Secorvo Security News
März 2006

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

Nr. 3, 5. Jhrg. 2006
Stand 26. März 2006

ISSN 1613-4311

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

Inhalt

Editorial: Der Grüffelo

„Zum Grüffelo? Sag, was ist das für ein Tier?“
„Den kennst Du nicht? Dann beschreib ich ihn Dir...“
Axel Scheffler, Julia Donaldson

Wie alt sind Ihre Kinder? Zwischen vier und zwölf? Dann kennen Sie zweifellos das wunderschöne Kinderbuch „Der Grüffelo“. Allen anderen sei die Geschichte schnell erzählt: Auf dem Weg durch den Wald begegnet die Maus ihren ärgsten Feinden – dem Fuchs, der Eule und der Schlange. Listig schlägt sie alle drei mit der Behauptung in die Flucht, sie sei mit dem Grüffelo verabredet – einem schrecklichen Tier, das sich bevorzugt von Fuchsspieß, gezuckerter Eule und Schlangenpüree ernähre.

Überrascht muss die Maus jedoch feststellen, dass es den Grüffelo tatsächlich gibt – und er genau so aussieht, wie sie ihn den Tieren in schillernden Worten beschrieben hat. In höchster Not behauptet sie, alle Tiere im Wald hätten Angst vor ihr – und beweist es, indem sie mit ihm Schlange, Eule und Fuchs aufsucht. Die nehmen sofort Reißaus, der Grüffelo aber ist tief beeindruckt – und ergreift selbst die Flucht, als die Maus erklärt, sie verspüre plötzlich Appetit auf eine Portion Grüffelogrütze ...

Die Erfolgsstrategie der Maus ist so einfach wie entwaffnend – der japanischen Kampfkunst Aikido ähnlich, die die Kraft des Angreifers nicht blockt, sondern umlenkt. Eine Technik, der sich auch die Scam Baiter bedienen, die die Versender von Betrugs-E-Mails der „Nigeria-Connection“ in Korrespondenzen verstricken und zur Versendung eigener Fotos verleiten. Möglicherweise ist dies eine Erfolgsstrategie im rechtsvollzugsarmen Cyberspace. Man stelle sich vor: Empfänger von Phishing-Mails, die die Betrüger mit falschen TANs auf präparierte Konten locken, als vorgebliche Geldboten Polizeikonten zur Überweisung anbieten oder mit Honeypots Hackern einen Crack vortäuschen – und beim Datendownload den Sound „Hab’ mich beim Hacken erwischen lassen“ installieren.

Keine Selbstjustiz – aber ein bisserl Sand im sich gerade organisierenden kriminellen Online-Getriebe könnte reinigend wirken.

1 Security News

1.1 Symantec Threat-Report

Am 07.03.2006 veröffentlichte Symantec die Ergebnisse ihres Sicherheitsreports für die zweite Jahreshälfte 2005. Danach ist ein deutlicher Anstieg der Internetkriminalität festzustellen, die vor allem professioneller und profitorientierter geworden ist. Insbesondere die Gefährdungen durch Bot-Netze und Schwachstellen in Webanwendungen haben deutlich zugenommen. Phishing bleibt eine ernst zu nehmende Bedrohung. Erschreckend: Die Entwicklung der Zahl neu entdeckter Viren und Würmer.

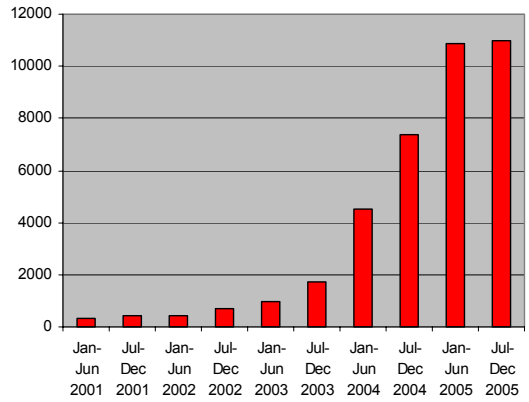

Abb.: Neue Viren und Würmer [Symantec]

1.2 Neues BSI-GSHB online

Die in den SSN 01/2006 vorgestellte aktualisierte Version des IT-Grundschutzhandbuches mit Unterteilung in IT-Grundschutz-Standards (BSI-Standard 100-1: Managementsysteme für Informationssicherheit, BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz) und IT-Grundschutzkataloge ist seit Anfang März online als PDF-Version verfügbar. Das Information Security Management basiert nun auf dem internationalen Standard ISO 27001; weite Teile des bisherigen IT-GSHB sind neu sortiert in den Katalogen zu finden. Die Änderungen wurden am 14.03.2006 auf der CeBIT vorgestellt.

1.3 Virenverseuchte Katzen?

Ja, Sie lesen richtig – mit Vogelgrippe hat dieser Beitrag allerdings rein gar nichts zu tun. Auf der diesjährigen Percom (IEEE International Conference on Pervasive Computing and Communications, 13.-17.03. 2006) wurde das Paper „Is your cat infected with a Computer Virus?" von Andrew Tanenbaum et al. zum Thema RFID-Viren mit dem Best Paper Award ausgezeichnet. Als proof-of-concept wurde ein Virus entwickelt, der sich in den 127 Zeichen fassenden Transponderspeicher eines Chips einschleusen lässt und die RFID-Middleware von Oracle infiziert.

1.4 Bürger-CERT

In seinem Newsletter vom 03.03.2006 stellt das BSI das gemeinsam mit Mcert gestartete Projekt Bürger-CERT vor. Ziel ist es, Bürger und kleine Unternehmen vor aktuellen Gefährdungen der IT-Sicherheit zu warnen und zu informieren. Die kostenlos herausgegebenen technischen Warnungen unterscheiden sich bislang jedoch kaum von anderen ebenfalls kostenfreien Diensten wie beispielsweise den DFN-CERT Advisories.

1.5 déjà-vu: Punkt im Pfad

Am 10.03.2006 berichtete Heise über eine von Reed Arvin entdeckte Möglichkeit, Berechtigungen durch ein installiertes ActiveState Perl zu eskalieren. ActiveState Perl stellt bei der Installation das Verzeichnis mit den Binaries an den Beginn des Systemsuchpfades und räumt dort allen Benutzern Schreibrechte ein. Dadurch kann ein nicht-privilegierter Benutzer einem Administrator beliebige Programme oder sogar DLLs unterschieben, die dann im Kontext des Administrators ausgeführt werden.

Dieses Verhalten ist unschön – aber alles andere als neu. Schon am 18.03.1993 wurde in der Unix-FAQ 2.13 davor gewarnt, den ´.´ (d. h. das aktuelle Verzeichnis, in dem sich beliebige Benutzeranwendungen befinden können) im Pfad zu führen. Auch 13 Jahre danach ist bei allen Betriebssys-

temen angeraten, den Pfad und darüber mögliche Kompromittierungsmöglichkeiten genau im Auge zu behalten.

1.6 Berechtigungseskalation

Ein weiteres Beispiel von Eskalations-Berechtigungen wurde von Ramon Kukla bei der Antivirensoftware Antivir von Avira (ehemals H+B EDV) festgestellt und am 11.03.2006 in full-disclosure veröffentlicht.

Die Fehlerursache liegt hier im Dienst „AntiVir PersonalEdition Classic Planer“, einem zum Virenschutz gehörenden Zeitplanungsdienst, der im System-Kontext läuft. Bei Updates wird über diesen Dienst ein Report erzeugt, der mit der Windows-Anwendung Notepad angezeigt wird – auch mit Systemberechtigungen, versteht sich. Ein Benutzer kann mit diesem Notepad System- und Konfigurationsdateien öffnen und ändern, obwohl er dazu gar keine Berechtigung besitzt. Auch die kostenpflichtige Premium-Variante der Lösung soll betroffen sein; eine Aktualisierung wird daher dringend empfohlen.

1.7 „Setzen, Sechs!“

Man könnte es für eine Satire halten: Die Washington Post berichtete am 15.03.2006 über die Ergebnisse der jährlichen Analyse der Sicherheit staatlicher Stellen in den USA. Eine der am schlechtesten bewerteten Behörden ist das Department for Homeland Security: Sie erhielt ein glattes „F“ für „failed“ – im dritten Jahr in Folge. Pikanterweise ist diese Behörde unter anderem für Terrorbekämpfung und „cyber security“ zuständig.

1.8 Datenbüchsen öffnen

Bereits im Oktober 2005 wurde der NIST Interagency Report 7250 Cell Phone Forensic Tools: An Overview and Analysis veröffentlicht. Dieser Bericht ist angesichts der am 27.02.2006 gemeldeten Handy-Trojaner brandaktuell: Er führt auf über 180 Seiten in guter und sehr detaillierter Form in die für forensische Analysen von mobilen Geräten verfügbare Software ein.

Insgesamt wurden 12 Toolkits evaluiert. Die im Dokument betrachteten Telefonie-Geräte haben teilweise einen engen Bezug zu Personal Digital Assistants (PDA), was auch durch die ihnen zu Grunde liegenden Betriebssysteme deutlich wird (Windows Mobile, Palm OS, RIM OS und Symbian).

Speziell für Manager und technische Entscheider, aber auch für Angreifer liest sich das Dokument zwischen den Zeilen wie eine Offenbarung hinsichtlich der Machbarkeit von Angriffen auf sensitive Daten in Mobiltelefonen. Bleibt zu ergänzen, dass ein starker Trend zu beobachten ist, Login/ Passwort-Kombinationen, PINs, TANs etc. auf solchen Geräten zu speichern. Zweifellos zur großen Freude derjenigen, die ein solch gut gefülltes Osterei „finden“.

1.9 Open Source Inspektion

Die ersten Ergebnissen der Open Source-Analyse der US-Regierung lesen sich auf den ersten Blick wie eine weitere Metrik, die die Welt nicht braucht. Die Ergebnisse liegen in einer Tabelle online vor und geben die Zahl der festgestellte Bugs pro 1.000 Zeilen Code an.

Die Messbarkeit im Bereich Sicherheit ist ein wichtiges, aber schwieriges Feld. Erfolgreiche Metriken erlauben konkrete Aussagen über betrachtete Entitäten. Auf den ersten Blick scheint die Metrik Fehler/ kLoC (1.000 Lines of Code) diesbezüglich wenig aussagekräftig. Sie ermöglicht zwar eine grobe Einschätzung, lässt aber keine Vergleichbarkeit zwischen den Projekten zu. Beispielsweise kann ein schwerer Fehler im Betriebssystem fataler sein als zehn leichte Bugs im Browser.

Der Ansatz der Autoren von Coverity geht jedoch über die reine Generierung von Metriken hinaus und nimmt mit den Verantwortlichen der betroffenen Projekte Kontakt auf, erläutert die festgestellten Schwachstellen und trägt so ein gutes Stück zur Verbesserung der Qualität von Open Source bei. Detailliertere Reports können auf Anfrage und nach erfolgter Registrierung bei Coverity heruntergeladen werden.

2 Secorvo News

2.1 Secorvo College aktuell

Der persönliche Kontakt zu den Referenten und die Möglichkeit, individuelle Fragestellungen in die Vorträge einfließen zu lassen, werden von unseren Seminarteilnehmern sehr geschätzt. Ein Mehrwert, dem wir mit unserem neuen Angebot Individuelles Coaching zukünftig noch mehr Gewicht verleihen. Sie erhalten im Seminarverlauf zusätzlich die Möglichkeit, individuelle Fragestellungen im „Vier-Augen-Gespräch“ mit einem ausgewählten Secorvo Security Consultant zu diskutieren.

www.secorvo.de/college

2.2 Wem die Stunde schlägt

Die Geschichte der Hans Unsicher GmbH, Ein (IT-)Drama, wie das Leben es schreibt. Sie erzählt vom Umgang des Mittelstands mit doch nicht ganz so unwahrscheinlichen Risiken („Uns wird schon nichts passieren“), vom Leichtsinn in Raten, versteckt in kleinen, alltäglichen Unternehmensentscheidungen: Ein etwas anderes Theaterstück über die ganz normalen Risiken des Unternehmerdaseins.

Uraufführung am 23.05.2006 in Rust (Anmeldung und nähere Informationen).

2.3 „DuD” im security-finder

Die von Secorvo entwickelte virtuelle Bibliothek zu IT-Sicherheit und Datenschutz erhält exklusive Inhalte: Ab dem 01.04.2006 werden Abonnenten des security-finder.de ausgewählte Beiträge aus früheren Jahrgängen der im Vieweg-Verlag erscheinenden Fachzeitschrift „Datenschutz und Datensicherheit“ (DuD) digital zugänglich gemacht – eine starke Bereicherung der inzwischen auf über 600 sorgfältig ausgewählten und kommentierten Publikationen angewachsenen elektronischen Fachbibliothek.

3 Veranstaltungshinweise

März 2006	
27.-28.03.	Datenschutz und Datensicherheit – DuD 2006 (COMPUTAS, Berlin)
28.-29.03.	D*A*CH Security 2006 (GI/Bitkom/TeleTrusT, Düsseldorf)
April 2006	
03.-07.04.	Information Security Management (Secorvo College, Karlsruhe)
25.-27.04.	Kommunikationsschutz und Datensicherheit (Secorvo College)
29.04. - 02.05.	15th EICAR Annual Conference (Eicar, Hamburg)
Mai 2006	
02.-03.05.	Security Awareness Symposium 2006 (Secorvo, Karlsruhe)
09.-10.05.	IT-Sicherheitsaudits (Secorvo College, Karlsruhe)
10.-11.05.	Datenschutzkongress 2006 (Euroforum, München)
11.05.	IT-Outsourcing sicher gestalten (Secorvo College, Karlsruhe)
16.-18.05.	Forensic Lab (Secorvo College, Karlsruhe)
23.05.	„Wem die Stunde schlägt“ (amec spie/Lampertz, Rust)
28.05. - 01.06.	Eurocrypt 2006 (IACR, St. Petersburg/RU)
30.05. - 01.06.	Web-Application Security (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