Secorvo Security News
Juli 2004

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

Nr. 7, 3. Jhrg. 2004
Stand 20. Juli 2004

ISSN 1613-4311

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

Inhalt

Editorial: Abschied von der Sicherheit

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts.

Gene Spafford,
Scientific American, 3/1989

Immer wieder gerne hervorgekramt und oft gebetsmühlenartig wiederholt – die vermeintliche Weisheit, dass 100%ige Sicherheit nicht erreichbar ist. Aber was sagt uns das? Häufig muss diese Einsicht als Rechtfertigung für Resignation herhalten: Wenn es ohnehin nicht sicher geht, warum dann überhaupt Aufwand betreiben?

Dabei ist die Erkenntnis irreführend. Tatsächlich gibt es 100%ige Sicherheit nicht. Viel schlimmer: Sicherheit gibt es nicht. Sofern man sie als einen Zustand versteht, der sich nicht partiell erreichen lässt – „ein bisschen schwanger“ geht eben auch nicht.

Zielführender, als die Sicherheit zu messen, ist daher die Bewertung des Schutzniveaus. Damit werden differenzierte Aussagen möglich – die Frage „Haben wir das Notwendige getan?“ lässt sich im Gegensatz zu „Sind wir sicher?“ mit Blick auf die realistischen Bedrohungen einerseits und die getroffenen Schutzmaßnahmen andererseits detailliert beantworten.

Allein auf diesem Weg ist eine sachgemäße Reaktion auf perfide neue Angriffsmuster, wie PWSteal.Refest oder Frame-Phishing möglich: Nur wer mit seinem System nicht im Administrator-Modus surft, einen Browser ohne Sicherheitslöcher und mit reduzierten „Features“ nutzt, sich mit einer Personal Firewall sichert, einen aktuellen Virenscanner verwendet, Security-Patches einspielt und die Sicherheitsmechanismen des Betriebssystems konfiguriert, hat seine Hausaufgaben gemacht.

Danach darf man wieder auf die Hersteller schimpfen – oder über die Unsicherheit der (IT-) Welt im Allgemeinen klagen. Wenn man dann noch Grund dazu hat.

1 Security News

1.1 Phishing mit Frames

Wie in den SSN 06/2004 berichtet, nehmen die Fälle von Phishing erheblich zu. Die verwendeten Techniken werden immer perfider: Mit einem neuen Trick gelingt es, die Eingabedaten eines Browser-Fensters, z. B. einer Online-Banking-Anwendung, an den Server eines anderen Fensters zu senden. Zwar sollten Cross-Domain-Sicherheitsmechanismen den Zugriff auf Frames anderer Domänen verhindern – das funktioniert jedoch bei den verbreitetsten Browsern (Internet Explorer, Netscape, Mozilla) nicht. Eine Demonstration dieser gravierende Schwachstelle ist seit dem 02.07.2004 online beim heise-Verlag zu finden. Opera war der erste Browser, bei dem dieses Sicherheitsloch am 19.07.2004 kurzfristig gestopft wurde; inzwischen gibt es Updates für alle gängigen Browser.

1.2 802.11i WLAN Security

Am 24.06.2004 wurde der lange erwartete Standard IEEE 802.11i verabschiedet, der verbesserte und erweiterte Sicherheitsmechanismen für Wireless LANs festlegt. Im Rahmen des Get IEEE 802 Programms wird der neue Standard übrigens ab Ende 2004 frei im Internet verfügbar sein.

Anfang des Jahres 2001 waren im Vorgänger-Standard Wireless Equivalent Privacy (WEP) schwer wiegende Sicherheitslücken gefunden worden. Daher nahmen einige Hersteller, die des Wartens auf den WEP-Nachfolger überdrüssig waren, schon Anfang 2003 unter der Bezeichnung WPA (WiFi Protected Access) einen Teil der jetzt verabschiedeten Neuerungen vorweg: die Authentifikation von WLAN-Clients durch RADIUS-Server nach 802.1x und eine TKIP/RC4-Verschlüsselung, die die bekannten Schwachstellen von WEP ausbügelt. Die wesentlichen Erweiterungen von IEEE 802.11i – inoffiziell auch „WPA2“ genannt – gegenüber WPA sind

- die Verwendung von CCMP/AES alternativ zu TKIP/RC4 als Standard-Verschlüsselungsverfahren,
- die Unterstützung sicherer „Ad-hoc“-WLANS und
- Methoden für die sichere Übergabe eines Clients zwischen Access-Points sowie für eine sichere Abmeldung.[1]

Aufgrund der Verwendung von AES erfordert der Wechsel zu 802.11i in der Regel einen Hardware-Upgrade von Access-Points und WLAN-Karten – oder einen schnellen Rechner, der der Netzwerkkarte die Ver- und Entschlüsselung abnimmt. Wer seine WLAN-Hardware erst in diesem Jahr gekauft hat, kann Glück haben und kommt möglicherweise mit einem Firmware-Upgrade aus – dank der langen Vorlaufzeit des Standards konnten Hersteller ihre Chips seit Ende 2003 anpassen.

Leer gehen die Besitzer älterer Geräte des 11-Mbit/s-Standards 802.11b aus. Ihnen wird meist nichts anderes übrig bleiben, als ihr WLAN durch ein darüber gestülptes VPN abzusichern. Wer auf den 54-Mbit/s-Standard 802.11g wechseln will, sollte darauf achten, dass die gewählte Lösung zumindest WPA unterstützt und die Hardware für 802.11i vorbereitet ist.

1.3 Online-Banking-Trojaner

Wie unter anderem am 02.07.2004 vom BSI und schon am 29.06.2004 von SANS berichtet wird, existiert ein neuer besonders heimtückischer Trojaner namens PWSteal.Refest. Er nistet sich als Browser Helper Object in den Internet Explorer ein und schneidet gezielt Daten mit, die verschlüsselt an die Domänen citibank.de, deutsche-bank.de und weitere Online-Banking-Server übertragen werden. Dabei werden die Daten vor der Verschlüsselung im Klartext abgegriffen und an einen Rechner im Internet versendet. Bester Schutz: ein anderer Browser, z. B. Mozilla.

---

1 Bei WPA kann ein Angreifer alle angemeldeten Clients ungehindert abmelden.

1.4 Digitale Spurensuche

Eine noch recht junge Disziplin der Informationssicherheit ist die digitale oder IT-Forensik. Ziel einer forensischen Analyse ist es, Systemeinbrüche nicht nur generell zu erkennen, sondern die digitalen Spuren des bzw. der Angreifer im Detail zu analysieren, um Rückschlüsse auf Vorgehensweise, Schäden sowie ggf. die Identität des Angreifers ziehen zu können.

IT-Forensiker werden mittlerweile durch eine Vielzahl mächtiger, oft kostenlos verfügbarer Tools unterstützt. Zwei dieser Tools, die auch von Secorvo bei forensischen Analysen eingesetzt werden, sind am 02.06.2004 in neuen Versionen erschienen: Das „Sleuth Kit“ sowie das zugehörige grafische Frontend „Autopsy“. Bei beiden Programmen handelt es sich um seit mehreren Jahren etablierte frei verfügbare UNIX-Tools, die sich vor allem auch hervorragend zur Analyse von Windows-PCs eignen.

Da eine erfolgreiche forensische Analyse neben geeigneten Tools auch eine entsprechende Expertise voraussetzt, findet man in jüngster Zeit immer mehr unterstützende Literatur zu dem Thema: zwei aktuelle White Paper (vom 26.06.2004 und vom 16.05.2004) dokumentieren auf anschauliche Weise die forensische Analyse eines Windows-PCs.

1.5 Spurenverwischung

Es mehren sich die Gründe für Hacker und Virenautoren, nervös zu werden: Anfang Juli 2004 gingen mehrere Meldungen über Fahndungserfolge und Haftstrafen aus Australien und Spanien durch die Presse.

Kurz darauf wurde am 04.07.2004 mit Bagle.ad der erste Computerwurm entdeckt, der seinen eigenen Quellcode mit verschickt. Böse Zungen vermuten, dass dies nicht als Nachhilfe für Möchtegern-Virenautoren gedacht war, sondern zum „Spurenverwischen“: Der Quellcode genügt damit nicht mehr als Beweis, dass ein Virenautor dingfest gemacht wurde.

1.6 Grundschutztool 3.1

Die überarbeitete Version 3.1 des BSI Grundschutztools ist am 05.07.2004 erschienen. Eine Demoversion kann von der Webseite des BSI geladen werden. Die Einzel-Lizenz kostet 765 €, ein Update 68,10 €. Neben einigen Änderungen der Datenbankroutinen wurden unter anderem die wichtigen neuen Bausteine Apache Webserver, Microsoft Exchange/Outlook und Internet Information Server ergänzt. Grundsätzlich ist es nun, wie Version 3.0 mit Servicepack 2, komplett zweisprachig (deutsch, englisch).

1.7 MD5-Passwort-Cracker

Am 03.07.2004 wurde über Slashdot der Dienst passcracking.com publik gemacht, der aus MD5-Hashes die zugehörigen Passwörter zurückrechnen kann – solange sie aus maximal acht Kleinbuchstaben oder Ziffern bestehen. Zu diesem Zweck hat das System die Hash-Werte aller 36^8 möglichen Passwörter vorberechnet. Diese Daten würden normalerweise gut 61 Terabyte Festplattenplatz füllen. Mit einem auf der Crypto 2003 veröffentlichten, optimierten Time/ Memory-Tradeoff kann der benötigte Speicherplatz jedoch zu Lasten einer deutlich höheren Rechenleistung beim Wiederfinden der richtigen Lösung auf eine vertretbare Größe beschränkt werden.

Ein auf demselben Prinzip beruhender „Advanced Instant NT Password Cracker“ wurde nach 200.000 Anfragen innerhalb von nur einer Woche wieder vom Netz genommen, ist aber seit dem 14.07.2004 wieder verfügbar.

Diese Entwicklung sollte auch die letzten Zweifler bewegen, hinreichend sichere Passwörter zu wählen. Zugleich wird deutlich, wie wichtig es ist, Kryptoalgorithmen nicht ad-hoc zu implementieren, sondern sie in etablierte, von Experten untersuchte Verfahrensweisen einzubetten: Unix-typisch „gesalzene“ Passwörter kann das Programm nämlich nicht knacken.

2 Secorvo News

2.1 IT Security Professional

Der von Secorvo College seit Anfang Mai angebotene Ausbildungsgang zum IT Security Professional erfreut sich wachsender Beliebtheit: Inzwischen haben zwei Teilnehmer den Ausbildungsgang absolviert; für den ab 2005 eine Abschlussprüfung mit Zertifikat (Certified IT Security Professional – CISP) angeboten wird.

Noch eine aktuelle Terminänderung: Das eintägige Seminar PKI für Fortgeschrittene wird im Anschluss an das PKI-Seminar am **30.09.2004** stattfinden.

2.2 White Paper: „Poststelle“

Das Modell der „virtuellen Poststelle“, das das Konzept eines Ende-zu-Ende-Schutzes für E-Mail durch die Idee einer zentralen Ver- und Entschlüsselungsinstanz ersetzt, findet immer mehr Anhänger – und wird inzwischen auch von mehreren Herstellern unterstützt. Die Vor- und Nachteile dieses Ansatzes und die größten Stolperfallen diskutieren Holger Mack und Dr. Markus Michels im neuen Secorvo White Paper „Praktischer Einsatz von E-Mail-Gateways“.

3 Veranstaltungshinweise

Juli 2004	
24.-29.07.	Black Hat Briefings (Black Hat, Las Vegas)
August 2004	
09.-13.08.	USENIX Security Symposium (USENIX, San Diego)
11.-13.08.	Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004 (Cambridge/Boston)
15.-19.08.	Crypto 2004 (IACR, Santa Barbara)
September 2004	
15.-17.09.	7th International Symposium on Recent Advances in Intrusion Detection – RAID (Sophia Antipolis)
20.-21.09.	Elektronische Geschäftsprozesse – EGP 2004 (Klagenfurt)
21.-22.09.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)
28.-29.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
30.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)

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