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

Secorvo Security News
Februar 2003

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 2, 2. Jhrg. 2003
Stand 28. Februar 2003

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

Inhalt

Editorial: Wie die Schildbürger die Signatur regulierten

Für Karl Simrock (1802-1876) wäre es ein gefundenes Fressen gewesen: Die Geschichte der Regulierung der elektronischen Signatur im Deutschland des 21. Jahrhunderts. Sie beginnt 1997 nach dreijähriger Reifung mit dem ersten nationalen Signaturgesetz der Welt, gewissermaßen dem dreieckigen Rathaus. Acht Seiten, ergänzt um eine zehnseitige Signaturverordnung, die alles Wesentliche in knappen Sätzen regeln – ganz untypisch deutsch und weltweit beachtet. Sogar die Verabschiedung eines 300 Seiten starken „Maßnahmenkatalogs“ ließ sich verhindern.

Die erhoffte Initialzündung für die Etablierung elektronischer Abläufe bleibt allerdings aus, denn das definierte Sicherheitsniveau ist so hoch, dass Wirtschaftlichkeit und Praktikabilität in Frage stehen. Zwar gibt es bald erste Zertifizierungsstellen, doch Anwendungen und Nutzer fehlen: Das dreieckige Rathaus hat keine Fenster.

Da kommt Ende 1999 die EU-Richtlinie mit mehr Markt: Statt technischer Festlegungen soll die Haftung der Anbieter hinreichende Sicherheit garantieren – das Dach wird abgedeckt, im Rathaus ist Licht. Nun regnet es aber hinein: Die Investitionen der Zertifizierungsanbieter drohen Makulatur zu werden. Prompt kommt das Dach wieder drauf: Zur fortgeschrittenen und qualifizierten Signatur gesellt sich im neuen Signaturgesetz die „freiwillige Akkreditierung“.

Damit es wieder hell wird, wird nun das Licht in Säcken ins Rathaus getragen: Die GDPdU fordert 2001 die „qualifizierte Signatur mit Anbieterakkreditierung“, das 3. VwVerfÄndG führt 2002 die „qualifizierte Signatur mit Einschränkung“ ein und die aktuelle StDÜV erfindet qualifizierte Zertifikate, die elf der Kriterien nicht erfüllen.

Glücklicherweise gab es im 19. Jahrhundert noch keine digitalen Signaturen. Sonst hätte die Regulierungswirklichkeit Simrocks Schildbürgern womöglich den literarischen Erfolg streitig gemacht.

1 Security News

1.1 Fortsetzungsgeschichte: IE und Windows Patches

Mit einem neuen Sammel-Patch vom 05.02.2003 (Update: 12.02.2003) dichtet Microsoft neu entdeckte, als „critical“ eingestufte Löcher im Internet Explorer, die einem Angreifer die Umgehung des Sicherheitsmodells und damit die Ausführung beliebigen Programmcodes auf der angegriffenen Maschine erlauben. Betroffen sind die Versionen 5.01, 5.5, 6.0 des IE.

http://www.microsoft.com/security/security_bulletins/ms03-004.asp

Der Patch schließt alle Sammel-Patches des Jahres 2002 ein:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;810847

Bereits Ende Januar (22.01.2003) veröffentlichte Microsoft ein Security Update für die Betriebssystemversionen Windows NT 4.0, die Terminal Server Edition, Windows 2000 und Windows XP, das einen als „critical“ eingestuften Fehler im (üblicherweise nur auf Servern aktivierten) Locator-Service behebt:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-001.asp

1.2 Steuerdaten-Übermittlungsverordnung, StDÜV

Am 28.01.2003 erließ der Bundesfinanzminister eine „Verordnung zur elektronischen Übermittlung von Steuererklärungen und sonstigen für das Besteuerungsverfahren erforderlichen Daten“ (Steuerdaten-Übermittlungsverordnung – StDÜV). Darin werden die Bedingungen für eine zulässige elektronische Übermittlung von Steuerdaten festgelegt:

http://www.dud.de/dud/documents/stduev-030128.pdf (pdf, 45 kB)

§ 7 StDÜV legt die Anforderungen an die in diesem Zusammenhang benötigten elektronischen Signaturen fest – und schafft damit neben einfachen, fortgeschrittenen, qualifizierten, qualifizierten mit Anbieterakkreditierung und qualifizierten mit Einschränkung eine neue, sechste Klasse von Signaturen, die sich von qualifizierten Signaturen durch den Verzicht auf elf ausgewählte Anforderungen unterscheidet.

1.3 NGSCBFW

„Next-Generation Secure Computing Base for Windows“ heißt seit dem 23.01.2003 die im August 2002 gestartete, bislang unter dem Codenamen „Palladium“ geführte und nicht unumstrittene Sicherheitsarchitektur von Microsoft, die ab 2005 Teil des Windows-Betriebssystems sein soll.

Alle geheimen Passwörter und Schlüssel sollen in einem in einer Hardware-Komponente verankerten Trusted Platform Module (TPM) vor unberechtigtem Zugriff Dritter geschützt werden. Die Ein-/Ausgabe-Kanäle sollen so um Authentifikationsmechanismen erweitert werden, dass kein Programm mehr Ein- oder Ausgaben vortäuschen oder abfangen kann – ein wirksames Handicap für Trojanische Pferde.

http://www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp

Welchen Preis hinsichtlich Flexibilität und Nutzbarkeit des Systems die Anwender für die unbestrittenen Sicherheitsgewinne zahlen müssen, ist dabei noch eine offene Frage.

1.4 The National Strategy to Secure Cyberspace

Im Februar 2003 veröffentlichte das Weiße Haus die Endfassung der „National Strategy to Secure Cyberspace“, deren Vorfassung am 17.09.2002 (nicht ganz freiwillig) öffentlich zur Diskussion gestellt worden war (siehe Secorvo Security News 4/2002).

http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (pdf, 980 kB)

Die Strategie verfolgt drei Ziele: den Schutz von Amerikas kritischen Infrastrukturen vor Cyber-Attacken, die Verringerung der Verletzlichkeit und die Minimierung von Schäden und Ausfallzeiten. Sie setzt fünf Prioritäten: Die Entwicklung eines nationalen Security Response Systems, eines Programms zur Verringerung der Verletzlichkeit, eines Awareness- und Trainings-Programms, den Schutz der Regierungsinfrastruktur sowie den Aufbau einer internationalen Sicherheitskooperation.

1.5 PKI-Forum bei OASIS

Das 1999 gegründete PKI-Forum, eine internationale Vereinigung der Anbieter von PKI-Lösungen, wurde am 04.11.2002 in OASIS (Organization for the Advancement of Structured Information Standards) integriert. OASIS ist ein 1993 gegründetes Konsortium von inzwischen mehr als 600 Unternehmen weltweit, das die Entwicklung offener technischer Standards fördert.

http://www.pkiforum.org
http://www.oasis-open.org

Am 07.01.2003 gründete OASIS ein „Technical Committee to Advance PKI Adoption for Secure Transactions“. Ziel dieser Arbeitsgruppe ist die Förderung von Public Key Infrastrukturen durch White Papers, Informationssammlungen und Standardisierungsaktivitäten, die der Lösungsinteroperabilität, der Orientierung am tatsächlichen Business-Bedarf und der Verbreitung digitaler Signaturen und Zertifikate dienen.

http://www.oasis-open.org/committees/pki/

1.6 Vorratsspeicherung

Im Zusammenhang mit dem Angebot von Flatrate-Internetzugängen ist eine Diskussion darüber entbrannt, ob die Speicherung von Verbindungsdaten (dynamische IP-Adresse, Datum, Uhrzeit) über das Ende der Nutzung hinaus zulässig ist, da sie zu Abrechnungszwecken nicht benötigt wird.

Sowohl ein für T-Online erstelltes Gutachten als auch die Datenschutz-Aufsichtsbehörde Darmstadt sind zu dem Ergebnis gekommen, dass eine solche Speicherung zulässig sei (Schreiben vom 14.01.2003):

http://www.dud.de/dud/documents/tdsl-rp-da-030114.pdf (pdf, 124 kB)

Ganz anders die Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vom 16.01.2003:

http://www.datenschutzzentrum.de/material/themen/presse/ipspeich.htm

Im gleichen Sinne äußert sich der Hamburgische Datenschutzbeauftragte, Dr. Hans-Hermann Schrader (28.01.2003):

http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/aktuelles/pressemeldung-2003-01-28-pdf,property=source.pdf (pdf, 56 kB)

1.7 Programm „DuD 2003“

Zum fünften Mal jährt sich die Fachkonferenz „Datenschutz und Datensicherheit“ – **DuD 2003** – am **05.-06.05.2003** in Berlin. Gemeinsam mit den Herausgebern der Fachzeitschrift „DuD“, Johann Bizer, Dirk Fox und Helmut Reimer, bietet der Veranstalter Computas eine zweitägige Konferenz mit Vorträgen namhafter Experten aus Politik, Industrie, Wissenschaft und Verwaltung zu zentralen, aktuellen Themen und (Streit-) Fragen des Datenschutzes und der IT-Sicherheit an.

http://www.computas.de/dud/dud2003.pdf
(pdf, 276 kB)

Diese Tagung erfreut sich jährlich steigender Teilnehmerzahlen und konnte sich als „feste Größe“ unter den deutschen Datenschutz-Veranstaltungen etablieren. Für „Wiederholungsteilnehmer“ winken Staffelpreise – und bei Anmeldung über Secorvo (an info@secorvo.de oder per Fax an 0721/6105-455) zudem zur Feier des Jubiläums ein Crémant-d‘Alsace des Weinguts Raymond Kieffer – jedem Kenner von Computas-Veranstaltungen ein Begriff.

2 Secorvo News

2.1 Secorvo College aktuell

Die sichere Konfiguration der Microsoft-Betriebssysteme gibt es nicht „out of the box“. Erfahrung nutzen bedeutet hier die Sicherheit Ihrer Systeme wirksam zu erhöhen.

Inside Windows Security, Windows 2000 und XP, 25.-26.03.2003

Angriffe auf Rechnersysteme selbst zu erleben und durchzuführen erleichtert die realistische Abschätzung der Gefahren, denen Ihre IT-Systeme ausgesetzt sind.

Defense Lab – Live Hacking, Angriffstechniken, Gegenmaßnahmen, 01.-02.04.2003

2.2 Neu: SSL-Zertifikate der PKI-1-Verwaltung

Das BSI hat den Betrieb der PKI-1-Verwaltung im Januar 2003 um die Ausstellung von SSL-Zertifikaten erweitert. Dazu wurden von Secorvo eine SSL-Studie und ein Umsetzungskonzept erstellt:

http://www.secorvo.de/publikationen/bsi-ssl-studie1.4.zip (pdf/zip, 316 kB)

http://www.secorvo.de/publikationen/bsi-ssl-umsetzungskonzept1.4.pdf (335 kB)

2.3 White Paper „VPN Basis-Interoperabilität“

Seit Ende Januar ist das sechste Secorvo White Paper verfügbar, diesmal zum Thema „VPN Basis-Interoperabilität“. Eine Kurzfassung der Untersuchung, in der das paarweise Zusammenspiel der VPN-Geräte von sechs Herstellern mit einer Basis-Sicherheitskonfiguration untersucht wurde, erschien in der Oktoberausgabe der Zeitschrift iX.

http://www.secorvo.de/whitepapers

3 Veranstaltungshinweise

März 2003	
25.-26.03.	Inside Windows Security (Secorvo College, Karlsruhe)
26.-28.03.	Workshop on Privacy Enhancing Technologies 2003 (TU Dresden)
April 2003	
01.-02.04.	Defense Lab (Secorvo College, Karlsruhe)
08.-09.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
13.-17.04.	RSA Conference 2003 (RSA, San Francisco)
Mai 2003	
05.-06.05.	DuD 2003 (Computas, Berlin)
06.-07.05.	Public Key Infrastrukturen (PKI) (Secorvo, Karlsruhe)
08.05.	PKI für Fortgeschrittene (Secorvo, Karlsruhe)
13.-15.05.	BSI-Kongress 2003 (BSI, Bonn)
19.-20.05.	IT Risk Management (ITRM 2003) (Computas, Karlsruhe)

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 Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
März 2003

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch

Secorvo Security Consulting GmbH

Nr. 3, 2. Jhrg. 2003
Stand 28. März 2003

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

Inhalt

Editorial: Von Keilen und groben Klötzen

Ein Mann, der sich für stark gehalten,
versuchte, einen Klotz zu spalten.

Geheimnisumwölkt und leicht verrucht lockt die Kryptografie Hobbyexperten wie das Lampenlicht die Sommermotten.

Doch schwang vergeblich er sein Beil,
der Klotz war gröber als der Keil.

Unter Kryptologen sind die Geschichten von vermeintlich „unbrechbaren neuen Verfahren“ Legende – ebenso wie ihre desillusionierende Kompromittierung.

Ein zweiter sprach: Ich werd’s schon kriegen! –
umsonst, der grobe Klotz blieb liegen.

Aber auch der umgekehrte Fall ist nicht selten: hoch intelligente und erfahrene Krypto-Experten, die sich an dem Versuch, ein neues Verfahren zu brechen, die Zähne ausbeißen.

Ein dritter kam nach Jahr und Tag,
dem glückt es auf den ersten Schlag.

Und dann gibt es den dritten Fall: Verfahren, die jahrelang genutzt werden, von deren Sicherheit Experten wie Laien überzeugt sind, die Eingang in Standards und Produkte gefunden haben – und eines Tages einem neuen kritischen Blick, der das danach so scheinbar Offensichtliche zu Tage fördert, zum Opfer fallen.

Diese Fälle sind zum Glück selten, auch wenn die jüngsten Erkenntnisse zu SSL, RSA und Kerberos gleich drei sehr prominente Verfahren betreffen.

War der nun wirklich gar so forsch?
Nein – nur der Klotz war seitdem morsch.

Zwar sind die Angriffe in realen Umgebungen nicht durchführbar. Aber sie zeigen: Erfahrung schützt vor Irrtum nicht.

Und sie sind zugleich eine Mahnung an die enthusiastischen Verfechter des Open Source-Paradigmas: Auch die Veröffentlichung des Source-Codes verhindert keine Fehler. Wir werden noch viele davon kennen lernen – sofern wir ein wenig Geduld mitbringen.

1 Security News

1.1 In Memoriam Roger Needham

Einer der Pioniere der Computer-Sicherheit ist tot. Roger Needham, langjähriger Cambridge-Professor und zuletzt Managing Director von Microsoft Research Ltd. verstarb Anfang März im Alter von 68 Jahren.

Seine wohl bekannteste Arbeit ist das 1978 zusammen mit Michael Schroeder veröffentlichte Authentifikationsverfahren, das die wissenschaftliche Grundlage des Kerberos-Protokolls bildet, mit dem sich heute beispielsweise die Benutzer von Windows 2000 am Domänen-Controller anmelden.

http://research.microsoft.com/users/needham/

1.2 Biometrie mit Problemen

In zahlreichen Pilotversuche zum Einsatz biometrischer Verfahren bei der Personenkontrolle steht derzeit die Gesichtserkennung auf dem Prüfstand. Insbesondere die Sie gilt als sehr attraktiv, da ein Foto als biometrisches Merkmal in Ausweisdokumenten im Gegensatz etwa zu Fingerabdrücken allgemein akzeptiert ist.

Allerdings haben die Verfahren im praktischen Einsatz noch einige Probleme. Bei einem Pilotprojekt zur Überprüfung von Flugreisenden am Nürnberger Flughafen war das System dem menschlichen Auge des geschulten Personals weit unterlegen.

http://www.heise.de/newsticker/data/jk-18.03.03-006/

Im Verlauf eines ähnlichen Versuchs am Flughafen von Sydney gelang es zwei japanischen Reisenden sogar, ihre Pässe zu tauschen, ohne dass dies von der automatischen Gesichtskontrolle bemerkt wurde.

http://australianit.news.com.au/articles/0,7204,6048331^15306^^nbv^,00.html

1.3 Sendmail-Bug bei „weitergereichten“ Mails

Sicherheitslücken in Sendmail sind ja an sich nichts Neues. Viele Anwender schützen ihre Sendmail-Installation deshalb durch einen vorgelagerten Sicherheits-Proxy der Firewall, der eine direkte Verbindung vom Internet zu einem Sendmail-basierten Mailserver verhindert.

Der jüngst entdeckte Heap-Overflow tritt jedoch bei der Bearbeitung des Mail-Envelope-Headers auf und betrifft somit auch Sendmail-Installationen, die hinter einer Firewall Deckung suchen. Patches sind verfügbar und entfernen auch gleich die gefährlichen Header-Zeilen, so dass selbst eine weitergeleitete Mail keinen Schaden mehr anrichten kann.

http://www.cert.org/advisories/CA-2003-07.html

1.4 „Side-Channel“ Angriffe auf SSL und RSA

Gleich drei aktuelle Angriffe machen sich „Randinformationen“ von SSL- bzw. RSA-Implementierungen zu nutze. Als Testobjekt für die praktische Demonstration diente den Autoren OpenSSL – der Quelle vieler SSL-Lösungen. Daher sind höchstwahrscheinlich auch andere Implementierungen betroffen.

Forscher der Eidgenössischen Technischen Hochschule Lausanne benutzen das Timing von schneller oder langsamer zurückgemeldeten Fehlermeldungen, um Hinweise zur Entschlüsselung von SSL-geschützten Nachrichten zu erhalten. Dieser ausgefeilte Angriff ist glücklicherweise nur unter sehr speziellen Umständen anwendbar und daher wenig praxisrelevant.

http://lasecwww.epfl.ch/memo_ssl.shtml

Zwei Stanford-Forscher messen die benötigte Zeit für die Ausführung der RSA-Operation, um den verwendeten geheimen Exponenten zu ermitteln. Hierüber könnte

beispielsweise der geheime Schlüssel eines SSL-Webservers ermittelt werden.

http://crypto.stanford.edu/~dabo/abstracts/ssl-timing.html

Und tschechische Kryptologen werten die unterschiedlichen Reaktionen auf verschiedene Fehlerfälle, die während eines SSL-Verbindungsaufbaus auftreten können, um einen SSL-Sitzungsschlüssel zu ermitteln oder eine RSA-Signatur im Namen des SSL-Servers zu fälschen. Auch dieser Angriff ist nur von beschränkter Praxisrelevanz: Er erfordert Millionen von fehlgeschlagenen SSL-Verbindungen, die für aufmerksame Systemadministratoren nicht zu übersehen wären.

http://eprint.iacr.org/2003/052/

Für OpenSSL wurden umgehend Patches gegen alle drei Attacken bereit gestellt.

http://www.openssl.org/

1.5 BVerfG urteilt zur TK-Überwachung

Am 12.03.2003 hat das Bundesverfassungsgericht (BVerfG) zwei Verfassungsbeschwerden von Journalisten zurückgewiesen, deren Telefone im Zuge der Verfolgung schwerer Straftaten abgehört wurden. Beschwerdeführer waren das ZDF, zwei seiner journalistischen Mitarbeiter und eine für das Magazin „Stern“ tätige Journalistin, die Informationen zu verschiedenen Kriminalfällen recherchierten.

Da angenommen wurde, dass die Journalisten mit den Beschuldigten in telefonischem Kontakt stehen, ordnete das Amtsgericht Frankfurt a.M. auf Antrag der Staatsanwaltschaft die Auskunft über entsprechende Verbindungsdaten der Telefongespräche an. Die Verfassungsbeschwerden richteten sich gegen diese richterliche Anordnung der TK-Überwachung.

Obwohl das BVerfG sowohl den Eingriff in das Fernmeldegeheimnis als auch den Eingriff in die Presse- und Rundfunkfreiheit der Beschwerdeführer anerkannte, hatten die Verfassungsbeschwerden keinen Erfolg. Zur Begründung gab das Gericht an, dass auch schwer wiegende Grundrechtseingriffe als verhältnismäßig anzusehen sind. Denn „angesichts der Schwere der in Rede stehenden Straftaten“ hätten die Gerichte „dem Gebot der wirksamen Strafverfolgung zu Recht den Vorrang eingeräumt“.

http://www.bverfg.de/bverfg_cgi/pressemitteilungen/frames/bvg20-03

1.6 Eindringen per Intrusion Detection System

Ein Buffer Overflow bei der Analyse des mitgeschnittenen Datenverkehrs durch das Open-Source Intrusion Detection System (IDS) „snort“ ermöglichte es Angreifern, mittels einer vorgeblichen Attacke auf RPC-Dienste in Wirklichkeit den IDS Server anzugreifen. Entdeckt wurde die Sicherheitslücke vom kommerziellen IDS-Hersteller ISS Inc.

http://www.snort.org/

1.7 Krypto-Schwäche in Kerberos v4

Eine neu entdeckte Schwäche im altbekannten Kerberos v4 Protokoll ermöglicht verschiedene Angriffe durch Kerberos-Benutzer und durch Administratoren fremder Verwaltungsbereiche („Realms“). Wer noch Kerberos v4 einsetzt, sollte den empfohlenen Patch installieren – oder gleich zu Kerberos v5 wechseln.

http://web.mit.edu/kerberos/www/advisories

1.8 Unendliche Geschichte: Windows-Patches

Immer wieder einen Blick wert ist die Security Bulletin Liste von Microsoft. Neu hinzu gekommen sind kritische Sicherheitslücken in der Windows Script Engine und in der DOS/NT Namenskonvertierung sowie Denial-of-Service gegen ISA Server und RPC.

http://www.microsoft.com/technet/security/current.asp

2 Secorvo News

2.1 Secorvo College aktuell

Über fünf Jahre Erfahrung mit der Konzeption, dem Aufbau und dem erfolgreichen Betrieb von Public Key Infrastrukturen bündelt Secorvo in dem Seminar-Paket „PKI“ und „PKI für Fortgeschrittene“:

- PKI – Public Key Infrastrukturen, 06.-07.05.2003.
- PKI für Fortgeschrittene, 08.05.2003.

Einsteigern in das Thema IT-Sicherheit bietet Secorvo außerdem jetzt einen einwöchigen Intensivkurs:

- IT-Sicherheitsmanagement von A (wie Audit) bis Z (wie Zertifizierung), 12.-16.05.2003

Für Teilnehmer dieses Seminars ist der Eintritt zur Veranstaltung der Karlsruher IT-Sicherheitsinitiative am 15.05.2003 kostenfrei.

2.2 Evaluierung der EU-Signaturrichtlinie

Im Oktober 2002 hatte die Europäische Kommission eine Evaluationsstudie über „rechtliche und marktbezogene Aspekte der Anwendung der Richtlinie“ (zu elektronischen Signaturen) ausgeschrieben. Ziel der Studie ist es, den aktuellen Stand der praktischen Umsetzung der Signaturrichtlinie in den einzelnen Mitgliedsstaaten zu dokumentieren.

Ein internationales Konsortium unter der Leitung von Professor Jos Dumortier (KU Leuven, ICRI, Belgien) hat diese Ausschreibung gewonnen. Das Team aus Jos Dumortier, Patrick an Eecke (Belgien), Georgia Skouma (Belgien), Hans Nilsson (Schweden) und Stefan Kelm von Secorvo wird die Studie voraussichtlich im Juli 2003 vorlegen.

3 Veranstaltungshinweise

April 2003	
09.04.	Lampertz-Sicherheitstag (Lampertz, Speyer)
13.-17.04.	RSA Conference 2003 (RSA, San Francisco)
Mai 2003	
05.-06.05.	DuD 2003 (Computas, Berlin)
06.-07.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
08.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
13.-15.05.	BSI-Kongress 2003 (BSI, Bonn)
15.05.	Karlsruher IT-Sicherheitsinitiative (KA-IT-Si, Karlsruhe)
12.-16.05.	IT-Sicherheitsmanagement von Audit bis Zertifizierung (Secorvo College, Karlsruhe)
19.-20.05.	IT Risk Management (ITRM 2003) (Computas, Karlsruhe)
20.-21.05.	Lotus Notes Security (Secorvo College, Karlsruhe)

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 Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
April 2003

Dirk Fox, Stefan Gora, Stefan Kelm
Hans-Joachim Knobloch

Secorvo Security Consulting GmbH

Nr. 4, 2. Jhrg. 2003
Stand 25. April 2003

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

Inhalt

Editorial: Am Zopf aus dem Sumpf

Was dem einen der Lösungsweg, ist dem anderen eine Vermeidungsstrategie: Die Zurückführung eines Problems auf ein anderes. Mathematiker lösen mit dieser Methode komplexe Herausforderungen: Sie formulieren eine Problemstellung so um, dass sie auf eine andere, bereits gelöste, zurückgeführt werden kann. Die Entwickler von Sicherheitslösungen beherrschen diese Technik auch. Allerdings erwischen sie, so scheint es, dabei häufiger ungelöste Probleme, auf die sie die Fragestellung zurückführen.

Ein klassisches Beispiel ist die Erzeugung digitaler Signaturen. Theoretisch mag die Signatur unfälschbar sein. Tatsächlich ist sie aber immer nur so sicher wie der geheime Signierschlüssel: Kann ein Angreifer ihn in Erfahrung bringen, ist die Sicherheit perdu. Also speichert man ihn auf einer Smartcard – und führt das Problem damit auf den Schutz der PIN zurück. Die kann ein Angreifer jedoch oft leicht gewinnen, wie Forscher der Universität Bonn 2001 am Beispiel des Signtrust-Clients „eTrust“ anschaulich vorführten [Cremers, Spalka, Langweg 2001].

Ein anderes Beispiel ist die Jahrzehnte alte Vision eines sicheren Betriebssystems: Integer muss es sein und Veränderungen durch nicht autorisierte Programme verhindern. Allein durch Signieren der Software lässt sich das Problem jedoch nicht lösen – sondern bestenfalls auf die Authentizität des Prüfschlüssels verschieben. Die von Compaq, HP, IBM, Intel und Microsoft gegründete Trusted Computing Platform Alliance (TCPA) versucht es nun mit der Einführung einer Hardware-Verankerung von Schlüsseln und Zufallsgeneratoren.

Vor allzu kühnen Hoffnungen sei allerdings gewarnt. Denn die Angriffe auf die Xbox zeigen: Auch Hardware ist modifizierbar. Und noch sind wir alle keine Barone, die sich mit beherztem Griff an den eigenen Zopf aus dem Sumpf ziehen können.

1 Security News

1.1 TCPA in der Kritik

Gleich an mehreren Fronten kam die Trusted Computing Platform Alliance (TCPA) in den vergangenen Wochen unter Beschuss: Die Datenschutzbeauftragten des Bundes und der Länder äußerten ihre Skepsis, dass die TCPA Architektur zur Aushebelung des Datenschutzes missbraucht werden könnte und fordern die vollständige und ausschließliche Kontrolle der Anwender über ihre mit TCPA geschützten Systeme. In dieselbe Richtung zielen die vier Forderungen, die der Chaos Computer Club anlässlich der CeBIT an die TCPA stellte. Und Protect Privacy e.V. hat für die Kritiker ein Web-Forum etabliert.

Auf technischer Ebene wurde Anfang April der Sicherheitsmechanismus der Microsoft Xbox – von vielen als Testlauf für mögliche TCPA Mechanismen angesehen – ausgehebelt: durch einen Buffer Overflow im Spiel „007 Agent Under Fire“ ist es sogar ohne Hardware-Eingriff möglich, Linux auf der Xbox zu starten.

Bei aller Skepsis und negativen Schlagzeilen darf jedoch nicht übersehen werden, dass TCPA oder vergleichbare Architekturen – fehlerfrei und datenschutzkonform umgesetzt – einen wichtigen Schritt zu mehr Sicherheit darstellen können.

1.2 Signaturbündnis geht an den Start

Fast sechs Jahre nach Inkrafttreten des ersten Signaturgesetzes in Deutschland haben Staat und Wirtschaft am 03.04.2003 das „Bündnis für elektronische Signaturen“ gegründet.

Das von der Bundesregierung im Schulterschluss mit mehreren Großunternehmen initiierte Bündnis soll dem Markt für elektronische Signaturen zum lang ersehnten Durchbruch verhelfen: Deutschland sei „Vorreiter im Recht. Aber leider nicht in der Praxis.“, so Staatssekretär Wewer auf der Gründungsveranstaltung. Zu den Konvergenzzielen des Bündnisses zählen insbesondere die Standardkonformität technischer Komponenten sowie die Förderung multifunktionaler Chipkarten.

Bemerkenswert ist, dass Innen-, Wirtschafts- und Finanzministerium an der Gründung gemeinsam mitwirkten. Das ist ein wichtiges Signal, denn diese Ministerien waren in der Vergangenheit nicht immer einer Meinung, wenn es um die Förderung elektronischer Signaturen ging.

1.3 Bundestag verabschiedet neues Urheberrecht

Nach dem Signaturgesetz und einigen damit verbundenen Gesetzesänderungen befindet sich Deutschland nun auch im Bereich des Urheberrechts auf dem Weg in die Informationsgesellschaft: Der Bundestag hat am 11.04.2003 den „Gesetzesentwurf zur Regelung des Urheberrechts in der Informationsgesellschaft“ verabschiedet.

Ähnlich wie der in den USA bereits in Kraft getretene Digital Millenium Copyright Act (DMCA) soll auch das neue deutsche Recht das Eigentum an digitalen Daten besser schützen – so soll insbesondere das Umgehen von Kopierschutzsystemen zukünftig verboten sein. Lediglich für bestimmte private Zwecke sowie für die Forschung sollen Ausnahmen erlaubt werden, die jedoch recht ungenau gefasst wurden.

Damit ist die Diskussion um die Neugestaltung des Urheberrechts keineswegs beendet: Etliche Industrieverbände sowie private Initiativen haben bereits massive Kritik an der Neuregelung geäußert; die Bundesregierung selbst kündigte inzwischen eine weitere Urheberrechtsnovelle an.

1.4 CERT Summary 1/2003

Bei der Vielzahl an Sicherheitslücken und Hacker-Angriffen, die täglich in diversen

Medien veröffentlicht werden, ist es auch dem versierten Systemadministrator nahezu unmöglich, den Überblick zu behalten und die richtigen Entscheidungen effizient zu treffen.

Diesem Umstand trägt das CERT/CC mit dem CERT Summary Rechnung: Diese einmal pro Quartal herausgegebene Zusammenfassung listet stichwortartig diejenigen Sicherheitsvorfälle des vergangenen Quartals auf, denen das CERT/CC eine besondere Bedeutung zumisst. Damit stellt es eine echte Bereicherung im „Informationsdschungel“ dar.

Das Ende März veröffentlichte CERT Summary für das 1. Quartal 2003 beschreibt zehn Schwachstellen in verbreiteten Softwarepaketen und gibt Verweise auf weiter führende Informationen. Es finden sich Informationen zu Lücken in sendmail, Microsoft Windows, Samba, SSH, usw.; siehe dazu auch die Ausgaben 1-3/2003 der Secorvo Security News.

1.5 CERT-Sicherheitswarnung „entwichen“

Bereits seit 1988 gibt das US-amerikanische CERT Coordination Center (CERT/CC) in Pittsburgh aktuelle Sicherheitswarnungen zu Angriffen und Sicherheitslücken heraus – die sog. CERT Advisories.

Diese Advisories beschreiben – ohne eine „Anleitung zum Hacken“ darzustellen – Sicherheitslücken in Programmen und Betriebssystemen sowie Lösungsmöglichkeiten zu deren Beseitigung. Die Veröffentlichung dieser Advisories geschieht dabei in der Regel nach einer fest vorgegebenen Informationspolitik: Wird eine Schwachstelle entdeckt, wird der Hersteller informiert, um diesem die Behebung der Schwachstelle (z. B. durch entsprechende Patches) zu ermöglichen. Erst danach wird die Öffentlichkeit durch Herausgabe eines Advisories über die gefundene (und behobene) Sicherheitslücke informiert.

Diese Informationspolitik wird seit vielen Jahren kontrovers diskutiert. Gegner führen als Argumentation regelmäßig an, dass neue Sicherheitslücken unmittelbar und mit allen Details (full disclosure) veröffentlicht werden müssten, um die Hersteller zur Behebung der Lücken zu „zwingen“.

Im März nun ist es offenbar einem Hacker gelungen, drei im Entwurfsstadium befindliche Advisories zu „stehlen“ und die zwischen dem CERT/CC und den Herstellern diskutierten vertraulichen Informationen an die Öffentlichkeit zu bringen, bevor ein Advisory veröffentlicht werden konnte. Ob hieraus Schaden entstand, ist nicht bekannt; der Vorfall zeigt jedoch, wie kontrovers die Informationspolitik der CERTs zur Zeit diskutiert wird.

1.6 „Evil Flag“ für IP-Pakete

Von der Fachwelt lange erwartet erschien pünktlich am 1. April 2003 RFC 3514, in dem Steven Bellovin, Co-Director der IETF Security Area das „Security Flag in the IPv4 Header“ spezifiziert. Es nutzt ein seit 1981 unbelegtes Bit im Kopf von IP Paketen, um anzuzeigen, ob das Paket harmlos ist oder bösartigen Intentionen dient.

Sobald die namhaften Hersteller die Nutzung dieses sogenannten „Evil Flag“ in den IP-Stacks ihrer Betriebssysteme implementiert haben, ist es nur noch ein kurzer Weg zur perfekten Firewall.

2 Secorvo News

2.1 Secorvo College aktuell

Das neue Seminarprogramm 2003/2 von Secorvo College ist erschienen. Es wurde um einen einwöchigen Intensivkurs zum Thema „Information Security Management“ erweitert, dessen erste drei Tage getrennt gebucht werden können:

- Information Security Management von A(udit) bis Z(ertifizierung), **12.-16.05.2003**.

2.2 IT Risk Management

Vom **19.-20.05.2003** findet die Konferenz IT Risk Management 2003 unseres Partners COMPUTAS Giesela Geuhs GmbH in Karlsruhe statt. Topthema: Awareness.

2.3 Let's do the time warp again

Die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) startet am **15.05.2003** (18 Uhr) zu einer Zeitreise zu den Höhepunkten der Geschichte der IT-Sicherheit – und lädt anschließend zum „Schlemmer-Networking". Referent ist Dirk Fox, Geschäftsführer von Secorvo und Herausgeber der Zeitschrift „Datenschutz und Datensicherheit" (DuD).

2.4 Security Awareness Symposium 2003

Ein wirkungsvoller Informationsschutz steht und fällt mit der aktiven Unterstützung durch alle Mitarbeiter des Unternehmens. Häufig jedoch werden Sicherheitsmaßnahmen als Arbeitsbehinderung gesehen, wird die eigene Verantwortung nicht wahrgenommen oder werden vernünftige Risikoannahmen als realitätsfern abgetan – und damit Bedrohungen der Informationssicherheit durch Mitarbeiter mitverursacht.

Durch geeignete Security Awareness-Maßnahmen können sowohl das erforderliche Grundwissen vermittelt, die Sensibilität der Mitarbeiter für Informationssicherheit erhöht als auch Einstellungen und Verhaltensweisen nachhaltig verändert werden.

Ziel des Security Awareness Symposiums 2003, das Secorvo gemeinsam mit zwei Partnern, dem E-Learning-Spezialisten digital spirit ag und der Agentur Dauth, Kaun & Partner am **24.-25.06.2003** im Technologiepark Karlsruhe durchführt, ist ein intensiver Erfahrungsaustausch mit und zwischen Unternehmen, die Security Awareness-Kampagnen planen oder bereits umsetzen. Dafür konnten Referenten mehrerer Großunternehmen gewonnen werden.

3 Veranstaltungshinweise

Mai 2003	
05.-06.05.	DuD 2003 (Computas, Berlin)
06.-07.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
08.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
12.-16.05.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
13.-15.05.	BSI-Kongress 2003 (BSI, Bonn)
15.05.	Let's do the time warp again (KA-IT-Si, Karlsruhe)
19.-20.05.	IT Risk Management (ITRM 2003) (Computas, Karlsruhe)
20.-21.05.	Lotus Notes Security (Secorvo College, Karlsruhe)
Juni 2003	
24.-25.06.	Security Awareness Symposium 2003 (Secorvo, Karlsruhe)
24.-26.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)

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 Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Mai 2003

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch, Dörte Neundorf

Secorvo Security Consulting GmbH

Nr. 5, 2. Jhrg. 2003
Stand 28. Mai 2003

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

Inhalt

Editorial: Entsorgung von E-Müll

Viele, vielleicht die meisten der aktuellen Probleme in der IT-Sicherheit sind „uralt“: Neben Buffer Overflows und Computerviren beschäftigen uns auch Werbe-E-Mails – neudeutsch „Spam“ – seit Jahren. Zahlreiche Anbieter durchforsten heute Webseiten und Newsgroups automatisiert nach E-Mail-Adressen und nutzen diese Millionen-Verteiler für elektronische Postwurfsendungen. Inzwischen hat Spam für viele Nutzer die Grenze einer erträglichen Belästigung überschritten. Für Endbenutzer und Administratoren ist dieser tägliche E-Müll zur zeit- und ressourcenintensiven Belastung geworden. Provider versuchen Spam einzuschränken; auch gibt es für gängige Mail-Programme Filter, mit denen E-Mails auf „verdächtige“ Textstücke untersucht werden können.

Dank der Findigkeit der Werber haben diese Maßnahmen aber nur mäßigen Erfolg. Daher befassen sich mittlerweile weltweit Gesetzgebung und Rechtsprechung mit dem Phänomen. Jüngst zogen in Florida gar E-Mail-Vermarkter gegen Anti-Spam-Organisationen vor Gericht. Einige Länder bereiten Gesetze vor, nach denen das unerwünschte Versenden von Werbe-E-Mails unter Strafe gestellt werden soll. Auch der am 06.05.2003 vom Kabinett vorgelegte Entwurf für ein neues Gesetzes gegen den unlauteren Wettbewerb (UWG) definiert „Werbung mit elektronischen Nachrichten, bei der die Identität des Absenders ... verheimlicht wird“ als „unzumutbare Belästigung“ – ignoriert aber die Tatsache, dass solche E-Mails meist aus dem Ausland kommen und das UWG somit nicht greift.

Auch auf Tagungen wird das Thema intensiv diskutiert, so jüngst auf einer „Spam Conference“ des MIT, der DuD-Konferenz (05.-06.05.2003) sowie dem Anti-Spam-Kongress des eco-Forums (21.05.2003) Von einer Lösung des Problems, das zeigen die Diskussionen, sind wir allerdings noch weit entfernt. Daher ist eine weitere Zunahme von Spam zu befürchten.

1 Security News

1.1 Signaturalgorithmen für Europa

Bereits seit Dezember 1998 werden im Rahmen der europäischen Standardisierungsinitiative EESSI Standards entwickelt, die die Umsetzung und Implementierung der EU-Direktive zu elektronischen Signaturen aus dem Jahr 1999 fördern sollen. Zu den inzwischen verabschiedeten Dokumenten zählen beispielsweise Zertifikatsprofile, Richtlinien für Zertifizierungsinstanzen und Anforderungen an sichere Signaturerstellungseinheiten.

Mit dem „ETSI Special Report“ (ETSI SR 002 176 V1.1.1), an dessen Entstehung auch Secorvo aktiv beteiligt war, wurde am 27.03.2003 nun auch die überfällige Spezifikation der „Algorithms and Parameters for Secure Electronic Signatures“ verabschiedet. Inhaltlich ist das Dokument der Publikation der „Geeigneten Kryptoalgorithmen“ durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vergleichbar, die einmal jährlich gemäß Signaturgesetz die für die kommenden sechs Jahre als geeignet anzusehenden Kryptoalgorithmen und Parameter „amtlich“ festlegt.

1.2 PKI Challenge legt Abschlussbericht vor

Noch immer ist die Interoperabilität eine der größten Herausforderungen bei Aufbau und Betrieb von Public Key-Infrastrukturen. Diesem Umstand trug die „PKI Challenge“ Rechnung, ein von der Europäischen Kommission und der Schweizer Regierung gefördertes Projekt, das im Januar 2001 unter der Führung der EEMA (European Forum for Electronic Business) initiiert wurde.

Ein Konsortium aus 13 Herstellern, Dienstanbietern, Forschungseinrichtungen und Beratungsunternehmen entwickelte eine Infrastruktur zur Untersuchung technischer Interoperabilitätsaspekte der Public Key-Zertifizierung. Darin wurden zahlreiche Produkte gegen eine Referenz-Implementation getestet, auf die man sich zuvor geeinigt hatte. Der Testplan umfasste auch die Cross-Zertifizierung von CAs sowie die Verifikation von Zertifikaten durch Endbenutzeranwendungen.

Der Abschlussbericht der PKI Challenge wurde am 29.04.2003 vorgelegt. Er enthält insbesondere technische Spezifikationen, die Beschreibung der durchgeführten Tests, der aufgetretenen Probleme sowie eine Reihe nützlicher Empfehlungen für den Aufbau von PKIs.

1.3 Signaturbündnis Niedersachsen

Das am 05.05.2003 veröffentlichte, vom Land Niedersachsen mit elf Unternehmen geschlossene „Bündnis für schnelle eSignatur-Lösungen Niedersachsen“ hat sich als Ziel gesetzt, flankierend zum Signaturbündnis der Bundesregierung bereits existierende Lösungen in Industrie und Verwaltung miteinander zu verknüpfen. Partner sind Cisco Systems, Deutsche Telekom, Microsoft Deutschland, BHW Bausparkasse, Empolis, Fujitsu-Siemens Computers, NordLB, Solvay, Volkswagen, die niedersächsischen Industrie- und Handelskammern und Sparkassen.

Mit der Initiative soll vor allem die private Nutzerakzeptanz gefördert werden. So können z. B. die mehr als 20.000 Mitarbeiterausweise der Volkswagen AG mit Signierfunktion zukünftig für elektronische Behördengänge genutzt werden.

1.4 ISIS-MTT-Compliance Criteria fertiggestellt

Die ISIS-MTT-Compliance-Criteria wurden am 26.05.2003 verabschiedet und am 27.05.2003 unter www.isis-mtt.org zum Download bereitgestellt. In diesem Dokument wird festgelegt, welche Kriterien ein Produkt erfüllen muss, um das Siegel „ISIS-MTT-konform“ und das entsprechende Logo führen zu dürfen.

Ziel der Siegelvergabe ist es, Anwendern schnell interoperable und damit einfach miteinander zu verwende Signatur- und Sicherheitsanwendungen zur Verfügung zu stellen.

Zum Erhalt des Siegels legen Hersteller oder Trustcenter-Betreiber in einem „Component Conformance Statement“ (CCS) fest, welchen Ausschnitt der ISIS-MTT-Spezifikation das Produkt erfüllt. Orientierung geben die in den Compliance Criteria festgelegten Produktklassen CA Server, OCSP Server, LDAP Server, VPN Server, Email-Client, SSL-Client, VPN-Client, Document-Signing Client, PKCS#11 Library, CSP und SigG conformant CSP. Zu den gewählten Funktionen ist ein Testbericht vorzulegen, der die mit Hilfe des von Secorvo entwickelten ISIS-MTT-Testbeds durchzuführenden Konformitäts-Tests belegt und dokumentiert.

Nach Prüfung des Berichtes durch ein zugelassenes Prüflabor (derzeit nur Secorvo) vergibt das ISIS-MTT-Board das Konformitätssiegel. Mit ersten Anträgen von interessierten Herstellern und Trustcenter-Betreibern wird in den kommenden Wochen gerechnet.

1.5 MS Windows Server 2003 Security Guide

Für Windows 2003 Server veröffentlichte Microsoft am 24.04.2003 einen „Security Guide“. In dem umfangreichen englischsprachigen Dokument werden zahlreiche ausführliche Hinweise zu Sicherungsmaßnahmen und dem Hardening von Systemen in Abhängigkeit vom Einsatzzweck (z. B. Domaincontroller, Fileserver etc.) gegeben. Sinnvolle Einstellungen werden vorgeschlagen und erläutert. Vervollständigt wird der Ratgeber durch Hilfsmittel wie Checklisten, Sicherheitsvorlagen und Skripte.

1.6 MS Patchmanagement

Das Tool HFNetChk des Herstellers Shavlik Technologies ermöglicht auf Microsoft-Betriebssystemen sowohl lokal als auch über das Netzwerk die Überprüfung des Patch-Levels. Die kürzlich freigegebene Version 4.0 erlaubt die Untersuchung einer Liste von Systemen (IP-Adressen) mit den Produkten Windows NT/2000/XP, IIS, MS-SQL Server, MS-Exchange Server, IE und MS-Office. Eine Funktion zum zentralen Download und dem Verteilen von Updates ist ebenfalls integriert.

Auf der HFNetChk-Engine basieren der Microsoft Baseline Security Analyzer (MBSA) und der Systems Management Server (SMS). Die kostenfreie Version von HFNetChkLT 4.0 kann bis zu 50 Systeme verwalten.

1.7 Aktuelle Security Advisories von Cisco

Nicht nur bei Microsoft werden mit schöner Regelmäßigkeit immer wieder neue Sicherheitslücken entdeckt – auch Netzwerkkomponenten, die ihr Dasein aus Sicht der meisten Anwender eher im Verborgenen fristen, sind davon betroffen und müssen ebenso wie Arbeitsplätze und Server in ein Patchmanagement einbezogen werden.

So veröffentliche Cisco am 08.05.2003 Advisories und Updates u. a. zu einem Buffer Overflow in der Administrationsoberfläche des ACS Authentifikationsservers und zu verschiedenen Schwächen im VPN 3000 Concentrator, die es im schlimmsten Fall erlauben, Firewalls per VPN-Gateway zu umgehen.

1.8 Security Tools: “Top 75”

Als Ergebnis einer Umfrage in der Newsgroup des Nmap Netzwerk-Scanners wurde eine Liste der 75 beliebtesten Sicherheits-Tools publiziert. Darin werden die Tools mit Bezugsquelle vorgestellt und bewertet. Diese Security Tools ermöglichen Administratoren, die Sicherheit ihrer Systeme und Netzwerke zu überprüfen – erleichtern allerdings auch die Durchführung von Angriffen.

2 Secorvo News

2.1 Secorvo College aktuell

Erstmalig führte Secorvo College vom 12. bis 16.05.2003 ein fünftägiges Seminar zum Information Security Management von A(udit) bis Z(ertifizierung) durch. Die positiven Rückmeldungen ermutigen uns, das Seminar erneut anzubieten – das nächste Mal in der Woche vom 22.-26.09.2003.

Vor der Sommerpause gibt es noch Gelegenheit zum Besuch zweier Seminare:

- Defense Lab – Life Hacking, Angriffstechniken und Gegenmaßnahmen, **17.-18.06.2003**
- IT-Sicherheit heute – Angriffe, Konzepte, Lösungen, **24.-26.06.2003**

2.2 Secorvo erstes ISIS-MTT-Prüflabor

Im Secorvo Security Labor werden seit 1999 IT-Sicherheitsprodukte im Kundenauftrag auf Funktionalität, Interoperabilität und Sicherheit geprüft. Vor der Beschaffung, Implementierung und Konfiguration komplexer Sicherheitslösungen werden zudem Integrationstests für Kundeninstallationen durchgeführt. Dafür stehen mehr als 300 Testinstallationen führender Sicherheitsprodukte (PKI, E-Mail, VPN, Firewall, Virenscanner etc.) bereit. Eine hohe Systematik bei der Testdurchführung und Dokumentation, sowie eine strikte Trennung der zu testenden Produkte durch Image-Dateien machen die Prüfergebnisse zudem reproduzierbar und übertragbar.

Am 14.05.2003 erhielt Secorvo vom ISIS-MTT-Board als erstes (und bisher einziges) Unternehmen die Zulassung als Prüflabor. Secorvo ist damit berechtigt, Konformitätstests für Hersteller von IT-Sicherheitssoftware und Betreiber von Trustcentern durchzuführen, auf deren Basis das ISIS-MTT-Board dann das ISIS-MTT-Konformitätssiegel vergibt.

2.3 Manche mögen's heiß

Nach einer spannenden Zeitreise durch die Geschichte der IT-Sicherheit (15.05.2003) lädt die Karlsruher IT-Sicherheitsinitiative, der die LuK GmbH & Co. oHG am 12.05. 2003 als neuer Partner beigetreten ist, zum nächsten Event: Am **03.07.2003** (18 Uhr) wird Oliver Stoll, Technical Director der WEB.DE AG, aus der Praxis des IT-Sicherheitsmanagements berichten – mit anschließendem Networking-Dinner am spanischen Buffet (u.A.w.g.).

3 Veranstaltungshinweise

Juni 2003	
17.-18.06.	Defense Lab (Secorvo College, Karlsruhe)
24.-25.06.	Security Awareness Symposium 2003 (Secorvo, Karlsruhe)
24.-26.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juli 2003	
03.07.	Manche mögen's heiß! (KA-IT-Si, Karlsruhe)
09.-10.07.	Einführung in die Praxis des betrieblichen DSB (Euroforum, Ffm)

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 Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Juni 2003

Dirk Fox, Stefan Gora, Stefan Kelm
Secorvo Security Consulting GmbH

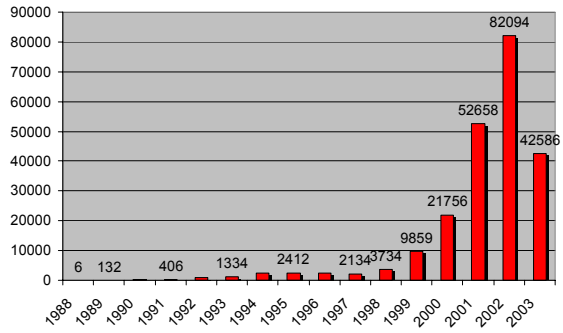
Nr. 6, 2. Jhrg. 2003
Stand 29. Juni 2003

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

Inhalt

Editorial: Keine Entwarnung

IT-Sicherheit ist kein neues Thema. Und auch die Bedrohungen, die durch die weltweite Vernetzung von Rechnern und Servern entstanden sind, dürften keinen Verantwortlichen mehr überraschen. Dennoch staunen gelegentlich selbst Experten: Die Zunahme der den CERTs gemeldeten Sicherheitsvorfälle mutet dramatisch an. In nur vier Jahren hat sich deren Anzahl verzwanzigfacht (2003: nur erstes Quartal).



Dabei berücksichtigen diese Zahlen nur die beobachteten Angriffe. Trotz steigender Sensibilität für IT-Sicherheit und verbesserter Schutzmechanismen erscheint es unwahrscheinlich, dass die Zahl der unerkannten Angriffe nicht ähnlich stark zugenommen hat.

Viele Unternehmen tragen dieser Entwicklung durch Sensibilisierung und Schulung der Mitarbeiter sowie regelmäßige Auditierung ihrer Sicherheitsinfrastruktur Rechnung. In wachsendem Maße gilt die Aufmerksamkeit auch Intrusion Detection Systemen, die die Aufdeckung „unbekannter" Eindringmethoden versprechen, sowie Methoden der Forensik, der „digitalen Spurensicherung", um im Entdeckungsfall eine gerichtsfeste Beweissicherung vornehmen zu können. Obwohl die Bedeutung der IT-Sicherheit in vielen Unternehmen kontinuierlich zunimmt und Bedrohungen immer professioneller begegnet wird, erlauben die schiere Zahl der Angriffe und die ständige Perfektionierung von (meist frei verfügbarer) Angriffssoftware keine Entwarnung.

IT-Sicherheit bleibt eine Herausforderung.

1 Security News

1.1 Bugs in Netzwerktreibern

Bei immer mehr Ethernetkarten wird ein Programmierfehler entdeckt, der bereits Anfang diesen Jahres veröffentlicht wurde: Durch eine fehlerhafte Initialisierung der Treibersoftware kann es vorkommen, dass „alter" Netzwerkverkehr beim Senden von IP-Paketen in Füll-Bytes übertragen wird. Das CERT/CC pflegt eine Liste aller betroffenen Netzwerktreiber, die regelmäßig aktualisiert wird.

1.2 Trojaner in vermeintlichem Windows-Update

Über die Webseite http://www.windows-update.com wird derzeit ein Trojanisches Pferd verteilt: Die vermeintliche Windows-Update-Datei update0932.exe enthält den Trojaner zasil. Schlimmer noch: Greift man mit dem Internet-Explorer ohne den Sammelpatch MS03-020 auf diese Datei zu, genügt das Aufrufen der Webseite, um den Schädling zu installieren.

Die offizielle Update-Seite von Microsoft unterscheidet sich von der gefälschten nur durch einen Bindestrich...

1.3 Sicherheitslücken in Lotus Notes

Kritische Schwachstellen in Betriebssystemen wie Windows und Linux sowie verbreiteten Anwendungen wie Sendmail oder dem Internet Explorer werden häufig veröffentlicht (vgl. auch die zurückliegenden Ausgaben der Secorvo Security News).

Dass auch andere, nicht weniger verbreitete Programmpakete von solchen Problemen betroffen sind, zeigt ein „CERT Advisory" vom 26.03.2003, welches gleich acht verschiedene Sicherheitslücken in Lotus Notes und Lotus Domino beschreibt.

Die Lücken erlauben unterschiedliche Angriffe über das Internet – so z. B. einen Denial-of-Service-Angriff gegen den Domino Web Server. Betroffen sind alle Lotus-Clients bis Version 5.0.12 und Server bis Version 6.0.1.

Da Lotus-Umgebungen in vielen Unternehmen zu den Standardanwendungen gehören, ist das Einspielen der Patches dringend zu empfehlen. Weil nicht alle Fehler durch die Patches korrigiert werden, empfiehlt sich zusätzlich ein Schutz betroffener Server durch geeignete Firewallregeln (z. B. blockieren von Port 1352/TCP).

1.4 Malware-Statistik

Die Kaspersky-Labs veröffentlichen allmonatlich eine Malware-Statistik der am häufigsten auftretenden Viren, Würmer und Trojaner. Nach dem Mai-Überblick vom 02.06.2003 dominieren die Würmer Sobig (22 %), Lentin (16 %) und Klez (15%) die Statistik mit riesigem Abstand vor Fizzer, dem Viertplatzierten (0,7 %).

1.5 Validierung von Zertifikatsketten

Zu den anspruchsvollsten – und in der Praxis leider noch immer weitest gehend ungelösten – Problemen einer jeden PKI gehört die Gültigkeitsprüfung von kompletten X.509-Zertifikatsketten bzw. –pfaden. Diesem Problem widmet sich seit einiger Zeit das US-amerikanische National Institute of Standards and Technology (NIST) mit der „Public Key Interoperability Test Suite (PKITS)". Ausgehend von einer Testspezifikation sowie etablierten PKI-Standards (z. B. X.509 und RFC 3280) wurde am 15.05.2003 eine neue Version der Test-Suite (v1.07) mit ausführlicher Beschreibung (pdf/zip, 311 kB) veröffentlicht, welche Hunderte von Zertifikaten, Sperrlisten, PKCS12-Dateien und S/MIME-Nachrichten enthält. Sie sollen zunächst eigenen Tests dienen. In einer weiteren Stufe soll später eine Referenzmenge der wichtigsten Tests definiert werden.

Vergleichbare Zertifikatspfad-Validierungen enthält auch das Mitte des vergangenen Jahres von Secorvo im Auftrag des TeleTrusT e.V. auf Open Source-Basis entwickelte ISIS-MTT Testbed, dessen Release 1.1 (Build 5) am 28.05.2003 freigegeben wurde.

1.6 Neuer Microsoft Guide

Seit dem 12.06.2003 ist ein neuer Ratgeber von Microsoft mit dem Titel „Improving Web Application Security“ (pdf, 5,8 MB) verfügbar. In dem über 900 Seiten starken englischsprachigen Dokument werden ausführliche Hinweise zur Konzeption und zum Betrieb sicherer Web-Applikationen gegeben. Gefährdungen und geeignete Schutzmaßnahmen werden allgemein und für Microsoft-Produkte vorgestellt. Der Guide enthält zusätzlich Checklisten und „How Tos“.

1.7 BSI-Studien zu Webservern

Zwei umfangreiche Studien hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) der Sicherheit der beiden derzeit verbreitetsten Webserver gewidmet: Microsofts Internet Information Server (IIS 4.0) und dem Open Source-Server Apache (v1.3 und v2.0).

Die beiden mehr als 150 Seiten starken Studien geben neben einer Einführung in die jeweilige Software eine Bewertung der Sicherheit der untersuchten Versionen und Hinweise für eine sichere Konfiguration und Administration. Da die den im April 2003 publizierten Ergebnissen zu Grunde liegenden Analysen bereits im November 2002 abgeschlossen wurden, müssen außerdem aktuelle Sicherheitshinweise der jeweiligen Hersteller berücksichtigt werden.

1.8 NIST-Empfehlung: MAC

Das US-amerikanische National Institute of Standards and Technology (NIST) arbeitet an einer Empfehlung für MAC-Algorithmen (Message Authentication Codes) auf der Basis von Blockchiffren. Der Draft der NIST Special Publication 800-38B vom November 2002 empfahl ursprünglich den Algorithmus RMAC als Ersatz für den durch eine „Konkatenations-Fälschung“ gebrochenen CBC-MAC (Cipher Block Chaining) des ISO-Standards 9797-1.

Aufgrund zahlreicher kritischer Kommentare sind anstelle der RMAC-Empfehlung nun EMAC und XCBC im Gespräch. Auf der Webseite des NIST findet sich seit dem 06.06.2003 eine Kurzbewertung der wesentlichen Eigenschaften aller drei MAC-Verfahren. Expertenkommentare sind explizit erbeten; die Kommentierungsfrist endet am 03.07.2003.

1.9 USENIX Security Symposium 2003

Bereits zum 12. Mal findet vom 04.-08.08.2003 mit dem USENIX Security Symposium eine der weltweit wichtigsten und innovativsten Sicherheitskonferenzen statt – diesmal in Washington, DC.

Auch in diesem Jahr besteht die Konferenz aus zwei parallelen Tracks: Neben der üblichen Vorstellung der eingereichten Konferenzbeiträge wird es wieder 90-minütige Spezialvorträge von eingeladenen Sprechern geben. Das Rahmenprogramm umfasst ferner ganztägige Tutorials, auf denen hochkarätige IT-Sicherheitsexperten detailliert zahlreiche Praxisthemen behandeln.

2 Secorvo News

2.1 Secorvo College aktuell

Ende Juni hat Secorvo College einen dritten Ausbildungspartner gewonnen: Neben der SAP AG und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ergänzen die Seminare von Secorvo College von nun an auch das Weiterbildungsangebot der T-Systems International GmbH.

Zum Vormerken: Ende September findet zum zweiten Mal das fünftägige Intensiv-Seminar „Information Security Management“ statt. Neben einer Einführung in alle relevanten Standards ist ein großer Teil des Seminars „Best Practices“ gewidmet.

2.2 Lotus PKI White Paper

Ab sofort ist ein neues Secorvo White Paper zum Thema „Einsatz der Lotus Domino-PKI 6“ elektronisch verfügbar (pdf, 149 kB). Das 24 Seiten starke Dokument beschreibt kompakt, wie die aktuelle Version 6 von Lotus Notes / Domino zur Realisierung von Sicherheitslösungen auf der Basis von X.509-Zertifikaten genutzt werden kann. Es fasst die Ergebnisse von umfangreichen Tests im Secorvo Security-Labor zusammen und richtet sich vor allem an Projektleiter und Mitarbeiter, die für den Einsatz und die Nutzung von Notes im Unternehmen verantwortlich sind.

2.3 Awareness-Symposium

Mit knapp 60 Teilnehmern, spannenden Vorträgen und intensiven Diskussionen war das erstmalig von Secorvo durchgeführte „Security Awareness Symposium 2003“ ein großer Erfolg. Die Teilnehmerunterlagen können über die Webseite bestellt werden.

2.4 Forensik-Konferenz

Die Fachgruppe SIDAR (Security – Intrusion Detection and Response) der Gesellschaft für Informatik e. V. (GI) veranstaltet vom 24.-25.11.2003 die erste Tagung „IT-Incident Management & IT-Forensics“. Auf der Tagung werden alle Fragen rund um die Behandlung von IT-Sicherheitsvorfällen – von der Erkennung und Bewertung von Angriffen bis hin zur Beweissicherung – diskutiert. Stefan Kelm (Secorvo) ist Mitglied des Programmkomitees, welches um Einreichung von Konferenzbeiträgen bis zum 30.06.2003 bittet.

3 Veranstaltungshinweise

Juli 2003	
03.07.	"Manche mögen's heiß" - Event zum IT-Sicherheitsmanagement (KA-IT-Si, Karlsruhe)
09.-10.07.	Einführung in die Praxis des betrieblichen DSB (Euroforum, Ffm)
20.-23.07.	31st Annual International Conference on Computer Audit, Control and Security (ISACA, Singapore)
August 2003	
04.-08.08.	12th USENIX Security Symposium (USENIX, Washington D.C.)
26.-27.08.	Einführung in die Praxis des betriebl. DSB (Euroforum, Berlin)
September 2003	
22.-26.09.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
29.09.-02.10.	Informatik 2003 – Teiltagung Sicherheit (GI, Frankfurt)
30.09.-01.10.	SAP-Sicherheit im Betrieb (Secorvo College, Karlsruhe)

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 Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Juli 2003

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch

Secorvo Security Consulting GmbH

Nr. 7, 2. Jhrg. 2003
Stand 24. Juli 2003

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

Inhalt

Editorial: Vertrauensfrage(n)

Zuviel Vertrauen ist häufig eine Dummheit,
zuviel Misstrauen immer ein Unglück.
Johann Nestroy

Leicht geht uns in der IT-Sicherheit das Wörtchen „Vertrauen“ über die Lippen: Wir sprechen von dem Sicherheitsziel „Vertraulichkeit“, von „Vertrauensinfrastrukturen“ und „vertrauenswürdigen Dritten”. Tatsächlich aber sind Schutzmaßnahmen nichts anders als „institutionalisiertes Misstrauen“: Wir schützen uns, weil wir hinsichtlich der Vertrauenswürdigkeit unserer zunehmend digitalen Welt so unsere Zweifel hegen.

Für diese vorsichtige Haltung gibt es viele gute Gründe. Allerdings: Im „wirklichen Leben“ gründen unser zwischenmenschlicher Umgang und unser Wirtschaftsleben auf dem Gegenteil – einer vorwiegend von Vertrauen geprägten Haltung unseren Kollegen, Kunden und Geschäftspartnern gegenüber. Das ist, wie wir heute wissen, nicht nur gut so, sondern auch volkswirtschaftlich bedeutsam: Die wirtschaftliche Entwicklung eines Landes wird inzwischen über „Vertrauensindizes“ prognostiziert.

Tatsächlich vertrauen wir fast täglich „blind“ – z. B. darauf, dass unser Gesprächspartner am Telefon auch derjenige ist, der zu sein er behauptet, dass ein Fax oder eine E-Mail vom angegebenen Sender stammt (wofür es technisch keinen Beleg gibt), und dass ein Gast oder Besucher die auf der Visitenkarte genannte Person ist. Das geht auch fast immer gut – und bestärkt uns in unserem Verhalten. Gefährlich wird es, wenn diese Vertrauensseligkeit ausgenutzt wird und dabei Schäden entstehen, wie z. B. im jüngst bekannt gewordenen Fall einer vermeintlichen Bestellung von 6.000 Kfz von Citroën durch das österreichische Innenministerium.

Dieses Dilemma ist die zentrale Herausforderung für die Informationssicherheit: Ihr muss das Kunststück gelingen, bei Kollegen und Mitarbeitern eine Prise gesunder Skepsis in das notwendige Grundvertrauen zu mischen – ohne Flexibilität und Kundenorientierung zu beeinträchtigen.

1 Security News

1.1 Kreditkartenmissbrauch analysiert

Das Bestellen von Waren und Dienstleistungen per Internet wird auch in Deutschland immer beliebter. In zunehmenden Maße wird dabei – nicht zuletzt aus Bequemlichkeit – auch die Zahlung über E-Mail oder Web-Formular abgewickelt, häufig unter Angabe der Kreditkartennummer.

Dass solche Transaktionen potenziell gefährlich sind, ist lange bekannt. Nun hat es zum ersten Mal eine Gruppe von Securityexperten aus dem „Honeynet"-Projekt geschafft, genauere Informationen über die Vorgehensweise der „Carders" beim Kreditkartenmissbrauch zu dokumentieren. Die Gruppe beobachtete über einen Zeitraum von mehreren Jahren verschiedene einschlägige Foren, insbesondere IRC-Netze, und veröffentlichte am 23.06.2003 ihre Ergebnisse in dem Bericht "Know Your Enemy: Automated Credit Card Fraud".

Besonders interessant ist die Darstellung heutiger „Carder"-Infrastrukturen, die inzwischen über stark automatisierte Tools verfügen sowie Informationen über Online-Händler verbreiten, die keine oder schwache Sicherheitsmechanismen einsetzen.

1.2 CERT-Statistik Q2/2003

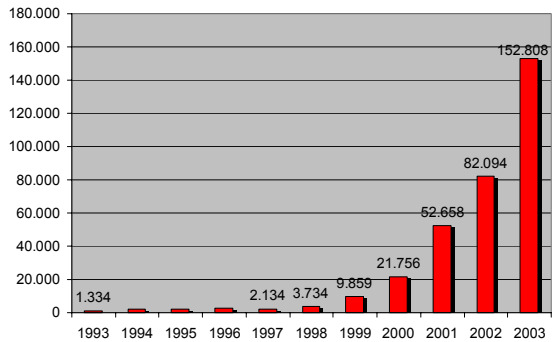


Abb. 1: Gemeldete Sicherheitsvorfälle des CERT/CC (2003: Prognose)

Am 15.07.2003 hat das CERT Coordination Center (CERT/CC) seine Quartalsstatistik veröffentlicht. Danach steigt die Zahl der berichteten Vorfälle nach wie vor steil – für die erste Jahreshälfte 2003 liegt der Wert knapp unter dem des Gesamtjahres 2002.

1.3 Bug in Microsofts HTML-Konverter

Das Konvertieren von Dateien in andere Formate ist eine Funktion des Microsoft Windows Betriebssystems. Sie ermöglicht Anwendungen z. B. die Anzeige und Speicherung von Dateien in HTML. Ein Fehler in der cut-and-paste Operation dieser Konverter-Routine wurde am 09.07.2003 publiziert. Er ermöglicht einem Angreifer, mit einer geeignet gestalteten HTML-E-Mail oder einer Webseite beliebigen Code auf dem Rechner des E-Mail-Empfängers respektive Web-Surfers (sofern dieser den Internet-Explorer verwendet) auszuführen.

Sicherheitseinstufung:

Windows 98/98 SE Windows NT 4.0 Server Windows 2000/XP	kritisch
Windows Server 2003	mittel

1.4 To update or not to update …

Seit dem 26.06.2003 ist das neue Windows 2000 Service Pack 4 verfügbar. Es enthält eine Vielzahl neuer Patches und alle Updates der vorhergehenden Service Packs. Die Installation verursacht allerdings in einigen Fällen Probleme: So warnt Microsoft vor Schwierigkeiten bei der Kombination von Terminaldiensten und dem .Net Framework 1.0 und einem Fehlverhalten des Key Management Service von Microsoft Exchange. Weitere Probleme traten beim Einsatz von Norton Internet Security 2001 auf: Nach der Installation von SP 4 war kein Internetzugriff mehr möglich. Symantec hat ein Update erstellt, welches mit der Option „Live-Update" *vor* der Installation des SP 4 heruntergeladen werden sollte.

In der Regel ist aus Sicherheitsgründen die Installation der aktuellsten Servicepacks zu empfehlen. Die Beispiele zeigen, dass dies jedoch nicht ohne vorausgehende Tests erfolgen sollte.

1.5 Bremen „Europäischer eGovernment Champion“

Bremen ist Sieger der Champions League des eGovernments: Aus dem Wettbewerb um den EU-Preis für vorbildliche Beispiele elektronischer Verwaltungsdienste ist bremen online services (bos), die eGovernment-Strategie der bremischen Verwaltung, am 08.07.2003 als Sieger in der Kategorie „Europäische Konkurrenzfähigkeit" hervorgegangen.

1.6 Hosten Sie Schmuddel-Seiten?

Die Spammer-Branche macht Ernst mit der Anonymität – zumindest mit der eigenen. Der am 11.07.2003 im Internet neu aufgetauchte Trojaner Migmaf erlaubt es, die Rechner nichts ahnender Remote- und Heim-Nutzer (bevorzugt solcher mit „always-on” DSL- oder Kabelmodem-Anschlüssen) nicht nur als Versender von Spam-Mails, sondern auch als Proxy-Server zu missbrauchen: Die Links in den verschickten Spam-E-Mails verweisen dabei nicht direkt auf den Webserver mit den beworbenen Inhalten, sondern auf einen der infizierten PCs; von dort leitet der Trojaner den Zugriff weiter.

Die Spammer sind dabei technisch auf der Höhe der Zeit: Per dynamischem DNS wird in Minutenabständen die IP-Adresse eines anderen missbrauchten PCs verwendet. Dadurch wird es Internet Service Providern praktisch unmöglich gemacht, die von den Spammern benutzten Systeme über eine IP-Filterung auszusperren.

Schutz vor dem beschriebenen Kapern durch Spammer (siehe Abb. 2) bietet eine sauber konfigurierte Personal Firewall.

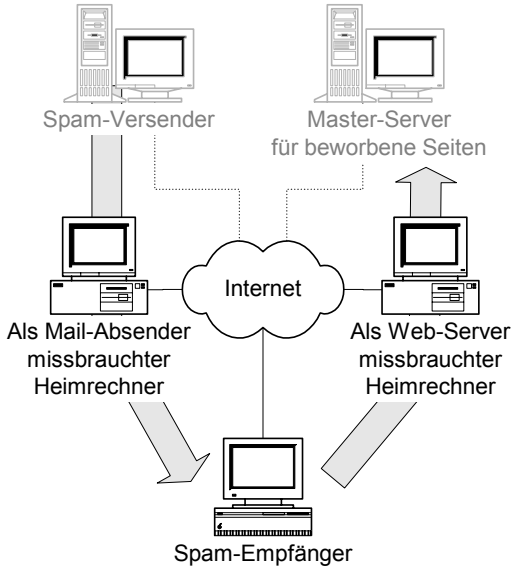


Abb. 2: Funktionsweise eines Trojaner-Spammers

1.7 Gefahr erkannt – Gefahr gebannt?

Zwei aktuelle Meldungen belegen, dass einige Sicherheitsprobleme trotz großer Publicity hartnäckig weiter bestehen:

Richard Smith – bekannt durch seine Untersuchungen über unerwünschte Zusatzinformationen in Office Dokumenten – meldete am 03.07.2003, dass noch immer viele Softwarehersteller ihre ActiveX-Controls als „sicher für Scripting“ markieren, obwohl sie bekannte Sicherheitsmängel aufweisen. Das legt den Verdacht nahe, dass sich die Prüfung dieser Hersteller auf „Absturzsicherheit“ beschränkt. Und die russische Softwarefirma ElcomSoft, deren Rechtsstreit mit Adobe weltweit Schlagzeilen machte, berichtet am 08.07.2003, dass auch zwei Jahre nach der ersten Veröffentlichung die von ElcomSoft entdeckten Sicherheitslücken in Acrobat und Acrobat Reader noch nicht beseitigt sind.

1.8 Denial of Service auf Ciscos IOS

Mit geeignet konstruierten IPv4-Paketen kann ein Denial-of-Service Angriff gegen

IOS-basierte Router von Cisco durchgeführt werden – das wurde am 16.07.2003 bekannt. Cisco stellt Vertragskunden Updates online zur Verfügung. Zur Erleichterung der Prüfung, ob eigene Geräte betroffen sind, hat Foundstone, Inc. eine Funktion zur Bestimmung der IOS-Version in das kostenfreie Tool SNS-Scan integriert.

2 Secorvo News

2.1 Secorvo College aktuell

Auf dem überarbeiteten Seminar „SAP-Sicherheit im Betrieb“ (30.09.-01.10.2003) beleuchten erfahrene Praktiker SAP-Systeme hinsichtlich der Stärken und Schwächen der Sicherheitsarchitektur und Sicherheitsfunktionalitäten von allen Seiten. Im Mittelpunkt stehen Konzepte und Maßnahmen zur Erreichung eines adäquaten Sicherheitsniveaus.

2.2 Neues Video zur „E-Mail Sicherheit“

Dass E-Mails offen wie eine „Postkarte” im Internet übertragen werden, gehört erfreulicherweise inzwischen fast zum Allgemeinwissen. Weniger bekannt ist allerdings, wie leicht es tatsächlich ist, mit frei verfügbaren Tools E-Mails abzuhören oder zu fälschen. Das ist vor allem deshalb bedenklich, weil immer mehr sensible Daten elektronisch übermittelt werden.

Um Mitarbeiter für einen bedachtsameren Umgang mit E-Mails zu sensibilisieren, hat Secorvo ein Lehrvideo entwickelt, das eindrucksvoll Angriffe auf elektronische Nachrichten demonstriert. Es hat eine Spielzeit von zehn Minuten und kann mit gängigen Flash-Playern abgespielt werden.

2.3 PKI-Symposium 2003

Noch ist das Programm in Vorbereitung – der Termin steht aber bereits: Das (vierte) „PKI-Symposium 2003“ wird am 07. und 08.10.2003 in Karlsruhe stattfinden. Über die Webseite können Sie sich schon jetzt einen Platz reservieren. Dort finden Sie auch Programme und Materialien der Symposien der Jahre 2000, 2001 und 2002.

3 Veranstaltungshinweise

August 2003	
04.-08.08.	12th USENIX Security Symposium (USENIX, Washington D.C.)
26.-27.08.	Einführung in die Praxis des betriebl. DSB (Euroforum, Berlin)
September 2003	
08.-10.09.	6th Internat. Symposium on Recent Adv. in Intrusion Detection RAID 2003 (CERT/CC, Pittsburg)
22.-26.09.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
29.09.-02.10.	Informatik 2003 – Teiltagung Sicherheit (GI, Frankfurt)
30.09.-01.10.	SAP-Sicherheit im Betrieb (Secorvo College, Karlsruhe)
Oktober 2003	
07.-08.10.	PKI-Symposium 2003 (Secorvo, Karlsruhe)

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 Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
August 2003

Dirk Fox, Hans-Joachim Knobloch,
Holger Mack, Dr. Markus Michels
Secorvo Security Consulting GmbH

Nr. 8, 2. Jhrg. 2003
Stand 22. August 2003

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

Inhalt

Editorial: „Eisberg rechts voraus!“

Der entsetzte Ruf vom Ausguck der Titanic, ausgestoßen am 14. April 1912 um 23:40 Uhr, steht für ein Ereignis, das die Welt erschüttert hat: den qualvollen und vermeidbaren Tod von über 1.500 Passagieren, verursacht durch die Hybris der Techniker, die das Schiff als „unsinkbar“ erklärten und nur 20 Rettungsboote vorsahen – zu wenig selbst für die Hälfte der Reisenden.

Haben wir aus diesem Unglück gelernt? Natürlich sind Unternehmens- und Behördennetze heute mit einer Firewall abgesichert. Was aber, wenn diese vom „Eisberg“ erwischt wird – durch einen unentdeckten Software-Fehler oder eine scheinbar harmlose Kommunikationsverbindung, die tatsächlich einen Trojaner auf Client-Systemen installiert, wie der aktuelle Blaster-Wurm?

Bei der Titanic mussten immerhin fünf Schotten volllaufen, bevor sie sank. Nur hatte niemand mit einem Eisberg gerechnet, der gleich fünf der Länge nach aufriss. In unseren Kommunikationsnetzen geben wir uns häufig mit einem Schott zufrieden – und glauben einfach nicht an den Eisberg. Wie Kapitän E.J. Smith: „*When anyone asks me how I can best describe my experience in nearly forty years at sea, I merely say, uneventful. (…) I never saw a wreck and never have been wrecked nor was I ever in any predicament that threatened to end in disaster of any sort.*“ (New York Times-Interview kurz vor der verhängnisvollen Jungfernfahrt der Titanic).

Kommt uns das nicht bekannt vor? „Bei uns ist noch nie etwas passiert.“ Stimmt vielleicht. Wenigstens hat es niemand bemerkt. Dürfen wir aber daraus Aussagen über die Zukunft ableiten? Da lohnt es, sich das Bonmot von Winston Churchill auf der Zunge zergehen zu lassen:

„*Der beste Zeitpunkt für eine Prognose ist kurz nach dem Ereignis.*“
Allerdings hilft sie dann nicht mehr viel.

1 Security News

1.1 Yet Another Worm – was tun gegen Blaster & Co.?

Wieder einmal treibt ein Wurm Publicity-trächtig sein Unwesen im Internet – diesmal quasi mit vorheriger Ansage. Die wichtigsten Maßnahmen, um sich vor den wohl unvermeidlichen Nachfolgern von Blaster, Slammer, Sobig & Co. zu wappnen, sind:

- Ein aktueller Virenscanner auf jedem (Windows-) PC gehört heute ebenso zum „Standard“ wie die Beherzigung einiger genereller Empfehlungen.
- Da vor allem Microsoft-Systeme im „Bull’s Eye“ der Virenschreiber stehen, ist das umgehende Einspielen kritischer Sicherheitsupdates hier besonders wichtig. Es wird mittlerweile von Microsoft durch einen E-Mail-Benachrichtigungsdienst unterstützt.
- PCs von Kleinunternehmen und Privatanwendern, ganz besonders solche mit „always-on“ Internetanschluss, müssen mit einer Personal-Firewall geschützt sein, die so konfiguriert ist, dass sie unerwartete Datenverbindungen nur nach manueller Freigabe zulässt oder generell blockiert.
- Unternehmen mit großen Netzen sollten Netzbereiche durch interne Firewall-Filter separieren. Im Fall eines Befalles ist es dann möglich, Würmer in kleineren Netzbereichen zu isolieren – wie Schotten im Ozeandampfer gegen eindringendes Wasser.

Gegen einen hässlichen Effekt der aktuellen Würmer ist kein Kraut gewachsen: Sobig verschickt seine Kopien unter Angabe falscher Absenderadressen, die er wie die Zieladressen auf einem infizierten System gefunden hat. Dadurch können Unbeteiligte in Verdacht geraten, Viren zu verschicken, auch wenn ihr System gar nicht infiziert ist. Technisch versierte Empfänger können zwar am E-Mail-Header erkennen, dass mit dem Transportweg der Nachricht etwas nicht stimmt. Doch auch diese versteckten Hinweise könnte schon die nächste Wurm-Generation verschleiern.

1.2 Web-Application Hacking

Firewalls und auch die verbreiteten Tools für Penetrationstests konzentrieren sich meist auf Angriffe auf der Netzwerkebene. Angriffe auf Anwendungsebene werden oft nicht erkannt. Kein Wunder, dass „Web-Application Hacking“ sich zunehmender Beliebtheit erfreut. Angriffe wie Cross-Site Scripting oder SQL Injection werden per HTTP-Protokoll getunnelt – gerne zynisch als „Firewall-friendly“ bezeichnet – und sind nur schwer von normalem Netzverkehr zu unterscheiden; teilweise entziehen sie sich sogar per SSL-Verschlüsselung dem Zugriff der Firewall.

Da andererseits Web-Applikationen in zunehmendem Maße für den Zugriff auf kritische Geschäftsdaten und Anwendungen eingesetzt werden, besteht dringender Handlungsbedarf. Leider ist die Suche nach Schwachstellen hier erheblich schwieriger zu automatisieren als auf Netzwerkebene, da Web-Applikationen häufig Eigenentwicklungen und die Schwachstellen damit meist „hausgemacht“ sind.

Eine dreiteilige Online-Artikelserie „Penetration Testing for Web Applications“ von Jody Melbourne und David Jorm, deren abschließender Teil am 20.08.2003 erschien, stellt typische Schwachstellen von Web-Applikationen vor und führt in das geeignete Vorgehen bei Penetrationstests ein. Zum gefahrlosen Erproben und Simulieren von Angriffen auf Web-Applikationen empfiehlt sich das freie Tool WebGoat.

1.3 Computerkriminalität statistisch

Das Bundeskriminalamt schlüsselt jährlich die erfassten Fälle von Computerkriminalität auf. Danach waren im Jahr 2002 zwei Drittel der insgesamt um 27,5 % auf 57.288

zurückgegangenen Fälle ein Betrug mittels rechtswidrig erlangter Debitkarten mit PIN.

Bei Computersabotage und Datenveränderung verzeichnet die Kriminalstatistik einen Anstieg um 54 % auf 1.327 Fälle. Die Aufklärungsquote erreicht im Durchschnitt respektable 50 %; bei Fällen von Datenveränderung und Computersabotage, die auch nicht autorisierte Zugriffe auf Rechner („Einbrüche“, „Hacking“) umfassen, lag sie mit 38 % unter dem Durchschnitt.

1.4 IT Security Benchmarks

Je stärker IT-Investitionen in den suchenden Blick der Controller geraten, desto wichtiger werden belastbare ROI-Nachweise. Dass solche Nachweise für die IT-Sicherheit besonders schwierig zu führen sind, ist ein offenes Geheimnis.

Ein viel versprechender Ansatz ist die Bestimmung von IT Security Benchmarks, die das erreichte Sicherheitsniveau und die Entwicklung der IT-Sicherheit im Unternehmen in Relation zu den Zielen bzw. im Vergleich zum Niveau anderer Unternehmen der Branche bewerten.

Das National Institute of Standards and Technology (NIST) hat am 12.08.2003 einen „Security Metrics Guide for Information Technology Systems“ veröffentlicht, der primär US-Behörden den Nachweis erleichtern soll, dass und in welchem Grad sie gesetzlichen Anforderungen an die IT-Sicherheit genügen.

Der Ansatz ist aber von weit allgemeinerem Interesse. Er beschreibt einen Prozess, mit dem – ausgehend von den Interessen der beteiligten Parteien, allgemeinen Organisationszielen und Sicherheitsleitlinien – eine passende IT Security Metrik entwickelt werden kann.

Im Anhang, der etwa zwei Drittel des knapp 100-seitigen Dokuments ausmacht, werden Beispielmetriken dargestellt, die auf dem bereits früher publizierten „Security Self-Assessment Guide for Information Technology Systems“ des NIST beruhen.

1.5 Linux erhält Common-Criteria-Zertifikat des BSI

Der „SuSE Linux Enterprise Server V8 with certification-sles-eal2 package“ der SuSE Linux AG hat am 28.07.2003 als erstes Open Source Betriebssystem ein Sicherheitszertifikat nach Common Criteria (CC) erhalten. Die Sicherheitsmechanismen dieser Linux-Version (User Identifikation, Authentifikation, Login-Prozess, ACLs, Rollen, User-Management etc.) wurden auf IBM xSeries 335 und 440 Systemen gemäß Zertifizierungslevel EAL2+ geprüft.

Details und nähere Informationen zu den geprüften Versionsständen der Komponenten des Linux-Softwarepakets finden sich im 55-seitigen Certification Report des BSI und in den 60-seitigen Sicherheitsvorgaben, nach denen evaluiert wurde. Anzumerken ist, dass keines der registrierten Protection Profiles nach CC zu Grunde gelegt wurde; die Linux-Version erfüllt lediglich eine Untermenge des Controlled Access Protection Profile.

Über die Aussagekraft einer CC-Zertifizierung hat Jonathan Shapiro (Johns Hopkins University) eine lesenswerte, ebenso kritische wie humorvolle Betrachtung verfasst.

1.6 Bundesbank tritt European Bridge-CA bei

Nach der SAP AG ist auch die Deutsche Bundesbank der European Bridge-CA beigetreten, einer Public Private Partnership unter der Leitung von TeleTrusT Deutschland e.V., an deren Konzeption auch Secorvo mitgewirkt hat. Damit können künftig Mitarbeiter der Bundesbank ohne weiteres S/MIME-Nachrichten mit den PKI-Nutzern der Bundesverwaltung, der Deutschen Bank AG, der SAP AG, der Siemens AG und der Telekom AG austauschen.

Die S/MIME-Interoperabilitätstests der Bridge-CA haben bereits weitere Unternehmen bestanden: BMW AG, Bundeswehr, Dresdner Bank AG, TC TrustCenter GmbH und Secartis AG.

1.7 WBT Datenschutz

Unter der fachlichen Mitwirkung von Dr. Johann Bizer, Herausgeber der Zeitschrift Datenschutz und Datensicherheit, hat der E-Learning-Spezialist digital spirit ein Web Based Training (WBT) zum Datenschutz im Unternehmen entwickelt.

2 Secorvo News

2.1 Secorvo College aktuell

Das fünftägige Intensivseminar „Information Security Management“ vom **22. bis 26.09.2003** erfreut sich schon jetzt zahlreicher Anmeldungen und verspricht daher nicht nur einen vertieften Einblick in Theorie und Praxis des ISM, sondern auch einen wertvollen Erfahrungsaustausch.

Die thematische Einführung an den beiden ersten Tagen des Seminars kann auch einzeln gebucht werden (aktuelle Seminarübersicht).

2.2 PKI-Woche 2003

Vom **06. bis 09.10.2003** steht der Technologiepark Karlsruhe unter dem Zeichen der „PKI-Woche 2003“. Sie beginnt mit dem Seminar „Public Key Infrastrukturen“, das eine umfassende, zweitägige Einführung in das Thema bietet, gefolgt vom schon traditionellen „PKI-Symposium“ mit Praxisberichten und aktuellen Themen, und schließt mit einem eintägigen Vertiefungsseminar am 09.10.2003 zu ausgewählten Themen der PKI-Realisierung.

Vier Tage intensives Erfahrungswissen, die auch getrennt gebucht werden können. Bis **02.09.2003** gilt der **Frühbucherrabatt**.

3 Veranstaltungshinweise

September 2003	
08.-10.09	5th Workshop on Cryptographic Hardware & Embedded Systems (CHES 2003, Köln)
16.-17.09.	Signatur Workshop 2003 (RegTP, Mainz)
22.-26.09.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
29.09.-02.10.	Informatik 2003 – Teiltagung Sicherheit (GI, Frankfurt)
30.09.-01.10.	SAP-Sicherheit im Betrieb (Secorvo College, Karlsruhe)
Oktober 2003	
	„PKI-Woche“ (Secorvo und Secorvo College)
06.-07.10.	Public Key Infrastrukturen (Secorvo College, Karlsruhe)
07.-08.10.	**PKI-Symposium 2003** (Secorvo)
09.10.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
07.-09.10.	ISSE 2003 (EEMA und TeleTrusT, Wien)
14.-15.10.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.10.	Defense Lab (Secorvo College, Karlsruhe)
November 2003	
10.-11.11.	ZertiFA 2003 (Computas, Köln)

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 Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
September 2003

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

Nr. 9, 2. Jhrg. 2003
Stand 22. September 2003

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

Inhalt

Editorial: Happy Birthday

Der 01.09.2003 war für Secorvo ein besonderes Datum. Daher erlauben wir uns diesmal ein Editorial in eigener Sache: Auf den Tag genau am 01.09.1998 hat die Secorvo Security Consulting GmbH mit fünf Mitarbeitern das „Licht der Welt“ erblickt. Zwischen diesen beiden Daten liegen 1.826 ereignisreiche Tage: 167 erfolgreiche Projekte, 135 Publikationen, 133 öffentliche Vorträge, 58 Seminare von Secorvo College mit mehr als 600 überdurchschnittlich zufriedenen Teilnehmern (Note 1,45) aus mehr als 200 Unternehmen und Behörden, und weit über eine Million Webseitenzugriffe.

Secorvo entstand 1998 aus der Vision eines vollständig unabhängigen, ausschließlich den eigenen Kunden verpflichteten und auf IT-Sicherheit spezialisierten Beratungsunternehmens mit besonders kompetenten und erfahrenen Consultants, die durch aktives Engagement in Fachgremien, durch die Mitgestaltung von Normen und Standards der IT-Sicherheit und nicht zuletzt durch Publikationen und hochwertige Projektarbeit einen nachhaltigen Beitrag zur Verbesserung der IT-Sicherheit in Unternehmen und Behörden leisten.

Dieser Vision sind wir treu geblieben – und konnten sie auch in vielerlei Hinsicht Wirklichkeit werden lassen: So ist das Beratungsteam auf zehn anerkannte Experten für IT-Sicherheit angewachsen, Standards wie MailTrusT und ISIS-MTT wurden maßgeblich von Secorvo entwickelt, und namhafte mittelständische und zahlreiche große Unternehmen sowie Landes- und Bundesbehörden haben Secorvo in den vergangenen fünf Jahren mit herausfordernden Projekten betraut.

Dass dieser Erfolg möglich war, verdanken wir neben dem Engagement und dem Einsatz unseres inzwischen 16-köpfigen Teams vor allem den vielen Kunden, die auf Secorvo vertraut haben. Wir sind stolz darauf, deren hohe Erwartungen nicht enttäuscht zu haben – für die Zukunft Ansporn und Anspruch zugleich.

1 Security News

1.1 PGP in neuem Gewand

Am 16.09.2003 stellte die PGP Corp. in London ihr neuestes Software-Release – „PGP Universal“ – der Öffentlichkeit vor. Diese neue Version basiert auf der seit über einem Jahrzehnt bekannten und verbreiteten Verschlüsselungssoftware von Phil Zimmermann, unterscheidet sich aber konzeptionell erheblich von allen Vorgängerversionen: PGP Universal implementiert eine serverbasierte (proxy-artige) Lösung, die transparent und automatisch sämtliche E-Mails (oder solche für festgelegte Kommunikationspartner) ver- und entschlüsselt. Auch mit Kommunikationspartnern, die über kein Schlüsselpaar verfügen, kann man mit PGP Universal gesichert kommunizieren.

Die wichtigste Neuerung bilden sogenannte „Domain Policies“, die es ermöglichen, eine organisationsweite Security Policy zentral zu definieren und duchzusetzen. Damit ist PGP Universal insbesondere für Unternehmen und Behörden interessant. Eine Übersicht finden Sie in einem Beitrag von Dr. Rainer Gerling und Stefan Kelm in der Zeitschrift „DuD“ (10/2003).

Zum Vormerken für Interessierte: Secorvo bietet am 03.-04.12.2003 ein zweitägiges Seminar an, in dem der betriebliche Einsatz von PGP, auch der neuen Produktversion, im Detail beleuchtet wird.

1.2 Kritischer RPC-Bug

Eine neue, als sehr kritisch einzustufende Schwachstelle im RPC-Dienst der Betriebssysteme Windows NT 4.0, 2000, XP und 2003 wurde am 10.09.2003 vom Microsoft veröffentlicht. Sie erlaubt einem Angreifer, über das Protokoll Netbios durch einen Heap Overrun beliebigen Code auf dem Zielsystem auszuführen. Eine Erläuterung mit Patch findet sich im Microsoft Security Bulletin MS03-039.

Delikat: Seit dem 16.09.2003, nur sechs Tage nach Veröffentlichung, ist im Internet ein Exploit zu finden, dass diese Schwachstelle ausnutzt. Wir testeten den Angriffscode im Secorvo Security Labor: Ein Angreifer erhält damit über ein neu angelegtes Konto mit Administrationsberechtigungen vollen Zugriff auf das Zielsystem.

Nach den Erfahrungen der vergangenen Monate muss davon ausgegangen werden, dass diese Schwachstelle sehr bald auch von Würmern ausgenutzt werden wird. Ein umgehendes Einspielen des Patches ist daher dringend zu empfehlen.

1.3 Gefälschte eBay-Server

Wie am 08.09.2003 bekannt wurde, haben Betrüger einen gefälschten eBay-Webserver aufgebaut, um an die Daten von eBay-Kunden zu kommen. Der Trick: Mit einer scheinbar von eBay stammenden E-Mail versuchen sie, ihre Opfer auf den vorgeblichen eBay-Server zu locken. Tatsächlich enthält die E-Mail mit dem korrekt aussehenden Link keinen Text, sondern ein Bild – das mit einer völlig anderen URL hinterlegt ist.

1.4 Trauen Sie Ihrem Browser?

Die Aufdeckung kritischer Schwachstellen in Betriebssystemen und Anwendungen ist leider mittlerweile an der Tagesordnung. Meist handelt es sich dabei um Programmierfehler („Bugs“), die es erlauben, z. B. den Rechner zum Absturz zu bringen oder lokale Dateien auszulesen. Dass immer wieder auch konzeptionelle Sicherheitslücken entdeckt werden, deren Ursache im mangelhaften Design der Software zu finden ist, ist oft weniger geläufig.

Ein prominentes Beispiel für derartige Schwachstellen sind die vom Dartmouth PKI Lab durchgeführten Forschungen zum Thema „Web Spoofing“. Nachdem dieser Begriff bereits 1996 zum ersten Mal in der Literatur auftauchte, testeten die Forscher aus Dartmouth in den vergangenen Jahren

vor allem die gängigen Browser auf Lücken und konnten dabei beeindruckende Ergebnisse erzielen: So gelang es ihnen – unter Verwendung von JavaScript auf präparierten Webseiten – einen Mozilla-Browser so zu überlisten, dass der Benutzer glaubte, eine sichere SSL-Verbindung zu nutzen. Tatsächlich waren sämtliche Fenster, Icons und Links „gefälscht"; sogar die Eingaben auf der Tastatur wurden überwacht.

Etliche detaillierte Lösungsvorschläge der Forscher, die schon Anfang 2002 publiziert wurden, haben leider bis heute keinen Einzug in die Anwendungen gehalten.

1.5 Digitalbilder: Echt oder retuschiert?

Dass Fotos mit zunehmenden Fortschritten in der digitalen Bildbearbeitung mehr und mehr an Beweiskraft verlieren, ist offenkundig. Ein neuer Ansatz zur Rettung der Authentizität digitaler Bilder versucht nun, anhand statistischer Eigenschaften des per Wavelet-Transformation mathematisch umgeformten Bildes Originalaufnahmen von manipulierten Bildern zu unterscheiden.

Dieser Ansatz trifft auch die Steganografie: Sie steht nun vor der Herausforderung, ein Verfahren zu finden, das bei veränderten Bildern die Statistik wieder „richtet".

1.6 GSM-Verschlüsselung unter Beschuss

Vom Israel Institute of Technology (Technion) in Haifa wurde am 03.09.2003 ein Angriff auf die GSM-Verschlüsselung veröffentlicht, der effizienter ist als alle bisher publizierten Attacken auf den Kryptoalgorithmus A5. Die Methode der Forschungsgruppe um Eli Biham reiht sich ein in den Trend, bei der Kryptanalyse zusätzliche Informationen zu nutzen – in diesem Fall aus Verbindungsaufbau und Fehlerkorrektur. Merke: Ein guter Algorithmus alleine ist höchtens die „halbe Miete" – das Einsatzumfeld ist ebenso von Bedeutung.

1.7 Private Internet-Nutzung

Die private Nutzung des dienstlichen Internetzugangs ist eines der derzeit heftigst diskutierten Themen. Zwar ist die Besteuerung als „Geld werter Vorteil" vom Tisch. Doch bei erlaubter oder auch nur geduldeter privater Nutzung unterliegt der Betrieb erheblichen Einschränkungen aus Telekommunikations- (TKG) und Teledienstedatenschutzgesetz (TDDSG), da der Arbeitgeber zum geschäftsmäßigen Anbieter von Telekommunikationsdiensten wird – auch, wenn er die Leistungen unentgeltlich bereitstellt. Denn Inhalts- und Verbindungsdaten einer privaten Kommunikation genießen den strengen Schutz des Fernmeldegeheimnisses (Art. 10 GG, § 87 TKG).

Zwei aktuelle Leitfänden zu diesem Thema klären die Rechtslage und unterstützen mit Mustervereinbarungen die betriebliche Regelung: Der Leitfaden „Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz" des Bundesdatenschutzbeauftragten (14.03.2003) und der BITKOM-Leitfaden „Die Nutzung von E-Mail und Internet im Unternehmen" (21.08.2003).

2 Secorvo News

2.1 Secorvo College aktuell

Die erste Oktoberwoche ist „PKI-Woche": In einer zweitägigen Einführung in Public Key Infrastrukturen vom **06.-07.10.2003** und einem eintägigen Vertiefungsseminar PKI für Fortgeschrittene am **09.10.2003** bietet Secorvo einen vertieften Einblick aus umfassender Beratungserfahrung in die Grundlagen und ausgewählte Herausforderungen der Konzeption und des Aufbaus von PKIs.

Seit der Ankündigung von NAI im Oktober des vergangenen Jahres, die PGP-Produktlinie einzustellen, war es um PGP stiller geworden. Nun hat sich die neue PGP Corporation mit neuen Produktversionen zurückgemeldet (siehe oben).

Anfang Dezember (**03.-04.12.2003**) stellen wir in unserem Seminar „PGP & Co. Im betrieblichen Einsatz“ vor, was sich hinter OpenPGP und den aktuellen Konzepten verbirgt, wie PGP sich zum Schutz von E-Mails und zur Verschlüsselung von Dateien in der Unternehmenspraxis einsetzen lässt und was PGP von anderen PKI-Lösungen unterscheidet.

Wegen der großen Nachfrage werden wir das Fünf-Tages-Intensivseminar „Information Security Management von A(udit) bis Z(ertifizierung)“ am **03.-07.11.2003** ein drittes Mal durchführen. Das Seminar vermittelt die wesentlichen Grundlagen eines verlässlichen Sicherheitsmanagements auf technischer und organisatorischer Ebene und liefert konkrete Hilfestellungen für Konzeption und Umsetzung in der Praxis.

http://www.secorvo.de/college

2.2 „IT – Aber sicher!“

Am **30.10.2003** wird Lutz Bleyer, Leiter Zentrale Security der Fiducia AG, im Rahmen des nächsten Events der „Karlsruher IT-Sicherheitsinitiative“ (KA-IT-Si) die Security Awareness-Kampagne der Fiducia „IT – Aber sicher!“ vorstellen. Beginn 18 Uhr, anschließend „Badisches Buffet“.

2.3 „ZertiFA 2003”

Um Licht ins Dunkel des Zertifikate-Dschungels zu bringen, haben Dr. Johann Bizer und Dirk Fox, Herausgeber der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“ mit COMPUTAS, einem für hochwertige Security-Konferenzveranstaltungen bekannten Anbieter, eine neue Fachtagung konzipiert. Auf der „ZertiFA 2003“ am **10. und 11.11.2003** im Kölner Hotel Hilton werden Zertifikate und Gütesiegel von BS 7799 über BSI-Grundschutz- und Datenschutzaudits bis ITSEC- und CC-Zertifizierungen vorgestellt und vor dem Hintergrund aktueller Erfahrungsberichte diskutiert.

3 Veranstaltungshinweise

September 2003	
29.09.-02.10.	Informatik 2003 – Teiltagung Sicherheit (GI, Frankfurt)
Oktober 2003	
06.-07.10.	Public Key Infrastrukturen (Secorvo College, Karlsruhe)
09.10.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
14.-15.10.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.10.	Defense Lab (Secorvo College, Karlsruhe)
30.10.	„IT – Aber sicher!“ (KA-IT-Si, Karlsruhe)
November 2003	
03.-07.11.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
10.-11.11.	ZertiFA 2003 (Computas, Köln)
11.-13.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
18.-19.11.	Inside Windows Security (Secorvo College, Karlsruhe)

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 Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Oktober 2003

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

Nr. 10, 2. Jhrg. 2003
Stand 20. Oktober 2003

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

Inhalt

Editorial: WYSIWY – B?

In festem Vertrauen auf unsere Erfahrung und Aufmerksamkeit sind wir überzeugt, dass bei kompetenter Nutzung des Internet nichts passieren könne – jedenfalls nicht uns. Schließlich vertrauen wir nicht naiv auf die Gutartigkeit der E-Mail-Anhänge unbekannter Absender, selbst bei bekannten Adressen sind wir skeptisch und öffnen sie nicht. HTML-formatierte E-Mails betrachten wir grundsätzlich nur in reinem Textformat, da sie über Web Bugs heimlich Rückmeldungen an den Sender auslösen können. Spam isolieren und löschen wir nach kurzer Prüfung – die „keep me off that list"-Option geflissentlich ignorierend. Und Updates sowie Sicherheits-Patches beziehen wir nur aus verlässlicher Quelle via CD.

Auch außerhalb des Firmennetzes nutzen wir das Internet ausschließlich mit (Personal) Firewall. ActiveX- und VisualBasic-Script-Komponenten filtern wir heraus, Flash-Intros werden übersprungen, PlugIns nicht automatisch installiert. Und wenn's ums Geld geht, sind wir noch vorsichtiger: Kreditkartennummern vertrauen wir keiner Webseite an, Passwort-Login und Online-Banking gibt es nur bei SSL-Verbindungen. Dabei prüfen wir: Ist das Zertifikat gültig? Wurde es für die gewählte Webseite ausgestellt? Ist der Schlüssel lang genug?

Zwar ist das Internet so nur noch mit Einschränkung nutzbar. Die Perfidie der Angreifer haben wir dennoch unterschätzt. So gehen wir meist davon aus, dass die Konfigurationsoberfläche kein Potemkinsches Dorf ist – haben wir doch das Credo „What You See is What You Get" tief verinnerlicht.

Wer aber garantiert uns, dass der Mechanismus vieler Werbe-Banner, eine Interaktionsbox zu simulieren, uns nicht beim Homebanking die SSL-Verbindung nur vortäuscht? Dass die URL-Anzeige im Browser auch den verbundenen Server anzeigt? Dass eine E-Mail vom angegebenen Sender stammt? Sollte das World Wide Web so zum „What You See is What You Believe", werden, wäre das der Anfang vom Ende dieses effizienten Mediums.

1 Security News

1.1 „U-Bahn-Spoofing" in Hamburg

Das News-Forums Symlink dokumentierte am 06.10.2003 eine Manipulation der Infobildschirme der Hamburger U-Bahn (siehe Fotos). Hacker hatten die Texte der eingeblendeten Nachrichten abgefangen und modifiziert. Dabei machten sie sich zu Nutze, dass die in vielen U-Bahn-Waggons installierten Windows95-Systeme ihre Meldungen an bestimmten U-Bahnhöfen über ungesicherte WLAN-Verbindungen beziehen. Auch wenn diese Aktion sicherlich mehr Unterhaltungswert als Gefährdungspotenzial besitzt, dokumentiert sie die inhärenten Sicherheitsprobleme heutiger WLAN-Lösungen.

1.2 Neue EU-Studien

Die im Juli 2003 von der EU-Kommission vorgelegte Studie "Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview" kommt zu dem Ergebnis, dass sich das Gleichgewicht zwischen Privatsphäre einerseits und Sicherheit andererseits durch moderne Kommunikationstechniken und staatliche Reaktionen auf Kriminalität und Terrorismus zu Ungunsten des individuellen Datenschutzes verschoben hat. Zugleich wurden die Vorbehalte hinsichtlich des Schutzes der Privatsphäre und der Sicherheit als Haupthindernis für die Akzeptanz von e-Commerce-Angeboten identifiziert. Die Studie untersuchte insbesondere die Auswirkungen der neuen Kommunikationstechnologien, z. B. die „elektronischen Spuren", die man im Internet oder beim Telefonieren mit dem Handy hinterlässt und die für andere Zwecke als die Strafverfolgung missbraucht werden könnten.

In einer zweiten, gerade fertig gestellten Studie trägt die europäische Kommission der in Art. 12 der EG-Richtlinie zu elektronischen Signaturen geforderten Prüfung der „Durchführung dieser Richtlinie" Rechnung.

Der Prüfbereicht "The legal and market aspects of electronic signatures" kommt zu dem Ergebnis, dass die Richtlinie in fast allen Mitgliedsstaaten (sowie den Beitrittskandidaten) umgesetzt wurde, variierende Interpretationen einzelner Artikel jedoch zu teils großen Unterschieden in der Anwendung sowie der nationalen Gesetzgebung geführt haben. Er identifiziert eine Reihe von Problemfeldern, die auf EU-Ebene Beachtung finden sollten, um die gewünschte Harmonisierung elektronischer Signaturen zu erreichen. Stefan Kelm, Security Consultant bei Secorvo, war als Autor an der Erstellung dieser Studie beteiligt.

1.3 IT-Grundschutz kompakt

Am 18.09.2003 wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) der „Leitfaden IT-Sicherheit" (IT-Grundschutz kompakt) publiziert (415 kB). In der 48-seitigen Broschüre werden die häufigsten Versäumnisse und die wichtigsten Sicherheitsmaßnahmen überschaubar und verständlich dargestellt. Ergänzt wird der Leitfaden durch eine Einführung zum IT-Grundschutzhandbuch sowie kurze Checklisten für die wichtigsten Bereiche.

1.4 Security Tools (Update)

Seit dem 01.10.2003 ist v2.5 beta 38 von Cain & Abel verfügbar. Das Multifunktionstool, welches viele Angriffsmöglichkeiten wie ARP-Spoofing und eine Reihe von Passwortcrackern enthält, bietet nun wie L0phtCrack die Möglichkeit, gesniffte SMB-Hashes direkt an den Passwortcracker zu übergeben. Dadurch können schwache Benutzerpasswörter bei NT 4.0 oder Windows 2000 im NTLM-Standard-Modus innerhalb von Stunden geknackt werden.

Der verbreitete Portscanner Nmap, der ständig weiterentwickelt wird, liegt seit dem 06.10.2003 in Version 3.48 vor und enthält nun über 650 Signaturen zur Erkennung von Diensten und Betriebssystemen.

1.5 Top 20 Security Bugs

Die von SANS in Zusammenarbeit mit internationalen Unternehmen erstellte und jährlich aktualisierte Liste der 20 häufigsten Sicherheitsschwächen unter Windows (10) und Unix/Linux (10) wurde am 08.10.2003 publiziert. An dieser Fassung haben das US-Department of Homeland Security sowie Sicherheitsbehörden aus Großbritannien und Kanada mitgewirkt.

1.6 Spam-Bounces – die Kehrseite der Medaille

Nicht nur Würmer à la Sobig verwenden gefälschte, aber real existierende E-Mail-Absender (vgl. Security News 8/2003), sondern auch immer mehr Spam-E-Mail-Versender segeln unter falscher Flagge. Da sich unter abertausenden Spam-Adressaten viele finden, die gar nicht existieren, gerade in Urlaub sind oder sich über die Spam-Mail beschwerden wollen, landen Abwesenheitsnotizen, Fehlermeldungen („Bounces“) und Beschwerden in der Mailbox des vermeintlichen Absenders – zumindest so lange, bis diese überquillt.

Am 09.10.2003 brachen die Mail-Server des zu QSC gehörenden Providers Ginko unter der Last solcher Spam-Bounces ein.

1.7 Fehler in OpenSSL

Am 30.09.2003 wurde eine mit hohem Risiko bewertete Schwachstelle im ASN.1-Parser publiziert, der sich in allen auf OpenSSL basierenden Implementierungen findet: Beim Einlesen manipulierter Zertifikate im Rahmen der SSL/TLS-Client-Authentifikation treten Pufferüberläufe auf, die einen Denial-of-Service Angriff auf SSL-Server ermöglichen. Ob auch die Ausführung von beliebigem Code möglich ist, ist noch unklar.

Besonders schwer wiegt der Fehler dadurch, dass die Überläufe auch dann auftreten, wenn ein bösartiger Client sein Zertifikat unverlangt sendet. Wer OpenSSL im Einsatz hat, sollte daher umgehend auf die entsprechend gesicherten Versionen 0.9.6k bzw. 0.9.7.c aktualisieren.

Die zu dieser Sicherheitslücke publizierten Advisories fördern nebenbei zu Tage, in wie vielen kommerziellen Produkten dieser Code enthalten ist. Die illustere Liste reicht von Cisco Routern und PIX Firewalls über den Apple Macintosh bis zu Novell.

OpenSSL ist nicht die einzige Open Source Crypto-Software, die aktuelle Sicherheitslücken vermeldet: Auch zu den beiden Secure-Shell Implementierungen LSH und OpenSSH wurden seit Mitte September mehrere Advisories publiziert.

1.8 Hacker stiehlt Spielequellcode

Üblicherweise erfährt die Öffentlichkeit wenig über erfolgreiche Einbrüche von Hackern und den angerichteten Schaden. In einem nun bekannt gewordenen Fall war dies anders: Ein Hacker, der möglicherweise eine Sicherheitslücke in Outlook nutzte, konnte um den 19.09.2003 Zugriff auf den Quellcode des noch unveröffentlichten zweiten Teils des populären Spiels Half-Life erlangen und verbreitete den Code anschließend im Internet.

Im Verlauf des vom Hersteller Valve Software bestätigten Vorfalls wurden von dem oder den Angreifern u. a. „Keystroke-Logger“, die per Software alle Tastendrücke des Benutzers aufzeichnen, auf Rechnern von Valve-Mitarbeitern installiert. Damit ein Spieler, der den internen Aufbau des Spiels kennt, keinen unfairen Vorteil daraus ziehen kann, müssen nun Teile von Half-Life 2 umgeschrieben werden. Dadurch wird sich das Erscheinen des Spiels über das für die Branche so wichtige Vorweihnachtsgeschäft hinaus verzögern.

Das Beispiel zeigt, dass die veröffentlichten Sicherheitsschwächen wichtiger Anwendungen (wie Outlook oder Internet Explorer) und Betriebssysteme keineswegs ein „theoretisches“ Problem darstellen, sondern zu erheblichen, wenn auch oft unveröffentlichten Schäden führen.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminar „IT-Security Management“ – buchbar als zweitägiges Intensiv- oder einwöchiges Grundlagenseminar (**03.-04.11.** bzw. **03.-07.11.2003**) – führt in Aufbau, Prozesse und Strukturen des Sicherheitsmanagements ein. Am Beispiel eines fiktiven Unternehmens werden Standards und rechtliche Rahmenbedingungen konkret.

Eine aktuelle „Standortbestimmung“ der IT-Sicherheit leistet das Seminar „IT-Sicherheit heute“ (**11.-13.11.2003**), das sich als inhaltliche Auffrischung und Einstieg in das Themengebiet eignet.

Nach den Würmer- und Virenattacken der vergangenen Monate aktueller denn je: Die sichere Konfiguration des Betriebssystems Windows (NT/2000/XP). Insider-Einblicke gewährt das Seminar „Inside Windows Security“ am **18.-19.11.2003**.

Hilfestellung für die Einführung von E-Mail-Verschlüsselung im Unternehmen und viele Tipps aus der Beratungspraxis bietet das Seminar E-Mail-Sicherheit am **25.-26.11.2003**.

2.2 “Anti-Spam-Symposium”

Mit einem „Anti-Spam-Symposium“ am **18.-19.11.2003** greift die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) die Diskussion des angemessenen Umgangs mit unerwünschten E-Mail-Nachrichten („Spam“) in Unternehmen auf. Namhafte Referenten werden diese Frage aus rechtlicher, technischer und organisatorischer Perspektive beleuchten. Das Symposium, für das Microsoft als Sponsor gewonnen werden konnte, richtet sich an alle mit Abwehrmaßnahmen gegen Spam befassten Verantwortlichen in Unternehmen und Behörden – IT-Leiter, Management, Techniker und Datenschutzbeauftragte (Heise-Ticker).

Programm und Anmeldung unter
http://www.anti-spam-symposium.de

3 Veranstaltungshinweise

Oktober 2003	
30.10.	„IT – Aber sicher!“ (KA-IT-Si, Karlsruhe)
November 2003	
03.-04.11.	IT-Security Management (Secorvo College, Karlsruhe)
03.-07.11.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
10.-11.11.	ZertiFA 2003 (Computas, Köln)
11.-13.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
18.-19.11.	Anti-Spam-Symposium (KA-IT-Si, Karlsruhe)
18.-19.11.	Inside Windows Security (Secorvo College, Karlsruhe)
24.-25.11.	IT Incident Management & Forensik (GI, Stuttgart)
25.-26.11.	E-Mail-Sicherheit (Secorvo College, Karlsruhe)
Dezember 2003	
03.-04.12.	PGP & Co. im Betrieb (Secorvo College, Karlsruhe)

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 Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
November 2003

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

Nr. 11, 2. Jhrg. 2003
Stand 21. November 2003

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

Inhalt

Editorial: Wer misst, misst Mist

Der vom allgegenwärtigen Spardruck ausgelöste Trend, Leistungen und Kostentreiber im Unternehmen durch Kennzahlen transparent zu machen, hat mit Balanced Scorecards und Benchmarks nach dem Management die IT erfasst.

Nun ist auch die IT-Sicherheit in den Fokus des „Erbsenzählens“ geraten. Zunächst einmal ist das nicht besonders verwunderlich. Denn IT-Sicherheit kostet Geld, und je besser sie funktioniert, desto weniger sichtbar ist sie – je schlechter sie funktioniert, desto kritischer wird sie beäugt. In beiden Fällen stehen die Kosten unter Rechtfertigungsdruck.

Hinzu kommt ein der Unternehmensleitung nicht immer leicht verständlich zu machendes, aber elementares Faktum: IT-Sicherheit ist kein „binärer Zustand“ – die beliebte „Sind wir sicher?“-Frage konnte noch kein IT-Sicherheitsverantwortlicher eindeutig mit „Ja“ oder „Nein“ beantworten (jedenfalls nicht ohne rot zu werden).

Die Wirklichkeit liegt – wie so oft – zwischen den Extremen. Wo aber liegt sie genau? Sind wir gut genug, um den Anforderungen von KontraG, GmbHG und Basel II zu genügen? Tun wir das Erforderliche? Entsprechen unsere Maßnahmen dem „Stand der Technik“? Wirken unsere Maßnahmen? Und nicht zuletzt: Werden wir besser?

Die Fragen sind nicht neu. Aber bisher haben wir es uns geleistet, sie unbeantwortet zu lassen. Den Kostendruck sollten wir nun als Chance nutzen, die IT-Sicherheit über Metriken zu einer Entwicklungsgröße im Unternehmen zu machen. Das ist eine anspruchsvolle Aufgabe, denn es fehlt an akzeptierten Messgrößen und Bewertungsschemata. Immerhin gibt es Beispiele, und erste Normierungsversuche, wie die jüngsten Publikationen des NIST und der CESG zeigen. Bei der Umsetzung sollten wir jedoch immer Einstein im Kopf behalten:

Nicht alles, was zählt, kann gezählt werden,
und nicht alles was gezählt werden kann, zählt.
Albert Einstein (1879-1955)

1 Security News

1.1 Neuer BfD im Amt

Am 14.11.2003 wurde nach langem politischen Ringen hinter den Kulissen und mit mehrmonatiger Verzögerung der von den Grünen vorgeschlagene ehemalige stellvertretende Hamburgische Datenschutzbeauftragte Peter Schaar vom Bundestag als Nachfolger von Joachim Jacob zum Bundesbeauftragten für den Datenschutz (BfD) gewählt.

Dafür, dass ihm die Arbeit nicht ausgeht, wollen die Parteikollegen sorgen: Nach dem rechtspolitischen Sprecher der Bundestagsfraktion, Jerzy Montag, soll geprüft werden, Verschlüsselungsschlüssel zukünftig beim BfD zu hinterlegen.

1.2 EU-Spam illegal

Mit Artikel 13 („Unerbetene Nachrichten") der EU-Datenschutzrichtlinie für elektronische Kommunikation vom 12.07.2002 (Amtsblatt der EG L 201/47, 31.07.2002) wurden per E-Mail, Fax oder SMS verschickte Nachrichten zum Zweck der Direktwerbung für illegal erklärt, wenn sie ohne „Opt-Out"-Hinweis oder unter Verschleierung der Absenderidentität gesendet werden. Die Richtlinie fordert sogar – sofern keine Kundenbeziehung besteht – aktives „Opt-In" als Voraussetzung. Die Richtlinie war bis zum 31.10.2003 in nationales Recht umzusetzen. Die Bundesregierung verpasste (auch) diesen Termin – damit gilt sie jetzt als übergeordnetes Recht.

Allerdings dürfte die Richtlinie ein „zahnloser Tiger" bleiben: Spammer agieren – sofern überhaupt feststellbar – fast immer aus Ländern außerhalb der EU.

1.3 (K)eine Linux-Backdoor

Am 05.11.2003 entdeckte eine Gruppe von Linux-Kernel-Entwicklern, dass jemand versucht hatte, eine Hintertür in die 2.6er Entwicklungsversion des Linux-Kernels einzubauen. Dem Quellcode wurden zwei Programmzeilen hinzugefügt, die es einem normalen Benutzer ermöglicht hätten, Administrationsberechtigung zu erlangen.

Die Änderung betraf allerdings nicht die „heilige" Kernel-Source-Referenz, sondern die an anderer Stelle exportierten Dateien im Concurrent Versioning System (CVS). Nach Angaben von Bitkeeper, dem Hersteller der Kernel-Source-Verwaltungssoftware, wäre eine Änderung des Referenzcodes unverzüglich festgestellt worden.

1.4 Noch mehr fehlerhafte ASN.1-Dekodierer

Dass auch Sicherheitssoftware Opfer von Fehlern in gemeinsam genutzten Funktionsbibliotheken sein kann, zeigen mehrere Schwachstellen, die kürzlich – wie in den Security News 10-2003 berichtet – in OpenSSL, mittlerweile aber auch in verschiedenen anderen SSL- und S/MIME-Produkten gefunden wurden.

Quelle dieser Bugs ist die „Abstract Syntax Notation" (ASN.1), die beschreibt, wie z. B. X.509-Zertifikate und geschützte S/MIME-Nachrichten für den Transport zu kodieren sind. Fehler in der ASN.1-Kodierung können bei zahlreichen Implementierungen zu Pufferüberläufen oder Denial-of-Service-Angriffen führen. Da diese Schwachstellen innerhalb von verbreiteten Krypto-Bibliotheken entdeckt wurden, sind weit mehr Hersteller von diesem Problem betroffen, als ursprünglich berichtet. Entsprechend aktualisierte Listen findet man beim CERT/CC.

1.5 Macht Microsoft ernst?

Die Anzeichen mehren sich, dass Microsoft künftig tatsächlich Sicherheit über Funktionalität stellen wird: In einer E-Mail an BugTraq warnt Microsoft-Mitarbeiter Michael Howard, Co-Autor von „Writing Secure Code", am 12.11.2003, dass die sicherere Grundkonfiguration des angekündigten Windows XP SP 2 zu fehlerhaftem Verhalten von Anwendungen führen kann.

1.6 VPN Key Cracker

Dass eine Schwäche des Internet Key Exchange Protokolls (IKE) eine Kompromittierung des häufig in IPsec-VPNs verwendeten „Preshared Key“ ermöglicht, ist seit April 2003 bekannt. Inzwischen gibt es auch Tools, die derartige Angriffe unterstützen, wie z. B. ikecrack. Seit Version 2.5 beta36 hat auch das beliebte Multifunktions-Sniff- und -Crack-Tool Cain eine solche Funktion, den „IKE Aggressive Mode Pre-Shared Keys Cracker“, integriert.

Seit dem 07.11.2003 ist der Scanner ike-probe verfügbar, der prüft, ob ein VPN-Gateway anfällig für diese Attacke ist.

1.7 Happy Birthday, Malware

Genau 20 Jahre war es am 03.11.2003 her, dass Fred Cohen im Rahmen seiner Doktorarbeit den ersten experimentellen Computervirus entwickelte. Was damals noch als theoretisches Hirngespinst erscheinen konnte, hat sich in der Zwischenzeit zur realen Plage und Bedrohung entwickelt und Anti-Virus-Software als ganz neue Produktklasse entstehen lassen.

Microsoft hat nun härtere Bandagen angelegt und am 05.11.2003 5 Mio. US $ Kopfprämien für Hinweise ausgesetzt, die zur Ergreifung der Viren-Entwickler von Blaster und Sobig führen. Angeblich häufen sich derzeit in Bagdad die Selbstanzeigen...

1.8 Stichwort: „Regression Bug“

„Regression Bug“ nennt es der Softwareentwickler, wenn sich bei einer beabsichtigten Verbesserung ein neuer oder gar ein alter, eigentlich schon behobener Fehler wieder einschleicht.

Auf ein Paradebeispiel dafür hat am 11.11.2003 Microsoft hingewiesen: Wer das am 09.09.2002 veröffentlichte Service Pack 1 (SP 1) zum Internet Explorer 6 nach dem am 20.06.2003 erschienenen SP 4 für Windows 2000 installiert, führt damit einen schwerwiegenden Fehler bei der Auswertung von SSL-Serverzertifikaten wieder ein, der einem SSL-Server die Ausstellung weiterer gültiger Zertifikate ermöglicht.

1.9 „RFID-Wanzensucher“

Am 06.11.2003 wurde der FoeBuD e.V., bekannt durch die jährliche Verleihung der BigBrother Awards für „Datenkraken“, von der Stiftung bridge mit einen Ideenpreis ausgezeichnet. Mit dem Preisgeld von 15.000 € wird nun ein Warngerät zum Aufspüren von RFID (Radio Frequency Identification) Transponderchips entwickelt.

Dahinter verbirgt sich ein ernsthaftes Datenschutzproblem: RFID Chips, die es erlauben, berührungslos einen eindeutigen ID-Code auszulesen, sind inzwischen so miniaturisiert, dass sie mit bloßem Auge kaum noch zu erkennen sind. Sie werden, auf Verpackungen oder Waren befestigt, von vielen als die „Wunderwaffe“ zur weiteren Rationalisierung von Logistik und Warenwirtschaft angesehen. Einmal mit einer Person in Verbindung gebracht, eröffnen sich faszinierende Möglichkeiten der Profilerstellung – vom Einkaufsverhalten im Laden (Bewegungsmuster) bis hin zur Verfolgung des Lebenszyklus einer Verpackung. Der Drang zum raschen Einsatz dieser neuen Technik könnte dabei wieder einmal der Beherrschung von Missbrauchsmöglichkeiten davoneilen (FoeBuD-Positionspapier vom 19.11.2003).

1.10 Bluetooth Security

Adam Laurie veröffentlichte am 11.11.2003 in BugTraq eine kurze, vierseitige Übersicht über aktuelle Angriffe und sicherheitsrelevante (Implementierungs-) Fehler in Bluetooth-Geräten. Die Anfälligkeit für Backdoor-Angriffe, SNARF-Attacken und das sogenannte „Bluejacking“ wies er für mehrere verbreitete Handy-Typen nach.

Zwar verfügt Bluetooth über zahlreiche, konzeptionell vergleichsweise gute Sicherheitsmechanismen; deren Wirksamkeit hängt allerdings in der Praxis von der Qualität der jeweiligen Implementierung ab.

2 Secorvo News

2.1 Secorvo College aktuell

Anfang November 2003 ist das Seminarprogramm von Secorvo College für das erste Halbjahr 2004 erschienen. Im Seminarkalender 2004 finden Sie eine ganzjährige Terminübersicht. In das Jahr 2004 startet Secorvo College mit zwei zentralen Themen: Information Security Management am **19.-23.01.2004** (auch als zweitägiges Seminar buchbar) und Public Key Infrastrukturen (PKI) vom **27.-28.01. 2004** – mit zusätzlichem Vertiefungstag am **29.01.2004**.

2.2 Whitepaper Information Security Management

Einen Überblick über die aktuelle Fassung des britischen Standards zur Informationssicherheit, BS 7799, gibt das am 06.11. 2003 erschienene White Paper von Jörg Völker: BS 7799 – Von „Best Practice“ zum Standard (pdf, 376 kB).

2.3 ISIS-MTT Siegel für Entrust Authority™

Nach eingehenden Tests im offiziellen ISIS-MTT-Prüflabor von Secorvo wurde dem „Entrust Authority™ Security Manager 7.0 for Windows" des kanadischen Unternehmens Entrust am 05.11.2003 als weltweit erstem Produkt das ISIS-MTT-Siegel in der Produktklasse „CA Server“ verliehen. Damit ist nun von unabhängiger Seite bestätigt, dass (und wie) Anwender mit dieser Software ISIS-MTT-konforme PKI-Zertifikate und Sperrlisten ausstellen können.

2.4 Video „E-Mail Security“

Das von Secorvo entwickelte Video „E-Mail Sicherheit“ steht nun auch, vertont mit einem „Native Speaker“, in englischer Sprache zur Verfügung. Diese Version ist als Intranet-Lizenz erhältlich und kann über die Secorvo-Webseiten bestellt werden.

3 Veranstaltungshinweise

November 2003	
25.-26.11.	E-Mail-Sicherheit (Secorvo College, Karlsruhe)
Dezember 2003	
03.-04.12.	PGP-Lösungen im Betrieb (Secorvo College, Karlsruhe)
08.-09.12.	IsSec 2003 (Computas, Berlin)
08.-10.12.	IT-Security- und Risk-Management (ZfU, Zürich)
Januar 2004	
19.-23.01.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
20.-21.01.	Einführung in die Praxis des betr. DSB (Euroforum, München)
27.-28.01.	Public Key Infrastrukturen (Secorvo College, Karlsruhe)
29.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2004	
03.-04.02.	DFN-CERT Workshop "Sicherheit in vernetzten Systemen" (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 Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Dezember 2003

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

Nr. 12, 2. Jhrg. 2003
Stand 17. Dezember 2003

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

Inhalt

Editorial: Patchwork

Was haben aktuelle Softwareversionen und neumodische Jeans gemeinsam? Ganz einfach: Beide sind nur mit Löchern echt.

Mittlerweile haben wir uns daran gewöhnt: Ein neues Programm ist ein unsicheres Programm. Nicht etwa, weil es nicht funktioniert oder ständig abstürzt – das war früher – sondern weil es mit Sicherheitslöchern ausgeliefert wird. Erst nach mehrmaligen Nachbesserungen reift es – Patch für Patch – zu einer Programm- oder Betriebssystemversion, die mit gutem Gewissen für den Produktivbetrieb frei gegeben werden kann.

Diese Entwicklung hat dazu geführt, dass sich die „Organisation der Flicken“ (Patchmanagement) zu einer neuen Disziplin der IT-Security gemausert hat, der das amerikanische NIST im vergangenen Jahr sogar eine Special Publication (SP 800-40) widmete. Keine einfache Disziplin. Nicht genug damit, dass ein rechtzeitiges Einspielen von Patches die Kenntnis von Sicherheitsloch und Flicken voraussetzt: Ohne Tests sollte ein Patch nicht in den operativen Betrieb „entlassen“ werden. Nicht selten verursachen Patches unerwünschte Seiteneffekte – es kann passieren, dass von systemspezifischen Bibliotheken abhängige Anwendungsprogramme anschließend den Dienst versagen. Bei einigen Software-Anbietern erlischt zudem die Betriebsgarantie, sobald das System unter modifiziertem Betriebssystemcode betrieben wird. Und die Zeit zwischen der Entdeckung eines Programmfehlers und der Verfügbarkeit eines „Exploits“ im Internet schrumpft kontinuierlich. Der Patch-Bezug selbst ist auch nicht frei von Fallen: Zahlreiche Empfänger sind den jüngsten, vermeintlich von Microsoft stammenden „Patch-E-Mails“ auf den Leim gegangen.

Zwar wissen wir nicht, ob die Sicherheits-Löcher wie die der Jeans kunstvoll und mit Vorsatz hineingerissen wurden. In einem unterscheiden sich Jeans und Programme jedoch sicher: Die Löcher in letzteren sind keine vorübergehende Modeerscheinung.

1 Security News

1.1 CERT für den Mittelstand

Computer Notfallteams (CERTs) existieren – auch in Deutschland – bereits seit einem Jahrzehnt. Meist richten sich die Dienstleistungen dieser CERTs, wie etwa die Bearbeitung von Sicherheitsvorfällen oder die Herausgabe von Sicherheitsbulletins, an größere Unternehmen. Auch Behörden und Forschungseinrichtungen betreiben eigene Notfallteams.

Bislang nicht bedient wurden jedoch klein- und mittelständische Unternehmen; dies hatte vor allem finanzielle Gründe. Diesem Umstand trug jetzt der Branchenverband BITKOM Rechnung: Am 09.12.2003 entließ er ein von einer Tochtergesellschaft getragenes Notfallteam für den Mittelstand, kurz Mcert, in den Echtbetrieb. Für eine Jahresgebühr ab € 50 (Basic) oder etwas individueller ab € 300 (Professional) stellt das Mcert Kunden z. B. Warnmeldungen über Software-Schwachstellen zur Verfügung. Zwar unterscheidet sich die Beispielmeldung kaum von den bis heute kostenlos verfügbaren Angeboten anderer CERTs (DFN-CERT, RUS-CERT, etc.), ein CERT mit klarem Mittelstands-Fokus wurde jedoch schon lange erwartet.

1.2 Biometrie-Fiasko

Am 27.11.2003 veröffentlichte das BSI den Abschlussbericht des Projekts BioFace, in dessen Verlauf vier verschiedene Gesichtserkennungssysteme beim BKA getestet wurden. Das ernüchternde Ergebnis: die Falsch-Rückweisungs-Rate (FRR) lag zwischen 64 % und 99,7 %. Das Urteil: Für einen Einsatz bei der Zutrittskontrolle „in keiner Weise akzeptabel“.

Ungeachtet solcher technischen Resultate haben just am selben Tag die Innen- und Justizminister der EU die Integration eines Chips in Visa und Aufenthaltstitel beschlossen – auf dem zukünftig Gesicht und Abdrücke zweier Finger gespeichert werden.

1.3 Murphy hat doch recht

Am 26.11.2003 führte eine für extrem unwahrscheinlich gehaltene Kette von Ereignissen zum ersten „unbeabsichtigten Distributed Denial-of-Service Angriff“ auf große Teile des europäischen DNS.

Die Chronologie: Anfang November wurde die Nord-Route des Transatlantik-Unterseekabels TAT-14 unterbrochen. Während der mehrwöchigen Reparaturarbeiten trat am 25.11.2003 auch bei der redundanten Süd-Route des Kabels ein Kabelbruch auf. Dadurch wurden die Europa-Verbindungen des amerikanischen Providers above.net gestört. Als dann am 26.11.2003 die Auto-Update Funktion der verbreiteten Personal-Firewall Software ZoneAlarm nach dem Server des Herstellers Zone Labs suchte, warteten europäische DNS-Server vergebens auf eine Antwort aus den USA – denn die DNS-Server von Zone Labs sind über above.net angebunden. Die Last der in kurzen Abständen vieltausendfach wiederholten DNS-Anfragen zwang kurz danach verschiedene DNS-Server in die Knie – ein neuer Beleg für die Unumstößlichkeit von Murphy’s Law.

Zone Labs wurde übrigens unabhängig von diesen Ereignissen am 15.12. vom Firewall-Marktführer Check Point übernommen.

1.4 Lücke in Zertifikatskette

Ab dem 07.01.2004 kann es zu Problemen mit SSL-Zertifikaten kommen, die von der VeriSign International Server CA – Class 3 ausgestellt wurden. Grund: Die Gültigkeit des Zertifikats einer unterhalb der VeriSign-Root-CA operierenden „intermediate CA“ läuft ab. Zwar hat VeriSign bereits 2001 auf dieses Problem hingewiesen und das Zertifikat bis 2011 verlängert. Das nun ablaufende Zertifikat befindet sich jedoch noch immer auf vielen Clients, vor allem Internet-Browsern. Das Problem lässt sich Server-seitig durch Übermitteln der neuen Zertifikatskette beim Verbindungsaufbau oder Client-seitig durch Download des neuen CA-Zertifikats beheben.

1.5 Neue Version des GSHB

Am 16.12.2003 erschien im Bundesanzeiger-Verlag die 5. Ergänzungslieferung zum IT-Grundschutzhandbuch des BSI. Darin wurden einige der Bausteine aktualisiert und Bausteine zu Outsourcing, IIS, Apache Webserver, Exchange/Outlook 2000 und der Archivierung von Daten ergänzt. Die Online-Version des neuen GSHB wird Ende Januar 2004 verfügbar sein.

Außerdem wurden zum 01.12.2003 das Prüfschema zur Durchführung einer Zertifizierung nach IT-Grundschutz, die Aufgaben des Zertifizierers und das Lizensierungsschema für IT-Grundschutz-Auditoren überarbeitet.

1.6 Einbruch bei Debian

Am 21.11.2003 wurde eine Kompromittierung verschiedener Server des Linux-Distributionsprojekts Debian entdeckt. Die Rekonstruktion des Vorfalls ergab, dass die Angreifer sich mit einem abgehörten Passwort eines Debian-Entwicklers auf einer Maschine anmeldeten und sich anschließend mit einem lokalen Root-Exploit Superuser-Rechte verschafften.

Hauptursache: Nachlässiges Patchmanagement. Denn die vom Root-Exploit ausgenutzte Sicherheitslücke im Linux-Kern war seit September bekannt und in Entwicklerversionen des Kernels schon eliminiert, wurde aber erst nach dem Vorfall im Kernel 2.4.23 beseitigt und auf den Debian-eigenen Servern gestopft.

1.7 Satelliten-Dialer

Mit ungebremster Kreativität legen sich die Dialer-Anbieter ins Zeug. Wie auf der Informationsseite dialerschutz.de ausführlich dargestellt, werden inzwischen sogar Verbindungen über Satelliten (Vorwahl 0088) von Dialer-Programmen genutzt. Die Kosten liegen bei gut 3 € pro Minute.

Mit Wirkung vom 14.12.2003 erklärte die RegTP daher Dialer, die nicht die registrierungspflichtige Vorwahl (0)9009 nutzen, als illegal: Für den geprellten „Nutzer“ entfällt damit die Zahlungspflicht.

1.8 Bürgerkarte in Österreich

Was in vielen europäischen Ländern noch immer ein Wunschtraum ist, soll in Österreich jetzt Wirklichkeit werden: die Einführung einer digitalen Bürgerkarte, mit der landesweit Behördengänge online und in abgesicherter Form erledigt werden können.

Das Konzept der Bürgerkarte genügt den Anforderungen des österreichischen Signaturgesetzes, gestattet jedoch explizit, dass „neue Speichermedien wie etwa USB-Tokens oder Handy-SIMs ebenfalls bürgerkartenfähig sein können.“ Es wurde bewusst darauf verzichtet, die in der Praxis noch immer wenig verbreiteten evaluierten „sicheren Signaturerstellungseinheiten“ zu fordern. Die Anerkennung derartiger elektronischer Signaturen durch andere EU-Mitgliedsstaaten könnte zwar daran scheitern (wie jüngst in der Studie der EU-Kommission erläutert), der praktische Nutzen der Karte steigt damit jedoch erheblich.

1.9 VDEW setzt auf ISIS-MTT

Am 01.09.2003 haben die sechs Spitzenverbände der deutschen Stromwirtschaft unter Führung des VDEW in einer gemeinsamen Erklärung die Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr innerhalb der Branche festgelegt. Mit Blick auf die Interoperabilität setzt das VEDIS Projekt dabei auf eine X.509-PKI und das Austauschformat S/MIME in der Ausprägung nach ISIS-MTT.

1.10 ENISA beschlossen

Das EU-Parlament hat am 20.11.2003 die Einrichtung einer Europäischen Agentur für Netzwerk- und Informationssicherheit (ENISA) beschlossen. Schon im Januar soll die zunächst auf fünf Jahre geplante und mit einem Budget von € 24,3 Mio. ausgestattete Behörde die Arbeit aufnehmen. Sitz und Besetzung sind noch umstritten.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminarangebot von Secorvo College startet im Januar mit dem fünftägigen Intensivseminar „Information Security Management von A(udit) bis Z(ertifizierung)“ (**19.-23.01.2004**), dessen erste beiden Tage (**19.-20.01.2004**) auch separat gebucht werden können. Konkretisiert werden die rechtlichen Anforderungen und Standards am Beispiel eines fiktiven Unternehmens.

Das Seminar „Public Key Infrastrukturen (PKI)“ (**27.-28.01.2004**) führt in Grundlagen, Aufbau und Organisation von Schlüsselinfrastrukturen ein – vor dem Hintergrund der Erfahrung von Secorvo aus zahlreichen PKI-Projekten. Für Experten folgt am **29.01.2004** eine eintägige Vertiefung („PKI für Fortgeschrittene“).

Im Februar (**10.-11.02.2004**) werden im „Live Hacking Lab“ spektakuläre und trickreiche Angriffe auf verbreitete Systeme und Anwendungen durchgeführt und analysiert.

2.2 DuD elektronisch

Zukünftig wird es die Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“ auch in digitaler Form geben. In den Genuss einer pdf-Fassung des Jahrgangs 2003 kommt vorab jeder, der die DuD bis zum **31.01.2004** über Secorvo mit einem speziellen Bestellformular abonniert.

2.3 Video “trojan horse”

Aufgrund des großen Erfolgs des viel gelobten Videos „E-Mail-Sicherheit“ und zahlreicher Anfragen wird ab Februar 2004 auch das Video „Trojanische Pferde“ in einer grundlegend überarbeiteten Fassung als Flash-Video in deutscher und englischer Sprache (mit „Native Speaker“) erhältlich sein. Beide wurden bereits von der Linde AG und der T-Systems als Unternehmenslizenz für den Einsatz im Intranet erworben.

3 Veranstaltungshinweise

Dezember 2003	
24.12.	Bescherung
Januar 2004	
19.-20.01.	IT-Security Management (Secorvo College, Karlsruhe)
19.-23.01.	Information Security Management (Secorvo College, Karlsruhe)
20.-21.01.	Einführung in die Praxis des betr. DSB (Euroforum, München)
27.-28.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
29.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2004	
03.-04.02.	Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
10.-11.02.	Live Hacking Lab (Secorvo College, Karlsruhe)
März 2004	
02.-03.03.	Lotus Notes Security (Secorvo College, Karlsruhe)
09.-10.03.	Einführung in die Praxis des betr. DSB (Euroforum, München)

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 Feedback an
redaktion-security-news@secorvo.de