Secorvo Security News
August 2006

Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Natalie Mareth, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 8, 5. Jhrg. 2006
Stand 17. August 2006

ISSN 1613-4311

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

Inhalt

Editorial: Feine Freunde

Das Wettrüsten zwischen den Entwicklern von Sicherheitstechnologien und den Erfindern von Penetrations- oder Umgehungsmöglichkeiten, gemeinhin „Hacker" genannt, durchzieht die Geschichte der IT-Sicherheit wie ein roter Faden.

Zwar stimuliert Wettbewerb bekanntlich die Qualität eines Produkts, und zweifellos wären ohne ein solches Stimulans weder Firewalls noch Hackingtools, weder Virenscanner noch Trojaner so leistungsstark und bedienungsfreundlich. Dennoch ist die Wirkung dieses Wettrüstens eher destruktiv und verursacht Kosten und Schäden.

Konnte man dem Wettkampf früher wenigstens in Ansätzen noch etwas Sportliches abgewinnen, da Viren und Würmer in der Regel keine komplexen Schadfunktionen enthielten und eher den Charakter eines „proof of concept" besaßen, haben kriminelle Interessen aus dem Wettkampf inzwischen eine Schlacht gemacht. Mit Spammern, Bot-Netzen, Warez-Servern und Phishing lässt sich Geld verdienen – oder zumindest waschen.

Aber nicht nur der Kampf ist härter geworden. Auch die Fronten verschwimmen. So verbreiten Softwarehersteller Copyright-Schutzmechanismen, die sich mit Stealth-Techniken im System verstecken oder wie Spyware verhalten (SSN 7/2006). Banken verwenden eigenartige Domain-Namen und führen wenig intuitive „Sicherheitsmerkmale" für ihr Online-Banking ein, die ein wechselndes und befremdliches Erscheinungsbild hervorrufen – und sich kaum mehr von einer Phishing-Seite unterscheiden lassen. Marketiers verschicken HTML-E-Mails mit versteckten URLs (um Empfängerreaktionen zu analysieren). Und Entwickler von Peer-to-Peer-Anwendungen wie Skype „perforieren" Firewalls trickreich mit dem verbindungslosen UDP-Protokoll – und etablieren so Kommunikationsverbindungen, die komplett an der Filterung vorbeilaufen.

Damit werden Hacking-Techniken zu Produkt-Features. Wer solche Freunde hat, braucht keine Feinde mehr.

1 Security News

1.1 Offene Fenster

Zum Patchday am 08.08.2006 wurden von Microsoft zwölf Sicherheits-Hotfixes veröffentlicht, von denen besonders die Sicherheitslücke im Server-Service und die so genannten RemoteExecution Schwachstellen erhebliche „Nachwirkungen“ haben dürften. Fatal ist, dass diese Lücken in fast allen Versionen der Windows-Familien 2000 / XP / 2003 inklusive Service Packs existieren – alle installierten Windows-Systeme, bei denen dieser Dienst ungeschützt aktiv ist, können derzeit automatisiert übernommen werden.

Die auf der Mailingliste Full Disclosure publizierte Schwachstelle im /proc-Filesystem, die lokalen Benutzern mit shell-Zugriff eine Privilegieneskalation bis auf root-Ebene erlaubt, erscheint dagegen fast als „harmloser“ Sonderfall.

Trotz Microsofts Paradigmenwechsel von der „Featuritis“ zur Softwaresicherheit als erster Priorität nimmt die Anzahl kritischer Schwachstellen nicht ab. Ohne sauber konfigurierte (Personal) Firewalls und ein konsequentes Patch-Management ist ein ausfallfreier IT-Betrieb inzwischen völlig undenkbar geworden.

1.2 Compliance

Am 07.07.2006 hat Microsoft seine zahlreichen Dokumente zu verschiedenen Themen der IT-Sicherheit um den Regulatory Compliance Planning Guide ergänzt. Darin werden auf 71 Seiten Maßnahmen zur Umsetzung der organisatorischen und technischen Anforderungen von Gesetzen und Standards mit Microsoft-Technologien und -Produkten dargestellt.

Vorgestellt und berücksichtigt werden Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), EG-Datenschutzrichtlinie sowie die ISO 17799 (2005). Zwar ist das Dokument mit „Microsoft-Brille“ geschrieben, enthält aber wertvolle Hinweise und Beispiele.

Es steht in engem Kontext anderer lesenswerter Microsoft-Dokumente zum Thema IT-Security wie dem Security Risk Management Guide, dem Security Monitoring and Attack Detection Planning Guide und dem etwas technischeren Windows Server 2003 Security Guide.

1.3 Rootkits auf der Blackhat

Auf der diesjährigen Blackhat vom 29.07.-03.08.2006 in Las Vegas wurden von Dino Dai Zovi und Joanna Rutkowska Rootkits für die neuen Intel- und AMD-Prozessoren präsentiert, die deren Virtualisierungstechniken nutzen. Bisherige Hardware Based Rootkits (SSN 04/2006) benötigten eine komplette virtuelle Maschine wie VMWare oder VirtualPC; die neue Generation führt die Virtualisierung im laufenden Betrieb durch und ist nicht einmal mehr an vermeintlichen Änderungen der Hardware erkennbar.

Schutz bietet derzeit nur die Deaktivierung der Virtualisierungsfunktionen im BIOS – sofern sie nicht benötigt werden.

1.4 Defcon Rocks

Die 14. Defcon vom 04.-06.08.2006, ebenfalls in Las Vegas, war etwas chaotischer organisiert als die Blackhat und begann mit zwei Stunden Verspätung. Die gebotenen Inhalte und das wohl "most hostile network on earth" machten diesen Mangel jedoch wett. Neben den verschiedenen Hacking-Events waren einige der „0-day attacks“ sehr spannend.

Unter anderem wurde vorgestellt, wie Systeme über Schwachstellen im WLAN-Treiber übernommen (Johnny Cache) und wie bei verbreiteten SmartPhones unter Windows CE 4.2 über Multi-Media Messages (MMS) beliebige Programmcodes zur Ausführung gebracht werden können (Collin Mulliner). Auch das Thema Blackberry-Security, insbesondere die Architektur, wurde von FX (Phenoelit) ausführlich beleuchtet.

1.5 PhishPharming

Deloitte veröffentlichte am 15.06.2006 den Global Security Survey 2006, Ergebnis einer Befragung von Datenschutz- und Sicherheitsbeauftragten weltweit tätiger Finanzinstitute über Art und Anzahl von Sicherheitsattacken. Eine wesentliche Beobachtung ist, dass systematische Angriffe, die auf finanziellen Gewinn abzielen, offenbar stark zunehmen. Mehr als die Hälfte der externen Angriffe (51 %) beruhten auf Phishing oder Pharming. Auch für das laufende Jahr zählen Identitätsdiebstahl und Betrug mit gefälschten Zugangsdaten zu den größten erwarteten Bedrohungen. Bei 58 % der Befragten rangieren Schutzmaßnahmen gegen diese Risiken unter den wichtigsten fünf Sicherheitsaktivitäten.

1.6 CrypTool v1.4

Die inzwischen unter Open-Source-Lizenz verbreitete Kryptografie-Lernsoftware CrypTool steht seit dem 31.07.2006 in der Version 1.4 zur Verfügung. CrypTool ermöglicht dem Nutzer einen anschaulichen Zugang zum Verständnis von kryptografischen Verfahren und deren Grenzen. Es wurde vor allem für die Mitarbeiter-Sensibilisierung und zu Ausbildungszwecken entwickelt (zur Historie siehe SSN 3/2002).

Neu sind neben Parametererweiterungen (längere Schlüssel, größere Dateien) und neu implementierten Verfahren und Angriffen unter anderem auch sehr verständliche Java-Animationen, die Schritt für Schritt die Funktionsweise der Verschlüsselung mit Caesar, Vigenère, Nihilist oder DES demonstrieren. Außerdem gibt es das Lernspiel „Der Zahlenhai“, das den Umgang mit Teilern und Primfaktoren veranschaulicht.

1.7 Standard-Kompass

Am 28.06.2006 hat der AK Sicherheitsmanagement des Bitkom Version 2.0 des „Kompass der IT-Sicherheitsstandards“ herausgegeben. Aktualisierung und Überarbeitung durch viele kompetente Autoren haben zu einem sehr informativen, 90seitigen „Standard-Werk“ beigetragen.

1.8 Auswertung Sommerquiz

Zahlreiche Zuschriften haben uns zu unserem Sommerquiz (SSN 07/2006) erreicht. Der kreativste Input kam von Hanno Langeweg aus Gjøvik in Norwegen – für seine Überlegungen bedanken wir uns mit einem Jahresabo für den Security-Finder.

Die meisten Kommentare bezogen sich auf die Annahme, dass bei ausgeschaltetem Telefon die Telefonnummer nicht in Erfahrung gebracht werden könne. Wird ein Mobiltelefon gezielt gestohlen, greift diese Annahme nicht: Die Telefonnummer des Opfers ist entweder bekannt oder kann leicht ermittelt werden. Häufig ist auch die eigene Nummer im Handy (nicht auf der SIM) gespeichert oder in Unterlagen notiert, die zusammen mit dem Handy entwendet werden (Handtasche o.ä.). Erwischt der Dieb ein eingeschaltetem Handy, kann er die Telefonnummer leicht ermitteln und sich damit die PUK besorgen.

Fazit: Die eigene Telefonnummer ist ein sehr schwaches alleiniges Authentisierungsmerkmal; O2 (und jedem anderen Helpdesk) empfehlen wir einen ausgefeilteren Authentisierungsprozess.

1.9 Ruf’ mich an, Kleines

In einem Fachvortrag setzte sich Doug Mohney am 02.08.2006 auf der Blackhat mit dem Thema Stimmanalyse in Callcentern und Großunternehmen kritisch auseinander. Als Schutz vor Social Engineering Angriffen erfreuen sich Stimmanalysesysteme mit Filtermechanismen (Whitelists, Blacklists, Word Spotting) und statistischer Stimm- und Stressanalyse derzeit großer Nachfrage. Tatsächlich stellen diese Systeme nicht nur ein attraktives Ziel für Identitätsdiebe dar, wie die zunehmende Anzahl von Angriffen auf Call-Center-Infrastrukturen zeigt, sondern sind auch datenschutzrechtlich problematisch: Sie erlauben die Erstellung von „Stimmprofilen“. Von da ist es nicht mehr weit bis zu „Stimmenspuren“, die wir im Netz hinterlassen – beispielsweise via Google Voice Search – und die systematisch recherchiert und missbraucht werden können.

2 Secorvo News

2.1 Secorvo College aktuell

In den Herbst startet Secorvo College mit zwei Anfang 2006 komplett renovierten „Klassikern“: dem Grundlagenseminar „IT-Sicherheit heute“ am 19.-21.09.2006 und dem Intensivseminar „PKI – Public Key Infrastrukturen“ vom 26.-29.09.2006.

Beide Seminare sind eine ausgewogene Mischung aus Theorie (Grundlagen, Hintergründe, Zusammenhänge) und Praxis (Vorführungen, Beispiele, Best Practices). Der Bewertung eines Teilnehmers des PKI-Seminars im Frühjahr 2006 haben wir nichts hinzuzufügen: *„Sehr gut strukturiertes Seminar für alle, die im Kontext PKI auf ‚Ballhöhe’ kommen wollen, aber auch für die, die es bereits sind.“*

Programm und Online-Anmeldung unter http://www.secorvo.de/college

2.2 TISP @ Secorvo College

Vor drei Jahren entwickelte TeleTrusT ein europäisches Expertenzertifikat für den Bereich Informationssicherheit – den „TeleTrusT Information Security Professional“, kurz TISP. Dieses Zertifikat wurde im Unterschied zu den zahlreichen internationalen Zertifikaten auf die spezifischen deutschen und europäischen Anforderungen zugeschnitten. In 18 Themenmodule sind die Inhalte gegliedert; Ausbildung und Prüfung erfolgen in deutscher Sprache.

Seit 2004 haben mehr als 100 Security-Experten die TISP-Ausbildung und –Zertifizierung absolviert. Drei Jahre Berufserfahrung und eine erfolgreiche Prüfung mit vorausgehender fünftägiger Intensivschulung sind dafür Voraussetzung.

Secorvo, selbst seit 1998 aktives Mitglied bei TeleTrusT, hat nun die Anerkennung als „TISP-Schulungsanbieter" beantragt und wird, vorbehaltlich der endgültigen Akkreditierung, am 20.-25.11.2006 die erste TISP-Schulung mit anschließender Prüfung durchführen.

3 Veranstaltungshinweise

August 2006	
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/US)
September 2006	
19.-21.09.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
26.-29.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2006	
04.-05.10.	Inside Windows Security (Secorvo College, Karlsruhe)
10.-12.10.	ISSE 2006 (TeleTrusT/EEMA, Rom/IT)
16.-20.10.	Information Security Management (Secorvo College, Karlsruhe)
17.-18.10.	DACH Mobility 2006 (GI/ÖCG/BITKOM/SI, München)
18.10.	KA-IT-Si-Jubiläumsfeier (KA-IT-Si, IHK Karlsruhe)
23.-27.10.	Systems 2006 (Messe München, München)
November 2006	
06.-07.11.	IT-Risk Management 2006 (COMPUTAS, Karlsruhe)
20.-25.11.	TISP-Schulung (Secorvo College, Karlsruhe)
26.11.	TISP-Prüfung (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

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

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