Secorvo Security News
Juni 2003

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

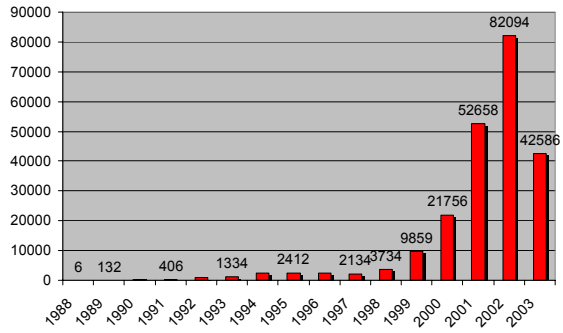
Nr. 6, 2. Jhrg. 2003
Stand 29. Juni 2003

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

Inhalt

Editorial: Keine Entwarnung

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



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

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

IT-Sicherheit bleibt eine Herausforderung.

1 Security News

1.1 Bugs in Netzwerktreibern

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

1.2 Trojaner in vermeintlichem Windows-Update

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

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

1.3 Sicherheitslücken in Lotus Notes

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

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

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

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

1.4 Malware-Statistik

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

1.5 Validierung von Zertifikatsketten

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

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

1.6 Neuer Microsoft Guide

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

1.7 BSI-Studien zu Webservern

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

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

1.8 NIST-Empfehlung: MAC

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

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

1.9 USENIX Security Symposium 2003

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

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

2 Secorvo News

2.1 Secorvo College aktuell

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

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

2.2 Lotus PKI White Paper

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

2.3 Awareness-Symposium

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

2.4 Forensik-Konferenz

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

3 Veranstaltungshinweise

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

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

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

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

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