Secorvo Security News
März 2004

Dirk Fox, Stefan Gora, Stefan Kelm
Secorvo Security Consulting GmbH

Nr. 3, 3. Jhrg. 2004
Stand 22. März 2004

ISSN 1613-4311

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

Inhalt

Editorial:
Rechtsfalle Privatnutzung

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Abs. 1 bezeichneten Unternehmens unbefugt (...) eine der in Abs. 1 (...) bezeichneten Handlungen gestattet (...).

Verletzung des Post- oder Fernmeldegeheimnisses, § 206 StGB

Zwar ist die Kuh des “geldwerten Vorteils” bei privater Nutzung von WWW und E-Mail im Unternehmen vom Eis. Dennoch hängt ein Damokles-Schwert über allen Unternehmen, die der Privatnutzung keinen Riegel vorgeschoben haben – als unvermeidliche Konsequenz des verfassungsrechtlich verankerten Fernmeldegeheimnisses. Die Auswirkungen sind dramatisch – und in vielen Unternehmen nicht einmal bekannt: Lassen sich private E-Mails nicht eindeutig identifizieren oder ausschließen, dann unterliegen auch Spam-E-Mails dem selben Schutz wie private Post. Als Service-Provider seiner Mitarbeiter ist der Arbeitgeber nämlich zur (unverstümmelten) Zustellung jeder Nachricht verpflichtet. Ein Löschen unliebsamer, oft mit schädlichen Dateianhängen (Viren) versehener E-Mails ist ein strafbewehrter Verstoß gegen § 206 StGB.

Aus dieser Konsequenz gibt es kein Entrinnen: Denn auch per Verzichtserklärung kann ein Grundrecht nicht abgetreten werden, mithin kann kein Mitarbeiter den Arbeitgeber zum Eingriff ermächtigen. Zumal die Freiwilligkeit einer solchen Zustimmung im Arbeitsverhältnis in Zweifel steht. Selbst eine stillschweigende Duldung privater Nutzung genügt, damit der Arbeitgeber zum Internet-Service-Provider mutiert. Bleibt nur eines: Wer zentral filtern will, muss die private Nutzung explizit verbieten – und die Einhaltung des Verbots regelmäßig prüfen.

1 Security News

1.1 Qualifizierte Massen-Signaturen

Ein in der PKI-Praxis noch immer kontrovers diskutiertes Problem ist die Fragestellung, wie sich fortgeschrittene oder „qualifizierte“ elektronische Signaturen nach EU-Richtlinie und deutschem Signaturgesetz mit Signaturen durch Server bzw. juristische Personen in Einklang bringen lassen. Obgleich dieses Thema bereits seit mehreren Jahren diskutiert wird, kam es erst im Zusammenhang mit der zum 01.01.2004 erforderlichen Umsetzung der EG-Richlinie zu elektronischen Rechnungen wieder auf dem Tisch.

Da dieses Problem nicht nur die Zertifizierungsdiensteanbieter, sondern auch die nationalen Aufsichtsbehörden (in Deutschland die RegTP) betrifft, hat sich die österreichische Aufsichtsstelle für elektronische Signaturen dieses Themas angenommen und am 16.03.2004 einen interessanten Entwurf eines „Positionspapiers zu Fragen der elektronischen Rechnung und der Serversignatur“ vorgelegt. Das Papier enthält konkrete Empfehlungen für die Gestaltung von Massensignaturen, die in ähnlicher Form auch in anderen EU-Ländern umsetzbar sein dürften.

1.2 ENISA: Holpriger Start

Die europäische Sicherheitsagentur ENISA (European Network Information Security Agency) mit provisorischem Sitz in Brüssel ist seit dem 18.03.2004 online. Ihre Aufgabe liegt unter anderem darin, die EU-Mitgliedsstaaten in Fragen der Netzwerk-Sicherheit zu beraten. Ihr Hauptsitz soll gemäß Beschluss vom 13.12.2003 in Griechenland aufgebaut werden. Derzeit ist die Stelle des Direktors ausgeschrieben.

Ein kritischer Blick auf den Webserver legt die Empfehlung nahe, auch die Stelle eines Administrators mit Grundkenntnissen in Webserver-Sicherheit auszuschreiben. Vielleicht würde dann die wenig vorbildliche Informationsfreigabe unterbunden: Unter anderem sind private IP-Adresse, ein Logfile und Skripte des Servers einsehbar.

1.3 NGWT – Next Generation Worm Tricks

Die inhaltlich immer glaubwürdigeren Massen-E-Mails mit Trojanern im Anhang waren ein Thema der SSN 01/2004. Seit einigen Wochen verbergen Würmer den schädlichen Anhang in Passwort geschützten Archiven (.zip, .rar) vor dem Zugriff der Antiviren-Software. Das zugehörige Kennwort wird im Text der E-Mail mitgeliefert – und tatsächlich von unzähligen Empfängern bereitwillig zum Aktivieren des anhängenden Schadprogramms eingetippt.

Darauf haben einige Hersteller von Antivirenlösungen reagiert: Sie entnehmen vor dem Scannen der E-Mail automatisiert die Passwörter und entdecken so Viren und Würmer auch in passwortgeschützten Anhängen. Das ist den Virenprogrammierern nicht verborgen geblieben: Seit Bagle.N werden die Kennwörter daher jetzt als Bild im gif-Format angehängt.

Will man nicht ständig mit den technischen Lösungen der Kreativität der Angreifer hinterherhinken, bleibt als einziger Ausweg eine wirkungsvolle und nachhaltige Mitarbeitersensibilisierung.

1.4 Einstufungs(s)pannen bei Sicherheitslücken

Oft fällt es Herstellern offenbar schwer, die Bedeutung von Sicherheitslücken richtig einzustufen. Zwei aktuelle Beispiele belegen dies: So wurde ein am 09.03.2004 von Microsoft veröffentlichtes Outlook-Update, welches eine mögliche Systemübernahme behebt, zunächst nicht als „kritisch“ bewertet. Und die aktuelle Version des ISS Internet Scanner schätzt die NT-Schwachstelle „NtservicesExeDos“ als „mittel“ ein – obwohl betroffenen Systemen keine Netzdienste mehr zur Verfügung stehen.

Daher ist bei Angaben von Herstellern und Tools zur Relevanz von Schwachstellen Vorsicht angeraten: Die Angaben sollten nur als Empfehlung verstanden werden und nie die eigene Bewertung ersetzen.

1.5 „Security“ schützt vor Lücken nicht

Über sicherheitskritische Schwachstellen in Programmen und Betriebssystemen wird in schöner Regelmäßigkeit berichtet. Sicherheitswarnungen, von Notfallteams „Advisories“ genannt, werden oft als Reaktion auf öffentlich diskutierte Sicherheitslücken publiziert. Vielfach handelt es sich dabei um Erkenntnisse von Security-Experten, die in verbreiteten Systemen gezielt nach Sicherheitslücken suchen.

Dass dabei insbesondere auch die Hersteller von Sicherheitsprodukten unter die Lupe genommen werden, verwundert nicht. Auch hier werden die Experten regelmäßig fündig: Allein im Februar diesen Jahres wurde eine Reihe von teils äußerst kritischen Lücken entdeckt. Betroffen waren u.a. Produkte wie ZoneAlarm, Symantec Firewall/VPN, Symantec Antivirus und Norton Internet Security. Ursache der Bugs waren „alte Bekannte“ wie Buffer Overflows oder Race Conditions.

Als besonders brisant erwiesen sich dabei Fehler, die in der noch recht jungen Produktklasse der so genannten „Intrusion Prevention Systeme“ gefunden wurden, deren Ziel – im Unterschied zu IDS – nicht das Erkennen, sondern die Verhinderung von Angriffen ist. So hat ein Angreifer in diversen ungepatchten Produkten des Herstellers ISS (Internet Security Systems) die Möglichkeit, eigene Code-Sequenzen ausführen zu lassen. Und die Fachzeitschrift c’t kommt in Ausgabe 5/2004 beim Test von Symantecs Gateway Security 5400 gar zu dem Ergebnis, der Schutz durch das Produkt sei „eher niedrig einzuschätzen“.

Noch kritischer ist eine Schwachstelle, die in Hardware-Sicherheitsmodulen (HSM) der Firma nCipher entdeckt wurde: Dort ist es einem lokalen Angreifer u.U. möglich, Zugriff auf kryptographische Schlüssel zu erhalten, die ja gerade durch diese Hardware besonders geschützt sein sollen.

Merke: Auch Hersteller von Security-Produkten sind nicht vor Sicherheitslücken gefeit. Daher sollten gerade diese Lösungen vor dem Produktiveinsatz intensiven Analysen unterzogen werden.

1.6 Raubkopieverbreitung über Firmensysteme

Die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. berichtet von der bislang weltweit größten Razzia gegen Raubkopierer. Dabei wurden vom 16. bis 18.03.2004 allein in Deutschland mehr als 800 Firmen, Rechenzentren und Privatwohnungen durchsucht. Zur Verbreitung der illegalen Kopien, die einen geschätzten Verlust in Höhe eines zweistelligen Millionen-Euro-Betrags verursacht haben, wurden offenbar im großen Stil Systeme von Rechenzentren, Firmen und Privatpersonen missbraucht. Unternehmensserver standen dabei wegen deren performanter Internetanbindung und der hohen Speicherkapazitäten im Fokus des nun ausgehobenen Hacker-Rings, der systematisch fremde Systeme übernommen und missbraucht haben soll.

Erheblich dürften auch die durch die Beschlagnahmungen entstanden Schäden in den betroffenen Unternehmen sein.

2 Secorvo News

2.1 Secorvo College aktuell

Anfang April (06.04.2004) bietet Secorvo College erstmalig einen eintägigen Intensiv-Workshop an, in dessen Verlauf typische Hacker-Vorgehensweisen gemeinsam durchgespielt werden: „Dem Hacker über die Schulter geschaut“. Um intensive praktische Übungen und Diskussionen sicherzustellen, ist die Teilnehmerzahl auf fünf Sicherheitsverantwortliche beschränkt.

Grundlegend überarbeitet, erweitert und aktualisiert wurde das nun dreitägige Seminar „E-Mail-Sicherheit“ (20.-22.04. 2004), das seit 1999 zahlreich besucht und kontinuierlich weiter entwickelt wurde. Erstmalig werden nun auch Server-basierte Verschlüsselungslösungen ausführlich behandelt.

Ende April (27.-29.04.2004) folgt der „Klassiker“: Das Seminar „IT-Sicherheit heute“ gibt einen Einblick in die zentralen Themen und aktuellen Fragestellungen der IT-Sicherheit – geeignet sowohl für einen intensiven thematischen Einstieg als auch als Auffrischung.

http://www.secorvo.de/college

2.2 Chefsache IT-Sicherheit

Mit einer halbtägigen Roadshow zum Thema IT-Sicherheit richten sich die IHKs in Baden-Württemberg derzeit an mittelständische Unternehmen. Die Veranstaltung klärt über zentrale IT-Risiken auf und stellt Lösungswege vor.

In Karlsruhe findet die Roadshow am 31.03.2004 in Zusammenarbeit mit der „Karlsruher IT-Sicherheitsinitiative“ in den Räumen der IHK statt. Die Partner der Initiative begleiten die Roadshow mit einer Ausstellung zum Thema. Im Anschluss referiert Dirk Fox, Geschäftsführer von Secorvo und Herausgeber der Zeitschrift „Datenschutz und Datensicherheit (DuD)“, über Anspruch und Wirklichkeit des Datenschutzes – einem „Drahtseilakt zwischen Genie und Wahnsinn“. Der Eintritt ist frei.

2.3 Microsoft erhält ISIS-MTT-Konformitätssiegel

Am 16.03.2004 hat der Microsoft Windows 2003 Certificate Service nach Prüfung durch das Secorvo Prüflabor vom ISIS-MTT-Board das ISIS-MTT-Konformitätssiegel erhalten. Damit ist die Microsoft-CA das dritte Produkt, dessen ISIS-MTT-Konformität in einem vereinheitlichten Testverfahren nachgewiesen wurde.

3 Veranstaltungshinweise

März 2004	
30.-31.03.	D-A-CH Security 2004 (GI, BITKOM, TeleTrusT; Basel)
31.03.	Chefsache IT-Sicherheit und Drahtseilakt zwischen Genie und Wahnsinn (IHK Karlsruhe)
April 2004	
06.04.04	Dem Hacker über die Schulter geschaut (Secorvo College)
20.-22.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
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.	Netzwerk Sicherheits-Forum 2004 (ComConsult, Königswinter)
11.-12.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
13.05.	PKI für Fortgeschrittene (Secorvo College, 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