secorvo
security consulting

# Secorvo Security News

**Dezember 2006**

## Editorial: Top five

Die Tyrannei der Listen, denen Nick Hornby 1995 in „High Fidelity“ ein Denkmal gesetzt hat, beschränkt sich längst nicht mehr auf die „Top Ten“ des Musikgeschäfts. Wer heute ein Buch sucht, kommt an den einschlägigen „Bestsellerlisten“ kaum vorbei, und jeder Online-Shop, der etwas auf sich hält, bietet auf Mausklick eine Übersicht der meistverkauften Produkte. Nun haftet diesen „Best of“ ein wenig der Ruch einer Aktienempfehlung an: Hat ein Produkt den Olymp einer Top-Liste erklommen, wird die Nennung zur „self fulfilling prophecy“ (Robert K. Merton). Dabei ist deren Zustandekommen oft nicht frei von Willkür: Erst kürzlich wurde ein Plattenproduzent überführt, große Bestände einer Neuerscheinung selbst aufgekauft zu haben, um mit dem Bestseller-Status die Verkäufe anzukurbeln. Eine probate Methode, um Ladenhüter in Saisonhits zu verwandeln.

Auch in der IT-Sicherheit geht der Trend zur Liste: SANS veröffentlicht seit sechs Jahren die „Top 20“ der Internet Security Attack Targets, OWASP pflegt seit 2003 die „OWASP Top Ten“ der kritischsten Fehler in Web-Anwendungen, und auf den Webseiten aller Anti-Viren-Hersteller findet man die „Viren des Monats“.

Bei so viel Orakel-Prominenz wollen wir uns nicht drücken – daher hier die Secorvo Top Five der Security-Trends 2007:

1. ***Sichere Softwareentwicklung***: Wenn die Software-Industrie hier nicht punktet, droht eine Regulierung der EU.
2. ***Awareness***: Angesichts zunehmender Mobilität und technischer Konvergenz wird das Nutzerverhalten zum Schlüsselfaktor.
3. ***Datenschutz***: Sensibilisierte Benutzer und gestärkte Aufsichtsbehörden reduzieren das verbreitete Vollzugsdefizit.
4. ***Best Practices***: Gestiegene (Haftungs-) Risiken lassen den Ruf nach Standards, Audits und Best Practices lauter werden.
5. ***Anti-Phishing***: Gelingt es nicht, den kriminellen Onlinekonten-Zugriff zu stoppen, kann das Vertrauen in das eBusiness kippen.

## Inhalt

secorvo
security consulting

# Security News

## BOSS reloaded

Am 01.12.2006 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Verfügbarkeit der Version 2.0 seiner Sicherheits-CD BOSS (BSI OSS Security Suite) bekannt gegeben. Sie umfasst Version 2.2.8 von Nessus mit deutsch übersetzter Oberfläche; die Nessus-Meldungen erscheinen allerdings nur in englisch. Unter den weiteren Tools zur Sicherheitsanalyse findet sich überraschend Version 0.10.10 des bekannten Sniffers Ethereal vom 11.03.2005 (statt einer aktuellen Version des Nachfolgers Wireshark).

Auch wenn die BOSS-CD aus den inzwischen zahlreichen Tool-Suites nicht signifikant hervor sticht – die Veröffentlichung ist ein Signal, dass das BSI weiterhin auf die Rechtmäßigkeit des Besitzes und der Verbreitung von Hacking-Tools setzt.

## Zero-Day und Hexenjagd

Seit Anfang Dezember gibt es einen öffentlichen und übersichtlichen Informationsdienst zu Echtzeitschwachstellen (Zero-Day Tracker). Darin werden erstmals alle Schwachstellen zusammengefasst, für die bereits technische Details zur Ausnutzbarkeit bekannt sind, der Hersteller aber noch keinen Patch veröffentlicht hat. Wichtig für IT-Sicherheitsmanager, die ihre Risiken aktiv steuern, sind die Angabe, wie lange eine ungepatchte Schwachstelle bereits bekannt ist (z.B. seit 393 Tagen) und wie zwischenzeitlich improvisiert werden kann. Ob zukünftig dort auch nicht behobene Fehler von Anwendungen, Datenbanken und Netzsoftware eingestellt werden, bleibt abzuwarten.

Von den Herstellern sollte das Angebot als Ansporn zur Verbesserung der Sicherheit in der Softwareentwicklung verstanden werden. Repressalien sind sicher die falsche Antwort, wie im Fall des Boarding Pass Generators "Create your own boarding pass" für Northwest Airlines versucht: Der PhD-Student Christopher Soghoian hatte darin ein seit über drei Jahren bekanntes organisatorisches Sicherheitsloch als Proof-of-Concept in Software umgesetzt.

## Final BS 25999-1:2006

Ende November 2006 wurde vom British Standards Institute (BSI) die Endfassung des BS 25999-1:2006 veröffentlicht. Dieser „Code of Practice for Business Continuity Management" gibt Empfehlungen für Notfall- und Notfallvorsorgeplanung in Unternehmen. Ein zweiter Teil, der eine Zertifizierung analog BS 7799-2 ermöglichen wird, soll 2007 folgen. Der neue Standard löst PAS 56 ab und wird ergänzt durch die im August 2006 veröffentlichten Empfehlungen PAS 77:2006 „IT Service Continuity Management".

Eine Gelegenheit zum Erfahrungsaustausch bietet vom 01.-02.02.2007 die Konferenz „3rd Annual: BUSINESS CONTINUITY 2007" in London.

## Fuzzing with JBroFuzz

Am 13.11.2006 wurde im OWASP-Projekt das Fuzzing-Tool JBroFuzz veröffentlicht. JBroFuzz ist ein „stateles network protocol fuzzer" zur Aufdeckung von Schwachstellen in Netzwerkprotokollen durch halbautomatisch generierte fehlerhafte Datenpakete. Die intuitive Oberfläche von JBroFuzz erlaubt auch Anfängern, die Funktionsweise von Fuzzing nachzuvollziehen und anzuwenden. Das in Java programmierte Tool steht plattformübergreifend zur Verfügung.

Die Architekturen von Web 2.0 stellen neue Anforderungen an die Sicherheit von Online-Anwendungen. Interessant, auch im Zusammenspiel mit JBroFuzz, ist das Mozilla-Plugin Firebug, mit dem sich die Sicherheit von Web-Applikationen schnell auf vielfältige Weise untersuchen lässt.

## DFN-PKI CA im Browser

Die oberste Zertifizierungsstelle des Deutschen Forschungsnetzes, die DFN-PCA, feiert 2006 ihren 10. Geburtstag. Dass sie nicht zum alten Eisen zählt, beweisen etliche Neuigkeiten, über die am Nikolaustag informiert wurde. Die spektakulärste darunter ist, dass das Root-Zertifikat der DFN-PCA ab sofort über einen direkten Zertifizierungspfad in die wichtigsten Standard-Browser verfügt.

Um dies zu realisieren wählte man nicht den teuren und aufwändigen Weg der direkten Einbindung in die Browser – vielmehr hat eine Kooperation mit der in den Browsern bereits enthaltenen Deutsche Telekom Root CA dazu geführt, dass störende Warnmeldungen, z.B. beim Aufbau einer SSL-Verbindung, der Vergangenheit angehören. Von diesem im Forschungsumfeld bislang weltweit einmaligen Schritt profitieren sowohl Endanwender mit kostenlosem Webserver-Zertifikat als auch die vielen Forschungseinrichtungen, die den Betrieb ihrer CA an die DFN-PKI ausgelagert haben.

## Virtuelle Kriminalität

Am 21.02.2005 veröffentlichte McAfee den ersten Bericht zum Thema virtuelle Kriminalität. Beschrieben wurde darin der Trend zum Missbrauch des Internet für Zwecke des organisierten Verbrechens.

Am 08.12.2006 wurde der zweite Bericht der Öffentlichkeit vorgestellt. Er enthält eine Reihe kon-

kreter Fallstudien und Zitate von Security-Experten zu virtueller Kriminalität. Zu den drei wesentlichen Erkenntnissen zählen (1) die Entstehung einer neuen Generation von Kriminellen, die das Internet für Straftaten nutzt, die bislang nicht oder nur schwer durchführbar waren; (2) die Entdeckung der Missbrauchsmöglichkeiten durch die organisierte Kriminalität, die insbesondere Großereignisse wie die Fußball-WM für virtuelle Straftaten ausnutzt; sowie (3) die noch immer unterschätzte Bedrohung durch Innentäter. Nur der Titel mag nicht passen – denn virtuell ist diese Kriminalität bei Weitem nicht.

### Honey-Clients

Die Honeypot-Technologie wird in der Regel server- oder netzwerkseitig – beispielsweise in Form kompletter Honeynets – betrieben. Einen interessanten anderen Ansatz verfolgen Client-Honeypots: Sie suchen selbst aktiv nach Schad-Software auf Webseiten, mit denen ungepatchte Browser angegriffen werden können.

Bereits 2005 stellte Microsoft Research mit dem Projekt „Strider HoneyMonkey“ eine Realisierung von XP-basierten Client-Honeypots vor (SSN 8/05). In den vergangenen Tagen wurden drei weitere viel versprechende Ansätze veröffentlicht:

- Bei Capture handelt es sich um einen „High Interaction Client Honeypot", der insbesondere Webseiten nach versteckten Viren, Würmern und Trojanern durchsucht und die Ergebnisse protokolliert. Capture läuft in einer virtuellen Umgebung, so dass das System nach einer Infizierung schnell „gesäubert“ werden kann.
- Wie Capture sucht auch Monkey Spider nach maliziösen Webseiten, hat eine deutlich weniger aufwändige Architektur und zählt eher zur Klasse der „Low Interaction Honeypots“. Es basiert unter anderem auf CWsandbox.
- Botspy schließlich geht einen Schritt weiter: Es beobachtet Bot-Netze, die häufig die Quelle für per E-Mail versandte Phishing- oder Viren-Nachrichten sind.

Fazit: Obwohl die Tools sich in einem frühen Entwicklungsstadium befinden, zeigen sie die Leistungsfähigkeit des Client-Honeypot-Ansatzes.

### Privatsphäre mit Microsoft

Vom 16.10.2006 datieren die „Privacy Guidelines for Developing Software Products and Services“ von Microsoft (v2.1). Einige der darin postulierten Prinzipien decken sich mit dem europäischen Datenschutzrecht – wie Datensparsamkeit, Transparenz und Nutzerkontrolle. Insgesamt ist das Dokument jedoch stark „sicherheitslastig“ und betont Integrität und Zugriffsschutz, vergisst aber das Prinzip der Zweckbindung. Auch die Checklisten der gut gemeinten beispielhaften Szenarien lesen sich mit europäischen Augen eigenwillig: Für das „anonyme Monitoring“ durch einen Internet-Provider wird die „explizite Zustimmung des Nutzers“ gefordert.

Immerhin wurde die Bedeutung des Datenschutzes von Microsoft durch die Integration der Guidelines in den „Trustworthy Computing Security Development Lifecycle (SDL)“ unterstrichen.

### Alle Jahre wieder...

...findet der DFN-CERT Workshop „Sicherheit in vernetzten Systemen“ in Hamburg statt – am 07.-08.02.2007 nun schon zum 14. Mal. Neben etlichen spannenden eingereichten Beiträgen bildet der eingeladene Vortrag zu „Stealth Malware – can good guys win?“ von Joanna Rutkowska ein Highlight.

### Augen auf beim Weihnachtskauf

Die Warnung der bayrischen Polizei vom 24.04.2006 vor dem Kauf von Plüschtieren mit eingebauter Überwachungskamera ist laut Pressemitteilung vom 11.12.2006 von mindestens einem Käufer ignoriert worden. Diesem drohen jetzt rechtliche Konsequenzen, da nach § 90 Telekommunikationsgesetz (TKG) schon der Besitz von Sendeanlagen, „die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind“ verboten ist. Vorsicht beim Kauf Ihrer Weihnachtsgeschenke!

## Secorvo News

### Secorvo College aktuell

In das Jahr 2007 startet Secorvo College mit den aktualisierten Seminarklassikern ISM – Information Security Management (23.-26.01.2007), PKI (30.01.-02.02.2007) und IT-Sicherheit heute (06.-08.02.2007), gefolgt von dem komplett überarbeiteten Seminar Erfolgsfaktoren für IT-Sicherheitsmanagement (26.02.-01.03.2007).

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

### T.I.S.P.

Auf seiner Sitzung am 07.12.2006 bei Secorvo hat sich das T.I.S.P.-Board darauf verständigt, 2007 eine Weiterentwicklung des erfolgreichen T.I.S.P. Zertifikats in Angriff zu nehmen. So ist geplant zusätzliche Spezialisten-Zertifikate zu entwickeln. Die zweite T.I.S.P.-Zertifikat-Schulung mit anschließender Prüfung wird Secorvo am 05.-09.03.2007 durchführen; mehrere Anmeldungen liegen bereits vor.

## Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

| Dezember 2006 | |
|---|---|
| 24.12. | Heiligabend |
| 27.-30.12. | 23. Chaos Communication Congress (CCC, Berlin) |
| **Januar 2007** | |
| 18.-19.01. | Tutorium "IT-Sicherheitskriterien im Vergleich" (DFN-CERT Services GmbH, Hamburg) |
| 23.-26.01. | Information Security Management – von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe) |
| 30.01.-02.02. | PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe) |
| **Februar 2007** | |
| 06.-08.02. | IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College, Karlsruhe) |
| 07.-08.02. | DFN-CERT Workshop: Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg) |
| 26.02.-01.03. | Erfolgsfaktoren für IT-Security Management (Secorvo College, Karlsruhe) |
| 26.-27.02 | Net-ID 2007 (Computas, Berlin) |

## Fundsachen

Auszug aus www.security-finder.de

Microsofts Security Risk Management Guide (v1.2) beschreibt einen vierphasigen Planungsprozess für ein effektives Security Risk Management System. Die Vorgehensweise basiert auf etablierten Industriestandards und Best Practices. Der Guide umfasst eine Sammlung von Excel-Tools.


## Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

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

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