Entsperrcode ersetzt.

Einzelheiten des Hacks sind in einer am 17.12.2004 anonym auf den CCC-Webseiten veröffentlichten Technologieanalyse dargestellt. Die Hacker bescheinigen darin dem System – außer, dass die Sperren gegen ein Auslesen der Firmware nicht aktiviert waren – ein „sehr gutes technisches Design“. Der Aufwand zum Brechen des Systems war offenbar deutlich höher als die Kosten Dutzender Fahrräder. Dass ihn die Hacker dennoch in Kauf nahmen, dürfte daran liegen, dass der Call-a-Bike-Chef den Code in einem Artikel als „nicht zu knacken“ bezeichnet hatte.

1.7 Schwachstelle PHP

Das am 17.04.2004 von Stefan Esser initiierte Hardened-PHP Projekt hat es sich zur Aufgabe gemacht, den Nutzern der besonders für CGI-Skripte beliebten Skriptsprache PHP mehr Sicherheit zu geben. Ein Hauptaugenmerk des Projekts liegt auf dem Schutz des Skript-Programmierers vor eigenen Fehlern und Unsauberkeiten. Aber auch Schwachstellen in PHP selbst treten bei der Arbeit an Hardened-PHP zu Tage. So zählt Esser in einem Advisory vom 15.12.2004 insgesamt sieben PHP-Schwachstellen auf; sie wurden in den am selben Tag veröffentlichten aktuellen PHP-Versionen beseitigt.

1.8 RFID-Studie online

Seit dem 20.12.2004 ist die BSI-Studie zu Risiken und Chancen des Einsatzes von RFID-Systemen (RIKCHA) vollständig online abrufbar. Die Studie fasst die Grundlagen der RFID-Technologie zusammen, betrachtet grundlegende Angriffsmöglichkeiten und Abwehrmaßnahmen und bietet Ausblicke auf Anwendungsfelder und künftige Entwicklungen.

1.9 Phisher auf der Lauer

Zu den neuen Tricks beim „Phishing“ nach Passwörtern gehört das am 08.12.2004 in einem Advisory der dänischen Firma Secunia veröffentlichte „Phishing mit Fenstern“, auf das praktisch alle aktuellen Browser herein fallen, solange Javascript aktiviert ist – d.h. faktisch leider bei fast allen Besuchern von Internet-Seiten.

Dabei lauert auf einer unbemerkt zum Phishing missbrauchten Seite ein Skript darauf, dass der Nutzer einen Link aktiviert, der ein neues Fenster zur Eingabe vertraulicher Daten öffnet. Ist der Name dieses Fensters dem Angreifer bekannt, kann das Skript den Inhalt des neuen Fensters dieses Namens augenblicklich mit einem gefälschten Formular überschreiben. Mittlerweile wird diese Methode auch beim bekannten c’t-Browsercheck demonstriert.

Vor dieser Phishing-Variante können die Anbieter von Homebanking- und E-Commerce-Seiten ihre Nutzer allerdings aktiv schützen, indem der Server bei jedem Aufruf einen neuen, nicht vorhersagbaren Fensternamen verwendet. Dann kann der Phisher lauern, bis er schwarz wird...

2 Secorvo News

2.1 Secorvo College aktuell

Für 2005 wurde das Weiterbildungsangebot von Secorvo College um mehrere Seminare erweitert. So haben wir das erfolgreiche Live Hacking Lab (26.-28.04. 2005) zu einem dreitägigen Seminar ausgebaut. Hinzu kommen zwei neue, thematisch ergänzende Seminare, die aktuelle Themen der Bedrohungsentwicklung aufgreifen: die Angriffe auf Web-Anwendungen und das Thema Computer Forensik (Web Application Security, 02.-04.05.2005 und Spurensuche im Web, 23.-25.05. 2005). Zwei weitere neue Seminare stellen die Systemsicherheit in den Mittelpunkt: IT-Sicherheit für Windows-Administratoren (07.-08.06.2005) und IT-Sicherheit für Unix-Administratoren (09.-10.06.2005).

2.2 Näher am Zug

Anfang Januar wird Secorvo neben dem Karlsruher Stadtgarten ein neues Domizil beziehen – in Fußweite vom Hauptbahnhof. Ab dem 10.01.2005 erreichen Sie uns daher unter der folgenden neuen Anschrift, Telefon- und Faxnummer:

Ettlinger Straße 12-14
D-76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

2.3 Verstärkung

Mitte November ist das Secorvo-Team erneut gewachsen. Jochen Schlichting verstärkt mit seinen Schwerpunkten Sicherheitspolicies, -architekturen, -analysen, Forensik und Systemsicherheit unser Consulting-Team. Er bringt mehr als zehn Jahre Berufserfahrung in der IT-Security Beratung mit. Natalie Mareth hat sich mit eSecurity-Lösungen und digitalen Signaturen beschäftigt. Ihre Kernaufgabe ist die Entwicklung eines neuen Service-Angebots – über das in einer der nächsten Security News mehr verraten wird.

3 Veranstaltungshinweise

Januar 2005	
25.-26.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
27.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2005	
14.-18.02.	RSA-Konferenz (San Francisco)
15.-17.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
21.-25.02.	Information Security Management (Secorvo College, Karlsruhe)
März 2005	
01.-02.03.	Computer Forensik Symposium 2005 (KA-IT-Si, Karlsruhe)
02.03.	Datenschutz kompakt (Secorvo College, Karlsruhe)
02.-03.03.	DFN-CERT Workshop (Hamburg)
15.-16.03.	D-A-CH Security (Darmstadt)
31.-01.04.	Black Hat Briefings (Amsterdam)
April 2005	
05.-07.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
05.-08.04.	Sicherheit 2005 (GI, Dortmund)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

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