Secorvo Security News
Januar 2003

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 1, 2. Jhrg. 2003
Stand 15. Januar 2003

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

Inhalt

Editorial: Besinnung auf ‚Basics‘

Der Technik-Hype ist nun auch in der IT-Sicherheit vorbei. Die Prävention durch innovative technische Lösungen hat in den vergangenen Jahren in vielen Unternehmen organisatorische Maßnahmen hintan stehen und bestehende Sicherheitskonzepte veralten lassen: Zu selten wurden Sicherheitskonzepte systematisch nachgeführt, Dokumentationen an Konfigurationsänderungen sicherheitsrelevanter Systeme begleitend angepasst oder Sicherheitsrichtlinien vor der Freigabe neuer Systeme aktualisiert – das dokumentieren Sicherheitsanalysen branchenübergreifend.

Auch Studien belegen diesen Trend: Bei einer Umfrage von silicon.de gaben nur 20 % der 483 befragten Unternehmen an, ein schriftliches IT-Sicherheitskonzept zu besitzen; nach der KES/KPMG-Studie existierte es immerhin bei 56 % von 260 Unternehmen; und Ernst & Young fand unter 459 befragten Managern gerade 57 %, die sich sicher waren, über ein IT-Sicherheitskonzept zu verfügen. Nach Aktualität und Pflegeprozess wurde nicht gefragt – ernüchternd daher eine weitere Zahl: Nur 40 % der Manager waren sicher, einen Angriff überhaupt zu bemerken.

Zum Glück haben sich die Prioritäten verschoben. Vielleicht aus Einsicht. Oder um Anforderungen des KontraG, einer Zertifizierung nach BS 7799 oder einem Grundschutz-Audit zu genügen. Aber sicher auch aufgrund knapper IT-Budgets stehen nun in vielen Unternehmen die Grundlagen der IT-Sicherheit wieder oben auf der „To Do“-Liste:

- die Überarbeitung von Sicherheitsrichtlinien und Security Policies,
- die systematische Vervollständigung des IT-Sicherheitskonzepts und
- die Sensibilisierung der Mitarbeiter durch Awareness-Maßnahmen.

Vielleicht wird 2003 ein „Jahr des Sicherheitsmanagements“.

1 Security News

1.1 Neue Patch Suite für Internet Explorer

Am 04.12.2002 hat Microsoft erneut einen Patch für den Internet Explorer veröffentlicht: Ein Fehler im Cross Domain Security Model ermöglicht es einem Angreifer, über eine manipulierte Webseite Zugriff auf lokale Dateien zu gewinnen und dort Programme zu starten. Der Fehler wurde von Microsoft zunächst als „moderat" eingestuft; zwei Tage später wurde die Einstufung auf „kritisch" korrigiert. Eine Installation des Patches wird dringend angeraten.

Betroffen ist der Internet Explorer in den Versionen 5.5 (mit Service Pack 2) und 6.0 (mit Service Pack 1). Weitere Informationen und der Software-Patch von Microsoft finden sich unter

http://www.microsoft.com/technet/security/bulletin/ms02-068.asp

1.2 MBSA v1.1

Im Rahmen des im Oktober 2001 öffentlichkeitswirksam gestarteten „Strategic Technology Protection Program" hat Microsoft ein hilfreiches Tool für die Online-Überprüfung installierter Microsoft Software auf fehlende Sicherheits-Updates und sicherheitsrelevante Konfigurationsfehler entwickelt: den „Microsoft Baseline Security Analyzer" (MBSA). Seit dem 04.12.2002 ist er in Version 1.1 (englische Fassung) verfügbar und kann unter

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp (2,7 MB)

abgerufen werden. Analysiert werden Windows NT 4.0, 2000 und XP, IIS ab v4.0, IE ab v5.01, SQL Server ab v7.0, Office ab v2000, Exchange ab v5.5 und Windows Media Player ab v6.4. Der MBSA erlaubt nicht nur eine lokale, sondern auch eine Remote Analyse.

1.3 Aktuelle SSH-Bugs

Die amerikanische Firma Rapid7 Inc. deckte am 16.12.2002 zahlreiche Fehler in unterschiedlichen Implementierungen des verbreiteten Secure Shell-Protokolls SSH auf. Die Fehler und die betroffenen SSH-Implementierungen sind im zuletzt am 09.01.2003 aktualisierten CERT-Advisory CA-2002-36 zusammengefasst.

http://www.cert.org/advisories/CA-2002-36.html

Als Schutzmaßnahme wird die Installation aktueller Programmversionen und Patches empfohlen.

1.4 Sperrungsverfügung

Am 06.02.2002 hatte die Bezirksregierung Düsseldorf nach zwei mündlichen Anhörungen im November und Dezember 2001 an rund 80 Internet-Zugangs-Provider in Nordrhein-Westfalen eine Sperrungsverfügung verschickt, in der sie unter Berufung auf § 18 Abs. 2 des Mediendienste-Staatsvertrags (MdStV). zur umgehenden Sperrung ausgewählter Internet-Seiten mit strafrechtlich relevanten, rechtsextremistischen Inhalten aufforderte.

Gegen diese äußerst umstrittene Verfügung hatten 38 Provider Widerspruch eingelegt. Denn unabhängig von der Frage der Verantwortlichkeit der Provider für die vermittelten Inhalte lassen sich Sperrungen durch einen Anbieter technisch leicht umgehen. Die Widerspruchsbescheide der Bezirksregierung wiesen – erwartungsgemäß – die Einprüche zurück. Regierungspräsident Jürgen Büssow wurde daraufhin am 25.10.2002 im Rahmen der Verleihung des „Big Brother Awards" die zweifelhafte Ehre einer „Tadelnden Erwähnung" zuteil.

Das Verwaltungsgericht Düsseldorf lehnte nun mit Beschluss vom 19.12.2002 drei dort anhängige Eilanträge von Internet-Providern ab. Damit sind die Verfügungen trotz erheblicher Zweifel am Sinn einer solchen Maßnahme rechtskräftig.

http://www.sperrungsanordnung.de

1.5 ECCp-109 gelöst

Am 15.10.2002 wurde eine weitere „Elliptic Curve Challenge“ der Firma Certicom gelöst. Die mit 10.000 $ dotierte Lösung der 1997 veröffentlichten Aufgabe der zweiten Schwierigkeitsstufe wurde von einem Team um Chris Monico, University of Notre Dame (Indiana) nach 549 Tagen gefunden. An der Suche waren zuletzt weltweit 10.300 Computer und 247 Teams beteiligt.

Bestimmt wurde der diskrete Logarithmus eines Punktes auf einer elliptischen Kurve über GF(*p*), mit einem *p* der Länge 109 bit.

http://www.nd.edu/~cmonico/eccp109

Der erforderliche Rechenaufwand lag in der theoretisch erwarteten Größenordnung – und damit um etwa den Faktor 100.000.000 unter dem Aufwand, der nach heutiger Kenntnis für einen erfolgreichen Angriff auf derzeit verwendete Elliptische Kurven über GF(*p*) mit 163 bit langen Werten *p* erforderlich wäre.

1.6 NSA-Richtlinien für Windows XP und Cisco

Das „Systems and Network Attack Center“ (SNAC) der National Security Agency der USA (NSA) hat Leitlinien für die sichere Konfiguration wichtiger Systeme (Windows NT, Windows 2000, Windows XP, Cisco Router) in amerikanischen Behörden entwickelt, die zum Download bereitgestellt werden:

http://www.nsa.gov/snac

Am 25.11.2002 wurde der 141-seitige „Guide to Securing Microsoft Windows XP“ (Stand: 30.10.2002) veröffentlicht:

http://www.nsa.gov/snac/winxp/guides/wxp-1.pdf (1,78 MB)

Am 10.12.2002 veröffentlichte die NSA ein Update des 291 Seiten starken „Cisco Router Security Configuration Guide“ (Stand: 27.09.2002):

http://www.nsa.gov/snac/cisco/guides/cis-2.pdf (1,44 MB)

1.7 Marmor, Stein und Eisen bricht...

Die von den Karlsruher Versicherungen und Secorvo unter der Schirmherrschaft des Karlsruher Oberbürgermeisters im Jahr 2000 initiierte „Karlsruher IT-Sicherheitsinitiative“, einem Forum für aktuelle und ganzheitliche Fragen der IT-Sicherheit, startet ihre diesjährigen Aktivitäten im Februar mit einer Vortragsveranstaltung am Donnerstag, **13.02.2003** um **18 Uhr**. **Hans-Jürgen Frase**, Geschäftsführer der LITCOS GmbH & Co. KG, wird über physischen Schutz für IT-Systeme vortragen.

Für das leibliche Wohl ist gesorgt. Der Kostenbeitrag beträgt 30 €; für Partner ist die Teilnahme unentgeltlich. Da wieder eine große Zahl von Teilnehmern erwartet wird, wird um Anmeldung – möglichst bis 06.02.2003 – an info@ka-it-si.de gebeten.

http://www.KA-IT-Si.de

2 Secorvo News

2.1 Secorvo College aktuell

IT-Sicherheit muss, allen neuen Techniken zum Trotz, immer noch (vielleicht sogar erst recht) vor allem als ein Management-Prozess verstanden werden, in den sich die Konzeption, Umsetzung, Freigabe, regelmäßige Prüfung und Überarbeitung von Sicherheitsmaßnahmen systematisch einbetten.

In unserem neu entwickelten **Seminar „IT-Security Management“** stellen wir die grundlegenden Elemente eines systematischen IT Security Managements vor, präsentieren „Best Practices“ und entwickeln mit Ihnen an einem Beispielunternehmen ein Management-System – von der Risiko-Analyse bis zur ROI-Berechnung.

Termin: **11.-12.02.2003** (Anmeldung).

http://www.secorvo.de/college/it-security-management.html

2.2 Awareness-Partnerschaft

Seit November 2002 hat Secorvo einen weiteren starken Partner: das für hochwertige e-Learning-Lösungen bekannte Unternehmen digital spirit AG mit Sitz in Berlin.

http://www.digital-spirit.de

Mit digital spirit bietet Secorvo Konzeption und Unterstützung bei Awareness-Kampagnen. Ein erstes konkretes Resultat der Partnerschaft hat offenbar den Nerv der Zeit getroffen: Das **Web based Training zum Thema IT-Sicherheit**, entwickelt von Medienpädagogen der Firma digital spirit mit fachlicher Unterstützung von Secorvo.

http://www.secorvo.de/leistungen/awareness.html

2.3 Video-Lizenzen

Die beiden Videos zu den Themen „Trojanische Pferde“ und „Safer Surfen“ werden vermehrt in Security-Awareness-Kampagnen großer Unternehmen eingesetzt. Dafür kann nun auch eine **Intranet-Lizenz ohne Nutzer-Begrenzung** zum Preis von 2.900 € (zzgl. MwSt.) erworben werden.

http://www.secorvo.de/video/

2.4 DuD 2003 – IT-RM 2003

Wie im vergangenen Jahr werden wir auch 2003 gemeinsam mit dem für sein außergewöhnliches Qualitätsniveau bekannten Veranstalter Computas drei Konferenzen mitgestalten. Zur Vormerkung in Ihrem Kalender schon einmal die Termine der beiden ersten Vernstaltungen:

- **DuD 2003** (Datenschutz und Datensicherheit): **05.-06.05.2003, Berlin**
- **IT-RM 2003** (IT-Risk Management): **19.-20.05.2003, Karlsruhe**

Das Programm und nähere Informationen zu diesen drei Konferenzen werden nach Abschluss der Planungen auf der Webseite der Firma Computas zu finden sein:

http://www.computas.de/konferen.html

3 Veranstaltungshinweise

Januar 2003	
22.-23.01.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
28.-29.01.	PKI – Public Key Infrastrukturen (Secorvo College, Karlsruhe)
30.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2003	
04.-05.02.	SAP-Sicherheit im Betrieb (Secorvo College, Karlsruhe)
11.-12.02.	IT-Security Management (Secorvo College, Karlsruhe)
13.02.	Marmor, Stein und Eisen bricht (KA-IT-Si, Karlsruhe)
18.-19.02.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
18.-20.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
24.-26.02.	Fast Software Encryption Workshop (IACR, Lund/SE)
25.-26.02.	Lotus Notes Security (Secorvo College, Karlsruhe)
25.-26.02.	10. DFN-CERT/PCA-Workshop (DFN-CERT, Hamburg)

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

Impressum

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

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feed-Back an
redaktion-security-news@secorvo.de