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.

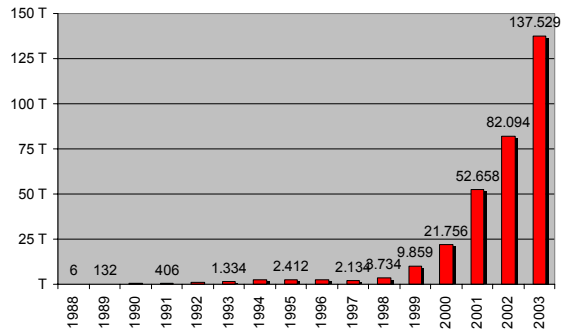
Bislang wurden vor allem die Protokolle HTTP und HTTPS als Tunnelmedien verwendet. Etliche Tools hierfür sind im Internet zu finden. Dass auch jedes andere Protokoll prinzipiell zum Tunneln missbraucht werden kann, demonstrierte die schweizerische Compass Security AG mit der Entwicklung eines DNS-Tunnel-Clients,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

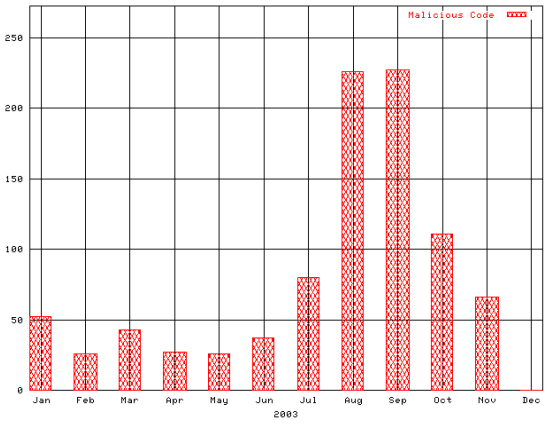
Der von Compass programmierte Client beinhaltet keinerlei Schadensroutinen und kann daher zur Überprüfung der eigenen Infrastruktur genutzt werden.

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