Secorvo Security News

Januar 2004

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

Nr. 1, 3. Jhrg. 2004
Stand 22. Januar 2004

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

Inhalt

Editorial: Paradigmatisch

Die Paradigmen der Informatik sind zahlreich. Ihre Volatilität aber leider hoch: Kein Jahr, in dem nicht ein neuer vermeintlicher „Paradigmenwechsel“ die Gazetten erobert. Dabei lohnt es zumindest in der IT-Sicherheit, sich gelegentlich auf bewährte Prinzipien zu besinnen und diese zur Analyse und Bewertung bestehender Sicherheitslösungen heranzuziehen.

Zwar kommen diese Prinzipien scheinbar primitiv in ihrer Allgemeinheit und zudem lächerlich bekannt daher – konsequent umgesetzt finden sie sich jedoch selten:

- **No Single Point of Failure**: Die Sicherheit keines Systems darf allein an einem Glied der Kette hängen: Reißt es, muss es eine zweite Schutzebene geben, die mindestens bis zur erfolgreichen Alarmierung hält. Leider finden sich immer noch in vielen Unternehmen nicht abgeschottete sensible Teilnetze – eingeschleppte Würmer können dort das Gesamtnetz lahm legen. Ebenso sind einstufige Firewalls hilflos, wenn sich in der Firmware ein Fehler findet – eine zweite „Verteidigungslinie“ eines anderen Herstellers brächte Abhilfe.
- **Least Privilege**: Jedem genau so viele Rechte, wie zur Aufgabenerfüllung erforderlich – nicht mehr, nicht weniger – und konsequenter Rechteentzug bei Aufgabenwechsel, damit keine „Rechtekumulation“ das Sicherheitskonzept unterläuft.
- **Checks and Balances**: Reviews und getrennte Rollen bei Konzeption und Umsetzung, verteilte Berechtigungen statt zentraler Einzelzuständigkeit – nur so lässt sich missbrauchbare „Machtkonzentration“ systematisch verhindern.

Keine Frage: Eine konsequente Umsetzung dieser Prinzipien ist aufwändiger als ihre Vermeidung. Was aber ist gefährlicher als ein vermeintlich „wasserdichtes“ Sicherheitskonzept mit Loch?

1 Security News

1.1 Viren „prosaisch“

Offenbar haben Autoren von Viren und Trojanern derzeit das technisch Machbare ausgereizt – sie besinnen sich wieder auf eine althergebrachte Disziplin ihrer „Kunst“ – das Tarnen und Täuschen.

So waren in den vergangenen Jahren allenfalls die Spam-Mails der Nigeria Connection amüsant zu lesen. Viren- und Trojaner-E-Mails konnte der geübte Blick hingegen schnell aufgrund der simplen Strickart aussortieren. Das hat sich mit aktuellen Schädlingen wie Sober.C, vor dem das BSI am 22.12.2003 warnte, und Xombe geändert. Deren Wirts-E-Mails tarnen sich als „Windows XP Service Pack“ zum Ersatz eines angeblich abgelaufenen „Beta Service Packs“, als Gegengift für den „Trojaner services.exe“, der „nicht einmal per Taskmanager beendet werden kann“[1], oder als Mitteilung über eine erfolgte Strafanzeige wegen „illegaler Downloads“ – samt korrekter Telefonnummer der Kripo Düsseldorf (allein die inkriminierte IP-Adresse gehört zu einem freien Adressblock in Brasilien).

Diese extrem plausibel gestalteten Anschreiben dürften auch manch skeptischen Empfänger zum Öffnen des Dateianhangs verleiten. Vermutlich erregt nicht einmal (mehr) der Hinweis Verdacht, dass vor der Installation ein eventuell vorhandener Virenscanner zu deaktivieren ist.

1.2 Zertifikatskettenlücke II

Wie in den Secorvo Security News 12/2003 vorausgesagt, hatten am 07.01.2004 diverse Browser wegen des ablaufenden VeriSign-CA-Zertifikats Probleme mit SSL-Zertifikaten. Dass dies nicht das einzige Problem blieb, war einer VeriSign-Sperrliste (CRL) zu verdanken, die zum selben Zeitpunkt auslief. Die Verfügbarkeit des Servers crl.versign.com brach daraufhin wegen der großen Zahl von Windows-PCs ein, die eine neue Sperrliste zu laden versuchten. VeriSign verzehnfachte kurzfristig die Server-Kapazität und entschuldigte sich für diesen Fauxpas.

Pikantes Randdetail: Symantec empfahl in diesem Zusammenhang seinen Kunden, die Sicherheitspolicy zu lockern – und die Prüfung zurückgezogener Zertifikate unter Windows zu deaktivieren.

1.3 Sicherheitslücke Backup

Wie am 09.01.2004 bekannt wurde, hat jetzt auch ein Backup-Programm Federn lassen müssen: Zur Durchführung der Datensicherung legt der Open Transaction Manager (OTM) von Veritas NetBackup Professional 3.5 eine Netzwerkfreigabe an. Da diese Berechtigung auf „Jeder/Vollzugriff“ eingestellt ist, können Unbefugte darauf während des Sicherungsvorgangs ohne Einschränkung über das Netzwerk zugreifen und Dateien und Ordner in der OTM Cache-Datei einsehen.

Eine Beschreibung der Schwachstelle und ein Workaround finden sich auf der Website des Herstellers. Alternativ wird ein Update auf Version 3.6 empfohlen.

1.4 11. DFN-CERT Workshop

Anfang Februar ist es wieder soweit: zum elften Mal wird im Kongresszentrum (CCH) in Hamburg der zweitägige DFN-CERT/PCA-Workshop stattfinden. Das auch diesmal sehr viel versprechende Programm dürfte auch 2004 wieder mehr als 350 Teilnehmer aus Forschung, Unternehmen und Behörden anlocken. Aktuelle Vorträge aus den Themengebieten PKI, Intrusion Detection, Chipkarten, sicheres Linux, ARP-Spoofing etc. stehen auf der Agenda. Auch Secorvo ist mit einem Beitrag vertreten: Stefan Kelm wird gemeinsam mit Dr. Rainer W. Gerling zum Thema „E-Mail-Verschlüsselungsproxies in der Praxis“ vortragen.

[1] Fußnote für Unix-Anwender: Dies entspricht in etwa dem „Trojaner /sbin/init“.

1.5 Microsoft-Tool reinigt Office-Dokumente

Dass Restinformationen in Office-Dateien verräterische Details früherer Dokumentenversionen mitliefern können, weiß mittlerweile auch Tony Blair, dessen am 30.01.2003 im Word-Format veröffentlichtes Irak-Dossier von der Presse genüsslich seziert wurde. Auch aus diesem Grund werden Dokumente zunehmend im PDF-Format publiziert. Für MS-Office-Nutzer, die ihre Dateien bedenkenlos direkt weitergeben möchten, veröffentlichte Microsoft am 05.01.2004 ein Remove Hidden Data Add-In Tool – verfügbar allerdings nur für Office XP und 2003.

Pikantes Randdetail auch hier: Sollte die Software nicht funktionieren, empfiehlt Microsoft, die Sicherheitspolicy zu lockern – und allen lokal installierten Makros in Add-Ins und Templates das Vertrauen auszusprechen.

1.6 ASN.1 zum Dritten...

Zunächst verursachte die fehlerhafte Dekodierung missgestalteter ASN.1-Protokollnachrichten Sicherheitslücken in SNMP-Modulen diverser Netzwerk-Produkte, dann in Sicherheitssoftware wie OpenSSL, die ASN.1-kodierte S/MIME-Nachrichten und X.509-Zertifikate auswertet. Forscher der Universität Oulu konnten nun nachweisen, dass auch Internet-Telefonie und Videokonferenzen nach dem Standard H.323 betroffen sind – das zugehörige Signalisierungsprotokoll H.225 kodiert seine Protokollnachrichten ebenfalls nach ASN.1.

Brisant werden diese Fehler dadurch, dass sie nicht nur in H.323-Produkten im engeren Sinne auftreten können, sondern auch in Firewalls, die H.225-Nachrichten für die Network Address Translation (NAT) interpretieren und modifizieren müssen. Am 13.01.2004 gab Cisco ein entsprechendes Security Advisory zu IOS und weiteren H.323-Produkten heraus. Microsoft veröffentlichte am selben Tag als Abhilfe für den hauseigenen ISA Server einen Hotfix, der allerdings mit Bedacht angewendet werden sollte: Ersten Berichten zufolge beendet der Hotfix ohne weitere Nachfrage die Dienste des ISA Servers.

Spätestens jetzt sollten Hersteller ihre Implementierungen aller Protokolle, die auf ASN.1 basieren, auf den Prüfstand stellen.

1.7 MBSA 1.2 in Deutsch

Die neue Version 1.2 des Baseline Security Analyzer (MBSA, siehe SSN 1/2003) von Microsoft für NT, 2000, XP, 2003, IIS und SQL-Server ist seit dem 19.01.2004 auch in deutscher Sprache verfügbar – und sollte nun auch für deutsche Versionen einwandfreie Analyseergebnisse liefern. Einzig die Patch-Beschreibung erfolgt nach wie vor in englischer Sprache und auch die ermittelten Links verweisen leider auf die amerikanischen Referenzseiten.

1.8 BDSG-Übergangsfrist

Am 23.05.2004 endet die Übergangsfrist, die die Neufassung des Bundesdatenschutzgesetzes (BDSG) vom Mai 2001 (in der aktuellen Fassung vom 14.01.2003) für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten einräumt, die vor dem 23.05.2001 begonnen wurde.

Die Novellierung umfasst einige grundsätzliche Änderungen, wie die Aufnahme der Prinzipien der Datensparsamkeit und Datenvermeidung, die Überarbeitung der „10 Gebote“ der technischen und organisatorischen Maßnahmen (Anlage zu § 9) sowie die Einführung eines noch gesetzlich auszugestaltenden Datenschutzaudits.

Unternehmen, die mehr als vier Arbeitnehmer mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, müssen innerhalb eines Monats schriftlich einen (internen oder externen) Datenschutzbeauftragten bestellen. Zudem sind eine Übersicht meldepflichtiger automatisierter Verarbeitungsverfahren und der jeweils Zugriffsberechtigten zu erstellen. Verstöße werden mit Bußgeldern von bis zu 250.000 € belegt.

2 Secorvo News

2.1 Secorvo College aktuell

Für Kurzentschlossene gibt es noch einige wenige freie Plätze auf dem Seminar Public Key Infrastrukturen (27.-28.01.2004) und der eintägigen Vertiefung PKI für Fortgeschrittene (29.01.2004).

Einen „eigenhändigen" Einblick in aktuelle Angriffstechniken erhalten Sie in der ausgeklügelten Laborumgebung des Live Hacking Lab, einer Kooperationsveranstaltung mit der schweizerischen Compass Security Network Computing AG (10.-11.02.2004).

Wegen der großen Nachfrage bietet Secorvo College das fünftägige Intensiv-Seminar Information Security Management von A(udit) bis Z(ertifizierung) ein zusätzliches Mal am 08.-12.03.2004 an.

http://www.secorvo.de/college

2.2 PKI in Windows XP/2003

Die aktualisierte und auf Windows XP und Windows 2003 Server erweiterte Fassung des mehr als 20.000 Mal herunter geladenen Secorvo White Papers „PKI-Unterstützung in Windows 2000" von Holger Mack liegt nun auch in englischer Sprache vor. Darin werden die PKI-Funktionalitäten der aktuellen Windows Versionen dargestellt und ihre Anwendung und Anwendbarkeit in der Praxis untersucht sowie die Unterschiede der PKI-Unterstützung in Windows 2000 und den Nachfolgern Windows 2003/XP verdeutlicht.

2.3 SSN – der 2. Jahrgang

Wer das vergangene Jahr unter der Security-Brille nochmals Revue passieren lassen möchte, findet jetzt den 2. Jahrgang der Secorvo Security News in einer PDF-Datei zusammengefasst – dem Trend zum Abnehmen nach den Feiertagen folgend auch als schlanke Zip-Datei.

3 Veranstaltungshinweise

Januar 2004	
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)
08.-09.03.	IT-Security Management (Secorvo College, Karlsruhe)
08.-12.03.	Information Security Management (Secorvo College, Karlsruhe)
09.-10.03.	Einführung in die Praxis des betr. DSB (Euroforum, München)
April 2004	
20.-21.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
27.-29.04.	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

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

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

Secorvo Security News
Februar 2004

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

Nr. 2, 3. Jhrg. 2004
Stand 20. Februar 2004

ISSN 1613-4311

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

Inhalt

Editorial: Virendialektik

Es ist also die Geschichte der Natur wie der menschlichen Gesellschaft, aus der die Gesetze der Dialektik abstrahiert werden. (...) 1. das Gesetz des Umschlagens von Quantität in Qualität (...)

Friedrich Engels, „Dialektik der Natur“ (1873-1882)

Seit Ende der 80er Jahre (des vergangenen Jahrhunderts) gibt es Viren, und seitdem auch Virenscanner – nichts wirklich Neues also. Die Schwerpunkte haben sich über die Jahre verschoben – es waren erst die Boot-, dann die Macro- und schließlich die E-Mail-Viren, die unausrottbar schienen. Dennoch lagen die Scanner regelmäßig vorn, denn die Verbreitungsgeschwindigkeit war weit geringer als das Update-Tempo der Antivirensoftware. Und auch die von Scannern verursachten Ablaufverzögerungen konnten trotz immer umfangreicherer Viren-Signatur-Dateien durch die Geschwindigkeitsfortschritte neuer Rechnergenerationen kompensiert werden.

Mit dem Virus „MyDoom“ und seinen Varianten droht nun aber die zunehmende Quantität in eine neue Qualität umzuschlagen. Der Verbreitungsmechanismus versucht, alle Register zu ziehen: Wechselnde Betreff-Zeile, E-Mail-Absenderadresse von Kollegen, sprachlich korrekte Nachrichten mit plausiblem „Subject“ und Textinhalt, gezippter Anhang – und gestartet wurde der Virus am Wochenende, zu einer Zeit, zu der der Arbeitseifer auch der Virenjäger weltweit gedämpft ist. Der Erfolg: Erstmals seit geraumer Zeit verbreitete sich ein Virus schneller als die neuen Virensignaturen der Anti-Viren-Software.

Aber auch die Angriffs-Wellen, die entdeckte Schwachstellen auslösen, werden immer steiler: Die Zeitspanne von der Entdeckung einer Schwachstelle bis zur Verfügbarkeit eines „Exploits“ und dessen Massenmissbrauch wird ständig kürzer. Sollte es zutreffen, dass seit dem 13.02.2004 Teile des Quellcodes von Windows NT/2000 im Internet kursieren, könnte auch bei den Exploits ein Qualitätssprung bevorstehen – hoffen wir, dass Microsoft seine Hausaufgaben gemacht hat.

1 Security News

1.1 E-Mail Ping-Pong

Weltweit litten seit dem 26.01.2004 Millionen Computernutzer unter dem E-Mail-Wurm MyDoom. Immerhin waren zumindest Unternehmensnetze dank zügiger Aktualisierung der zentralen Virenschutz-Gateways nach ein bis zwei Tagen überwiegend vor dem Virus geschützt.

Dabei trat allerdings eine in den Auswirkungen schwer wiegende Nebenwirkung von Viren wie MyDoom, Sobig und Co., die sich mit falschen, aber existierenden Absenderadressen verbreiten, zu Tage: Virenschutz-Gateways schicken meist automatisch eine Viren-Warnung an den vermeintlichen Versender der virenverseuchten E-Mail. So kann trotz ausreichenden Virenschutzes das „Echo“ des Wurms die E-Mailboxen überquellen lassen. Einzelne Lösungen senden sogar eine Kopie der verseuchten E-Mail im Anhang zurück.

Das Ping-Pong-Spiel, das entsteht, wenn zwei solche Gateways aufeinander treffen, kann man sich leicht ausmalen. Den Anbietern von Virenschutz-Gateways ist daher dringend zu raten, bei der Entdeckung von Würmern, die für falsche Absenderadressen bekannt sind, keine automatischen Antwort-E-Mails zu erzeugen.

1.2 Firewall-Intelligenz-Bugs

In den vergangenen Wochen wurden gleich mehrere Schwachstellen in Check Points Firewall-1 entdeckt, die den voreingestellten „Eigenintelligenz“-Eigenschaften der Firewall zuzuschreiben sind:

- Am 26.01.2004 wurde der ASN.1-Bug in H.323-Modulen, vor dem wir zuletzt in den SSN 1/2004 gewarnt haben, auch in der Firewall-1 aufgespürt.
- Am 04.02.2004 wurde ein Pufferüberlauf beim VPN-Verbindungsaufbau gemeldet, über den älteren Produkttypen Code untergeschoben werden kann.
- Am selben Tag wurde ein weiterer Pufferüberlauf im HTTP Security Server der Firewall gemeldet, der versucht, mittels „Application Intelligence“ Angriffe auf Anwendungsebene abzuwehren.

Durch diese Schwachstellen kann ein Angreifer potenziell die ganze Firewall „knacken“. Es ist zu befürchten, dass mit der Integration immer komplexerer intelligenter Sicherheitsfunktionen in Firewall-Produkte auch Schwachstellen dieser Art häufiger auftreten werden. Vielleicht erlebt dann die klassische P-A-P Firewall-Architektur mit getrennten Maschinen für Paketfilter und Application-Gateway eine unerwartete Renaissance.

1.3 Tunnelrisiken

Das sogenannte „Tunneln“ von Netzwerkpaketen ist schon seit geraumer Zeit als kritische Schwachstelle vieler Kommunikationsprotokolle bekannt: Angreifer nutzen hierbei die Möglichkeit, Informationen in verbreiteten Standardprotokollen – z. B. HTTP – zu „verstecken“, um beispielsweise zentrale Firewalls zu umgehen.

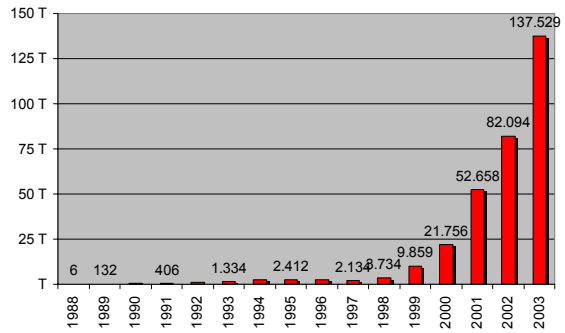
Bislang wurden vor allem die Protokolle HTTP und HTTPS als Tunnelmedien verwendet. Etliche Tools hierfür sind im Internet zu finden. Dass auch jedes andere Protokoll prinzipiell zum Tunneln missbraucht werden kann, demonstrierte die schweizerische Compass Security AG mit der Entwicklung eines DNS-Tunnel-Clients, den sie kostenlos zur Verfügung stellt.

Mit Hilfe dieses Clients ist es möglich, beliebige Netzwerkpakete in reguläre DNS-Anfragen und –Antworten einzupacken. Da DNS (Domain Name Service) zur Umwandlung von Hostnamen in IP-Adressen das zentrale Kommunikationsprotokoll im Internet darstellt, wird es auch von vielen Unternehmens-Firewalls nicht blockiert.

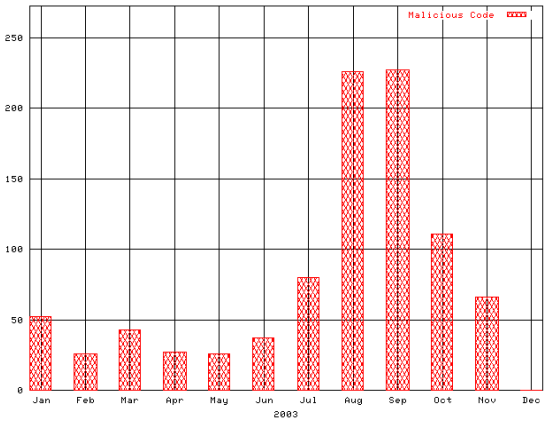
Der von Compass programmierte Client beinhaltet keinerlei Schadensroutinen und kann daher zur Überprüfung der eigenen Infrastruktur genutzt werden.

1.4 CERT-Statistiken

Kurz nach Erscheinen der Security News 1/2004 aktualisierte das CERT Coordination Center an der Carnegie Mellon University am 22.01.2004 die Statistik der gemeldeten Vorfälle: Danach stieg deren Zahl im Jahr 2003 erneut um fast 70 %.



Auch das European CSIRT Network pflegt eine öffentliche CERT-Statistik mit interessanten Ergebnissen. So zum Beispiel die folgende Zählung der je CERT im vergangenen Jahr monatlich durchschnittlich bearbeiteten Fälle bösartigen Codes, die einen extremen Anstieg ab Juli belegt:



1.5 Sicherheitsrisiko IPv6?

In einer Kolumne vom 14.01.2004 äußerte sich der Sicherheits-Experte Simson Garfinkel skeptisch über den von IPv6, der nächsten Generation des Internet-Protokolls zu erwartenden Sicherheitsgewinn. Zwar seien in IPv6 IPsec-Verschlüsselung und andere neue Sicherheitsfunktionen enthalten. Andererseits aber wird jede umfangreiche neue Protokoll-Implementierung unweigerlich auch zahlreiche neue Programmierfehler und Sicherheitsprobleme mit sich bringen.

Wie zum postwendenden Beweis von Garfinkels These wurde am 04.02.2004 ein Denial-of-Service Angriff per IPv6 auf OpenBSD entdeckt – ein Betriebssystem, das für den hohen Stellenwert der Sicherheit bei seiner Entwicklung bekannt ist. Die Lücke wurde am 08.02.2004 gestopft.

Fast zeitgleich wurde beim 47. RIPE Meeting am 26.-30.01.2004 die Forderung erhoben, IPv6-Adressen in die weltweiten DNS Root-Nameserver einzutragen. Dabei wurde als technisches Problem primär die Verlängerung der DNS-Antworten gesehen – nicht aber der nicht unwahrscheinliche Ausfall ganzer nationaler Top-Level-Domains, verursacht durch eine IPv6-Schwachstelle. Diesen Fall mag man sich auch lieber nicht vorstellen.

1.6 Jetzt auch Microsoft...

Der schon in den SSN 11/2003 diskutierte Fehler in der ASN.1-Bibliothek (Abstract Syntax Notation 1) wurde am 10.02.2004 auch in den Microsoft-Betriebssystemen NT 4.0, 2000 und XP entdeckt. Dabei kann ein Pufferüberlauf ausgelöst und beliebiger Code ausgeführt werden. Ähnliche Fehler sind auch bei anderen ASN.1-Implementierungen bekannt geworden.

Die Installation des entsprechenden, von Microsoft bereitgestellten Patches wird dringend angeraten. Während der Endredaktion dieser Security News wurde bereits das erste Exploit veröffentlicht...

2 Secorvo News

2.1 Secorvo College aktuell

Wegen der großen Nachfrage bieten wir das Seminar Information Security Management von A(udit) bis Z(ertifizierung) an einem zusätzlichen Termin, vom **08.-12.03.2004** an. Die ersten beiden Tage bilden eine inhaltlich abgeschlossene Ein-

heit und können getrennt als Seminar IT-Security Management (**08.-09.03.2004**) gebucht werden.

http://www.secorvo.de/college

2.2 KA-IT-Si-Event

Das nächste Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) findet am **31.03.2004** im Karlsruher Technologiepark statt. Dirk Fox, Herausgeber der Fachzeitschrift DuD, wird Anspruch und Wirklichkeit des Datenschutzes in der Unternehmenspraxis beleuchten: Drahtseilakt zwischen Genie und Wahnsinn. Beginn 18 Uhr, anschließend Buffet-Networking.

2.3 Neues Video

Seit Anfang Februar ist das neueste Secorvo-Lehrvideo in deutscher und englischer Sprache verfügbar – das Thema: „Trojanische Pferde“. Dabei handelt es sich um eine professionell überarbeitete Version des seit 2002 erhältlichen und sehr nachgefragten Videos. Dank der verwendeten Flash-Technologie ist es äußerst ressourcenschonend. Die Intranet-Version wird zudem mit Steuerungsmöglichkeit (Stopp, Vor- und Zurückspulen) geliefert. Weitere Sprachversionen sowie Themen für neue Videos sind zur Zeit in Vorbereitung.

2.4 Der Klassiker: DuD 2004

Schon zum sechsten Mal findet am **03.-04.05.2004** die Fachkonferenz DuD 2004 in Berlin statt, die der für seine hochwertigen Konferenzen bekannte Veranstalter COMPUTAS gemeinsam mit den Herausgebern der Fachzeitschrift Datenschutz und Datensicherheit (DuD) konzipiert und organisiert. Nicht nur jährlich steigende Teilnehmerzahlen belegen, dass dieses etablierte Forum von und für Experten aus Unternehmen, Behörden und der Politik für viele Datenschutzbeauftragte und IT-Sicherheitsverantwortliche zum „Muss“ geworden ist: In diesem Jahr lagen schon lange vor Programmveröffentlichung zahlreiche Anmeldungen vor.

3 Veranstaltungshinweise

März 2004	
02.-03.03.	Lotus Notes Security (Secorvo College, Karlsruhe)
08.-09.03.	IT-Security Management (Secorvo College, Karlsruhe)
08.-12.03.	Information Security Management (Secorvo College, Karlsruhe)
09.-10.03.	Einführung in die Praxis des betr. DSB (Euroforum, München)
31.03.	Drahtseilakt zwischen Genie und Wahnsinn (KA-IT-Si, Karlsruhe)
April 2004	
20.-21.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
27.-29.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Mai 2004	
03.-04.05.	Datenschutz und Datensicherheit – DuD 2004 (COMPUTAS, Berlin)
04.-05.05.	Inside Windows Security (Secorvo College, Karlsruhe)
11.-12.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
13.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)

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

Impressum

ISSN 1613-4311

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

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

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

Secorvo Security News
März 2004

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

Nr. 3, 3. Jhrg. 2004
Stand 22. März 2004

ISSN 1613-4311

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

Inhalt

Editorial:
Rechtsfalle Privatnutzung

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Abs. 1 bezeichneten Unternehmens unbefugt (...) eine der in Abs. 1 (...) bezeichneten Handlungen gestattet (...).

Verletzung des Post- oder Fernmeldegeheimnisses, § 206 StGB

Zwar ist die Kuh des “geldwerten Vorteils” bei privater Nutzung von WWW und E-Mail im Unternehmen vom Eis. Dennoch hängt ein Damokles-Schwert über allen Unternehmen, die der Privatnutzung keinen Riegel vorgeschoben haben – als unvermeidliche Konsequenz des verfassungsrechtlich verankerten Fernmeldegeheimnisses. Die Auswirkungen sind dramatisch – und in vielen Unternehmen nicht einmal bekannt: Lassen sich private E-Mails nicht eindeutig identifizieren oder ausschließen, dann unterliegen auch Spam-E-Mails dem selben Schutz wie private Post. Als Service-Provider seiner Mitarbeiter ist der Arbeitgeber nämlich zur (unverstümmelten) Zustellung jeder Nachricht verpflichtet. Ein Löschen unliebsamer, oft mit schädlichen Dateianhängen (Viren) versehener E-Mails ist ein strafbewehrter Verstoß gegen § 206 StGB.

Aus dieser Konsequenz gibt es kein Entrinnen: Denn auch per Verzichtserklärung kann ein Grundrecht nicht abgetreten werden, mithin kann kein Mitarbeiter den Arbeitgeber zum Eingriff ermächtigen. Zumal die Freiwilligkeit einer solchen Zustimmung im Arbeitsverhältnis in Zweifel steht. Selbst eine stillschweigende Duldung privater Nutzung genügt, damit der Arbeitgeber zum Internet-Service-Provider mutiert. Bleibt nur eines: Wer zentral filtern will, muss die private Nutzung explizit verbieten – und die Einhaltung des Verbots regelmäßig prüfen.

1 Security News

1.1 Qualifizierte Massen-Signaturen

Ein in der PKI-Praxis noch immer kontrovers diskutiertes Problem ist die Fragestellung, wie sich fortgeschrittene oder „qualifizierte“ elektronische Signaturen nach EU-Richtlinie und deutschem Signaturgesetz mit Signaturen durch Server bzw. juristische Personen in Einklang bringen lassen. Obgleich dieses Thema bereits seit mehreren Jahren diskutiert wird, kam es erst im Zusammenhang mit der zum 01.01.2004 erforderlichen Umsetzung der EG-Richlinie zu elektronischen Rechnungen wieder auf dem Tisch.

Da dieses Problem nicht nur die Zertifizierungsdiensteanbieter, sondern auch die nationalen Aufsichtsbehörden (in Deutschland die RegTP) betrifft, hat sich die österreichische Aufsichtsstelle für elektronische Signaturen dieses Themas angenommen und am 16.03.2004 einen interessanten Entwurf eines „Positionspapiers zu Fragen der elektronischen Rechnung und der Serversignatur“ vorgelegt. Das Papier enthält konkrete Empfehlungen für die Gestaltung von Massensignaturen, die in ähnlicher Form auch in anderen EU-Ländern umsetzbar sein dürften.

1.2 ENISA: Holpriger Start

Die europäische Sicherheitsagentur ENISA (European Network Information Security Agency) mit provisorischem Sitz in Brüssel ist seit dem 18.03.2004 online. Ihre Aufgabe liegt unter anderem darin, die EU-Mitgliedsstaaten in Fragen der Netzwerk-Sicherheit zu beraten. Ihr Hauptsitz soll gemäß Beschluss vom 13.12.2003 in Griechenland aufgebaut werden. Derzeit ist die Stelle des Direktors ausgeschrieben.

Ein kritischer Blick auf den Webserver legt die Empfehlung nahe, auch die Stelle eines Administrators mit Grundkenntnissen in Webserver-Sicherheit auszuschreiben. Vielleicht würde dann die wenig vorbildliche Informationsfreigabe unterbunden: Unter anderem sind private IP-Adresse, ein Logfile und Skripte des Servers einsehbar.

1.3 NGWT – Next Generation Worm Tricks

Die inhaltlich immer glaubwürdigeren Massen-E-Mails mit Trojanern im Anhang waren ein Thema der SSN 01/2004. Seit einigen Wochen verbergen Würmer den schädlichen Anhang in Passwort geschützten Archiven (.zip, .rar) vor dem Zugriff der Antiviren-Software. Das zugehörige Kennwort wird im Text der E-Mail mitgeliefert – und tatsächlich von unzähligen Empfängern bereitwillig zum Aktivieren des anhängenden Schadprogramms eingetippt.

Darauf haben einige Hersteller von Antivirenlösungen reagiert: Sie entnehmen vor dem Scannen der E-Mail automatisiert die Passwörter und entdecken so Viren und Würmer auch in passwortgeschützten Anhängen. Das ist den Virenprogrammierern nicht verborgen geblieben: Seit Bagle.N werden die Kennwörter daher jetzt als Bild im gif-Format angehängt.

Will man nicht ständig mit den technischen Lösungen der Kreativität der Angreifer hinterherhinken, bleibt als einziger Ausweg eine wirkungsvolle und nachhaltige Mitarbeitersensibilisierung.

1.4 Einstufungs(s)pannen bei Sicherheitslücken

Oft fällt es Herstellern offenbar schwer, die Bedeutung von Sicherheitslücken richtig einzustufen. Zwei aktuelle Beispiele belegen dies: So wurde ein am 09.03.2004 von Microsoft veröffentlichtes Outlook-Update, welches eine mögliche Systemübernahme behebt, zunächst nicht als „kritisch“ bewertet. Und die aktuelle Version des ISS Internet Scanner schätzt die NT-Schwachstelle „NtservicesExeDos“ als „mittel“ ein – obwohl betroffenen Systemen keine Netzdienste mehr zur Verfügung stehen.

Daher ist bei Angaben von Herstellern und Tools zur Relevanz von Schwachstellen Vorsicht angeraten: Die Angaben sollten nur als Empfehlung verstanden werden und nie die eigene Bewertung ersetzen.

1.5 „Security“ schützt vor Lücken nicht

Über sicherheitskritische Schwachstellen in Programmen und Betriebssystemen wird in schöner Regelmäßigkeit berichtet. Sicherheitswarnungen, von Notfallteams „Advisories“ genannt, werden oft als Reaktion auf öffentlich diskutierte Sicherheitslücken publiziert. Vielfach handelt es sich dabei um Erkenntnisse von Security-Experten, die in verbreiteten Systemen gezielt nach Sicherheitslücken suchen.

Dass dabei insbesondere auch die Hersteller von Sicherheitsprodukten unter die Lupe genommen werden, verwundert nicht. Auch hier werden die Experten regelmäßig fündig: Allein im Februar diesen Jahres wurde eine Reihe von teils äußerst kritischen Lücken entdeckt. Betroffen waren u.a. Produkte wie ZoneAlarm, Symantec Firewall/VPN, Symantec Antivirus und Norton Internet Security. Ursache der Bugs waren „alte Bekannte“ wie Buffer Overflows oder Race Conditions.

Als besonders brisant erwiesen sich dabei Fehler, die in der noch recht jungen Produktklasse der so genannten „Intrusion Prevention Systeme“ gefunden wurden, deren Ziel – im Unterschied zu IDS – nicht das Erkennen, sondern die Verhinderung von Angriffen ist. So hat ein Angreifer in diversen ungepatchten Produkten des Herstellers ISS (Internet Security Systems) die Möglichkeit, eigene Code-Sequenzen ausführen zu lassen. Und die Fachzeitschrift c’t kommt in Ausgabe 5/2004 beim Test von Symantecs Gateway Security 5400 gar zu dem Ergebnis, der Schutz durch das Produkt sei „eher niedrig einzuschätzen“.

Noch kritischer ist eine Schwachstelle, die in Hardware-Sicherheitsmodulen (HSM) der Firma nCipher entdeckt wurde: Dort ist es einem lokalen Angreifer u.U. möglich, Zugriff auf kryptographische Schlüssel zu erhalten, die ja gerade durch diese Hardware besonders geschützt sein sollen.

Merke: Auch Hersteller von Security-Produkten sind nicht vor Sicherheitslücken gefeit. Daher sollten gerade diese Lösungen vor dem Produktiveinsatz intensiven Analysen unterzogen werden.

1.6 Raubkopieverbreitung über Firmensysteme

Die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. berichtet von der bislang weltweit größten Razzia gegen Raubkopierer. Dabei wurden vom 16. bis 18.03.2004 allein in Deutschland mehr als 800 Firmen, Rechenzentren und Privatwohnungen durchsucht. Zur Verbreitung der illegalen Kopien, die einen geschätzten Verlust in Höhe eines zweistelligen Millionen-Euro-Betrags verursacht haben, wurden offenbar im großen Stil Systeme von Rechenzentren, Firmen und Privatpersonen missbraucht. Unternehmensserver standen dabei wegen deren performanter Internetanbindung und der hohen Speicherkapazitäten im Fokus des nun ausgehobenen Hacker-Rings, der systematisch fremde Systeme übernommen und missbraucht haben soll.

Erheblich dürften auch die durch die Beschlagnahmungen entstanden Schäden in den betroffenen Unternehmen sein.

2 Secorvo News

2.1 Secorvo College aktuell

Anfang April (06.04.2004) bietet Secorvo College erstmalig einen eintägigen Intensiv-Workshop an, in dessen Verlauf typische Hacker-Vorgehensweisen gemeinsam durchgespielt werden: „Dem Hacker über die Schulter geschaut“. Um intensive praktische Übungen und Diskussionen sicherzustellen, ist die Teilnehmerzahl auf fünf Sicherheitsverantwortliche beschränkt.

Grundlegend überarbeitet, erweitert und aktualisiert wurde das nun dreitägige Seminar „E-Mail-Sicherheit“ (20.-22.04. 2004), das seit 1999 zahlreich besucht und kontinuierlich weiter entwickelt wurde. Erstmalig werden nun auch Server-basierte Verschlüsselungslösungen ausführlich behandelt.

Ende April (27.-29.04.2004) folgt der „Klassiker“: Das Seminar „IT-Sicherheit heute“ gibt einen Einblick in die zentralen Themen und aktuellen Fragestellungen der IT-Sicherheit – geeignet sowohl für einen intensiven thematischen Einstieg als auch als Auffrischung.

http://www.secorvo.de/college

2.2 Chefsache IT-Sicherheit

Mit einer halbtägigen Roadshow zum Thema IT-Sicherheit richten sich die IHKs in Baden-Württemberg derzeit an mittelständische Unternehmen. Die Veranstaltung klärt über zentrale IT-Risiken auf und stellt Lösungswege vor.

In Karlsruhe findet die Roadshow am 31.03.2004 in Zusammenarbeit mit der „Karlsruher IT-Sicherheitsinitiative“ in den Räumen der IHK statt. Die Partner der Initiative begleiten die Roadshow mit einer Ausstellung zum Thema. Im Anschluss referiert Dirk Fox, Geschäftsführer von Secorvo und Herausgeber der Zeitschrift „Datenschutz und Datensicherheit (DuD)“, über Anspruch und Wirklichkeit des Datenschutzes – einem „Drahtseilakt zwischen Genie und Wahnsinn“. Der Eintritt ist frei.

2.3 Microsoft erhält ISIS-MTT-Konformitätssiegel

Am 16.03.2004 hat der Microsoft Windows 2003 Certificate Service nach Prüfung durch das Secorvo Prüflabor vom ISIS-MTT-Board das ISIS-MTT-Konformitätssiegel erhalten. Damit ist die Microsoft-CA das dritte Produkt, dessen ISIS-MTT-Konformität in einem vereinheitlichten Testverfahren nachgewiesen wurde.

3 Veranstaltungshinweise

März 2004	
30.-31.03.	D-A-CH Security 2004 (GI, BITKOM, TeleTrusT; Basel)
31.03.	Chefsache IT-Sicherheit und Drahtseilakt zwischen Genie und Wahnsinn (IHK Karlsruhe)
April 2004	
06.04.04	Dem Hacker über die Schulter geschaut (Secorvo College)
20.-22.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
27.-29.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Mai 2004	
03.-04.05.	Datenschutz und Datensicherheit – DuD 2004 (COMPUTAS, Berlin)
04.-05.05.	Inside Windows Security (Secorvo College, Karlsruhe)
10.-13.05.	Netzwerk Sicherheits-Forum 2004 (ComConsult, Königswinter)
11.-12.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
13.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)

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

Impressum

ISSN 1613-4311

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

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

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

Secorvo Security News
April 2004

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

Nr. 4, 3. Jhrg. 2004
Stand 18. April 2004

ISSN 1613-4311

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

Inhalt

Editorial: Rechtsfalle revisited

Alles sollte so einfach wie möglich gemacht werden, aber nicht einfacher.

Albert Einstein

Die Implikationen einer Privatnutzung von WWW- und E-Mail-Diensten im Unternehmen liegen zahlreichen Verantwortlichen im Magen, das haben die vielen Reaktionen auf das Editorial der SSN 03/2004 eindrucksvoll bestätigt. Die Zuspitzung auf § 206 StGB hat jedoch das Gesamtproblem stark verkürzt:

Festzuhalten ist: Als unproblematisch gilt die automatisierte zentrale Löschung von schädlichen Anhängen (Viren, trojanischen Pferden), da hier das mutmaßliche Einverständnis des Empfängers angenommen werden kann – § 87 TKG verpflichtet Provider sogar zu Schutzmaßnahmen.

Kritisch hingegen ist das zentrale Löschen von vermeintlichem Spam – sogar bei ausschließlich dienstlicher Nutzung: Ohne explizites Einverständnis des Nutzers oder eine geeignete Betriebsvereinbarung verstößt der Arbeitgeber gegen § 303a StGB:

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Spamabwehr erfordert jedoch keineswegs zwingend die zentrale Löschung:

- Das Abweisen von E-Mails am SMTP-Gateway, z. B. durch IP-Blocking, vermeidet ein Filtern und Löschen.
- Ein Aussortieren Spam-verdächtiger E-Mails in einen Quarantäne-Bereich ist nach herrschender Meinung untadelig.
- Wird Spam-verdächtige E-Mail vom zentralen Filter lediglich markiert und erfolgt die Löschung erst beim Empfänger, ist dies sogar bei zulässiger Privatnutzung unbedenklich.

In jedem Fall empfiehlt sich der Abschluss einer Betriebsvereinbarung – und eine Filter- und Löschlösung unter Nutzerkontrolle.

1 Security News

1.1 Overflow in Ethereal

Eines der Standard-Tools, die sowohl von Security-Experten als auch von Hackern eingesetzt werden, ist seit Jahren der sehr mächtige und kostenlos verfügbare Sniffer Ethereal. Er ermöglicht es, den kompletten Netzwerkverkehr mitzuschneiden, um beispielsweise Protokolle zu überwachen oder Verbindungen zu rekonstruieren.

Wie zuletzt in den SSN 03/2004 thematisiert, sind jedoch auch viele Sicherheits-Tools nicht frei von Schwachstellen. Nun hat es Ethereal „erwischt“: Am 22.03.2004 wurden gleich vier teilweise kritische Schwachstellen aufgedeckt, die – wen wundert es – ihre Ursache u. a. in einem „klassischen“ Buffer Overflow haben. Da das Tool sehr Hardware-nah programmiert wurde, sind von den Fehlern nicht nur Windows-, sondern auch alle Unix-Varianten betroffen. Administratoren, die Ethereal einsetzen, sollten nur noch die mittlerweile verfügbare korrigierte Version 0.10.3 verwenden, um nicht Opfer eines zweifellos bald kursierenden Exploits zu werden.

1.2 Cisco Global Exploiter

Unter der Bezeichnung „Cisco Global Exploiter“ ist seit kurzem ein Tool zur Überprüfung von neun bekannten Cisco-Schwachstellen verfügbar. Das Perl-Skript vereinfacht die Untersuchung von Routern und Switches auf Schwachstellen, kann aber – selbst von technisch unversierten „Skript-Kiddies“ – auch für Angriffe missbraucht werden. Ein Update von Systemen mit diesen Schwachstellen wird daher dringend empfohlen.

Die am 07.04.2004 publizierte Schwachstelle – eine fest in der Software verankerte UserID/Kennwort Kombination der Management-Lösungen Wireless Lan Solution Engine und Hosting Solution Engine – dürfte bald auch Teil des Exploits sein.

1.3 TKG im Bundesrat

Nicht zuletzt dank des Engagements der Branchenverbände, insbesondere eco und VATM, hatte die Bundesregierung in letzter Sekunde die umstrittene Vorratsspeicherung von Verbindungsdaten für die Sicherheitsbehörden aus der Novelle des Telekommunikationsgesetzes (TKG), die am 12.03.2004 vom Deutschen Bundestag verabschiedet wurde, herausgenommen. Sogar eine Entschädigung der Diensteanbieter bei Überwachungsmaßnahmen ist vorgesehen. Wie erwartet kam am 02.04.2004 prompt die von mehreren Bundesländern angekündigte Ablehnung im Bundesrat (BR-Drs. 200/04). Erschreckend die Änderungswunschliste der Länder:

- Verpflichtung von TK-Anbietern zur 6-monatigen Speicherung von Verkehrsdaten,
- Verpflichtung der Mobilfunkbetreiber zur Erhebung der Kunden-Bestandsdaten bei Prepaid-Karten,
- Möglichkeit eines Zugriffs auf personenbezogene PINs und Passwörter,
- Streichung der Entschädigung für Auskünfte im automatisierten Verfahren.

Auch die Einschränkung der Verpflichteten auf Unternehmen, die TK-Dienste für die Öffentlichkeit anbieten und mindestens 1.000 Teilnehmer versorgen, ist wieder auf dem Tisch. Damit könnten doch noch alle Unternehmen, die eine Privatnutzung ihrer TK-Dienste zulassen, in den Kreis der Verpflichteten aufrücken.

1.4 Neue ISIS-MTT Version

Am 16.03.2004 verabschiedete das ISIS-MTT Board die neue Version 1.1 der PKI-Interoperabilitätsspezifikation. Wichtigste Neuerung ist die Aufnahme des Profils für XML-Signatur und -Verschlüsselung als neuer Teil 8 von ISIS-MTT. Daneben wurden teils unnötig strenge Profilierungsanforderungen gelockert, um die Interoperabilität mit weit verbreiteter Anwendungssoftware zu verbessern.

Die Bedeutung des Standards ISIS-MTT hat in den vergangenen Monaten weiter zugenommen. So ist ISIS-MTT inzwischen obligatorischer Baustein des E-Government-Frameworks SAGA und, in der neuen Version 1.1, technische Grundlage für das Signaturbündnis. Ebenfalls am 16.03.2004 wurde auf der Grundlage eines Prüfberichts von Secorvo das ISIS-MTT Siegel in der Produktklasse „CA Server“ für die Certificate Services des Microsoft Windows Server 2003 verliehen.

1.5 Windows versus Linux

Eine am 19.03.2004 erschienene Studie von Forrester Research versucht, die seit mehreren Jahren heiß diskutierten Frage, ob Windows oder Linux das sicherere Betriebssystem sei, methodisch sauber zu beantworten. Über ein Jahr untersuchte Forrester Sicherheitslücken und Patches und legte als Vergleichsmetrik die Schwere bekannt gewordener Sicherheitslücken und die Zeit zwischen Bekanntgabe und Behebung zu Grunde. Das Ergebnis: Microsoft veröffentlichte Patch-Releases am schnellsten, hatte aber die meisten Sicherheitslücken der höchsten Einstufung (nach NISTs ICAT Database for Severe Computer Vulnerabilities).

Dieser Ansatz, mit dem sich Vorteile für Windows und Debian-Linux ergaben, wurde am 06.04.2004 postwendend von den großen Linux-Distributoren kritisiert, da sämtliche Lücken über einen Kamm geschoren würden, ohne auf die spezifischen Auswirkungen einzugehen. Zugleich belohnt die Metrik Hersteller, die die Bekanntgabe von Sicherheitslücken so lange wie möglich hinauszögern – und schüttet damit Öl in die seit einigen Jahren schwelende Debatte über den richtigen Zeitpunkt der Veröffentlichung von Sicherheitslücken.

Neben der Erkenntnis, dass bis zu allgemein akzeptierten Metriken für IT-Sicherheit noch ein Stück Weges vor uns liegt, ist anzunehmen, dass der Disput um die Studie zumindest den Absatz des 899 US $ teuren Dokuments fördert.

1.6 SigG-Novelle

Am 01.04.2004 wurde der mit Spannung erwartete Entwurf des SigG-Änderungsgesetzes nebst Begründung veröffentlicht. Der Großteil der vorgesehenen Änderungen bzw. Klarstellungen dient dazu, den Weg für eine einfache, weitest gehend elektronische Beantragung und Ausgabe von Signaturkarten zu ebnen.

Dadurch sollen die etablierten Verfahren für die Ausgabe von EC-, Bank- oder Versicherungskarten auch für Signaturkarten nutzbar gemacht werden – um der elektronischen Signatur endlich zum lange ersehnten Durchbruch zu verhelfen.

1.7 VPN-Sicherheitslücken

Gleich mehrere Implementierungen von ISAKMP/IKE, dem Schlüsselaustauschdienst für IPsec-VPNs, gerieten in den vergangenen Wochen in die Kritik:

- Am 17.03.2004 wurde eine Denial-of-Service Attacke gegen den ISAKMP-Dienst von OpenBSD veröffentlicht.
- Cisco veröffentlichte am 08.04.2004 ein Advisory, wonach einige IOS-Router und Catalyst-Switches durch missgeformte ISAKMP/IKE-Pakete gezielt zum Absturz gebracht werden können.

Den Vogel abgeschossen hat der mittlerweile auch in Linux integrierte ISAKMP-Dienst „Racoon“ des KAME-Projekts, der, wie am 07.04.2004 gemeldet wurde, zwischen September 2001 und April 2004 unbemerkt bei der ISAKMP-Variante mit RSA-Signatur zwar die verwendeten Zertifikate, nicht aber die eigentliche Signatur über die ausgetauschten Protokolldaten überprüft hat.

Dies bestätigt – im Nachhinein – Niels Ferguson und Bruce Schneier, die bereits Anfang 2000 vor der zu hohen Komplexität des IPsec-Standards warnten.

2 Secorvo News

2.1 Secorvo College aktuell

Auf vielfachen Wunsch haben wir das Seminarangebot von Secorvo College um ein Intensivseminar zum Datenschutz erweitert. Einen umfassenden Überblick über die im Mai 2001 neu geregelten Anforderungen des BDSG und unsere Erfahrungen mit der praktischen Umsetzung aktueller Datenschutzanforderungen in Unternehmen erhalten Sie – kurz vor Ablauf der BDSG-Übergangsfrist (vgl. SSN 01/2004) – erstmalig am 18.05.2004.

2.2 IT-Sicherheitsforum 2004

Das IT-Sicherheits-Forum der ComConsult Akademie zählt seit einigen Jahren zu den herausragenden Events der IT-Sicherheit. Das Programm 2004 beinhaltet aktuelle Vorträge zu Themen wie IDS in der Praxis, Sicherheit von Webanwendungen, Patch-Management und XML-Sicherheit. Abgerundet wird die Veranstaltung durch drei ganztägige Tutorien sowie diverse Praxis-Workshops. Stefan Kelm wird über Aufgaben und Strategien von CERTs referieren.

2.3 Midvision 2004

Die IT-Fachmesse für den Mittelstand, Midrange Welt und Midvision 2004, wird in diesem Jahr am 13.-14.05.2004 zum zweiten Mal in der Neuen Messe Karlsruhe stattfinden – diesmal mit dem thematischen Schwerpunkt „IT-Sicherheit“ und einem begleitenden zweitägigen Kongress. Auch die Karlsruher-IT-Sicherheitsinitiative (KA-IT-Si) ist vertreten: Mit Ausstellern, einem Event am 13.05.2004 und zwei Vorträgen auf dem begleitenden Fachkongress.

2.4 DuD 2004

Der Fachkonferenz DuD 2004 (03.-04.05. 2004) „droht“ ein neuer Teilnehmerrekord: schon jetzt haben sich mehr als 80 Teilnehmer angemeldet (Anmeldung).

3 Veranstaltungshinweise

April 2004	
27.-29.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Mai 2004	
03.-04.05.	Datenschutz und Datensicherheit – DuD 2004 (COMPUTAS, Berlin)
04.-05.05.	Inside Windows Security (Secorvo College, Karlsruhe)
10.-13.05.	IT-Sicherheits-Forum 2004 (ComConsult, Königswinter)
13.-14.05.	Midvision 2004 (KA-IT-Si/KMKG, Karlsruhe)
11.-12.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
13.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
18.05.	Datenschutz kompakt (Secorvo College, Karlsruhe)
Juni 2004	
14.-15.06.	IT-Security Management (Secorvo College, Karlsruhe)
14.-18.06.	Information Security Management (Secorvo College, Karlsruhe)
29.-30.06.	Security Awareness Symposium 2004 (Karlsruhe)

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

Impressum

ISSN 1613-4311

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

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

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

Secorvo Security News
Mai 2004

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

Nr. 5, 3. Jhrg. 2004
Stand 28. Mai 2004

ISSN 1613-4311

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

Inhalt

Editorial: Vom Wichtigen

Das Wichtigste im Leben ist, zu wissen,
was das Wichtigste ist.

Otto Milo (Aphoristiker, 1902-1980)

Es ist wie im „wirklichen Leben“: Entscheidungen über Maßnahmen der IT-Sicherheit sind eine tägliche Herausforderung. Denn natürlich sind Zeit und Mittel begrenzt und damit Prioritätensetzungen unvermeidlich.

Begrenzt ist aber auch die Perspektive der beiden wichtigsten Entscheider – die des Verantwortlichen für IT-Sicherheit und die der Budget-verantwortlichen Geschäftsleitung. Schlimmer: Beide haben eine unterschiedliche Perspektive – und das liegt auch noch in der Natur der Sache.

Ein typischer Fall: Der IT-Leiter wählt für eine kritische Netz-Komponente ein Produkt mit Austausch-Garantie innerhalb weniger Stunden. Als die Geschäftsleitung das erfährt, wird sie blass: Die betroffene geschäftskritische Anwendung verträgt eine Ausfallzeit von nur wenigen Minuten.

Kern des Problems: Die Geschäftsleitung interessiert nur das Risiko, der IT-Sicherheitsverantwortliche kümmert sich um das Sicherheitsniveau. Das ist nicht dasselbe: Die Risikoperspektive zielt auf eine fallbezogene Kosten-Nutzen-Entscheidung, ob ein Risiko in Kauf genommen, transferiert (Versicherung, Outsourcing) oder durch Vorbeugung reduziert wird, nicht aber auf eine Verbesserung des Sicherheitsniveaus.

Denn das geschäftliche Risiko leitet sich nicht (allein) aus realen Bedrohungen ab, sondern muss die Kritikalität der betroffenen Anwendung für das Kerngeschäft berücksichtigen. Sicherheitsbeauftragte kennen aber häufig die maximalen Ausfallzeiten nicht, die sie für ein IT-System garantieren müssen, und der Geschäftsleitung sind die konkreten Bedrohungen der genutzten Systeme und Daten oft unbekannt.

Risiko-adäquate Prioritätensetzung in der IT-Sicherheit gelingt daher nur mit Kenntnis des „Business Impact“ betroffener IT-Systeme und Daten einerseits und deren realer Bedrohungen andererseits.

1 Security News

1.1 RSA-576 faktorisiert

Am 27.04.2004 ging die Nachricht durch die Ticker, dass die 576-bit-Challenge der Firma RSA gelöst sei. Tatsächlich wurde die 174 Dezimalstellen lange Zahl bereits am 03.12.2003 zerlegt. Die Faktorisierung gelang einem Team der Universität Bonn um Professor Franke mit Unterstützung durch das Institut für Experimentelle Mathematik in Essen und das BSI. Die verteilte Berechung erfolge auf einem Linux-Cluster mit 144 PCs (400 MHz, Pentium II) und verwendete den General Number Field Sieve-Algorithmus – mit einem Aufwand von umgerechnet 13.200 MIPS-Jahren.

Interessant dabei: Dieser Faktorisierungserfolg bestätigt die Prognose, die Secorvo vor drei Jahren auf der Basis der Faktorisierungserfolge der vergangenen 30 Jahre gestellt hat (siehe Bild), und die weit weniger dramatisch ausfiel als viele Expertenwarnungen und die Erwartung des BSI. Danach wäre 2004 erstmals die Faktorisierung einer 630 bit langen Zahl zu erwarten gewesen – was nun eher unwahrscheinlich erscheint. Selbst die frühestens für das Jahr 2020 vorausgesagte Faktorisierung eines 1024 bit langen RSA-Schlüssels könnte sich daher noch als zu pessimistische Befürchtung erweisen – allen Warnern zum Trotz, die seit Jahren Schlüssellängen von 2048 bit und mehr empfehlen oder gar das baldige Ende von RSA prophezeihen.

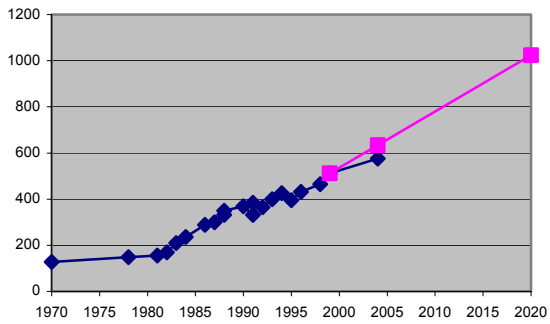


Bild: Secorvo-Prognose 2001 [BoFT_02]

1.2 TCP-Schwachstelle

Das im September 1981 in RFC 793 spezifizierte TCP (Transmission Control Protocol) ist heute das zentrale Protokoll des Internet. Da überrascht es, dass erst im Jahr 2004 eine inhärente Schwachstelle dieses Protokolls aufgedeckt wird: Der Standard erlaubt – aus guten Gründen – bestehende TCP-Verbindungen durch ein Reset-Paket (RST) abzubrechen. Diese Eigenschaft wird zur Schwachstelle, wenn das RST-Paket nicht vom einem der beiden Verbindungspartner gesendet wird, sondern von einem Dritten. Besonders kritisch ist, wenn so Verbindungen gekappt werden, über die Backbone-Router im Internet ihre Routing-Informationen austauschen. Der Angreifer muss allerdings die 32 bit lange, zum Schutz gegen dererlei Attacken zufällig gewählte so genannte Sequence-Number kennen – und dazu entweder die Verbindung belauschen oder sie erraten.

Am 20.04.2004 schlug nun das US-CERT aufgrund einer am gleichen Tag veröffentlichten Studie von Paul Watson Alarm: Häufig akzeptieren TCP-Implementierungen jede Sequence-Number in einem Fenster von 64 kB Größe. Hierdurch wird der effektiv zu durchsuchende Schlüsselraum für den Angreifer von 2^{32} auf 2^{16} Möglichkeiten reduziert. Er muss also maximal 65.536 Pakete schicken – anders als 1981 ist das heute eine Angelegenheit von nur wenigen Minuten.

Fast zeitgleich wurde von der IETF am 19.04.2004 ein Internet-Draft veröffentlicht, der diese Schwachstelle beheben soll. Pikanterweise hat Cisco ein Patent auf das dort beschriebene Verfahren eingereicht. Dieses Vorgehen wurde prompt von Open-Source-Vertretern kritisiert. In OpenBSD findet sich ein anderer Ansatz zur Behebung der Schachstelle: Dort wird die ebenfalls vom Angreifer zu ratende Quell-Portnummer nicht fortlaufend, sondern ebenfalls zufällig gewählt. So gewinnt man die fehlenden 16 bit des effektiven Schlüsselraums wieder zurück.

1.3 Kommt DNSSEC?

Eines der wichtigsten Kommunikationsprotokolle im Internet ist das Domain Name System (DNS), welches für die Zuordnung von IP-Adressen und Hostnamen verantwortlich ist. Dass DNS – genau wie alle anderen verbreiteten Protokolle, die sich des DNS bedienen – über keinerlei Sicherheitsmechanismen verfügt, ist seit Jahren bekannt; bereits Mitte der 90er Jahre wurde daher die IETF-Arbeitsgruppe DNSSEC gegründet, um das Protokoll abzusichern.

Erste technische Drafts zu DNSSEC wurden bald veröffentlicht; ebenso schnell kam man jedoch zu der Einsicht, dass zur Einführung von DNS – insbesondere auf Ebene der Root-Nameserver – vor allem organisatorische Probleme zu überwinden sind. Im Jahr 2000 untersuchte die DENIC eG mit Untersützung von Secorvo die flächendeckende Einführung von DNSSEC innerhalb der Top Level Domain .de. Die Studie kam zu dem Ergebnis, dass DNSSEC im großen Stil noch nicht einsetzbar war. Jüngst legte auch das BSI eine Studie vor, die zu vergleichbaren Resultaten kommt.

Immerhin: Der erste Schritt auf Anwendungsseite ist getan. Die neueste Version 9.3 des im Internet am häufigsten eingesetzten Nameservers BIND unterstützt die DNSSEC-Protokolle. Auch liefen erste erfolgreiche Pilotprojekte. Nun bleibt abzuwarten, ob einerseits andere Hersteller nachziehen und andererseits die wichtigen Betriebsprozesse zur Einführung von DNSSEC so etabliert werden können, dass auch Top Level Domains und die Root-Nameserver DNSSEC anbieten können. Dann erst entfalten Security-Protokolle wie SSL ihre volle Wirkung.

1.4 T-Online-Authentifikation

Die Authentifikation beim Zugriff auf E-Mail-Postfächer erfolgt bei T-Online implizit über das Einwahl-Login. Ein zusätzliches Passwort wird daher beim Zugriff auf die Mailbox nicht mehr benötigt.

Das verursacht bei T-DSL-Router-Zugängen, die von mehreren Personen genutzt werden, ein Problem: Beim Zugriff auf die T-Online-Mailbox werden automatisch die E-Mails des T-DSL-Inhabers abgerufen. Schlimmer: Gelingt es einem Nachbarn (oder „war driver“), sich in ein via T-DSL mit dem Internet verbundenes WLAN einzuklinken, hat er unmittelbaren Zugriff auf den Mail-Account des WLAN-Betreibers.

Seit Kurzem bietet T-Online daher die Möglichkeit, für den E-Mail-Account einen POP3-Passwortschutz einzurichten.

1.5 Sicherheitsloch Schutzsoftware

In den vergangenen Wochen waren wieder mehrere Sicherheitsprodukte Thema von Security Advisories. Am 13.05.2004 wurden schwer wiegende Schwachstellen der verbreiteten Norton Personal Firewall und von Norton Internet Security (Symantec) in verschiedenen Versionen aufgedeckt. Manipulierte DNS- und NetBIOS-Pakete können Heap oder Buffer Overflows und damit die Ausführung beliebigen Codes verursachen. Das Einspielen von Updates oder die Aktivierung der LiveUpdate-Funktion ist daher dringend angeraten. Nachdem am 24.05.2004 auch ein fehlerhaftes ActiveX-Control in Norton Antivirus bekannt wurde, das die Ausführung beliebigen Codes erlaubt, folgte am 26.04.2004 der Virenscanner von F-Secure: Er erkennt die aktuelle Sobig.G-Variante nicht in LHA-komprimierten Dateien – und kann über manipulierte LHA-Anhänge zum Absturz gebracht werden. Zum Schutz vor diesen Angriffen sollten die vom Hersteller für die Client- und die Serverkomponenten bereit gestellten Patches installiert werden.

Schließlich wurde am 15.05.2004 der aktuelle Source Code von Ciscos Router- und Switch-Betriebssystem IOS v12.3 im Internet publiziert. Zwar ist der Code inzwischen nicht mehr auf den Seiten von Securitylab verfügbar; mit gezielten Angriffen auf neue Schwachstellen sollte in den kommenden Wochen jedoch gerechnet werden.

2 Secorvo News

2.1 Secorvo College aktuell

Gerne hätten wir unser Ausbildungsangebot zur IT-Sicherheit schon 1999 vom Start weg mit einem international anerkannten Abschluss vervollständigt. Weil jedoch alle international verbreiteten Zertifikate sich inhaltlich entweder an der eingeschränkten Perspektive der Revision bzw. an spezifisch amerikanischen, insbesondere rechtlichen Rahmenbedingungen orientieren oder auf eine Multiple-Choice-Prüfung beschränken, bieten wir nun einen eigenen Ausbildungsgang zum „IT Security Professional“ an.

Der Ausbildungsgang orientiert sich an der an Hochschulen bewährten Kombination aus Pflicht- und Wahlveranstaltungen: Die Teilnahme an fünf Seminaren von Secorvo College, darunter „IT-Sicherheit heute“ und je ein Seminar aus den Bereichen „Grundlagen“, „Lösungen“ und „Systeme“ qualifiziert zum „IT Security Professional“.

Mit einer theoretischen und praktischen Prüfung, die ab 2005 mindestens zweimal jährlich angeboten wird, können Sie das Zertifikat zum „Certified IT Security Professional“ erwerben.

http://www.secorvo.de/college

2.2 Security Awareness Symposium 2004

Inzwischen steht das Programm des diesjährigen zweiten Security Awareness-Symposium am 29.-30.06.2004. Nach Fiducia, Münchener Rück, RWE, SAP und der Schweizerischen Armee (2003) werden in diesem Jahr BASF, BMW, FinanzIT und T-Systems über ihre Awareness-Aktivitäten berichten. Weiter steht die Frage der Nachhaltigkeit der Sensibilisierung im Mittelpunkt der Veranstaltung, zu der sich schon jetzt Sicherheitsverantwortliche zahlreicher Unternehmen angemeldet haben. Die Teilnahmegebühr liegt bei 390 € (zzgl. MwSt.).

3 Veranstaltungshinweise

Juni 2004	
07.-08.06.	IT Risk Management 2004 (COMPUAS, Köln)
13.-18.06.	16th Computer Security Incident Handling Conference, Budapest (FIRST, Budapest)
14.-15.06.	IT-Security Management (Secorvo College, Karlsruhe)
14.-18.06.	Information Security Management (Secorvo College, Karlsruhe)
22.-23.06.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.-30.06.	Security Awareness Symposium 2004 (Secorvo, Karlsruhe)
August 2004	
09.-13.08.	USENIX Security Symposium (San Diego)
September 2004	
21.-22.09.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)

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

Impressum

ISSN 1613-4311

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

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

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

Secorvo Security News
Juni 2004

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

Nr. 6, 3. Jhrg. 2004
Stand 25. Juni 2004

ISSN 1613-4311

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

Inhalt

Editorial: Chefsache

„IT-Sicherheit ist Chefsache“: Eine oft genutzte, als Slogan missbrauchte, zur Phrase gedroschene – aber tatsächlich zutreffende Behauptung. Allerdings meist falsch oder sogar gänzlich unverstanden. Über 55% der Befragten einer aktuellen Studie von silicon.de bewerten sie als „wichtig“ oder sogar „sehr wichtig“ (32%). Da lohnt ein kritischer Blick.

Zunächst einmal ist die Aussage trivial: Handelt es sich bei IT-Sicherheit um eine Angelegenheit, um die sich ein Unternehmen kümmern muss, dann liegt die Verantwortung dafür natürlich bei der Unternehmensleitung – wo auch sonst.

Tatsächlich hat die Aussage größere Tragweite. Kaum ein Unternehmen, bei dem heute nicht zumindest einzelne, wenn nicht zentrale oder gar alle Geschäftsprozesse in erhebliche Abhängigkeit von Teilbereichen der eingesetzten Informationstechnik geraten sind. Die zuvor verwendeten (manuellen) Prozesse wurden fast immer vollständig abgelöst – daher existieren nur noch sehr selten Ersatzprozesse für den Fall des Ausfalls. Nur noch wenige Unternehmen würden heute einen eintägigen IT-Ausfall problemlos „wegstecken“, fast alle könnte ein einwöchiger Ausfall in eine Existenz bedrohende Schieflage bringen.

Nur: Die wenigsten Unternehmen kümmern sich um dieses Problem so, wie es die „Sorgfalt eines ordentlichen Geschäftsmanns“ (§ 43 GmbHG) „und gewissenhaften Geschäftsleiters“ (§ 93 AktG) gebieten. Das Aktienrecht fordert sogar explizit und zwingend die Einrichtung eines Überwachungssystems zur Erkennung von „den Fortbestand des Unternehmens gefährdenden Entwicklungen“ (KontraG, § 91 AktG).

Zwar kann die Geschäftsleitung das Thema delegieren. Wählt sie jedoch nicht sorgfältig geeignete Mitarbeiter dafür aus, gibt sie die für die Umsetzung erforderlichen Mittel nicht frei oder kontrolliert sie nicht die Qualität des Ergebnisses, verletzt sie ihre Sorgfaltspflicht – und haftet im Schadensfall.

1 Security News

1.1 „Phishing“ auf dem Vormarsch

Die Fälle von Betrugsversuchen durch so genanntes „Phishing“ nehmen auch im deutschsprachigen Raum zu. E-Mails, die angeblich von E-Business-Angeboten wie z. B. Ebay oder einer Direktbank stammen, fordern den Benutzer dazu auf, seine Accountdaten zu überprüfen. Klickt der Empfänger auf den in der E-Mail enthaltenen Link, landet er auf einer Webseite, die wie die Originalseiten aussieht – tatsächlich aber von Betrügern angelegt wurde. Dabei nutzen einige „Phisher“ Sicherheitsschwächen von Browsern, wie z. B. die am 18.06. 2004 gemeldete Schwachstelle von Opera, mit der die dem Benutzer angezeigte URL manipuliert werden kann.

Fällt der Empfänger auf den Bluff herein und gibt bereitwillig Konto- oder Kreditkartennummer, PIN und womöglich eine TAN ein, kann der Angreifer selbst auf den Account zugreifen. Dabei lassen sich „Phishing“-E-Mails leicht erkennen: Seriöse Anbieter versenden grundätzlich keine E-Mails dieser Art.

1.2 Studie von silicon.de

Nach einer Pause von drei Jahren hat silicon.de am 04.06.2004 eine zweite umfangreiche Studie zur IT-Sicherheit auf der Basis von über 1.000 Fragebögen vorgelegt. Zahlreiche Ergebnisse sind wenig überraschend, interessant allerdings das eine oder andere Detail:

- Dramatisch erscheint der Anstieg der Angriffe mit Trojanischen Pferden: Gaben in der ersten Studie nur 20% der Befragten Sicherheitsvorfälle mit Trojanern an, stieg die Zahl in der aktuellen bereits auf 42%.
- Direkt auf den Schutz des Netzwerks folgt als zweitwichtigster Faktor einer effektiven IT-Sicherheit das Sicherheitsbewusstsein der Mitarbeiter: fast 90% der Befragten stuften es als „sehr wichtig“ (63%) oder „wichtig“ ein. Auch die große Resonanz auf das 2. Deutsche Security Awareness Symposium (29.-30.06.2004) bestätigt diesen Trend.
- Als „Daumengröße“ zur Abschätzung des Investitionsvolumens für IT-Sicherheit scheint sich ein Wert von 5-10% des IT-Budgets einzuschwingen: Mehr als ein Drittel der befragten Unternehmen liegt in diesem Bereich, ein weiteres Drittel knapp darüber oder darunter.

1.3 Happy Birthday, Diffie!

Der (Mit-) Entdecker der Public Key Kryptographie Whitfield Diffie feierte am 05.06. 2004 seinen 60. Geburtstag. Auch von uns ein herzliches Prosit auf Diffie, der – mittlerweile in der Funktion des Chief Security Officer von Sun – seit seiner bahnbrechenden Entdeckung zusammen mit Martin E. Hellman Mitte der 70er Jahre weder seine Haarpracht noch seinen Spaß an (Datenschutz-motivierten) Cracks verloren hat.

1.4 Hilfe bei Wurmbefall

Nach Feststellung eines Viren- oder Wurmbefalls stellt sich die Frage „Was tun?“ Aus Sicherheitsperspektive ist die Empfehlung eindeutig: System-Image bzw. Backup zurückspielen oder das System neu aufsetzen. In manchen Fällen können die Schädlinge auch durch das Starten des Betriebssystems im abgesicherten Modus und anschließendem manuellen Entfernen beseitigt werden.

Alternativ können spezielle Virus Removal Tools wie Stinger des Herstellers NAI hilfreich sein – die sicherste Methode bleibt aber ein Neuaufsetzen der betroffenen Systeme. Das effektivste Verfahren ist jedoch der vorbeugende Einsatz aktueller Virenscanner und die regelmäßige Aktualisierung der zugehörigen Viren-Informationsdatenbank.

1.5 MS Antivirus-Guide

Von Microsoft wurde am 15.06.2004 ein „Antivirus Defense-in-Depth Guide“ zur Verfügung gestellt. Warum das englischsprachige, 90seitige pdf-Dokument als ausführbare MSI-Installer-Datei zum Download angeboten wird, entzieht sich allerdings dem Verständnis.

Das umfassende Werk enthält nicht sehr viel Neues: Neben den hinlänglich bekannten Standardmaßnahmen werden einige sinnvolle weitere Schutzmöglichkeiten wie z. B. der Einsatz von Software Restriction Policies aufgezeigt.

1.6 Fluggastdaten in die USA

Am 17.05.2004 hat die EU-Kommission entgegen den Protesten von Datenschützern und dem Europäischen Parlament der vom US-Kongress zum Schutz vor Terroristen geforderten Übermittlung von Flugpassagierdaten an die USA zugestimmt, die bereits seit Monaten praktiziert wird. 34 Datenfelder je Passagier dürfen nun 3,5 Jahre von den zuständigen US-Behörden gespeichert werden – nach Ansicht der Kritiker ein eklatanter Verstoß gegen die EG-Datenschutzrichtlinie.

1.7 PC/SC Draft 2.0

Totgesagte leben länger: Die 1997 mit der Vision eines vereinheitlichten und Plattform-unabhängigen Standards für Smart-Cards, Lesegeräte und Anwendungen angetretene PC-SC-Workgroup veröffentlichte schon im Dezember 1997 die erste Spezifikation PC/SC v1.0. Seitdem war es ruhig um diesen wichtigen Standard. Anfang Juni 2004 wurde nun Version 2.0 der Spezifikation zum „public review“ frei gegeben.

1.8 WLAN-Router-Attacken

Viele der mittlerweile weit verbreiteten DSL- und WLAN-Router werden ohne weiter gehende Sicherheitseinstellungen betrieben. Den Benutzern ist dabei offenbar nicht klar, dass sie so ein „Bürgerfunknetz“ betreiben, das ohne ihr Wissen auch von Dritten verwendet und für Angriffe missbraucht werden kann. Treten im ersten Fall „nur“ zusätzliche Verbindungskosten auf, ist der zweite wesentlich schwerwiegender. Denn kann ein Unternehmen als Quelle eines Angriffs mit Hilfe seines Providers einen ungeschützten DSL-Zugang identifizieren, wird sich der Geschädigte mit Klagen und Schadensersatzforderungen zunächst an den Betreiber des Anschlusses wenden.

Doch auch vermeintlich sicher konfigurierte Systeme können anfällig sein: Der Router WG602v1 des Herstellers Netgear enthielt eine undokumentierte Hintertür in Form eines fest programmierten Administratorzugangs. Die Schwachstelle wurde am 04.06.2004 durch ein Update der Firmware behoben. Nur wenige Tage später, am 18.06.2004, wurde allerdings eine weitere Zugangsmöglichkeit über das Netzwerk-Management-Protokoll SNMP bekannt, über die die Konfiguration verändert und das System unbrauchbar gemacht werden können. Das Einspielen der aktuellen Firmware wird daher dringend empfohlen.

1.9 Home Made Router-Security

Da die Firmware zahlreicher Router und anderer Netzwerkgeräte auf Programmcode basiert, der unter der GNU General Public License (GPL) entwickelt wurde, haben sich einige Hersteller inzwischen dazu durchgerungen, Teile Ihres Quellcodes oder zumindest Bibliotheken zur Verlinkung mit eigener Software ebenfalls zu publizieren. Wer über das entsprechende technische Know-How verfügt, kann damit das Betriebssystem seines Routers anpassen und weitere, durch die Hardware unterstützte Sicherheitsfunktionen wie etwa virtuelle LANs implementieren.

So werden beispielsweise für das Modell WRT54G des Herstellers Linksys der Quellcode und zusätzliche kommerzielle und selbst entwickelte Firmware-Versionen

angeboten sowie offene Firmware-Versionen in Projekten wie OpenWRT weiterentwickelt.

1.10 SQL-Injection in Oracle E-Business Suite

Die Oracle E-Business Suite 11i ist, wie am 03.06.2004 gemeldet wurde, für einen Angriff durch SQL-Injection verletzlich. Ebenso betroffen ist Oracle Apps in allen 11er Versionen. Einem versierten Angreifer kann es so gelingen, mit seinem Browser in den Eingabefeldern SQL-Befehle absetzen, die direkt vom Applikationsserver an die Datenbank übertragen und ausgeführt werden. Zur Abhilfe werden ein Update und der Einsatz von Filterungstechniken auf Applikationsebene empfohlen.

2 Secorvo News

2.1 Secorvo College aktuell

Nach der Sommerpause in den Monaten Juli und August, die in diesem Jahr wieder zu zahlreichen internationalen Security-Events an attraktiven Urlaubsorten lädt – darunter Turku, Las Vegas, San Diego, Toulouse, Sophia Antipolis und Klagenfurt – startet das College-Programm des zweiten Halbjahrs 2004 im September mit Seminaren zu Lotus Notes Security und Public Key Infrastrukturen.

http://www.secorvo.de/college

2.2 Nexus erhält ISIS-MTT-Konformitätssiegel

Am 27.05.2004 hat der Certificate Manager 5.3 von Nexus nach Prüfung durch das Secorvo Prüflabor vom ISIS-MTT-Board das ISIS-MTT-Konformitätssiegel als CA-Server erhalten. Damit liegt nunmehr das vierte Produkt vor, dessen ISIS-MTT-Konformität in einem vereinheitlichten Testverfahren nachgewiesen wurde. Weitere Produkte werden derzeit auf ISIS-MTT-Konformität untersucht.

3 Veranstaltungshinweise

Juni 2004	
29.-30.06.	Security Awareness Symposium 2004 (Secorvo, Karlsruhe)
Juli 2004	
12.-13.07.	Foundations of Computer Security FCS'04 (Turku)
24.-29.07.	Black Hat Briefings (Black Hat, Las Vegas)
August 2004	
09.-13.08.	USENIX Security Symposium (USENIX, San Diego)
23.-26.08.	19th IFIP International Information Security Conference (Toulouse)
September 2004	
15.-17.09.	7th International Symposium on Recent Advances in Intrusion Detection – RAID (Sophia Antipolis)
20.-21.09.	Elektronische Geschäftsprozesse – EGP 2004 (Klagenfurt)
21.-22.09.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)

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

Impressum

ISSN 1613-4311

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

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

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

Secorvo Security News
Juli 2004

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

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

ISSN 1613-4311

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

Inhalt

Editorial: Abschied von der Sicherheit

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

Gene Spafford,
Scientific American, 3/1989

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

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

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

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

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

1 Security News

1.1 Phishing mit Frames

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

1.2 802.11i WLAN Security

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

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

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

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

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

1.3 Online-Banking-Trojaner

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

---

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

1.4 Digitale Spurensuche

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

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

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

1.5 Spurenverwischung

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

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

1.6 Grundschutztool 3.1

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

1.7 MD5-Passwort-Cracker

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

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

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

2 Secorvo News

2.1 IT Security Professional

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

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

2.2 White Paper: „Poststelle“

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

3 Veranstaltungshinweise

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

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

Impressum

ISSN 1613-4311

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

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

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

Secorvo Security News
August 2004

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

Nr. 8, 3. Jhrg. 2004
Stand 23. August 2004

ISSN 1613-4311

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

Inhalt

Editorial: DES – Ein Nachruf

"NIST determined that the strength of the DES algorithm is no longer sufficient to adequately protect Federal government information."

Jetzt ist es amtlich: Das NIST hat am 26.07.2004 offiziell angekündigt, den DES-Standard FIPS 46-3 zurückzuziehen.

Erinnern wir uns: Seit 1977 prägte der DES – vom National Bureau of Standards als FIPS 46-1 publiziert –, das weltweit erste standardisierte Verschlüsselungsverfahren, sowohl die Kryptoanalyse als auch die Diskussion über die Rolle des amerikanischen Geheimdienstes NSA, zeitweilig in „No Such Agency" umgetauft. Der DES entstand 1975 aus einer Entwicklung des IBM-Kryptologen Feistel, der Lucifer-Cipher. Tatsächlich reduzierte die NSA für den Standard die ursprüngliche Schlüssellänge von 128 auf 64 bit – und machte weitere 8 bit zu Paritätsbits. Schon damals war diese Schlüssellänge von 56 bit Stein des Anstoßes; mit der Geheimhaltung des Entwurfs der S-Boxen aber nährte die NSA zudem den Verdacht, eine Hintertür im Algorithmus verborgen zu haben.

Biham und Shamir gelang 1990 eine Attakke auf den DES; sie war theoretisch bedeutsam, aber nicht praxisrelevant. Erst die Koordination von mehreren 10.000 PCs über das Internet, die in Idle-Zeiten DES-Schlüssel durchprobierten, versetzte dem DES Ende 1997 den „Todesstoß": Die erste DES-Challenge wurde so in 140 Tagen gelöst. Schließlich schockte Mitte 1998 der DES-Cracker der EFF, der ein Cluster von Spezialchips verwendete, die Krypto-Welt: In weniger als drei Tagen war der Key der zweiten DES-Challenge gefunden. Abgelöst wurde der DES mit der Veröffentlichung des Advanced Encryption Standard 2001 (FIPS 197). Der mehrjährige Auswahlprozess fand in der Fachöffentlichkeit statt – und wurde selbst von kritischen Beobachtern wie Bruce Schneier als sachlich und fair bewertet. Mit dem DES hat die Krypto-Gemeinde nun nicht allein einen Algorithmus, sondern auch ein verbindendes, lieb gewonnenes Feindbild verloren.

1 Security News

1.1 WinXP SP 2 verfügbar

Nach einigen Verzögerungen ist am 10.08.2004 das lange angekündigte Servicepack 2 für Windows XP erschienen. Neben zahlreichen Bugfixes enthält es insbesondere im Bereich Sicherheit einige Neuerungen: Unter anderem wurde die Funktionalität der Personal Firewall erweitert, und sicherheitsrelevante Einstellungen können nun übersichtlich im „Security Center“ eingesehen werden.

Die verbesserten Funktionen der Personal Firewall sind allerdings nicht ganz „State-of-the-art“, da beispielsweise ausgehende Verbindungen nicht überwacht werden. Ein gewisser Basisschutz ist durch die Firewall jedoch gegeben; für sensible Bereiche wird dennoch der Einsatz einer dedizierten Personal Firewall empfohlen. Die Virenschutz-Meldungen im Security Center hängen maßgeblich von den integrierten Produkten von Drittherstellern ab – und nicht alle Hersteller liefern diese Meldungen.

Microsoft scheint jedenfalls auf dem richtigen Weg zu sein. Allerdings: Nur wenige Tage, nachdem das SP 2 erschien war, tauchten bereits die ersten Probleme auf: Offenbar gibt es Schwierigkeiten, die knapp 270 Megabyte große Datei fehlerfrei zu installieren. Es wird von Systemabstürzen und Datenverlusten berichtet. Microsoft selbst veröffentlichte jetzt eine (leider nicht sortierte) Liste von über 200 Anwendungsprogrammen, die nach der Installation unter Umständen nicht mehr richtig funktionieren.

Pikanterweise finden sich auf dieser Liste auch Microsoft-Lösungen wie Word und Outlook. Microsoft macht also offenbar gründlich ernst mit dem eigenen Anspruch, nunmehr mehr auf die Sicherheit als auf Abwärtskompatibilität zu setzen. Fazit: Für dieses Servicepack gilt einmal mehr: Vor dem Roll-Out ausgiebig innerhalb einer geschlossenen Testumgebung prüfen.

1.2 Déjà-vu bei Check Point

Am 28.07.2004 wurde von ISS auf eine Sicherheitsschwäche beim VPN-Verbindungsaufbau von Check Points Produktlinie VPN-1 hingewiesen – ein Déjà-vu-Erlebnis in doppelter Hinsicht: Nicht nur, dass die Schwachstelle einmal mehr in den ASN.1-Bibliotheken liegt, auf die schon häufig, in den SSN zuletzt im Januar hingewiesen wurde. Auch das aktuelle Advisory von Check Point hat auffällige Ähnlichkeit einem früheren vom Mai 2004.

1.3 Acrobat ohne Netz

Seit dem 12.08.2004 wurden in kurzer Folge mehrere Sicherheitslücken in Adobes Acrobat veröffentlicht, die auch den Reader und sowohl Windows- als auch Unix-Versionen betreffen. Da der Acrobat Reader auf Arbeitsplätzen praktisch aller Betriebssysteme inzwischen zur Standardausstattung gehört, wird ein Wechsel auf die aktuelle Version angeraten, obwohl die Funktionenvielfalt der neueren Versionen die Wahrscheinlichkeit einer Sicherheitslücke zweifellos grundsätzlich erhöht.

1.4 Biometrische Realität

Am 06.08.2004 wurde von BSI, BKA und Fraunhofer-IGD der öffentliche Abschlussbericht der Studie „BioFinger“ zu Fingerabdruck-Systemen in überarbeiteter Form (Erstfassung: 20.05.2004) veröffentlicht. Die Studie attestiert dem besten System eine Falschakzeptanzrate von 0,1% – bei einer Falschzurückweisungsrate von 2%. Übersetzt heißt das: Damit nur jeder tausendste Attentäter in ein Flugzeug kommt, müssen bei jedem voll besetzten Jumbo sechs bis acht Passagiere unfreiwillig am Boden bleiben.

Möglich, dass Studienergebnisse dieser Art dazu beigetragen haben, dass die Forderung der USA, ab Oktober nur noch Pässe mit digitalen Fingerprint-Daten zuzulassen, am 10.08.2004 vom US-Kongress für ein Jahr zurückgestellt wurde.

1.5 Sicherheitsloch in PuTTY

Am 03.08.2004 wurde ein kritischer Fehler in dem bei Administratoren sehr beliebten Telnet/SSH-Client PuTTY entdeckt. Er erlaubt es einem Angreifer, via Spoofing oder über einen gehackten Server beliebigen Code auf dem Client-System auszuführen. Der Autor Simon Tatham empfiehlt dringend ein Upgrade auf Version 0.55.

1.6 Musterrichtlinien des BSI

Das BSI stellte am 07.06.2004 Musterrichtlinien zur IT-Sicherheit als Teil des BSI-Grundschutzhandbuchs elektronisch bereit. Sie umfassen ein Übersichtsdokument und neun Beispielkonzepte und –Richtlinien, die sich an unterschiedliche Adressatenkreise richten und eine Hilfestellung bei der Entwicklung eigener Security Policies bieten sollen. Die einzelnen Regelungsvorschläge wurden um zahlreiche Referenzen auf die entsprechenden Maßnahmen des Grundschutzhandbuchs (GSHB) ergänzt. Leider sind diese Querbezüge weder in der Word- noch der pdf-Version des Dokuments mit den Maßnahmenbeschreibungen des GSHB verlinkt, was die Nutzung aufwändig gestaltet.

1.7 MD5: Keine Panik

Auf der diesjährigen Kryptographen-Konferenz Crypto 2004 (15.-19.08.2004) kündigten chinesische Wissenschaftler an, sie hätten Kollisionen in den Hash-Algorithmen MD4, MD5 und SHA-0 entdeckt. Diese Ankündigung sorgte unter Krypto-Experten für einige Aufregung; es gab sogar Gerüchte, die Angriffe ließen sich auf heutige Algorithmen wie den SHA-1 übertragen.

Tatsächlich scheinen die Wissenschaftler Kollisionen gefunden zu haben, die denselben Hashwert zu unterschiedlichen Eingangswerten liefern. Der Weg zu einem praktikablen Angriff ist dennoch weit. So hatte Hans Dobbertin bereits 1996 Kollisionen für den MD5 beschrieben. Der Algorithmus gilt seitdem als unsicher – gebrochen wurde er indes bis heute nicht.

1.8 Bluetooth-Distanzangriff

Einer Gruppe von WLAN- und Bluetooth-Experten gelang am 03.08.2004 ein sogenannter Snarf-Angriff mit einem modifizierten Bluetooth-Adapter und einer Hochleistungsantenne über eine Distanz von 1,8 km. Die Annahme, dass Bluetooth nur im Abstand von maximal 100-150 m für Angriffe genutzt werden kann, ist damit widerlegt. Bluetooth sollte in Handys daher im Hidden-Modus betrieben oder besser gänzlich deaktiviert werden.

1.9 WPA im Verdacht

Der WLAN-Sicherheitsstandard WPA(2), über den in den letzten SSN berichtet wurde, kam am 26.07.2004 ins Gerede. Bei näherem Hinsehen entpuppte sich der beschriebene Angriff jedoch als „ganz normale“ Wörterbuch-Attacke auf das hinter WPA liegende RADIUS-Protokoll, die durch ein starkes EAP-Authentifikationsprotokoll und gut gewählte Shared-Secrets zwischen RADIUS-Server und WLAN-Access-Point verhindert werden kann.

1.10 SANS XP Survival Guide

Die „Lebenserwartung“ eines ungeschützten und mit dem Internet verbundenen PCs ist innerhalb eines Jahres von durchschnittlich 40 auf unter 20 Minuten gesunken. Das SANS Internet Storm Center ermittelt diesen Erwartungswert aus monatlich mehr als 1 Mio. Einzelmessungen. Im Mai wurde mit acht Minuten ein historischer Tiefststand erreicht. Als Anleitung für eine sichere Anfangskonfiguration und einen einigermaßen sicheren Betrieb empfiehlt sich der von SANS herausgegebene XP Survival Guide („Surviving the first day“).

1.11 BSI-Kongress 2005

Der 9. IT-Sicherheitskongress des BSI am 10.-12.05.2005 wird wie gewohnt in Bonn (Bad Godesberg) stattfinden. Anfang August hat das Programmkomitee den „Call for Papers“ veröffentlicht: Interessierte sind

aufgerufen, bis zum 08.10.2004 eine Kurzzusammenfassung (vier Seiten) mit Gliederung ihres Beitrags einzureichen.

2 Secorvo News

2.1 Secorvo College aktuell

Auf vielfachen Teilnehmerwunsch ergänzen wir – erstmalig am 23.09.2004 – unser Seminar Lotus Notes Security um einen Workshop, dessen Inhalte in Abstimmung mit den Teilnehmern aus folgendem Themenpool ausgewählt werden:

- Gruppen und Gruppenkonzepte
- ID-Administrationswerkzeuge
- Log Files
- Passwort Synchronisation
- Roaming User
- Antispam und Antivirus
- ECL
- Security Best Practices
- Betriebssystem-Sicherheit
- Notes Security Architecture Exposed

Dieser Workshop kann zusammen mit dem Seminar Lotus Notes Security oder separat gebucht werden; Frühbucher zahlen bis zum 31.08.2004 nur 580 € (zzgl. MwSt.). Weitere Auskünfte erteilt Frau Bradatsch (bradatsch@secorvo.de, 0721/6105-500).

http://www.secorvo.de/college

2.2 25. SSN-Jubiläum

Die vorliegende Ausgabe der Secorvo Security News ist die 25. – und unser Anspruch an Inhalt und Qualität entspricht nach wie vor dem, den wir im Editorial der Erstausgabe im Juli 2002 formulierten.

Seitdem hat uns viel Lob erreicht, und zahlreiche Unternehmen verbreiten die News inzwischen über ihr Intranet. Das freut und ehrt uns. Einer unveränderten Publikation der News als vollständiges .pdf stimmen wir grundsätzlich zu – und freuen uns über eine kurze Benachrichtigung: als Balsam für unsere Motivation.

3 Veranstaltungshinweise

September 2004	
20.-21.09.	Elektronische Geschäftsprozesse – EGP 2004 (Klagenfurt)
21.-22.09.	Lotus Notes Security (Secorvo College, Karlsruhe)
23.09.	Lotus Notes Security – Advanced (Secorvo College, Karlsruhe)
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)
28.-29.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
30.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Oktober 2004	
12.-13.10.	Live Hacking Lab (Secorvo College, Karlsruhe)
26.-27.10.	Inside Windows Security (Secorvo College, Karlsruhe)
November 2004	
02.-04.11.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
09.-11.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
22.-26.11.	Information Security Management (Secorvo College, Karlsruhe)

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

Impressum

ISSN 1613-4311

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

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

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

Secorvo Security News
September 2004

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

Nr. 9, 3. Jhrg. 2004
Stand 28. September 2004

ISSN 1613-4311

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

Inhalt

Editorial: Schicksal Patchen

Vor gut sieben Jahren erheiterte die angeblich von Bill Gates provozierte Pressemitteilung von General Motors, die in 13 Punkten beschrieb, was wäre, wenn Autos mit einer Technologie wie der von Microsoft gebaut würden. Drei Kostproben: „Wenn man bestimmte Manöver ausführt, z. B. eine Linkskurve, stellt sich das Auto ab und weigert sich, neu zu starten. Man muss dann den Motor neu installieren.“ Oder: „Das Airbag-System würde bei jedem Unfall fragen: ‚Sind Sie sicher?’ bevor es auslöst.“ Und: „Man muss den <Start>-Knopf drücken, um den Motor auszuschalten.“

Tatsächlich: Zwischen der Qualität eines Autos und der von Software lagen Welten. Ein Daimler mit Bluescreen? Ein Porsche, der selbstständig bootet? Ein BMW, der ‚Die Anwendung reagiert nicht’ meldet? Undenkbar. Warum aber war und ist Software nicht so fehlerarm wie ein Auto?

Der Grund ist einfach: Die präzise Produktion von Achsen, Kolben und Getrieben hat im Maschinenbau eine weit über 100jährige Tradition. Anders als die Softwaretechnik – sie existiert noch keine 20 Jahre. Denn allen theoretischen Ansätzen zum Trotz gebiert noch immer Erfahrung den größten Fortschritt. So versagten Fahrzeuge vor 80 Jahren – bei niedrigerer Geschwindigkeit und Belastung – weit häufiger als heute.

Vermutlich wäre GM heute zurückhaltender mit ihrer Replik. Denn in modernen Fahrzeugen werkeln inzwischen bis zu 50 vernetzte Kleinstrechner, um Antrieb, Beleuchtung, Sicherheitseinrichtungen und Steuerung zu koordinieren und an die Umgebungsbedingungen anzupassen. Der Preis: 2003 war die Fahrzeugelektronik Pannenursache Nr. 1. Wir werden also weiterhin damit leben müssen, dass Software Fehler enthält – im Schnitt 20 je 1.000 Programmzeilen, darunter auch Sicherheitslücken. Damit bleibt bis auf Weiteres das „Flicken“ (Patchen) eine wichtige Security-Disziplin. Allerdings unter verschärften Randbedingungen: Exploits sind inzwischen im Schnitt nach 5,8 Tagen verfügbar.

1 Security News

1.1 Erfahrungen mit XP SP 2

Im Schnitt treten bei 10 % aller Systeme nach der Installation des Service Pack 2 für Windows XP Probleme auf – das jedenfalls behauptet eine am 31.08.2004 veröffentlichte Studie des Asset Management Providers AssetMetrix auf der Basis von 340 befragten Unternehmen mit insgesamt 44.000 PCs. Dabei fanden sich signifikante Unterschiede zwischen kleineren und großen Netzen: Bei weniger als 100 Arbeitsstationen gab es bei gut 12 % der Systeme Probleme, während in grösseren Netzen nur etwa 6 % betroffen waren.

SANS führt derzeit ebenfalls eine (Online-) Umfrage zu Erfahrungen mit SP 2 durch. Zwischenstand: 42 % der knapp 2.100 Befragten hatten keine Schwierigkeiten, dafür aber 10 % große, nicht lösbare Probleme – und 12 % mussten ihre Systeme komplett neu aufsetzen. Trotz des nicht vernachlässigbaren Anteils negativer Erfahrungen raten wir aus Sicherheitsgründen weiterhin zur SP 2-Installation – jedoch erst nach intensiven Tests.

1.2 Abenteuer E-Banking

Das Erkennen von Phishing-E-Mails ist für viele Online-Banking-Anwender eine Herausforderung, nicht zuletzt wegen der perfide verfeinerten Tarntechniken der Absender. Wiederholt wurde von Fällen berichtet, in denen Kunden bereitwillig PIN und TANs preisgaben – und die Transfers der Täter erst in letzter Sekunde von der Bank rückgängig gemacht werden konnten. SANS publizierte am 10.09.2004 sechs Empfehlungen für Webseitenanbieter zur Erkennung von Phishing-Angriffen. Ein absolutes Muss für Entwickler ist Gunter Ollmanns 42seitiger Phishing Guide vom 23.09.2004.

Weit dramatischer jedoch ist die Wirkung des am 07.09.2004 erstmalig dokumentierten Trojaners Bizex-E, der eine knapp drei Wochen alte Schwachstelle des Internet Explorers ausnutzt – und systematisch PIN- und TAN-Eingaben abfängt. Für je einen Kunden der Dresdner Bank und der Postbank ist belegt, dass auf diesem Weg die PIN und eine gültige TAN entwendet und damit je ein vierstelliger €-Betrag auf ein Konto in Lettland überwiesen wurden. Beide Überweisungen konnten von den Banken noch gestoppt werden. Weitere vielleicht „erfolgreiche“ Fälle sind, auch bei anderen Banken, höchst wahrscheinlich.

Gegen Angriffe dieser Art hilft vor allem die Verwendung eines möglichst Fehler freien und restriktiv konfigurierten Browsers. Dafür ist seit Jahren (bekanntermaßen) der Internet Explorer nicht erste Wahl. Diese Überzeugung vertritt nun auch das BSI – zumindest kann man das Interview mit Sprecher Michael Dickopf zu diesem Anlass (Berliner Zeitung vom 10.09.2004) so lesen. Das Portal www.bsi-fuer-buerger.de empfiehlt unverblümter: „Um auf Nummer sicher zu gehen: Wechseln Sie den Browser“.

1.3 Es geht auch ohne...

Eine wichtige Ursache zahlreicher erfolgreicher Viren-, Wurm- und Trojaner-Attacken sind die administrativen Berechtigungen vieler Windows-PC-Nutzer. Erst diese hohe Berechtigungsstufe erlaubt die Installation und Deinstallation beliebiger Software. Daher wird schon lange empfohlen, Anwender nur mit eingeschränkten Rechten auszustatten. Neben dem Widerstand der Nutzer gegen den Rechteentzug sind Probleme mit Anwendungen, die Daten in Systemverzeichnisse schreiben oder auf geschützte Bereiche der Registry zugreifen, häufigstes Umsetzungshindernis.

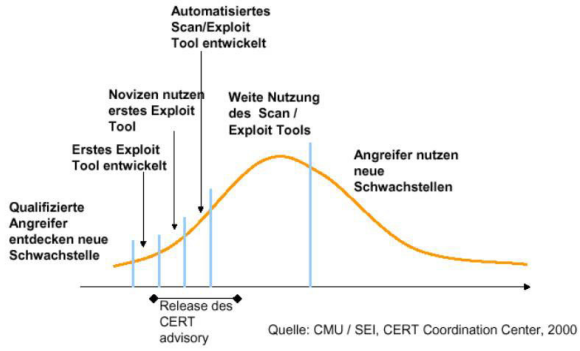
Oft gibt es jedoch eine (undokumentierte) Möglichkeit, die betroffene Anwendung auch ohne Administrationsrechte zu betreiben. Angeregt durch einen Beitrag in c't 15/2004 wurde solchen Problemlösungen die Webseite www.noadmin.de gewidmet. Zur Zeit können dort in einem Forum Tipps ausgetauscht werden; der Aufbau einer umfassenden Datenbank ist geplant.

1.4 Hacme Bank v1.0

Von Foundstone wurde am 08.09.2004 das kostenfreie Tool Hacme Bank veröffentlicht, eine Webapplikation, in die typische Schwachstellen integriert wurden. Gedacht ist es zur Schulung von Systemverantwortlichen und Entwicklern: Sie sollen die Schwachstellen mit geeigneten Analysetools entdecken. Solchermaßen sensibilisiert werden sie anschließend Schwachstellen in eigenen Applikationen hoffentlich selbst erkennen bzw. schon in der Entwicklungsphase vermeiden.

1.5 Laws of Vulnerabilities

Unter dem Titel "Laws of Vulnerabilities" publizierte Gerhard Eschelbeck, CTO von Qualsys, auf den diesjährigen Black Hat Briefings am 28.07.2004 in Las Vegas die Ergebnisse einer Auswertung von 6,5 Mio. Device Scans. Danach benötigen Unternehmen ab dem Bekanntwerden schwer wiegender Schwachstellen derzeit im Schnitt 62 Tage, um die Hälfte ihrer internen Systeme zu patchen, und 21 Tage für die Hälfte der direkt vom Internet aus erreichbaren Systeme.



Da die Zeitspanne zwischen Bekanntwerden einer Schwachstelle und der Verfügbarkeit eines Exploits oder der Ausnutzung durch einen Wurm immer kürzer wird – nach Symantecs aktuellem Security Thread Report vom 22.09.2004 schrumpfte sie in der ersten Jahreshälfte 2004 auf sechs (!) Tage – sollte ein wirksames Patch-Management derzeit ganz oben auf der Agenda des Security-Managements geführt werden.

1.6 Frechheit siegt...

Die marktführende Online-Handelsplattform Ebay wurde Ende August für einige Stunden außer Betrieb gesetzt – allerdings nicht durch eine Distributed Denial of Service Attacke, wie man vermuten könnte. Eine Privatperson hatte ganz dreist beim Provider intergenia die Domänen ebay.de und amazon.de bestellt. Der automatisierte KK-Antrag zur Übertragung der Domäne wurde von Amazon abgelehnt. Von Ebay kam jedoch keine Reaktion, und so wurde der korrekte DNS-Eintrag durch den der Webseite der Privatperson ersetzt.

Merke: Nicht nur in komplexen Anwendungen, sondern auch in einfachsten Prozessen kann der Wurm drin sein – und nicht unerhebliche Umsatzausfälle verursachen.

1.7 Gefahr durch VxWorks?

Frank Denis publizierte am 04.09.2004 auf der Mailing-Liste full disclosure eine kritische Schwachstelle von Storage Devices, die einen Controller von Engenio (ehemals LSI Logic) verwenden. Diese Devices werden u.a. in Fibre-Channel Switches von Brocade und in Storage-Systemen der Hersteller Storagetek (D series) und IBM (DS4xxx series, ehemals FAStT) sowie weiteren, wie SGI und Teradata eingesetzt.

Durch den Fehler kann das Device mit Hilfe spezieller IP-Pakete zum Absturz gebracht werden; in bestimmten Fällen ist ein Datenverlust möglich. Je nach Einsatzumfeld können die Auswirkungen eines solchen Angriffs erheblich sein. Vor diesem Hintergrund stimmen die Reaktionen der betroffenen Hersteller sehr nachdenklich: Nicht genug damit, dass die schon Mitte Juni durch Frank Denis informierten Hersteller trotz mitgesandtem funktionierenden Exploit, sofern überhaupt, erst nach mehreren Wochen reagierten. Sollte der Fehler, wie Storagetek behauptet, dem verwendeten Betriebssystem VxWorks zuzuordnen sein, dann könnten zahlreiche weitere Systeme betroffen sein. Der Hersteller Windriver war jedoch angeblich nicht bereit, sich des Falls ohne Lizenznachweis anzunehmen.

2 Secorvo News

2.1 Secorvo College aktuell

Die “Herbstsaison” hat begonnen. Mit dem gefragten „Live Hacking Lab“, das wir gemeinsam mit der Schweizer Compass Security und einem umfangreichen Laboraufbau durchführen, lassen wir Sie zwei Tage lang, vom **12.-13.10.2004**, einen Blick in die Hexenküche aktueller Angriffsmethoden werfen – von Spoofing und Sniffing über inside-out-Attacken bis hin zu SQL-Injektion und Cross-Site-Scripting.

Daran schließt sich am **14.10.2004** ein eintägiger Aufbauworkshop an, der Internet-Angriffe, LAN-Attacken und Penetrationstests vertieft.

http://www.secorvo.de/college

2.2 Und da waren es sechs...

Am 01.09.2004 konnte Secorvo auf sechs erfolgreiche Unternehmensjahre zurückblicken. Über 200 erfolgreiche Projekte, mehr als 650 zufriedene Teilnehmer aus über 220 namhaften Unternehmen, die an Seminaren von Secorvo College teilgenommen hatten, über 150 Fachpublikationen und mehr als 160 Fachvorträge sowie 1,5 Mio. Webseitenzugriffe auf Artikel, White Paper und 25 Security News dokumentieren unsere Entwicklung – auf die wir auch ein wenig stolz sind.

2.3 Secorvo wächst

Aufgrund der in den vergangenen Monaten erheblich gestiegenen Zahl von Projektanfragen erweitern wir unser Team. Ab dem 01.10.2004 wird Petra Barzin uns verstärken. Sie bringt neun Jahre Berufserfahrung in der IT-Sicherheit mit und hat sich u.a. als Autorin der Signatur-Interoperabilitätsspezifikation und der RFC 3039 (Qualified Certificates) sowie als Mitentwicklerin der SecuDE-Bibliothek einen Namen gemacht.

3 Veranstaltungshinweise

September 2004	
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)
Oktober 2004	
12.-13.10.	Live Hacking Lab (Secorvo College, Karlsruhe)
14.10.	Live Hacking Lab – Aufbauworkshop (Secorvo College)
26.-27.10.	Inside Windows Security (Secorvo College, Karlsruhe)
November 2004	
02.-04.11.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
09.-10.11.	Computer Forensic Symposium (Secorvo/VICCON, Karlsruhe)
09.-11.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
22.-23.11.	IT-Security Management (Secorvo College, Karlsruhe)
22.-26.11.	Information Security Management (Secorvo College, Karlsruhe)
Dezember 2004	
06.-07.12.	IsSec/ZertiFA 2004 (COMPUTAS, Berlin)

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

Impressum

ISSN 1613-4311

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

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

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

Secorvo Security News
Oktober 2004

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

Nr. 10, 3. Jhrg. 2004
Stand 29. Oktober 2004

ISSN 1613-4311

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

Inhalt

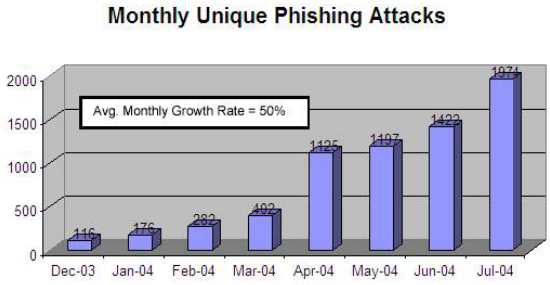
Editorial: Auf Phishfang

Erhoffe das Beste und sei gefasst auf das Schlimmste. (Anonymus)

Seit einem Jahr ist das gezielte Abgreifen von persönlichen Authentifikationsdaten in Mode. Im Hacker-Jargon wird das Ergattern von „hacked accounts“, so genannten „phishes“, seit 1996 als „phishing“ bezeichnet. Damals waren AOL-Accounts das Ziel; Phishes galten in Hackerkreisen als digitale Währung.

Mit dem Aufkommen von Spam haben sich Vorgehensweise und Angriffsziel geändert: In vermeintlich von einer Bank stammenden E-Mails, die das Corporate Design des Geldinstituts täuschend echt nachbilden, werden die Empfänger aufgefordert, eine verlinkte Webseite zu besuchen und dort ihre Authentifikationsdaten einzugeben, wie User-ID, PIN und TANs. Perfider noch ist verstecktes Phishing via Cross Site Scripting, mit Hidden Frames oder URL Obfuscation.

Bislang sind vor allem amerikanische Banken und Privatnutzer von diesen Angriffen betroffen. In Deutschland sind nur wenige Fast-Schadensfälle bekannt – die Überweisungen konnten noch rechtzeitig gestoppt werden. Das muss aber nicht so bleiben: Der Phishing Attack Trend Report der Anti-Phishing Working Group vom 30.08.2004 weist für den Zeitraum von Dezember 2003 bis Juli 2004 einen monatlichen Anstieg der Phishing-Angriffe um im Mittel 50 % aus.



Außer Aufklärung ist bisher kein Kraut dagegen gewachsen. Nur ein Positives lässt sich der neuen Plage abgewinnen: Vielleicht steigt durch Phishing die Sensibilität der Nutzer – auch in den Unternehmen.

1 Security News

1.1 Neue SANS Top 20

Am 08.10.2004 erschien Version 5.0 der SANS Top 20: Einer Liste der 20 kritischsten Internetschwachstellen, je zehn für Windows- und für Unix-Systeme, inklusive einer Auflistung der wichtigsten Patches. Sie wird jährlich aus den Einschätzungen zahlreicher internationaler Sicherheitsexperten zusammen gestellt. Diesmal auf Platz eins: die Standard-Installation von HTTP-Servern und die BIND-Implementierung des DNS. Auch eine deutsche Version der Top 20 ist verfügbar.

1.2 Scanner ausgetrickst

Jeder Virenscanner beherrscht heute die Analyse von .zip-Dateien. Am 18.10.2004 veröffentlichte iDefense jedoch eine perfide Methode, mit der sich diese Funktion bei vielen gängigen Virenscannern austricksen lässt: Setzt man im Header der .zip-Datei die Größenangabe der Originaldatei auf Null, überspringen diese Scanner das Archiv – die Dekompression beim Empfänger funktioniert jedoch weiterhin. Ein Update der Virenscanner-Software ist sehr zu empfehlen.

1.3 Linux strikes back

Nachdem Microsoft in Anzeigen und mit Veröffentlichungen zu belegen versucht, dass Linux das unsicherere Betriebssystem ist, hat sich nun Nicholas Petreley, ehemals Redakteur der Zeitschrift LinuxWorld, an einen Sicherheitsvergleich gewagt – sicherlich auch als Replik auf die umstrittene Studie von Forrester Research vom 19.03.2004 (siehe SSN 04/2004). Das Ergebnis der von Petreley am 25.10.2004 publizierten Studie, in der er 40 aktuelle Schwachstellen von Windows Server 2003 und Red Hat Enterprise Linux Advanced Server v3 verglich: Unter Anlegung gleicher Maßstäbe waren nur 10 % der Red Hat Bugs als schwer wiegend einzustufen, jedoch 50 % der Windows-Bugs.

Aus diesem Ergebnis ist nicht – und schon gar nicht generell – abzuleiten, dass Linux sicherer ist als Windows, wohl aber, dass in der Momentaufnahme von Petreley deutlich mehr der veröffentlichten Microsoft-Schwachstellen schwerwiegend waren. Über die nicht veröffentlichten und die unentdeckten Schwachstellen lässt sich nur spekulieren.

1.4 JPEG-of-Death

Bilder können nicht nur verbotenen und jugendgefährdenden Inhalts sein, sondern auch ein Trojanisches Pferd enthalten – das belegt Microsofts Warnmeldung vom 14.09.2004 (aktualisiert am 12.10.2004). Durch einen kritischen Fehler, der alle Betriebssystem- und Anwendungsprogrammversionen von Microsoft betrifft, kann das Öffnen von manipulierten (JPEG-) Bildern einem Angreifer die Ausführung beliebigen Programmcodes ermöglichen.

Seit dem 29.09.2004 sind solche Bilder unter der martialischen Bezeichnung „JPEG-of-Death“ in Umlauf, die den JPEG-of-Death-Exploit enthalten. Sie schieben dem System durch einen Buffer-Overflow einen kleinen Trojaner unter. Der Angreifer erhält über das Netzwerk Zugriff auf die Kommandozeile des angegriffenen Systems und kann es so kontrollieren. Um den Trojaner zu aktivieren genügt das bloße Ansehen eines manipulierten Bildes – auf einer Webseite, als Anhang oder sogar innerhalb einer E-Mail. Die Schwachstelle betrifft auch das weniger gebräuchliche Windows Metafile-Format (.emf/.wmf), wie ein weiteres Exploit von K-OTIK belegt.

Als Gegenmaßnahme sollten umgehend die Microsoft-Patches MS04-28 und MS04-32 installiert werden, da inzwischen schon „Baukästen“ zur Herstellung derartiger Bilder über das Internet verbreitet werden. Auch ein Update des Virenscanners kann helfen: Zahlreiche Hersteller haben ihre Signaturen angepasst und erkennen jetzt auch manipulierte Bilder.

1.5 Erfolgreiche Bug Bounty

Das Konzept des Bug Bounty Programms der Mozilla-Gemeinde vom 05.08.2004, für die Entdeckung jeder relevanten Schwachstelle eine Belohnung von 500 $ in bar auszuloben, scheint aufzugehen. Die ersten Prämien wurden am 14.09.2004 ausgezahlt – und die festgestellten Schwachstellen umgehend behoben. Ein Update auf die jeweils aktuellen Versionen von Mozilla, Thunderbird und Firefox wird empfohlen.

1.6 Samba Bug

Noch immer wirkt er weiter: Der am 30.09.2003 erstmals veröffentlichte Fehler im ASN.1-Parser von OpenSSL (SSN 10/2003), der in vielen Implementierungen eingesetzt wird – und von zahlreichen vergleichbaren Fehlern anderen in verbreiteten Produkten begleitet wurde (siehe SSN 11/2003, 1/2004, 2/2004, 8/2004). Am 13.09.2004 wurde ein solcher Bug in smbd festgestellt: Durch entsprechend präparierte Pakete können sowohl der Dämon als auch das Serversystem über das Netzwerk „abgeschossen“ werden. Die Installation des zur Verfügung gestellten Patches oder ein Update auf die aktuelle Version 3.0.7 wird dringend empfohlen.

1.7 Pufferüberlauf dank XML

Als Sprache für die Kodierung komplexer Datenelemente hat XML mittlerweile ASN.1 und proprietäre Formate in vielen Bereichen verdrängt. Dies ist sicherlich auch der Erwartung zu verdanken, dass XML-Datenstrukturen einfacher zu handhaben sein sollten als solche in ASN.1.

Zumindest aus dem Blickwinkel der Sicherheit müssen an dieser Erwartung mittlerweile Abstriche gemacht werden: Am 12.10.2004 veröffentlichte Microsoft den Patch für eine Sicherheitslücke bei der XML-Verarbeitung durch das hauseigene WebDAV-Modul, und am 26.10.2004 meldete ein Security-Alert, dass sich in aktuellen Versionen der weit verbreiteten XML-Bibliothek libxml2 des Gnome-Projekts ein halbes Dutzend Pufferüberläufe finden lassen. Tags darauf wurde Version 2.6.15 von libxml2 veröffentlicht, die diese Lücken stopfen soll.

Möglicherweise ist dies der Anfang einer zweiten Folgefehler-Geschichte, wie wir sie im ASN.1-Bereich erleben mussten (s.o.) – dann wäre zu befürchten, dass ähnliche Fehler in einer Implementierung nach der anderen entdeckt werden.

1.8 Vorsicht bei Browser-Eingaben

Dass JavaScript und andere aktive Inhalte sicherheitskritisch sein können, ist bekannt. Am 20.10.2004 wurden jetzt zwei weitere Probleme veröffentlicht, diesmal im Zusammenhang mit dem so genannten „tabbed browsing“, einer Funktionalität vieler Browser, mehrere Webseiten innerhalb eines Browserfensters darzustellen.

Tabbed Browsing kann immer dann problematisch sein, wenn JavaScript aktiviert ist: Die Eingaben, die ein Benutzer scheinbar auf der Webseite z.B. seiner Online-Bank tätigt, können durch geeignet manipulierte Skripte auf anderen Servern landen, wenn entsprechende Webseiten gleichzeitig (innerhalb eines anderen „Tabs“) im Browser angezeigt werden. Betroffen sind alle gängigen Browser in den aktuellen Versionen (siehe auch SSN 7/2004).

Solange keine Patches der Hersteller verfügbar sind, schützen nur die bekannten Verhaltenstipps: JavaScript nach Möglichkeit deaktivieren, URLs immer direkt aufrufen (nicht über Links) sowie andere Seiten (Tabs) schließen, bevor vertrauliche Daten wie Passwörter, PIN oder TAN in ein HTML-Formular eingegeben werden.

Ähnliche Probleme sind seit Jahren im Zusammenhang mit Java-Applets bekannt: Falls Java aktiviert ist, hat der Benutzer keine Kontrolle darüber, wann ein Java-Applet im Browser abläuft. Es kann auch erst dann gestartet werden, wenn der Benutzer längst auf anderen Webseiten „unterwegs“ ist.

2 Secorvo News

2.1 Secorvo College aktuell

Dreimal haben Sie in diesem Jahr noch Gelegenheit, von unseren Erfahrungen zu profitieren – auf dem Grundlagenseminar "IT-Sicherheit heute" vom **09.-11.11.2004**, der Einführung in das "IT-Security Management" vom **22.-23.11.2004** und dem einwöchigen Intensivseminar "Information Security Management" vom **22.-26.11.2004**. Auf Grund der großen Nachfrage empfehlen wir Ihnen bei Interesse eine baldige Anmeldung unter

http://www.secorvo.de/college

2.2 Neues Video in Arbeit

Nach dem großen Erfolg unserer Flash-Videos „Trojanisches Pferd" und „E-Mail-Sicherheit" zur Sensibilisierung der Mitarbeiter haben wir auf Kundenwunsch mit der Entwicklung eines neuen Videos zum Thema „Passwortsicherheit" begonnen. Das zehnminütige Video zeigt die Leistungsfähigkeit heutiger Passwort-Cracker, motiviert für die Verwendung hinreichend sicherer Passworte und zeigt, wie sich gute Passworte bilden und merken lassen.

Die Fertigstellung des Videos ist für Mitte Januar geplant; gerne können Sie ein Exemplar vormerken lassen.

2.3 IsSec und ZertiFA 2004

Anfang Dezember (**06.-07.12.2004**) finden die traditionellen COMPUTAS-Fachkonferenzen IsSec und ZertiFA im Herzen Berlins statt – in diesem Jahr als gemeinsame Veranstaltung unter dem Vorsitz von Stefan Kelm, Johann Bizer und Dirk Fox.

2.4 DuD 2005

Für Ihren Kalender: Die Konferenz DuD 2005 – Datenschutz und Datensicherheit findet vom **18.-19.04.2005** in Berlin statt.

3 Veranstaltungshinweise

November 2004	
09.-11.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
22.-23.11.	IT-Security Management (Secorvo College, Karlsruhe)
22.-26.11.	Information Security Management (Secorvo College, Karlsruhe)
23.-24.11.	Einführung in die Praxis des DSB (Euroforum, Wiesbaden)
Dezember 2004	
05.-09.12.	Asiacrypt 2004 (IACR, Jeju Island/Korea)
06.-07.12.	IsSec/ZertiFA 2004 (COMPUTAS, Berlin)
09.-10.12.	Einführung in die Praxis des DSB (Euroforum, Düsseldorf)
16.12.	Nächstes KA-IT-Si-Event (KA-IT-Si, Karlsruhe)
Januar 2005	
25.-26.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
27.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)

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

Impressum

ISSN 1613-4311

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

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

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

Secorvo Security News
November 2004

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

Nr. 11, 3. Jhrg. 2004
Stand 30. November 2004

ISSN 1613-4311

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

Inhalt

Editorial: Weniger ist weniger

Denken wir an Überwachung, so fallen uns Kameras, Abhöranordnungen und Lauschangriff, E-Mail-Filterung und Strafverfolgungsbehörden ein. Die Welt des „Großen Bruders“ hört, sieht und liest mit – und uns beschleichen klamme Gefühle, wenn wir uns eine Rundherumbeobachtung vorstellen.

Tatsächlich aber trügt unsere Wahrnehmung. Denn die Kernbedrohung unserer gesellschaftlichen Freiheit schlummert in einer weit weniger sichtbaren Gefahr. Sie kommt auf viel leiseren Sohlen daher – als die uns Deutschen vielleicht besonders eigene Neigung zur Dokumentation, zur Sammlung und Verschriftlichung, die dazu führt, dass wir das Mögliche archivieren – manchmal mehr als zulässig, fast immer mehr als erforderlich. Das gilt bei weitem nicht nur für Behörden – auch deutsche Unternehmen sind Weltmeister im Speichern, und vergessen das Löschen.

In seiner Grundsatzentscheidung zum Volkszählungsgesetz hat das Bundesverfassungsgericht 1983 so treffend formuliert: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, (...) kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“

Heute sollte man hinzufügen: Wer weiß, dass Vorgänge dokumentiert, gespeichert und zukünftig möglicherweise in ganz anderem Kontext ausgewertet werden, *wird* gehemmt *sein*, selbstbestimmt zu entscheiden. Aus dieser Perspektive könnten sich Ermächtigungen der Strafverfolgungsbehörden, sofern sie verhältnismäßig bleiben, als weit harmloser erweisen als etwa das geplante Anti-Diskriminierungsgesetz, das lückenlose Entscheidungsdokumentationen zur Folge haben dürfte.

„Liberty dies by inches”, konstatierte der kürzlich verstorbene Rechtsexperte Heinz Schueler schon 1979. Wie recht er hatte.

1 Security News

1.1 Phishing revisited

Die Perfidie von Phishing-Attacken nimmt weiter zu. Erste Phisher sind jetzt eine Ehe mit Schadprogrammen eingegangen. So wurde am 03.11.2004 eine Phishing-E-Mail gemeldet, deren aktiver Anhang die „hosts"-Datei im Windows-Verzeichnis system32/drivers/etc modifiziert. In dieser Datei werden IP-Adressen fest zugeordnet; üblicherweise findet sich hier nur die Lokalhost-Adresse 127.0.0.1. Werden in dieser Datei beliebigen Hostnamen, z.B. Webadressen, feste IP-Adressen zugewiesen, sind sie damit „fest verdrahtet": Der Browser bemüht dann nicht das DNS-Protokoll, um die korrekte Adresse zu finden, sondern nimmt die hier eingetragene – der ahnungslose Surfer sieht im Browserfenster die richtige WWW-Adresse, wird aber auf eine falsche Seite umgelenkt, ohne dass das für ihn erkennbar wäre.

1.2 IT-Grundschutzprofile

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 17.11.2004 auf ihrer Webseite drei Grundschutz-Profile jeweils für kleine, mittlere und große Unternehmen veröffentlicht, die die Umsetzung des BSI-Grundschutzhandbuchs vereinfachen sollen.

Analog zum „Leitfaden IT-Sicherheit kompakt" enthält die Handreichung für kleine Unternehmen eine Checkliste, die eine gute Hilfestellung darstellt. Bei den Profilen für mittlere (112 S.) und große Unternehmen (117 S.) werden die Vorgehensweise im Detail sowie sinnvoller Weise auch der Einsatz des Grundschutz-Tools vorgestellt. Praxisnah werden beim Profil für große Unternehmen zusätzlich mögliche Problemfälle und Lösungsmöglichkeiten aufgezeigt.

1.3 Internetspionage per Satellit

Laut einer aktuellen Untersuchung von Forschern der Ruhr-Universität Bochum konnten bei satellitengestützten Internetverbindungen einiger Provider unverschlüsselte Daten von und über andere Nutzer recht einfach in Erfahrung gebracht werden.

Es wird empfohlen, die auch sonst im Internetverkehr üblichen Sicherheitsmaßnahmen wie die Verwendung von verschlüsselten Protokollen zu nutzen.

1.4 Erste Bank mit IT-Grundschutz-Zertifikat

Das BSI konnte am 16.11.2004 die Vergabe des ersten IT-Grundschutz-Zertifikats an eine Bank vermelden: die PSD-Bank Westfalen-Lippe e. G. mit Sitz in Münster hat als erste Bank eine IT-Grundschutz-Zertifizierung erfolgreich durchgeführt.

1.5 SigG-Novelle

Am 19.11.2004 hat der Bundestag in zweiter und dritter Lesung das deutsche Signaturgesetz (SigG) novelliert. Zentrale Änderung: Für die Beantragung eines qualifizierten Signaturschlüssel-Zertifikats genügt nunmehr ein PIN-TAN-basierter Prozess – der eigenhändig unterschriebene Antrag mit Vorlage des Personalausweises ist bei bestehenden Kunden nicht mehr erforderlich. Damit kommt die Novelle einer zentralen Forderung der deutschen Banken entgegen, die eine Vereinfachung der Prozesse gefordert hatten, um ihre Bankkarten zu Signaturkarten aufwerten zu können.

Die Bundesregierung erhofft sich mit diesem Schritt eine erhebliche Ausweitung der nach wie vor nur marginalen Verbreitung qualifizierter Signaturen in Deutschland; freilich fehlen trotz dieser Verfahrensvereinfachung noch immer die seit vielen Jahren versprochenen Anwendungen für „Otto Normalsignierer", die für ihn einen erkennbaren Zusatznutzen darstellen und einen Technikwechsel rechtfertigen.

1.6 DNS-Ping-Pong

Dass auch in Protokollen aus der “Ur-Zeit” des Internet immer wieder Schwachstellen entdeckt werden, wird inzwischen niemanden mehr überraschen. Häufig handelt es sich dabei zum Glück nicht um konzeptionelle Schwachstellen, die einen Austausch aller Implementierungen des Protokolls erfordern würden, sondern um Programmierfehler. Manchmal jedoch sind davon dank „Code-Wiederverwendung“ zahlreiche Produkte betroffen.

So erging es nun auch dem vielleicht wichtigsten Protokoll – DNS, dem Domain Name System. Am 09.11.2004 warnte das britische NISCC in einem Advisory, dass verschiedene Hersteller das DNS-Protokoll in ihren Produkten fehlerhaft implementieren. Danach reagieren DNS-Server unter Umständen auf die einer DNS-Anfrage folgende Antwort mit einer erneuten DNS-Antwort. Dadurch können sehr schnell „DNS-Stürme“ ausgelöst werden, sofern zwei von diesem Fehler betroffene DNS-Server beteiligt sind – ein Szenario, das in großen Firmen-Netzwerken nicht unwahrscheinlich sein dürfte.

Analog zu bereits 1996 berichteten ähnlichen Problem auf UNIX-Systemen könnten Server durch geeignet Pakete auch dazu gebracht werden, sich selbst entsprechende Anfragen zu senden.

1.7 PDA-Forensik

IT-Forensik wird als Teildisziplin der IT-Sicherheit immer wichtiger. In forensischen Analysen tauchen dabei immer häufiger Untersuchungen zu Mini-Organizern auf, auch Personal Digital Assistants (PDAs) genannt, da diese vor allem im Firmenumfeld an Bedeutung gewinnen.

Dieser Entwicklung trägt jetzt das US-amerikanische National Institute of Standards and Technology (NIST) Rechnung: In den am 10.11.2004 vorgestellten „Guidelines on PDA Forensics“ erläutert das NIST die spezifischen Merkmale einer PDA-Analyse (u.a. am Beispiel von Palm OS und Pocket PC), führt in forensische Vorgehensweisen ein und stellt einige Tools vor, auf die in einem umfangreichen Begleitdokument im Detail eingegangen wird.

2 Secorvo News

2.1 Secorvo College aktuell

Im neuen Jahr startet Secorvo College mit einem zweitägigen Seminar zu Public Key Infrastrukturen (PKI) (25.-26.01.2005), an das sich am 27.01.2005 ein eintägiges PKI-Vertiefungsseminar für Fortgeschrittene anschließt. Im Februar folgen das Grundlagenseminare IT-Sicherheit heute (15.-17. 02.2005) sowie das fünftägige Schlüsselseminar zum Information Security Management (21.-25.02.2005), dessen erste drei Tage auch getrennt gebucht werden können. Erstmals wird am 21.-22.06.2005 auch die Prüfung zum „Certified IT-Security Professional“ abgenommen.

http://www.secorvo.de/college

2.2 Lead Auditor

Am 15.11.2004 wurde Jörg Völker, Autor eines der mit über 13.000 Downloads meistgelesenen Secorvo Whitepaper zum Information Security Management, als Lead Auditor nach dem Information Security Management (ISM) Standard BS 7799 zertifiziert. Das berechtigt ihn zur Durchführung von offiziellen Audits gemäß BS 7799, zur Vorbereitung auf oder der Abnahme von einer offiziellen BS 7799-Zertifizierung, die inzwischen auch in Deutschland zunehmend in den Fokus der Informationssicherheit stehen.

2.3 Forensik-Symposium

Am **01.-02.03.2005** veranstaltet Secorvo im Rahmen der Karlsruher IT-Sicherheitsinitiative ein Computer Forensik Symposium: ausgewiesene Experten aus unterschiedlichen Bereichen (BKA, Interpol, Recht und Technik) versprechen eine eineinhalb tägi-

ge intensive Beschäftigung mit forensischen Fragestellungen. Nicht zuletzt besteht im Rahmen des gemeinsamen Dinners ausreichend Möglichkeit zum Erfahrungsaustausch. Eine frühzeitige Anmeldung wird empfohlen.

2.4 Delegation und Haftung

Nicht nur Geschäftsführer, sondern auch IT-Leiter, IT-Sicherheitsverantwortliche und Datenschutzbeauftragte tragen eine erhebliche Verantwortung für den reibungslosen und gesetzeskonformen Betrieb der Informationstechnik eines Unternehmens.

Was bedeutet das im Falle eines Vorfalls? Wer haftet unter welchen Voraussetzungen gegenüber wem? Muss der IT-Leiter bei Regressforderungen mit seinem Vermögen gerade stehen?

Die Vielzahl der zu diesen Fragen kursierenden Behauptungen, Gerüchte und Befürchtungen ersetzt Professor Dr. Michael Bartsch auf der kommenden Veranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **16.12.2004** (Beginn: 18 Uhr) durch belastbare Fakten.

Wir freuen uns, mit Prof. Bartsch nicht nur einen ausgewiesenen Experten in diesen Fragen, sondern auch einen brillianten Redner gewonnen zu haben – wer schon einmal das Vergnügen hatte, ihn zu hören, wird diesen Termin nicht verpassen wollen; allen anderen sei er wärmstens empfohlen. Im Anschluss an Vortrag und Diskussion haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim kulinarischen Ausklang – "Buffet-Networking", sozusagen.

2.5 DuD 2005

Schon wirft sie ihre Schatten voraus: Die Konferenz „Datenschutz und Datensicherheit“ (DuD), seit sechs Jahren von COMPUTAS in enger Kooperation mit den Herausgebern und Autoren der Fachzeitschrift DuD veranstaltet. Zum Vormerken in Ihrem Kalender: **18.-19.04.2005**, Berlin.

3 Veranstaltungshinweise

Dezember 2004	
05.-09.12.	Asiacrypt 2004 (IACR, Jeju Island/Korea)
06.-07.12.	IsSec/ZertiFA 2004 (COMPUTAS, Berlin)
09.-10.12.	Einführung in die Praxis des DSB (Euroforum, Düsseldorf)
16.12.	Verantwortung, Delegation und Haftung (KA-IT-Si, Karlsruhe)
Januar 2005	
25.-26.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
27.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2005	
15.-17.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
21.-25.02.	Information Security Management (Secorvo College, Karlsruhe)
März 2005	
01.-02.03.	Computer Forensik Symposium 2005 (KA-IT-Si, Karlsruhe)

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

Impressum

ISSN 1613-4311

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

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

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

Secorvo Security News

Dezember 2004

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

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

ISSN 1613-4311

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

Inhalt

Editorial: Bekenntnis

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

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

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

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

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

1 Security News

1.1 Immer wieder MD5

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

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

1.2 WLAN-Schnorrer erwischt

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

1.3 Neues ISIS-MTT-Profil

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

1.4 NSA-Guide zu MacOS X

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

1.5 PGP Global Directory

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

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

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

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

1.6 Trojanisierte Fahrräder

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

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

1.7 Schwachstelle PHP

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

1.8 RFID-Studie online

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

1.9 Phisher auf der Lauer

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

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

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

2 Secorvo News

2.1 Secorvo College aktuell

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

2.2 Näher am Zug

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

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

2.3 Verstärkung

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

3 Veranstaltungshinweise

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

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

Impressum

ISSN 1613-4311

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

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

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