# Secorvo Security News
## November 2003

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

Nr. 11, 2. Jhrg. 2003
Stand 21. November 2003

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

## Inhalt



## Editorial: Wer misst, misst Mist

Der vom allgegenwärtigen Spardruck ausgelöste Trend, Leistungen und Kostentreiber im Unternehmen durch Kennzahlen transparent zu machen, hat mit Balanced Scorecards und Benchmarks nach dem Management die IT erfasst.

Nun ist auch die IT-Sicherheit in den Fokus des „Erbsenzählens“ geraten. Zunächst einmal ist das nicht besonders verwunderlich. Denn IT-Sicherheit kostet Geld, und je besser sie funktioniert, desto weniger sichtbar ist sie – je schlechter sie funktioniert, desto kritischer wird sie beäugt. In beiden Fällen stehen die Kosten unter Rechtfertigungsdruck.

Hinzu kommt ein der Unternehmensleitung nicht immer leicht verständlich zu machendes, aber elementares Faktum: IT-Sicherheit ist kein „binärer Zustand“ – die beliebte „Sind wir sicher?“-Frage konnte noch kein IT-Sicherheitsverantwortlicher eindeutig mit „Ja“ oder „Nein“ beantworten (jedenfalls nicht ohne rot zu werden).

Die Wirklichkeit liegt – wie so oft – zwischen den Extremen. Wo aber liegt sie genau? Sind wir gut genug, um den Anforderungen von KontraG, GmbHG und Basel II zu genügen? Tun wir das Erforderliche? Entsprechen unsere Maßnahmen dem „Stand der Technik“? Wirken unsere Maßnahmen? Und nicht zuletzt: Werden wir besser?

Die Fragen sind nicht neu. Aber bisher haben wir es uns geleistet, sie unbeantwortet zu lassen. Den Kostendruck sollten wir nun als Chance nutzen, die IT-Sicherheit über Metriken zu einer Entwicklungsgröße im Unternehmen zu machen. Das ist eine anspruchsvolle Aufgabe, denn es fehlt an akzeptierten Messgrößen und Bewertungsschemata. Immerhin gibt es Beispiele, und erste Normierungsversuche, wie die jüngsten Publikationen des NIST und der CESG zeigen. Bei der Umsetzung sollten wir jedoch immer Einstein im Kopf behalten:

*Nicht alles, was zählt, kann gezählt werden,*
*und nicht alles was gezählt werden kann, zählt.*
*Albert Einstein (1879-1955)*

# 1 Security News

## 1.1 Neuer BfD im Amt

Am 14.11.2003 wurde nach langem politischen Ringen hinter den Kulissen und mit mehrmonatiger Verzögerung der von den Grünen vorgeschlagene ehemalige stellvertretende Hamburgische Datenschutzbeauftragte Peter Schaar vom Bundestag als Nachfolger von Joachim Jacob zum Bundesbeauftragten für den Datenschutz (BfD) gewählt.

Dafür, dass ihm die Arbeit nicht ausgeht, wollen die Parteikollegen sorgen: Nach dem rechtspolitischen Sprecher der Bundestagsfraktion, Jerzy Montag, soll geprüft werden, Verschlüsselungsschlüssel zukünftig beim BfD zu hinterlegen.

## 1.2 EU-Spam illegal

Mit Artikel 13 („Unerbetene Nachrichten") der EU-Datenschutzrichtlinie für elektronische Kommunikation vom 12.07.2002 (Amtsblatt der EG L 201/47, 31.07.2002) wurden per E-Mail, Fax oder SMS verschickte Nachrichten zum Zweck der Direktwerbung für illegal erklärt, wenn sie ohne „Opt-Out"-Hinweis oder unter Verschleierung der Absenderidentität gesendet werden. Die Richtlinie fordert sogar – sofern keine Kundenbeziehung besteht – aktives „Opt-In" als Voraussetzung. Die Richtlinie war bis zum 31.10.2003 in nationales Recht umzusetzen. Die Bundesregierung verpasste (auch) diesen Termin – damit gilt sie jetzt als übergeordnetes Recht.

Allerdings dürfte die Richtlinie ein „zahnloser Tiger" bleiben: Spammer agieren – sofern überhaupt feststellbar – fast immer aus Ländern außerhalb der EU.

## 1.3 (K)eine Linux-Backdoor

Am 05.11.2003 entdeckte eine Gruppe von Linux-Kernel-Entwicklern, dass jemand versucht hatte, eine Hintertür in die 2.6er Entwicklungsversion des Linux-Kernels einzubauen. Dem Quellcode wurden zwei Programmzeilen hinzugefügt, die es einem normalen Benutzer ermöglicht hätten, Administrationsberechtigung zu erlangen.

Die Änderung betraf allerdings nicht die „heilige" Kernel-Source-Referenz, sondern die an anderer Stelle exportierten Dateien im Concurrent Versioning System (CVS). Nach Angaben von Bitkeeper, dem Hersteller der Kernel-Source-Verwaltungssoftware, wäre eine Änderung des Referenzcodes unverzüglich festgestellt worden.

## 1.4 Noch mehr fehlerhafte ASN.1-Dekodierer

Dass auch Sicherheitssoftware Opfer von Fehlern in gemeinsam genutzten Funktionsbibliotheken sein kann, zeigen mehrere Schwachstellen, die kürzlich – wie in den Security News 10-2003 berichtet – in OpenSSL, mittlerweile aber auch in verschiedenen anderen SSL- und S/MIME-Produkten gefunden wurden.

Quelle dieser Bugs ist die „Abstract Syntax Notation" (ASN.1), die beschreibt, wie z. B. X.509-Zertifikate und geschützte S/MIME-Nachrichten für den Transport zu kodieren sind. Fehler in der ASN.1-Kodierung können bei zahlreichen Implementierungen zu Pufferüberläufen oder Denial-of-Service-Angriffen führen. Da diese Schwachstellen innerhalb von verbreiteten Krypto-Bibliotheken entdeckt wurden, sind weit mehr Hersteller von diesem Problem betroffen, als ursprünglich berichtet. Entsprechend aktualisierte Listen findet man beim CERT/CC.

## 1.5 Macht Microsoft ernst?

Die Anzeichen mehren sich, dass Microsoft künftig tatsächlich Sicherheit über Funktionalität stellen wird: In einer E-Mail an BugTraq warnt Microsoft-Mitarbeiter Michael Howard, Co-Autor von „Writing Secure Code", am 12.11.2003, dass die sicherere Grundkonfiguration des angekündigten Windows XP SP 2 zu fehlerhaftem Verhalten von Anwendungen führen kann.

## 1.6 VPN Key Cracker

Dass eine Schwäche des Internet Key Exchange Protokolls (IKE) eine Kompromittierung des häufig in IPsec-VPNs verwendeten „Preshared Key“ ermöglicht, ist seit April 2003 bekannt. Inzwischen gibt es auch Tools, die derartige Angriffe unterstützen, wie z. B. ikecrack. Seit Version 2.5 beta36 hat auch das beliebte Multifunktions-Sniff- und -Crack-Tool Cain eine solche Funktion, den „IKE Aggressive Mode Pre-Shared Keys Cracker“, integriert.

Seit dem 07.11.2003 ist der Scanner ike-probe verfügbar, der prüft, ob ein VPN-Gateway anfällig für diese Attacke ist.

## 1.7 Happy Birthday, Malware

Genau 20 Jahre war es am 03.11.2003 her, dass Fred Cohen im Rahmen seiner Doktorarbeit den ersten experimentellen Computervirus entwickelte. Was damals noch als theoretisches Hirngespinst erscheinen konnte, hat sich in der Zwischenzeit zur realen Plage und Bedrohung entwickelt und Anti-Virus-Software als ganz neue Produktklasse entstehen lassen.

Microsoft hat nun härtere Bandagen angelegt und am 05.11.2003 5 Mio. US $ Kopfprämien für Hinweise ausgesetzt, die zur Ergreifung der Viren-Entwickler von Blaster und Sobig führen. Angeblich häufen sich derzeit in Bagdad die Selbstanzeigen...

## 1.8 Stichwort: „Regression Bug“

„Regression Bug“ nennt es der Softwareentwickler, wenn sich bei einer beabsichtigten Verbesserung ein neuer oder gar ein alter, eigentlich schon behobener Fehler wieder einschleicht.

Auf ein Paradebeispiel dafür hat am 11.11.2003 Microsoft hingewiesen: Wer das am 09.09.2002 veröffentlichte Service Pack 1 (SP 1) zum Internet Explorer 6 nach dem am 20.06.2003 erschienenen SP 4 für Windows 2000 installiert, führt damit einen schwerwiegenden Fehler bei der Auswertung von SSL-Serverzertifikaten wieder ein, der einem SSL-Server die Ausstellung weiterer gültiger Zertifikate ermöglicht.

## 1.9 „RFID-Wanzensucher“

Am 06.11.2003 wurde der FoeBuD e.V., bekannt durch die jährliche Verleihung der BigBrother Awards für „Datenkraken“, von der Stiftung bridge mit einen Ideenpreis ausgezeichnet. Mit dem Preisgeld von 15.000 € wird nun ein Warngerät zum Aufspüren von RFID (Radio Frequency Identification) Transponderchips entwickelt.

Dahinter verbirgt sich ein ernsthaftes Datenschutzproblem: RFID Chips, die es erlauben, berührungslos einen eindeutigen ID-Code auszulesen, sind inzwischen so miniaturisiert, dass sie mit bloßem Auge kaum noch zu erkennen sind. Sie werden, auf Verpackungen oder Waren befestigt, von vielen als die „Wunderwaffe“ zur weiteren Rationalisierung von Logistik und Warenwirtschaft angesehen. Einmal mit einer Person in Verbindung gebracht, eröffnen sich faszinierende Möglichkeiten der Profilerstellung – vom Einkaufsverhalten im Laden (Bewegungsmuster) bis hin zur Verfolgung des Lebenszyklus einer Verpackung. Der Drang zum raschen Einsatz dieser neuen Technik könnte dabei wieder einmal der Beherrschung von Missbrauchsmöglichkeiten davoneilen (FoeBuD-Positionspapier vom 19.11.2003).

## 1.10 Bluetooth Security

Adam Laurie veröffentlichte am 11.11.2003 in BugTraq eine kurze, vierseitige Übersicht über aktuelle Angriffe und sicherheitsrelevante (Implementierungs-) Fehler in Bluetooth-Geräten. Die Anfälligkeit für Backdoor-Angriffe, SNARF-Attacken und das sogenannte „Bluejacking“ wies er für mehrere verbreitete Handy-Typen nach.

Zwar verfügt Bluetooth über zahlreiche, konzeptionell vergleichsweise gute Sicherheitsmechanismen; deren Wirksamkeit hängt allerdings in der Praxis von der Qualität der jeweiligen Implementierung ab.

# 2 Secorvo News

## 2.1 Secorvo College aktuell

Anfang November 2003 ist das Seminarprogramm von Secorvo College für das erste Halbjahr 2004 erschienen. Im Seminarkalender 2004 finden Sie eine ganzjährige Terminübersicht. In das Jahr 2004 startet Secorvo College mit zwei zentralen Themen: Information Security Management am **19.-23.01.2004** (auch als zweitägiges Seminar buchbar) und Public Key Infrastrukturen (PKI) vom **27.-28.01. 2004** – mit zusätzlichem Vertiefungstag am **29.01.2004**.

## 2.2 Whitepaper Information Security Management

Einen Überblick über die aktuelle Fassung des britischen Standards zur Informationssicherheit, BS 7799, gibt das am 06.11. 2003 erschienene White Paper von Jörg Völker: BS 7799 – Von „Best Practice“ zum Standard (pdf, 376 kB).

## 2.3 ISIS-MTT Siegel für Entrust Authority™

Nach eingehenden Tests im offiziellen ISIS-MTT-Prüflabor von Secorvo wurde dem „Entrust Authority™ Security Manager 7.0 for Windows" des kanadischen Unternehmens Entrust am 05.11.2003 als weltweit erstem Produkt das ISIS-MTT-Siegel in der Produktklasse „CA Server“ verliehen. Damit ist nun von unabhängiger Seite bestätigt, dass (und wie) Anwender mit dieser Software ISIS-MTT-konforme PKI-Zertifikate und Sperrlisten ausstellen können.

## 2.4 Video „E-Mail Security“

Das von Secorvo entwickelte Video „E-Mail Sicherheit“ steht nun auch, vertont mit einem „Native Speaker“, in englischer Sprache zur Verfügung. Diese Version ist als Intranet-Lizenz erhältlich und kann über die Secorvo-Webseiten bestellt werden.

# 3 Veranstaltungshinweise

| | |
|---|---|
| **November 2003** | |
| 25.-26.11. | E-Mail-Sicherheit (Secorvo College, Karlsruhe) |
| **Dezember 2003** | |
| 03.-04.12. | PGP-Lösungen im Betrieb (Secorvo College, Karlsruhe) |
| 08.-09.12. | IsSec 2003 (Computas, Berlin) |
| 08.-10.12. | IT-Security- und Risk-Management (ZfU, Zürich) |
| **Januar 2004** | |
| 19.-23.01. | Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe) |
| 20.-21.01. | Einführung in die Praxis des betr. DSB (Euroforum, München) |
| 27.-28.01. | Public Key Infrastrukturen (Secorvo College, Karlsruhe) |
| 29.01. | PKI für Fortgeschrittene (Secorvo College, Karlsruhe) |
| **Februar 2004** | |
| 03.-04.02. | DFN-CERT Workshop "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg) |

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

## Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

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