Secorvo Security News
April 2004

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

Nr. 4, 3. Jhrg. 2004
Stand 18. April 2004

ISSN 1613-4311

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

Inhalt

Editorial: Rechtsfalle revisited

Alles sollte so einfach wie möglich gemacht werden, aber nicht einfacher.

Albert Einstein

Die Implikationen einer Privatnutzung von WWW- und E-Mail-Diensten im Unternehmen liegen zahlreichen Verantwortlichen im Magen, das haben die vielen Reaktionen auf das Editorial der SSN 03/2004 eindrucksvoll bestätigt. Die Zuspitzung auf § 206 StGB hat jedoch das Gesamtproblem stark verkürzt:

Festzuhalten ist: Als unproblematisch gilt die automatisierte zentrale Löschung von schädlichen Anhängen (Viren, trojanischen Pferden), da hier das mutmaßliche Einverständnis des Empfängers angenommen werden kann – § 87 TKG verpflichtet Provider sogar zu Schutzmaßnahmen.

Kritisch hingegen ist das zentrale Löschen von vermeintlichem Spam – sogar bei ausschließlich dienstlicher Nutzung: Ohne explizites Einverständnis des Nutzers oder eine geeignete Betriebsvereinbarung verstößt der Arbeitgeber gegen § 303a StGB:

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Spamabwehr erfordert jedoch keineswegs zwingend die zentrale Löschung:

- Das Abweisen von E-Mails am SMTP-Gateway, z. B. durch IP-Blocking, vermeidet ein Filtern und Löschen.
- Ein Aussortieren Spam-verdächtiger E-Mails in einen Quarantäne-Bereich ist nach herrschender Meinung untadelig.
- Wird Spam-verdächtige E-Mail vom zentralen Filter lediglich markiert und erfolgt die Löschung erst beim Empfänger, ist dies sogar bei zulässiger Privatnutzung unbedenklich.

In jedem Fall empfiehlt sich der Abschluss einer Betriebsvereinbarung – und eine Filter- und Löschlösung unter Nutzerkontrolle.

1 Security News

1.1 Overflow in Ethereal

Eines der Standard-Tools, die sowohl von Security-Experten als auch von Hackern eingesetzt werden, ist seit Jahren der sehr mächtige und kostenlos verfügbare Sniffer Ethereal. Er ermöglicht es, den kompletten Netzwerkverkehr mitzuschneiden, um beispielsweise Protokolle zu überwachen oder Verbindungen zu rekonstruieren.

Wie zuletzt in den SSN 03/2004 thematisiert, sind jedoch auch viele Sicherheits-Tools nicht frei von Schwachstellen. Nun hat es Ethereal „erwischt“: Am 22.03.2004 wurden gleich vier teilweise kritische Schwachstellen aufgedeckt, die – wen wundert es – ihre Ursache u. a. in einem „klassischen“ Buffer Overflow haben. Da das Tool sehr Hardware-nah programmiert wurde, sind von den Fehlern nicht nur Windows-, sondern auch alle Unix-Varianten betroffen. Administratoren, die Ethereal einsetzen, sollten nur noch die mittlerweile verfügbare korrigierte Version 0.10.3 verwenden, um nicht Opfer eines zweifellos bald kursierenden Exploits zu werden.

1.2 Cisco Global Exploiter

Unter der Bezeichnung „Cisco Global Exploiter“ ist seit kurzem ein Tool zur Überprüfung von neun bekannten Cisco-Schwachstellen verfügbar. Das Perl-Skript vereinfacht die Untersuchung von Routern und Switches auf Schwachstellen, kann aber – selbst von technisch unversierten „Skript-Kiddies“ – auch für Angriffe missbraucht werden. Ein Update von Systemen mit diesen Schwachstellen wird daher dringend empfohlen.

Die am 07.04.2004 publizierte Schwachstelle – eine fest in der Software verankerte UserID/Kennwort Kombination der Management-Lösungen Wireless Lan Solution Engine und Hosting Solution Engine – dürfte bald auch Teil des Exploits sein.

1.3 TKG im Bundesrat

Nicht zuletzt dank des Engagements der Branchenverbände, insbesondere eco und VATM, hatte die Bundesregierung in letzter Sekunde die umstrittene Vorratsspeicherung von Verbindungsdaten für die Sicherheitsbehörden aus der Novelle des Telekommunikationsgesetzes (TKG), die am 12.03.2004 vom Deutschen Bundestag verabschiedet wurde, herausgenommen. Sogar eine Entschädigung der Diensteanbieter bei Überwachungsmaßnahmen ist vorgesehen. Wie erwartet kam am 02.04.2004 prompt die von mehreren Bundesländern angekündigte Ablehnung im Bundesrat (BR-Drs. 200/04). Erschreckend die Änderungswunschliste der Länder:

- Verpflichtung von TK-Anbietern zur 6-monatigen Speicherung von Verkehrsdaten,
- Verpflichtung der Mobilfunkbetreiber zur Erhebung der Kunden-Bestandsdaten bei Prepaid-Karten,
- Möglichkeit eines Zugriffs auf personenbezogene PINs und Passwörter,
- Streichung der Entschädigung für Auskünfte im automatisierten Verfahren.

Auch die Einschränkung der Verpflichteten auf Unternehmen, die TK-Dienste für die Öffentlichkeit anbieten und mindestens 1.000 Teilnehmer versorgen, ist wieder auf dem Tisch. Damit könnten doch noch alle Unternehmen, die eine Privatnutzung ihrer TK-Dienste zulassen, in den Kreis der Verpflichteten aufrücken.

1.4 Neue ISIS-MTT Version

Am 16.03.2004 verabschiedete das ISIS-MTT Board die neue Version 1.1 der PKI-Interoperabilitätsspezifikation. Wichtigste Neuerung ist die Aufnahme des Profils für XML-Signatur und -Verschlüsselung als neuer Teil 8 von ISIS-MTT. Daneben wurden teils unnötig strenge Profilierungsanforderungen gelockert, um die Interoperabilität mit weit verbreiteter Anwendungssoftware zu verbessern.

Die Bedeutung des Standards ISIS-MTT hat in den vergangenen Monaten weiter zugenommen. So ist ISIS-MTT inzwischen obligatorischer Baustein des E-Government-Frameworks SAGA und, in der neuen Version 1.1, technische Grundlage für das Signaturbündnis. Ebenfalls am 16.03.2004 wurde auf der Grundlage eines Prüfberichts von Secorvo das ISIS-MTT Siegel in der Produktklasse „CA Server“ für die Certificate Services des Microsoft Windows Server 2003 verliehen.

1.5 Windows versus Linux

Eine am 19.03.2004 erschienene Studie von Forrester Research versucht, die seit mehreren Jahren heiß diskutierten Frage, ob Windows oder Linux das sicherere Betriebssystem sei, methodisch sauber zu beantworten. Über ein Jahr untersuchte Forrester Sicherheitslücken und Patches und legte als Vergleichsmetrik die Schwere bekannt gewordener Sicherheitslücken und die Zeit zwischen Bekanntgabe und Behebung zu Grunde. Das Ergebnis: Microsoft veröffentlichte Patch-Releases am schnellsten, hatte aber die meisten Sicherheitslücken der höchsten Einstufung (nach NISTs ICAT Database for Severe Computer Vulnerabilities).

Dieser Ansatz, mit dem sich Vorteile für Windows und Debian-Linux ergaben, wurde am 06.04.2004 postwendend von den großen Linux-Distributoren kritisiert, da sämtliche Lücken über einen Kamm geschoren würden, ohne auf die spezifischen Auswirkungen einzugehen. Zugleich belohnt die Metrik Hersteller, die die Bekanntgabe von Sicherheitslücken so lange wie möglich hinauszögern – und schüttet damit Öl in die seit einigen Jahren schwelende Debatte über den richtigen Zeitpunkt der Veröffentlichung von Sicherheitslücken.

Neben der Erkenntnis, dass bis zu allgemein akzeptierten Metriken für IT-Sicherheit noch ein Stück Weges vor uns liegt, ist anzunehmen, dass der Disput um die Studie zumindest den Absatz des 899 US $ teuren Dokuments fördert.

1.6 SigG-Novelle

Am 01.04.2004 wurde der mit Spannung erwartete Entwurf des SigG-Änderungsgesetzes nebst Begründung veröffentlicht. Der Großteil der vorgesehenen Änderungen bzw. Klarstellungen dient dazu, den Weg für eine einfache, weitest gehend elektronische Beantragung und Ausgabe von Signaturkarten zu ebnen.

Dadurch sollen die etablierten Verfahren für die Ausgabe von EC-, Bank- oder Versicherungskarten auch für Signaturkarten nutzbar gemacht werden – um der elektronischen Signatur endlich zum lange ersehnten Durchbruch zu verhelfen.

1.7 VPN-Sicherheitslücken

Gleich mehrere Implementierungen von ISAKMP/IKE, dem Schlüsselaustauschdienst für IPsec-VPNs, gerieten in den vergangenen Wochen in die Kritik:

- Am 17.03.2004 wurde eine Denial-of-Service Attacke gegen den ISAKMP-Dienst von OpenBSD veröffentlicht.
- Cisco veröffentlichte am 08.04.2004 ein Advisory, wonach einige IOS-Router und Catalyst-Switches durch missgeformte ISAKMP/IKE-Pakete gezielt zum Absturz gebracht werden können.

Den Vogel abgeschossen hat der mittlerweile auch in Linux integrierte ISAKMP-Dienst „Racoon“ des KAME-Projekts, der, wie am 07.04.2004 gemeldet wurde, zwischen September 2001 und April 2004 unbemerkt bei der ISAKMP-Variante mit RSA-Signatur zwar die verwendeten Zertifikate, nicht aber die eigentliche Signatur über die ausgetauschten Protokolldaten überprüft hat.

Dies bestätigt – im Nachhinein – Niels Ferguson und Bruce Schneier, die bereits Anfang 2000 vor der zu hohen Komplexität des IPsec-Standards warnten.

2 Secorvo News

2.1 Secorvo College aktuell

Auf vielfachen Wunsch haben wir das Seminarangebot von Secorvo College um ein Intensivseminar zum Datenschutz erweitert. Einen umfassenden Überblick über die im Mai 2001 neu geregelten Anforderungen des BDSG und unsere Erfahrungen mit der praktischen Umsetzung aktueller Datenschutzanforderungen in Unternehmen erhalten Sie – kurz vor Ablauf der BDSG-Übergangsfrist (vgl. SSN 01/2004) – erstmalig am 18.05.2004.

2.2 IT-Sicherheitsforum 2004

Das IT-Sicherheits-Forum der ComConsult Akademie zählt seit einigen Jahren zu den herausragenden Events der IT-Sicherheit. Das Programm 2004 beinhaltet aktuelle Vorträge zu Themen wie IDS in der Praxis, Sicherheit von Webanwendungen, Patch-Management und XML-Sicherheit. Abgerundet wird die Veranstaltung durch drei ganztägige Tutorien sowie diverse Praxis-Workshops. Stefan Kelm wird über Aufgaben und Strategien von CERTs referieren.

2.3 Midvision 2004

Die IT-Fachmesse für den Mittelstand, Midrange Welt und Midvision 2004, wird in diesem Jahr am 13.-14.05.2004 zum zweiten Mal in der Neuen Messe Karlsruhe stattfinden – diesmal mit dem thematischen Schwerpunkt „IT-Sicherheit“ und einem begleitenden zweitägigen Kongress. Auch die Karlsruher-IT-Sicherheitsinitiative (KA-IT-Si) ist vertreten: Mit Ausstellern, einem Event am 13.05.2004 und zwei Vorträgen auf dem begleitenden Fachkongress.

2.4 DuD 2004

Der Fachkonferenz DuD 2004 (03.-04.05. 2004) „droht“ ein neuer Teilnehmerrekord: schon jetzt haben sich mehr als 80 Teilnehmer angemeldet (Anmeldung).

3 Veranstaltungshinweise

April 2004	
27.-29.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Mai 2004	
03.-04.05.	Datenschutz und Datensicherheit – DuD 2004 (COMPUTAS, Berlin)
04.-05.05.	Inside Windows Security (Secorvo College, Karlsruhe)
10.-13.05.	IT-Sicherheits-Forum 2004 (ComConsult, Königswinter)
13.-14.05.	Midvision 2004 (KA-IT-Si/KMKG, Karlsruhe)
11.-12.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
13.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
18.05.	Datenschutz kompakt (Secorvo College, Karlsruhe)
Juni 2004	
14.-15.06.	IT-Security Management (Secorvo College, Karlsruhe)
14.-18.06.	Information Security Management (Secorvo College, Karlsruhe)
29.-30.06.	Security Awareness Symposium 2004 (Karlsruhe)

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

Impressum

ISSN 1613-4311

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

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

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