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