Secorvo Security News
Juli 2005

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

Nr. 7, 4. Jhrg. 2005
Stand 29. Juli 2005

ISSN 1613-4311

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

Inhalt

Editorial: Wilder Westen

Als ich nach Bloody Corner kam, sah ich von weitem her:
Die Summe unter meinem Namen hatte zwei Stellen mehr.
Ein Prämienjäger sagte: Pfeifer, ich wart' schon auf dich!
Ich fuhr herum, pfiff einen Ton –
dann sprach mein Colt für mich.

Bald zwei Jahre ist es her: Am 05.11.2003 setzte Microsoft im Rahmen des Antivirus Reward Program Kopfgelder in Höhe von insgesamt 5 Mio. US$ für Hinweise aus, die zur Identifikation und Ergreifung der Entwickler von Blaster, Sobig, MyDoom et. al. führen (SSN 11/2003). Mit der Verurteilung des Deutschen Sven Jaschan, Autor des Sasser-Wurms, am 08.07.2005 zu 21 Monaten Haft auf Bewährung kommt nun das erste Kopfgeld zur Auszahlung: Die beiden Whistleblower aus der „Szene“, die die entscheidenden Hinweise auf Jaschan gaben, erhalten 250.000 US$.

Zweifellos schreien die ausufernde Verbreitung von Viren und Würmern und die irrsinnigen Schadenssummen geradezu nach unkonventionellen Maßnahmen, um einer Entwicklung Einhalt zu gebieten, die die Informationstechnik als Ganzes existentiell zu bedrohen beginnt.

Dennoch drängt sich die Frage auf, ob diese medienwirksam in Szene gesetzten Kopfgelder noch angemessen sind. Der Maßnahme haftet nicht nur ein Hauch Selbstjustiz an, sondern sie verzerrt auch die Verhältnisse: Die Belohnungen deutscher Behörden für Hinweise auf Geiselnehmer, Mörder und Raubmörder bewegen sich zwischen 1.000 und 5.000 €. Ist daraus nun zu schließen, dass die Ergreifung eines Virenprogrammierers so begrüßenswert ist wie die Verhaftung von 50 bis 250 Kapitalverbrechern?

Bleibt zu hoffen, dass diese auf die Verursacher nahezu spurenloser Straftaten ausgesetzten monströsen Kopfgelder wenigstens zur Selbstanzeige motivieren...

Jetzt sitz’ ich hinter Gittern, von Zweifeln angenagt.
Vielleicht war doch des Denkers Plan
so gut nicht wie er sagt.
Er sagte: Es bringt Dir 10.000 Dollar, wenn Du's wagst
zum Sheriff ins Büro zu geh'n,
Dich vorstellst und ihm sagst:
Grüß Gott, ich bin der Pfeifer, ich komm' selber wie ihr seht,
um die Belohnung zu kassier'n, die auf meinen Kopf steht!
Reinhard Mey, Die Ballade vom Pfeifer

1 Security News

1.1 MBSA 2.0 verfügbar

Seit dem 01.07.2005 ist der Microsoft Baseline Security Analyser (MBSA) in der Version 2.0 verfügbar – ein seit Dezember 2002 angebotenes Tool (SSN 1/2003), das die Duchführung lokaler und Remote-Scans von Windows-Systemen auf Sicherheitsschwächen ermöglicht und detaillierte Vorschläge für Abhilfemaßnahmen liefert. Neu hinzugekommen sind neben einer verbesserten Bewertung der festgestellten Schwachstellen und fehlenden Patches umfangreiche Hilfefunktionen sowie die Unterstützung von Office XP und 64 bit Windows-Versionen. MBSA 2.0 ist kostenfrei und zu Microsofts Windows Server Update Services kompatibel.

1.2 Anwendungs-Bugs

Beim Thema Patch Management darf man die Anwendungen nicht vernachlässigen – auch diese können Schwachstellen aufweisen, die eine Übernahme des Systems mit dem Rechteprofil des Benutzers erlauben.

Das beweist eine am 05.07.2005 veröffentlichte Schwachstelle in Adobes Acrobat Reader 5.0.9 und 5.0.10 unter UNIX und Linux, die es einem Angreifer ermöglichen kann, durch Zusendung eines geeignet konstruierten PDF-Dokuments beliebigen Code auf dem Empfängersystem auszuführen. Ein Update auf die aktuelle Version des Readers wird empfohlen.

Eine ähnliche Schwachstelle wurde am 12.07.2005 in Microsoft Word 2000 und Word 2002 entdeckt: Ein Buffer Overflow erlaubt die Ausführung von Angriffscode über ein Word-Dokument. Passende Updates sind inzwischen verfügbar.

1.3 Exploits mit Trojaner

So genannte Exploits, das sind über das Internet verbreitete Quellcode-„Häppchen“, die neue sicherheitsrelevante Lücken in Betriebssystemen oder Anwendungen vorführen, verwenden häufig einen Codeabschnitt, der bei Ausführung des Programmcodes eine Kommandozeilen-Shell auf dem befallenen System startet.

Am 26.07.2005 wurde bekannt, dass zahlreiche der im Internet kursierenden Exploits versteckte Trojaner, Rootkits oder Schadensroutinen enthalten – dort wurde jeweils der Shellcode ersetzt. Jeder, der diesen manipulierten Code ausprobiert oder ihn sogar unverändert in ein Analysetool integriert, installiert beim ersten Starten einen Trojaner oder ein Rootkit auf seinem System – oder wird von einer rekursiven Löschfunktion („`rm -rf /*`“) überrascht.

1.4 CSI/FBI-Studie 2005

Seit dem 18.07.2005 ist der zehnte jährlich von CSI und FBI publizierte Computer Crime and Security Survey 2005 verfügbar, der aufgrund der regelmäßigen Durchführung und der rund 700 Befragten ein sehr repräsentatives Bild der Entwicklung der IT-Security in den USA zeichnet (siehe auch Studien-Überblick in SSN 4/2002).

Die Ergebnisse sind immer wieder erhellend: So liegen die durchschnlittlichen jährlichen Ausgaben für IT-Sicherheit bei 200-300 US$ je Mitarbeiter, hat der Missbrauch von WLANs erheblich zugenommen und verschlüsseln schon 68% der Unternehmen ihre Daten während der Übertragung.

1.5 Vorsorgeüberwachung

Mit seiner Entscheidung vom 27.07.2005 (1 BvR 668/04) hat das Bundesverfassungsgericht die Regelung des niedersächsischen „Gesetzes über die öffentliche Sicherheit und Ordnung“ (SOG) über die Zulässigkeit einer Telefonüberwachung zur „Vorsorge für die Verfolgung oder die Verhütung dieser Straftaten“ (§ 33a) als mit dem Grundgesetz nicht vereinbar und daher nichtig erklärt.

Ein wichtiges Urteil, denn es setzt erstmals seit den New Yorker Terroranschlägen vom 11.09.2001 den ausufernden Begehrlichkeiten und Kompetenzerweiterungen deutscher Strafverfolgungs- und Sicherheitsbe-

hörden eine verfassungsrechtliche Grenze. Bleibt zu hoffen, dass auch der Bundesinnenminister die Begründung liest.

1.6 Security-Checklisten

Mit dem Cyber Security Research and Development Act des Jahres 2002 wurde das amerikanische NIST verpflichtet, Checklisten zu entwickeln, die es erlauben, das für Hard- und Software bestehende und mit deren Nutzung einher gehende Risiko in US-Bundesbehörden zu minimieren. Das NIST startete daraufhin das „Security Configuration Checklists Program for IT Products“ und veröffentlichte am 26.05.2005 die gleichnamige NIST Special Publication SP 800-70 und das NIST Beta Checklists Repository.

Die Checklisten im Repository sind derzeit nach elf Kategorien sortiert, die mit sicherheitsrelevanten Checklisten anderer Regierungsorganisationen (u.a. NSA, DISA, CIS) und von Herstellern befüllt werden. Inzwischen finden sich darin insgesamt schon mehr als 50. Ziel ist, auf der Basis standardisierter Checklisten und des Austauschs von Erfahrungen die Voraussetzungen für ein vereinheitlichtes „Basis-Sicherheitsniveau“ zu entwickeln. Die eingereichten Checklisten werden daher vom NIST mit 32 formalen Rahmenparametern charakterisiert.

Das NIST plant, für Checklisten, die von Herstellern eingereicht werden, ein SP 800-70-Konformitätssiegel zu vergeben. Im Fall eines Siegelerhalts verpflichten sich die teilnehmenden Hersteller, die Garantie der Herstellerserviceverträge auf die Anwendung dieser Checklisten auszudehnen. Noch gibt es weder eine einheitliche Struktur noch das geplante Siegel, daher wurde das Repository auch als „Beta“ eingestuft. Einen Vorgeschmack auf mögliche zukünftige standardisierte Checklisten gibt die Spezifikation des Extensible Configuration Checklist Description Format (XCCDF). Allerdings warten auch die NIST-eigenen Dokumente noch auf die Umsetzung in XCCDF.

1.7 Postraub anno 2005

Am 07.06.2005 musste die Citybank öffentlich den Verlust eines Backup-Bands mit ca. 4 Mio. Kundendatensätzen während eines Transports durch United Parcel Service (UPS) einräumen. Die vermissten Datensätze enthalten u.a. auch die Social Security Numbers – und bilden damit die Grundlage für zukünftige Identitätsdiebstähle. Kein Einzelfall: Ameritrade vermisst seit Jahresanfang ein Band mit 200.000 Kundendaten, Time Warner verlor ein Tape mit Daten von 600.000 Kunden, und der Bank of America fehlen seit Mai 2005 100.000 Kundendatensätze.

Die Sicherheitslücke scheint systematisch zu sein: Offenbar umfass(t)en die Sicherheitskonzepte zwar die Erstellung von Backups, nicht aber den Umgang mit dieser höchst sensiblen Konzentration kritischer Daten. So waren die Daten auf den Bändern weder verschlüsselt, noch erfolgte der Versand unter besonderen Sicherheitsauflagen, wie z.B. dem Rückgriff auf einen besonders vertrauenswürdigen und sicherheitsüberprüften Kurier.

1.8 PKI-Token-Evaluierung

Immer häufiger kommen – nicht nur in PKI-Umgebungen – Hardware-Token wie USB-Sticks oder Smartcards zum Einsatz, um vor allem kryptographisches Schlüsselmaterial geeignet vor Missbrauch zu schützen. Jedoch funktionieren diese Token nicht immer mit der gewünschten Anwendung, bzw. bestimmte Anforderungen an die Sicherheit werden entgegen den Herstellerangaben nicht erfüllt.

Die DFN-CERT Services GmbH hat daher gemeinsam mit SURFnet mehrere dieser Hardware-Tokens intensiven Tests unterzogen. Die Autoren des Reports prüften die Verwendbarkeit von USB-Token zur PKI-Unterstützung in verschiedenen Standard-Anwendungen (u.a. Internet Explorer, Outlook, Mozilla, Acrobat) unter Windows und Linux. Mangels Teststellungen durch die Hersteller konnten von ursprünglich 20 ausgewählten nur acht Token getestet werden, von denen nur sechs aktiv Private-

Key Operationen im Token durchführen. Von diesen wiederum ist nur ein einziges in der Lage, Operationen mit asymmetrischen Schlüsseln durchzuführen, die länger sind als 1024 bit.

Das Ergebnis der Untersuchung ist wenig überraschend: Microsoft-Anwendungen und aktuelle Windows-Versionen werden allgemein gut unterstützt, auch wenn dem Benutzer einiges Mitdenken abgefordert wird. Bei Windows-Anwendungen, die über die PKCS#11-Schnittstelle bedient werden, traten bei verschiedenen Token Fehler auf. Auch decken sich Herstellerangaben nicht immer mit der Realität. Die Unterstützung für Linux bleibt vergleichsweise rudimentär.

2 Secorvo News

2.1 Secorvo College aktuell

Am 20.09.2005 startet das Programm des zweiten Halbjahrs 2005. In den bis dahin verbleibenden beiden Monaten werden alle Seminare einem gründlichen „Lifting“ und alle Vorträge – wie in jeder Seminarpause – einer systematischen Aktualisierung und Überarbeitung unterzogen.

Mehr noch: Unser Seminarangebot 2006 wird um neue Seminare zu aktuellen und spannenden Themen der IT-Sicherheit erweitert – mehr dazu im September. Auf ein Wiedersehen in Karlsruhe!

http://www.secorvo.de/college

2.2 eco-AK “Sicherheit”

Nach dem großen Zuspruch, den die Sitzung des von Dirk Fox geleiteten Arbeitskreises „Sicherheit“ des eco e.V. zum Thema „Zertifizierte Sicherheit“ am 08.04.2005 fand, wird die nächste Sitzung des Arbeitskreises am 16.09.2005 das Thema „Forensik“ vertiefen – wieder in den Räumen der Karlsruher Secorvo Security Consulting GmbH. Programm und Anmeldung sind in Bälde auf der Webseite des eco-Arbeitskreises verfügbar. Interessierte können sich in den E-Mail-Verteiler des Arbeitskreises aufnehmen lassen.

3 Veranstaltungshinweise

Juli 2005	
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	
05.-09.09.	Computer Network Forensics Workshop 2005 (IEEE/Create-Net, Athen/GR)
16.09.	Forensik (AK „Sicherheit“ des eco e.V.)
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)
25.-27.10.	Spurensuche im Web (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