Secorvo Security News
August 2003

Dirk Fox, Hans-Joachim Knobloch,
Holger Mack, Dr. Markus Michels
Secorvo Security Consulting GmbH

Nr. 8, 2. Jhrg. 2003
Stand 22. August 2003

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

Inhalt

Editorial: „Eisberg rechts voraus!“

Der entsetzte Ruf vom Ausguck der Titanic, ausgestoßen am 14. April 1912 um 23:40 Uhr, steht für ein Ereignis, das die Welt erschüttert hat: den qualvollen und vermeidbaren Tod von über 1.500 Passagieren, verursacht durch die Hybris der Techniker, die das Schiff als „unsinkbar“ erklärten und nur 20 Rettungsboote vorsahen – zu wenig selbst für die Hälfte der Reisenden.

Haben wir aus diesem Unglück gelernt? Natürlich sind Unternehmens- und Behördennetze heute mit einer Firewall abgesichert. Was aber, wenn diese vom „Eisberg“ erwischt wird – durch einen unentdeckten Software-Fehler oder eine scheinbar harmlose Kommunikationsverbindung, die tatsächlich einen Trojaner auf Client-Systemen installiert, wie der aktuelle Blaster-Wurm?

Bei der Titanic mussten immerhin fünf Schotten volllaufen, bevor sie sank. Nur hatte niemand mit einem Eisberg gerechnet, der gleich fünf der Länge nach aufriss. In unseren Kommunikationsnetzen geben wir uns häufig mit einem Schott zufrieden – und glauben einfach nicht an den Eisberg. Wie Kapitän E.J. Smith: „*When anyone asks me how I can best describe my experience in nearly forty years at sea, I merely say, uneventful. (…) I never saw a wreck and never have been wrecked nor was I ever in any predicament that threatened to end in disaster of any sort.*“ (New York Times-Interview kurz vor der verhängnisvollen Jungfernfahrt der Titanic).

Kommt uns das nicht bekannt vor? „Bei uns ist noch nie etwas passiert.“ Stimmt vielleicht. Wenigstens hat es niemand bemerkt. Dürfen wir aber daraus Aussagen über die Zukunft ableiten? Da lohnt es, sich das Bonmot von Winston Churchill auf der Zunge zergehen zu lassen:

„*Der beste Zeitpunkt für eine Prognose ist kurz nach dem Ereignis.*“
Allerdings hilft sie dann nicht mehr viel.

1 Security News

1.1 Yet Another Worm – was tun gegen Blaster & Co.?

Wieder einmal treibt ein Wurm Publicity-trächtig sein Unwesen im Internet – diesmal quasi mit vorheriger Ansage. Die wichtigsten Maßnahmen, um sich vor den wohl unvermeidlichen Nachfolgern von Blaster, Slammer, Sobig & Co. zu wappnen, sind:

- Ein aktueller Virenscanner auf jedem (Windows-) PC gehört heute ebenso zum „Standard“ wie die Beherzigung einiger genereller Empfehlungen.
- Da vor allem Microsoft-Systeme im „Bull’s Eye“ der Virenschreiber stehen, ist das umgehende Einspielen kritischer Sicherheitsupdates hier besonders wichtig. Es wird mittlerweile von Microsoft durch einen E-Mail-Benachrichtigungsdienst unterstützt.
- PCs von Kleinunternehmen und Privatanwendern, ganz besonders solche mit „always-on“ Internetanschluss, müssen mit einer Personal-Firewall geschützt sein, die so konfiguriert ist, dass sie unerwartete Datenverbindungen nur nach manueller Freigabe zulässt oder generell blockiert.
- Unternehmen mit großen Netzen sollten Netzbereiche durch interne Firewall-Filter separieren. Im Fall eines Befalles ist es dann möglich, Würmer in kleineren Netzbereichen zu isolieren – wie Schotten im Ozeandampfer gegen eindringendes Wasser.

Gegen einen hässlichen Effekt der aktuellen Würmer ist kein Kraut gewachsen: Sobig verschickt seine Kopien unter Angabe falscher Absenderadressen, die er wie die Zieladressen auf einem infizierten System gefunden hat. Dadurch können Unbeteiligte in Verdacht geraten, Viren zu verschicken, auch wenn ihr System gar nicht infiziert ist. Technisch versierte Empfänger können zwar am E-Mail-Header erkennen, dass mit dem Transportweg der Nachricht etwas nicht stimmt. Doch auch diese versteckten Hinweise könnte schon die nächste Wurm-Generation verschleiern.

1.2 Web-Application Hacking

Firewalls und auch die verbreiteten Tools für Penetrationstests konzentrieren sich meist auf Angriffe auf der Netzwerkebene. Angriffe auf Anwendungsebene werden oft nicht erkannt. Kein Wunder, dass „Web-Application Hacking“ sich zunehmender Beliebtheit erfreut. Angriffe wie Cross-Site Scripting oder SQL Injection werden per HTTP-Protokoll getunnelt – gerne zynisch als „Firewall-friendly“ bezeichnet – und sind nur schwer von normalem Netzverkehr zu unterscheiden; teilweise entziehen sie sich sogar per SSL-Verschlüsselung dem Zugriff der Firewall.

Da andererseits Web-Applikationen in zunehmendem Maße für den Zugriff auf kritische Geschäftsdaten und Anwendungen eingesetzt werden, besteht dringender Handlungsbedarf. Leider ist die Suche nach Schwachstellen hier erheblich schwieriger zu automatisieren als auf Netzwerkebene, da Web-Applikationen häufig Eigenentwicklungen und die Schwachstellen damit meist „hausgemacht“ sind.

Eine dreiteilige Online-Artikelserie „Penetration Testing for Web Applications“ von Jody Melbourne und David Jorm, deren abschließender Teil am 20.08.2003 erschien, stellt typische Schwachstellen von Web-Applikationen vor und führt in das geeignete Vorgehen bei Penetrationstests ein. Zum gefahrlosen Erproben und Simulieren von Angriffen auf Web-Applikationen empfiehlt sich das freie Tool WebGoat.

1.3 Computerkriminalität statistisch

Das Bundeskriminalamt schlüsselt jährlich die erfassten Fälle von Computerkriminalität auf. Danach waren im Jahr 2002 zwei Drittel der insgesamt um 27,5 % auf 57.288

zurückgegangenen Fälle ein Betrug mittels rechtswidrig erlangter Debitkarten mit PIN.

Bei Computersabotage und Datenveränderung verzeichnet die Kriminalstatistik einen Anstieg um 54 % auf 1.327 Fälle. Die Aufklärungsquote erreicht im Durchschnitt respektable 50 %; bei Fällen von Datenveränderung und Computersabotage, die auch nicht autorisierte Zugriffe auf Rechner („Einbrüche“, „Hacking“) umfassen, lag sie mit 38 % unter dem Durchschnitt.

1.4 IT Security Benchmarks

Je stärker IT-Investitionen in den suchenden Blick der Controller geraten, desto wichtiger werden belastbare ROI-Nachweise. Dass solche Nachweise für die IT-Sicherheit besonders schwierig zu führen sind, ist ein offenes Geheimnis.

Ein viel versprechender Ansatz ist die Bestimmung von IT Security Benchmarks, die das erreichte Sicherheitsniveau und die Entwicklung der IT-Sicherheit im Unternehmen in Relation zu den Zielen bzw. im Vergleich zum Niveau anderer Unternehmen der Branche bewerten.

Das National Institute of Standards and Technology (NIST) hat am 12.08.2003 einen „Security Metrics Guide for Information Technology Systems“ veröffentlicht, der primär US-Behörden den Nachweis erleichtern soll, dass und in welchem Grad sie gesetzlichen Anforderungen an die IT-Sicherheit genügen.

Der Ansatz ist aber von weit allgemeinerem Interesse. Er beschreibt einen Prozess, mit dem – ausgehend von den Interessen der beteiligten Parteien, allgemeinen Organisationszielen und Sicherheitsleitlinien – eine passende IT Security Metrik entwickelt werden kann.

Im Anhang, der etwa zwei Drittel des knapp 100-seitigen Dokuments ausmacht, werden Beispielmetriken dargestellt, die auf dem bereits früher publizierten „Security Self-Assessment Guide for Information Technology Systems“ des NIST beruhen.

1.5 Linux erhält Common-Criteria-Zertifikat des BSI

Der „SuSE Linux Enterprise Server V8 with certification-sles-eal2 package“ der SuSE Linux AG hat am 28.07.2003 als erstes Open Source Betriebssystem ein Sicherheitszertifikat nach Common Criteria (CC) erhalten. Die Sicherheitsmechanismen dieser Linux-Version (User Identifikation, Authentifikation, Login-Prozess, ACLs, Rollen, User-Management etc.) wurden auf IBM xSeries 335 und 440 Systemen gemäß Zertifizierungslevel EAL2+ geprüft.

Details und nähere Informationen zu den geprüften Versionsständen der Komponenten des Linux-Softwarepakets finden sich im 55-seitigen Certification Report des BSI und in den 60-seitigen Sicherheitsvorgaben, nach denen evaluiert wurde. Anzumerken ist, dass keines der registrierten Protection Profiles nach CC zu Grunde gelegt wurde; die Linux-Version erfüllt lediglich eine Untermenge des Controlled Access Protection Profile.

Über die Aussagekraft einer CC-Zertifizierung hat Jonathan Shapiro (Johns Hopkins University) eine lesenswerte, ebenso kritische wie humorvolle Betrachtung verfasst.

1.6 Bundesbank tritt European Bridge-CA bei

Nach der SAP AG ist auch die Deutsche Bundesbank der European Bridge-CA beigetreten, einer Public Private Partnership unter der Leitung von TeleTrusT Deutschland e.V., an deren Konzeption auch Secorvo mitgewirkt hat. Damit können künftig Mitarbeiter der Bundesbank ohne weiteres S/MIME-Nachrichten mit den PKI-Nutzern der Bundesverwaltung, der Deutschen Bank AG, der SAP AG, der Siemens AG und der Telekom AG austauschen.

Die S/MIME-Interoperabilitätstests der Bridge-CA haben bereits weitere Unternehmen bestanden: BMW AG, Bundeswehr, Dresdner Bank AG, TC TrustCenter GmbH und Secartis AG.

1.7 WBT Datenschutz

Unter der fachlichen Mitwirkung von Dr. Johann Bizer, Herausgeber der Zeitschrift Datenschutz und Datensicherheit, hat der E-Learning-Spezialist digital spirit ein Web Based Training (WBT) zum Datenschutz im Unternehmen entwickelt.

2 Secorvo News

2.1 Secorvo College aktuell

Das fünftägige Intensivseminar „Information Security Management“ vom **22. bis 26.09.2003** erfreut sich schon jetzt zahlreicher Anmeldungen und verspricht daher nicht nur einen vertieften Einblick in Theorie und Praxis des ISM, sondern auch einen wertvollen Erfahrungsaustausch.

Die thematische Einführung an den beiden ersten Tagen des Seminars kann auch einzeln gebucht werden (aktuelle Seminarübersicht).

2.2 PKI-Woche 2003

Vom **06. bis 09.10.2003** steht der Technologiepark Karlsruhe unter dem Zeichen der „PKI-Woche 2003“. Sie beginnt mit dem Seminar „Public Key Infrastrukturen“, das eine umfassende, zweitägige Einführung in das Thema bietet, gefolgt vom schon traditionellen „PKI-Symposium“ mit Praxisberichten und aktuellen Themen, und schließt mit einem eintägigen Vertiefungsseminar am 09.10.2003 zu ausgewählten Themen der PKI-Realisierung.

Vier Tage intensives Erfahrungswissen, die auch getrennt gebucht werden können. Bis **02.09.2003** gilt der **Frühbucherrabatt**.

3 Veranstaltungshinweise

September 2003	
08.-10.09	5th Workshop on Cryptographic Hardware & Embedded Systems (CHES 2003, Köln)
16.-17.09.	Signatur Workshop 2003 (RegTP, Mainz)
22.-26.09.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
29.09.-02.10.	Informatik 2003 – Teiltagung Sicherheit (GI, Frankfurt)
30.09.-01.10.	SAP-Sicherheit im Betrieb (Secorvo College, Karlsruhe)
Oktober 2003	
	„PKI-Woche“ (Secorvo und Secorvo College)
06.-07.10.	Public Key Infrastrukturen (Secorvo College, Karlsruhe)
07.-08.10.	**PKI-Symposium 2003** (Secorvo)
09.10.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
07.-09.10.	ISSE 2003 (EEMA und TeleTrusT, Wien)
14.-15.10.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.10.	Defense Lab (Secorvo College, Karlsruhe)
November 2003	
10.-11.11.	ZertiFA 2003 (Computas, Köln)

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