Secorvo Security News
November 2004

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

Nr. 11, 3. Jhrg. 2004
Stand 30. November 2004

ISSN 1613-4311

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

Inhalt

Editorial: Weniger ist weniger

Denken wir an Überwachung, so fallen uns Kameras, Abhöranordnungen und Lauschangriff, E-Mail-Filterung und Strafverfolgungsbehörden ein. Die Welt des „Großen Bruders“ hört, sieht und liest mit – und uns beschleichen klamme Gefühle, wenn wir uns eine Rundherumbeobachtung vorstellen.

Tatsächlich aber trügt unsere Wahrnehmung. Denn die Kernbedrohung unserer gesellschaftlichen Freiheit schlummert in einer weit weniger sichtbaren Gefahr. Sie kommt auf viel leiseren Sohlen daher – als die uns Deutschen vielleicht besonders eigene Neigung zur Dokumentation, zur Sammlung und Verschriftlichung, die dazu führt, dass wir das Mögliche archivieren – manchmal mehr als zulässig, fast immer mehr als erforderlich. Das gilt bei weitem nicht nur für Behörden – auch deutsche Unternehmen sind Weltmeister im Speichern, und vergessen das Löschen.

In seiner Grundsatzentscheidung zum Volkszählungsgesetz hat das Bundesverfassungsgericht 1983 so treffend formuliert: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, (...) kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“

Heute sollte man hinzufügen: Wer weiß, dass Vorgänge dokumentiert, gespeichert und zukünftig möglicherweise in ganz anderem Kontext ausgewertet werden, *wird* gehemmt *sein*, selbstbestimmt zu entscheiden. Aus dieser Perspektive könnten sich Ermächtigungen der Strafverfolgungsbehörden, sofern sie verhältnismäßig bleiben, als weit harmloser erweisen als etwa das geplante Anti-Diskriminierungsgesetz, das lückenlose Entscheidungsdokumentationen zur Folge haben dürfte.

„Liberty dies by inches”, konstatierte der kürzlich verstorbene Rechtsexperte Heinz Schueler schon 1979. Wie recht er hatte.

1 Security News

1.1 Phishing revisited

Die Perfidie von Phishing-Attacken nimmt weiter zu. Erste Phisher sind jetzt eine Ehe mit Schadprogrammen eingegangen. So wurde am 03.11.2004 eine Phishing-E-Mail gemeldet, deren aktiver Anhang die „hosts"-Datei im Windows-Verzeichnis system32/drivers/etc modifiziert. In dieser Datei werden IP-Adressen fest zugeordnet; üblicherweise findet sich hier nur die Lokalhost-Adresse 127.0.0.1. Werden in dieser Datei beliebigen Hostnamen, z.B. Webadressen, feste IP-Adressen zugewiesen, sind sie damit „fest verdrahtet": Der Browser bemüht dann nicht das DNS-Protokoll, um die korrekte Adresse zu finden, sondern nimmt die hier eingetragene – der ahnungslose Surfer sieht im Browserfenster die richtige WWW-Adresse, wird aber auf eine falsche Seite umgelenkt, ohne dass das für ihn erkennbar wäre.

1.2 IT-Grundschutzprofile

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 17.11.2004 auf ihrer Webseite drei Grundschutz-Profile jeweils für kleine, mittlere und große Unternehmen veröffentlicht, die die Umsetzung des BSI-Grundschutzhandbuchs vereinfachen sollen.

Analog zum „Leitfaden IT-Sicherheit kompakt" enthält die Handreichung für kleine Unternehmen eine Checkliste, die eine gute Hilfestellung darstellt. Bei den Profilen für mittlere (112 S.) und große Unternehmen (117 S.) werden die Vorgehensweise im Detail sowie sinnvoller Weise auch der Einsatz des Grundschutz-Tools vorgestellt. Praxisnah werden beim Profil für große Unternehmen zusätzlich mögliche Problemfälle und Lösungsmöglichkeiten aufgezeigt.

1.3 Internetspionage per Satellit

Laut einer aktuellen Untersuchung von Forschern der Ruhr-Universität Bochum konnten bei satellitengestützten Internetverbindungen einiger Provider unverschlüsselte Daten von und über andere Nutzer recht einfach in Erfahrung gebracht werden.

Es wird empfohlen, die auch sonst im Internetverkehr üblichen Sicherheitsmaßnahmen wie die Verwendung von verschlüsselten Protokollen zu nutzen.

1.4 Erste Bank mit IT-Grundschutz-Zertifikat

Das BSI konnte am 16.11.2004 die Vergabe des ersten IT-Grundschutz-Zertifikats an eine Bank vermelden: die PSD-Bank Westfalen-Lippe e. G. mit Sitz in Münster hat als erste Bank eine IT-Grundschutz-Zertifizierung erfolgreich durchgeführt.

1.5 SigG-Novelle

Am 19.11.2004 hat der Bundestag in zweiter und dritter Lesung das deutsche Signaturgesetz (SigG) novelliert. Zentrale Änderung: Für die Beantragung eines qualifizierten Signaturschlüssel-Zertifikats genügt nunmehr ein PIN-TAN-basierter Prozess – der eigenhändig unterschriebene Antrag mit Vorlage des Personalausweises ist bei bestehenden Kunden nicht mehr erforderlich. Damit kommt die Novelle einer zentralen Forderung der deutschen Banken entgegen, die eine Vereinfachung der Prozesse gefordert hatten, um ihre Bankkarten zu Signaturkarten aufwerten zu können.

Die Bundesregierung erhofft sich mit diesem Schritt eine erhebliche Ausweitung der nach wie vor nur marginalen Verbreitung qualifizierter Signaturen in Deutschland; freilich fehlen trotz dieser Verfahrensvereinfachung noch immer die seit vielen Jahren versprochenen Anwendungen für „Otto Normalsignierer", die für ihn einen erkennbaren Zusatznutzen darstellen und einen Technikwechsel rechtfertigen.

1.6 DNS-Ping-Pong

Dass auch in Protokollen aus der “Ur-Zeit” des Internet immer wieder Schwachstellen entdeckt werden, wird inzwischen niemanden mehr überraschen. Häufig handelt es sich dabei zum Glück nicht um konzeptionelle Schwachstellen, die einen Austausch aller Implementierungen des Protokolls erfordern würden, sondern um Programmierfehler. Manchmal jedoch sind davon dank „Code-Wiederverwendung“ zahlreiche Produkte betroffen.

So erging es nun auch dem vielleicht wichtigsten Protokoll – DNS, dem Domain Name System. Am 09.11.2004 warnte das britische NISCC in einem Advisory, dass verschiedene Hersteller das DNS-Protokoll in ihren Produkten fehlerhaft implementieren. Danach reagieren DNS-Server unter Umständen auf die einer DNS-Anfrage folgende Antwort mit einer erneuten DNS-Antwort. Dadurch können sehr schnell „DNS-Stürme“ ausgelöst werden, sofern zwei von diesem Fehler betroffene DNS-Server beteiligt sind – ein Szenario, das in großen Firmen-Netzwerken nicht unwahrscheinlich sein dürfte.

Analog zu bereits 1996 berichteten ähnlichen Problem auf UNIX-Systemen könnten Server durch geeignet Pakete auch dazu gebracht werden, sich selbst entsprechende Anfragen zu senden.

1.7 PDA-Forensik

IT-Forensik wird als Teildisziplin der IT-Sicherheit immer wichtiger. In forensischen Analysen tauchen dabei immer häufiger Untersuchungen zu Mini-Organizern auf, auch Personal Digital Assistants (PDAs) genannt, da diese vor allem im Firmenumfeld an Bedeutung gewinnen.

Dieser Entwicklung trägt jetzt das US-amerikanische National Institute of Standards and Technology (NIST) Rechnung: In den am 10.11.2004 vorgestellten „Guidelines on PDA Forensics“ erläutert das NIST die spezifischen Merkmale einer PDA-Analyse (u.a. am Beispiel von Palm OS und Pocket PC), führt in forensische Vorgehensweisen ein und stellt einige Tools vor, auf die in einem umfangreichen Begleitdokument im Detail eingegangen wird.

2 Secorvo News

2.1 Secorvo College aktuell

Im neuen Jahr startet Secorvo College mit einem zweitägigen Seminar zu Public Key Infrastrukturen (PKI) (25.-26.01.2005), an das sich am 27.01.2005 ein eintägiges PKI-Vertiefungsseminar für Fortgeschrittene anschließt. Im Februar folgen das Grundlagenseminare IT-Sicherheit heute (15.-17. 02.2005) sowie das fünftägige Schlüsselseminar zum Information Security Management (21.-25.02.2005), dessen erste drei Tage auch getrennt gebucht werden können. Erstmals wird am 21.-22.06.2005 auch die Prüfung zum „Certified IT-Security Professional“ abgenommen.

http://www.secorvo.de/college

2.2 Lead Auditor

Am 15.11.2004 wurde Jörg Völker, Autor eines der mit über 13.000 Downloads meistgelesenen Secorvo Whitepaper zum Information Security Management, als Lead Auditor nach dem Information Security Management (ISM) Standard BS 7799 zertifiziert. Das berechtigt ihn zur Durchführung von offiziellen Audits gemäß BS 7799, zur Vorbereitung auf oder der Abnahme von einer offiziellen BS 7799-Zertifizierung, die inzwischen auch in Deutschland zunehmend in den Fokus der Informationssicherheit stehen.

2.3 Forensik-Symposium

Am **01.-02.03.2005** veranstaltet Secorvo im Rahmen der Karlsruher IT-Sicherheitsinitiative ein Computer Forensik Symposium: ausgewiesene Experten aus unterschiedlichen Bereichen (BKA, Interpol, Recht und Technik) versprechen eine eineinhalb tägi-

ge intensive Beschäftigung mit forensischen Fragestellungen. Nicht zuletzt besteht im Rahmen des gemeinsamen Dinners ausreichend Möglichkeit zum Erfahrungsaustausch. Eine frühzeitige Anmeldung wird empfohlen.

2.4 Delegation und Haftung

Nicht nur Geschäftsführer, sondern auch IT-Leiter, IT-Sicherheitsverantwortliche und Datenschutzbeauftragte tragen eine erhebliche Verantwortung für den reibungslosen und gesetzeskonformen Betrieb der Informationstechnik eines Unternehmens.

Was bedeutet das im Falle eines Vorfalls? Wer haftet unter welchen Voraussetzungen gegenüber wem? Muss der IT-Leiter bei Regressforderungen mit seinem Vermögen gerade stehen?

Die Vielzahl der zu diesen Fragen kursierenden Behauptungen, Gerüchte und Befürchtungen ersetzt Professor Dr. Michael Bartsch auf der kommenden Veranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **16.12.2004** (Beginn: 18 Uhr) durch belastbare Fakten.

Wir freuen uns, mit Prof. Bartsch nicht nur einen ausgewiesenen Experten in diesen Fragen, sondern auch einen brillianten Redner gewonnen zu haben – wer schon einmal das Vergnügen hatte, ihn zu hören, wird diesen Termin nicht verpassen wollen; allen anderen sei er wärmstens empfohlen. Im Anschluss an Vortrag und Diskussion haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim kulinarischen Ausklang – "Buffet-Networking", sozusagen.

2.5 DuD 2005

Schon wirft sie ihre Schatten voraus: Die Konferenz „Datenschutz und Datensicherheit“ (DuD), seit sechs Jahren von COMPUTAS in enger Kooperation mit den Herausgebern und Autoren der Fachzeitschrift DuD veranstaltet. Zum Vormerken in Ihrem Kalender: **18.-19.04.2005**, Berlin.

3 Veranstaltungshinweise

Dezember 2004	
05.-09.12.	Asiacrypt 2004 (IACR, Jeju Island/Korea)
06.-07.12.	IsSec/ZertiFA 2004 (COMPUTAS, Berlin)
09.-10.12.	Einführung in die Praxis des DSB (Euroforum, Düsseldorf)
16.12.	Verantwortung, Delegation und Haftung (KA-IT-Si, Karlsruhe)
Januar 2005	
25.-26.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
27.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2005	
15.-17.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
21.-25.02.	Information Security Management (Secorvo College, Karlsruhe)
März 2005	
01.-02.03.	Computer Forensik Symposium 2005 (KA-IT-Si, 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