Secorvo Security News
Juni 2005

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

Nr. 6, 4. Jhrg. 2005
Stand 27. Juni 2005

ISSN 1613-4311

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

Inhalt

Editorial: Es wird ernst

Seit Jahren registrieren wir steigende Vorfallszahlen – jährlich eine Verdreifachung der Anzahl neuer Viren, Würmer und Trojaner, eine Verdoppelung der vom CERT registrierten Angriffsarten und einen rapiden Anstieg der in verbreiteter Software gefundenen kritischen Sicherheitslücken.

Allerdings: Der Anstieg der veröffentlichten – und nach unserer Beobachtung auch der der tatsächlichen – Schadensfälle entwickelte sich bislang moderat. Als Ursache dafür werden häufig wachsende Sensibilität der Verantwortlichen und die Etablierung wirksamer Schutzmaßnahmen vermutet.

Eine genaue Analyse der Angriffe und Schadensfälle zeigt jedoch, dass dies nicht die Hauptursache ist. Denn das vergleichsweise geringe Schadensniveau verdanken wir im Kern der Harmlosigkeit der Attacken:

- Die Entwickler von Viren und Würmern konzentrierten sich bisher auf Verbreitungs- und Tarnfunktionen; die Schadensroutinen waren oft primitiv und meist wirkungslos.
- Die Verbreitungsmechanismen waren ungezielt und nur auf große öffentliche Sichtbarkeit ausgelegt.
- Schäden wurden meist durch Programmierfehler verursacht; finanziell profitierten die Angreifer nicht.

Das ändert sich jedoch derzeit. Vermehrt lassen sich gezielte Angriffe beobachten, hinter denen wirtschaftlich interessante Geschäftsmodelle erkennbar werden: Im Auftrag entwickelte Trojaner, die Unternehmen aushorchen, ausgeklügelte Phishing-Attacken und Verschlüsselungs-Trojaner, die erst nach Lösegeldzahlung das Passwort preisgeben.

Daher wird es dringlich, die unseren Schutzmaßnahmen zu Grunde liegenden Annahmen zu überprüfen – denn gezielt geplante und professionell umgesetzte kriminelle Angriffe schaffen eine grundsätzlich neue Situation.

Die „Zeit der Spiele“ ist vorbei – es wird ernst.

1 Security News

1.1 Malcode Analysetools

David Zimmer vom Sicherheitsdienstleister iDefense hat am 07.06.2005 unter dem Namen Malcode Analyst Pack sieben Tools zur Analyse von Windows-Schadsoftware veröffentlicht. Darunter findet sich auch ein kleiner DNS-Server, der alle Anfragen an die IP-Adresse eines Forensikers lenkt. Die ebenfalls enthaltene Shell Extension zur Anzeige von Datei-Hashsummen im Explorer verwendet zwar noch den MD5 als Hashfunktion; da die Sammlung unter GPL Lizenz veröffentlicht wurde, steht einer Ersetzung durch den SHA nichts im Wege.

Dem wollte das BSI offenbar nicht nachstehen: Es veröffentlichte am 17.06.05 unter dem Namen BOSS (BSI OSS Security Suite) eine Knoppix CD mit Open Source Security Tools, darunter einer grafisch bedienbaren Version des Nessus Scanners. Dem beliebten Security Scanner wurde eine deutsche Oberfläche verpasst, die für versierte Nessus-User allerdings etwas gewöhnungsbedürftig ist. Da die Ergebnisse weiterhin in Englisch dargestellt werden und eine Übersetzung der inzwischen über 7.000 Nessus-Plugins recht aufwändig sein dürfte, sind Zweifel am Sinn dieser Eindeutschung angebracht. Auch wenn einige weitere Tools wie beispielsweise NMap mitgeliefert werden, besitzen spezialisierte Knoppix-Versionen wie Knoppix-STD deutlich umfangreichere Möglichkeiten.

Schließlich erschien am 22.06.2005 eine aktualisierte Fassung der Auditor Security Collection CD, eine der mächtigsten Sammlungen aktueller Versionen wichtiger Tools zur Durchführung von Sicherheitsanalysen.

1.2 Remote Desktop Attacke

Mit der am 10.06.05 erschienenen Version 2.7.3 des Auditwerkzeugs Cain&Abel ist es möglich – einen geeigneten Netzzugang vorausgesetzt – die Schutzmechanismen einer Remote Desktop Protocol Sitzung im Rahmen einer Man-in-the-Middle Attacke zu unterlaufen und die Tastatureingaben aufzuzeichnen. Betroffen von dieser Möglichkeit sind alle aktuellen Windows Releases (WXP SP2 / W2K3 SP1), auf denen die Terminal Services eingesetzt werden. Der Angriff funktioniert dank der integrierten ARP Poison Routing-Technolgie auch in geswitchten Netzwerkinfrastrukturen.

Ermöglicht wird dieser Angriff durch ein grob fehlerhaftes Design der initialen Public-Key Authentifikation bei Microsoft: Der generierte Public-Key des Terminal Servers, der bei der Initialisierung der Terminal-Session verwendet wird, wird mit einem Private Key signiert, der fest kodiert im Betriebssystem vorhanden und damit für jedermann auslesbar ist (mstlsapi.dll).

Zum Schutz vor diesem Angriff bleibt für eine sichere Remote Administration von Windows Systemen (XP/2003) auf Basis von RDP nur der konsequente Einsatz der Virtual Private Network Funktionalität.

1.3 VoIP-Scanning

Viele Hacker- und Analyse-Tools werden in den aktuellen Versionen mit Funktionen zum Mitschneiden von VoIP-Datenströmen ausgeliefert, mit denen Telefonate als wav-Datei gespeichert werden können.

Mit diesen Analysetools lassen sich sehr eindrucksvolle Demonstrationen gestalten – z. B. durch die Aufnahme eines via ARP-Poisoning umgelenkten Telefonats im internen Netz. Aber Vorsicht: Das Belauschen und Mitschneiden eines Telefongesprächs, selbst die „näheren Umstände“ (Zeitpunkt, Teilnehmer) auch eines erfolglosen Verbindungsversuchs ohne Wissen der Kommunikationspartner ist ein strafbewehrter Verstoß gegen § 88 TKG, der das in Artikel 10 Grundgesetz garantierte Fernmeldegeheimnis schützt – unabhängig vom Motiv des Abhörvorgangs und unabhängig davon, ob der Betreiber der Anlage geeignete Schutzmaßnahmen getroffen hat.

Für WLAN-Verbindungen gelten verschärfte Bedingungen: § 89 TKG enthält ein explizites Abhörverbot für Funkanlagen, das nicht nur Telefonverbindungen umfasst,

sondern alle Nachrichten, die für die Funkanlage nicht bestimmt sind. Erfolgt ein unbeabsichtigter Empfang, unterliegen die Daten der Geheimhaltung und dürfen nicht an Dritte weitergegeben werden.

1.4 Bluetooth-Angriff

Zwei israelische Forscher präsentierten am 06.06.05 einen Bericht, in welchem sie den erfolgreichen Angriff auf einen zentralen Sicherheitsmechanismus von Bluetooth – die PIN beim Pairing von Geräten – darstellen. Durch ein Belauschen des Pairing-Prozesses kann eine kurze PIN (4 Zeichen) selbst auf veralteten PCs (Pentium III, 450 MHz) in weniger als einer Sekunde (0,3 sec) bestimmt werden.

Zusätzliche Relevanz erlangt der Angriff dadurch, dass die Autoren auch beschreiben, wie ein Angreifer per Funk zwei bereits „gepaarte" Bluetooth-Geräte zum erneuten Pairing veranlassen kann – um auch deren PIN zu gewinnen.

1.5 Phisher-Test

Phishing-Angriffe nehmen nicht nur in ihrer Anzahl stetig zu – die verschickten E-Mails sind auch immer schwieriger von „echten" E-Mails zu unterscheiden. Wer mag, kann sein diesbezügliches Urteilsvermögen beim (zweiten) „Phishing IQ Test" der Firma MailFrontier auf die Probe stellen: Für zehn Beispiele (eBay, Amazon, Bank of America etc.) ist zu entscheiden, ob es sich um eine Phishing-Mail handelt.

Der Test schärft nicht nur die eigene Urteilsfähigkeit, sondern bietet dank ausführlicher Erläuterungen auch eine gute Hilfestellung bei der Gestaltung eigener Online-Dienstleistungen. Am ersten Test haben sich angeblich mehr als 225.000 Personen beteiligt.

1.6 SHA-Angriff publiziert

Für Kryptologen interessant: Die Autoren des SHA-Angriffs (siehe SSN 02/2005), die Forschungsgruppe um Wang, haben am 17.06.2005 ihre für die Crypto 2005 eingereichte Forschungsarbeit zu SHA-0 und SHA-1 öffentlich zugänglich gemacht.

1.7 Win Security Monitoring

Microsoft hat am 06.06.2005 einen Security Monitoring and Attack Detection Planning Guide veröffentlicht, der Hilfestellung bei der Konfiguration und Nutzung der Microsoft Windowxs Security Event Logs für ein wirksames Security Monitoring leistet. Im Anhang des 53seitigen Dokuments finden sich außerdem Empfehlungen für die Konfiguration der Audit Policy in den Group Policy Settings.

2 Secorvo News

2.1 Secorvo College aktuell

Nach einer Sommerpause in den Monaten Juli und August startet das College-Programm des zweiten Halbjahrs 2005 im September mit Seminaren zu Public Key Infrastrukturen (20.-21./22.09.2005) und Web-Application Security (27.-29.09.2005). Wir freuen uns, wenn wir Sie im Herbst auf einem unserer Seminare begrüßen dürfen.

http://www.secorvo.de/college

2.2 Suchen in Security News

Viele Leser schätzen die seit Juli 2002 monatlich erscheinenden Secorvo Security News wegen der zahlreichen Links auf wertvolle Originaldokumente. Bisher war die Suche nach älteren Links jedoch mühsam: Es gelang bestenfalls mit einer Volltextsuche in den pdf-Dateien des Jahrgangsarchivs, und gelegentlich hatte sich die gesuchte URL inzwischen verändert.

Daher finden sich inzwischen alle in den Secorvo Security News zitierten Dokumente vollständig im Security Finder und ermöglichen so eine thematische Recherche und eine regelmäßige Aktualisierung der Links. Mit dem Erscheinen der vorliegenden Juni-Ausgabe der SSN können jetzt auch SSN-Jahrgänge komplett im Security Finder durchsucht werden.

Zur Erinnerung: Bis 30.06.2005 gibt es den Security Finder noch zum Einstiegspreis.

2.3 Thitz gestaltet Plakat

Der Secorvo-Künstler Thitz hat für SWR3 das Plakat des diesjährigen New Pop Festival gestaltet – und folgt damit James Rizzie und Chales Kaufman, die 2003 und 2004 die Plakate entwarfen. Ein weiterer Meilenstein auf dem Weg zum Weltruhm – erst Ende 2004 hielt er mit einer Tüte zur Gründung Einzug in die „Sammlung Frieder Burda“ in Baden-Baden.

2.4 Security Awareness 2005

Die Materialien des diesjährigen dritten Security Awareness Symposium am 21. und 22.06.2005 sind jetzt – wie auch die der Vorjahresveranstaltungen – auf CD erhältlich – darunter die Präsentationen der Security Awareness Kampagnen von Bosch, Novartis und SAP, eine Vorstellung der Initiative „Deutschland sicher im Netz“ und ein Vortrag von Herrn Prof. Dr. Zerr zur Evaluation und Erfolgskontrolle von Awareness-Maßnahmen. Die CDs der beiden Vorjahresveranstaltungen enthalten Darstellungen der Kampagnen von BASF, BMW, Fiducia, Münchener Rück, RWE, der Schweizerischen Armee und T-Systems sowie weiterführende Materialien und eine Fotodokumentation der Ausstellung auf dem Symposium 2003.

2.5 Forensische Analysen

Die zunehmende Anzahl und „Qualität“ interner und externer Angriffe führt immer häufiger zu größeren Schadensfällen. In der Praxis treten damit verstärkt Fragestellungen nach dem Schadensumfang, der Zielsetzung des Angreifers und hinterlassenen Spuren für eine mögliche Strafverfolgung auf. Antworten auf diese und ähnliche Fragen kann eine Forensische Analyse liefern. Secorvo bietet diese Dienstleistung bereits seit einiger Zeit an – die wachsende Nachfrage hat uns nun dazu veranlasst, das entsprechende Leistungsangebot deutlich zu überarbeiten und zu konkretisieren.

3 Veranstaltungshinweise

Juli 2005	
05.-07.07	Western European Workshop on Research in Cryptography (WEWoRC, Leuven-Heverlee)
27.-28.07.	Black Hat Briefings (Black Hat USA, Las Vegas)
29.-31.07.	Defcon 13 (Defcon, Las Vegas)
August 2005	
01.-05.08.	14th USENIX Security Symposium (Usenix, Baltimore/US)
14.-18.08.	Crypto 2005 (IACR, Santa Barbara/US)
September 2005	
20.-21.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
22.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
27.-29.09.	Web-Application Security (Secorvo College, Karlsruhe)
Oktober 2005	
04.10.	Datenschutz kompakt (Secorvo College, Karlsruhe)
05.-06.10.	Inside Windows Security (Secorvo College, Karlsruhe)
11.-13.10.	IT-Sicherheit heute (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

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