Secorvo Security News
Juni 2006

Dirk Fox, Stefan Gora, Kai Jendrian,
Stefan Kelm, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 6, 5. Jhrg. 2006
Stand 19. Juni 2006

ISSN 1613-4311

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

Inhalt

Editorial: Weltmeister

Bei der wichtigsten Nebensache der Welt zählt Deutschland auch 2006 allen Unkenrufen zum Trotz zu den Favoriten. Nicht nur da: Im internationalen Vergleich liegen wir bei Telefonüberwachungen (Abhöranordnungen je Bürger) auf Rang vier, hinter Italien, den Niederlanden und der Schweiz.

Durch das mit der Verbreitung von Handys geänderte Nutzerverhalten sind auch immer mehr Kontaktpersonen von Abhörmaßnahmen betroffen. Die Wahrscheinlichkeit einer Gesprächsüberwachung ist hier inzwischen 30 mal so hoch wie in den USA.

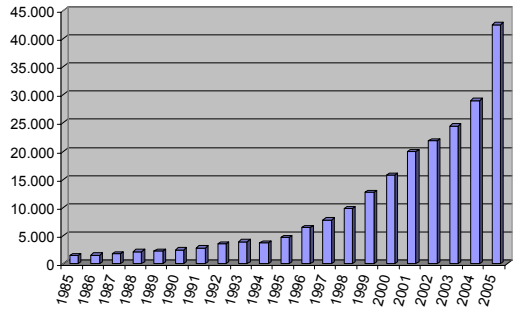


Bild: *Telefonüberwachungsanordnungen*

Erschreckend sind die durch Studien belegten Seiteneffekte dieser Entwicklung: Die schiere Zahl der Anordnungen macht die Durchbrechung des grundrechtlich geschützten Fernmeldegeheimnisses zur Formsache: Von 300 untersuchten richterlichen Beschlüssen entsprachen drei Viertel nicht den gesetzlichen Vorgaben, die Hälfte der Richter unterschrieb einfach den Beschlussentwurf des Staatsanwalts.

„Weder Staatsanwälte noch Richter mochten sich die Ansicht zu eigen machen, dass der Richtervorbehalt als eine besondere Form des Grundrechtsschutzes für die Betroffenen anzusehen sei“ (Backes et.al.). Die vorgeschriebene Benachrichtigung der Betroffenen erfolgte entweder gar nicht (66 %, Albrecht et.al.) oder beschränkte sich auf die Beschuldigten – „es fehlte jede Sensibilität dafür, dass es sich hierbei um Grundrechtseingriffe handelt.“

Dann doch lieber ein Weltmeistertitel für eine Leistung, auf die man stolz sein darf.

1 Security News

1.1 Admin – nein danke!

Hatte Microsoft noch im April 2004 berichtet, dass ca. 95 % aller Angestellten lokale Administrator-Rechte besitzen, so deuten aktuelle Bemerkungen darauf hin, dass sich dieses Verhältnis jetzt umkehren könnte. Das würde die Aussagen Microsofts in einem aktuellen White-Paper zur Information Security bei Microsoft bestätigen – dort wird unter „Lessons Learned and Best Practices“ gefordert: „consolidate local administrator accounts“.

Derzeit verursacht ein Verzicht auf lokale Administrationsrechte häufig Probleme. Für deren Analyse und Behebung hat Microsoft am 23.05.2006 den „Microsoft Standard User Analyzer“ zur Verfügung gestellt.

Der Trend, Administrator-Rechte nicht als Statussymbol, sondern als Sicherheitsrisiko zu betrachten, ist positiv zu bewerten. Halbherzige Work-Arounds sollte man dabei allerdings tunlichst vermeiden (siehe SSN 09/2005). Ein konsequenter Entzug von Admin-Rechten bei Microsoft könnte die Beseitigung von Problemen in diesem Zusammenhang deutlich beschleunigen: „Go, Microsoft, go!“

1.2 Un-SSL-Zertifikate?

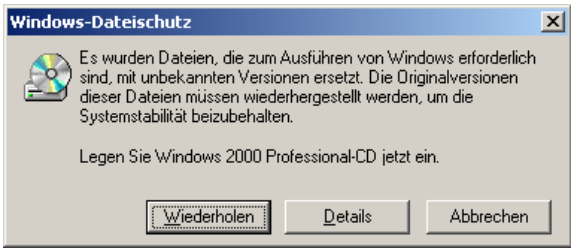
Für ein wenig Aufregung sorgte die Meldung vom 03.06.2006, zukünftige Versionen der populären Mozilla-Browser würden Root-Zertifikate der israelischen StartCom-CA beinhalten. Diese waren Anfang 2006 ins Gerede gekommen, nachdem bekannt wurde, dass man bei StartCom Zertifikate ohne Identitätsprüfung beantragen konnte.

Die Aufregung erscheint unangemessen: Einerseits erlauben die Listen der vorinstallierten Root-Zertifikate *sämtlicher* Browser seit jeher keinerlei Rückschlüsse auf die Qualität der ausgestellten Zertifikate. Und andererseits haben auch andere CAs wie Verisign schon 1996 Zertifikate für E-Mail-Adressen wie root@localhost ausgestellt.

Auch den Mozilla-Entwicklern ist die Problematik längst bekannt, wie interne Diskussionen zeigen. Schon jetzt enthält beispielsweise Firefox (v1.5.0.4) Root-Zertifikate von gut drei Dutzend Firmen, denen man mit der Installation des Browsers automatisch vertraut. Um die Zertifikate bewerten zu können, hilft also nur ein Blick in die Zertifizierungsrichtlinien der jeweiligen CA.

Da kein Anwender sämtliche CA-Policies kennen dürfte, erscheint die Aufregung über die StartCom-Zertifikate ungerechtfertigt. Oder wissen Sie, wie „NetLock Halozatbiztonsagi Kft.“ und „The Go Daddy Group, Inc.“ die Identifikationsprüfung durchführen?

Besonders vorsichtige Zeitgenossen empfehlen daher das Löschen aller vorinstallierten Root-Zertifikate. Dies führt allerdings unter Windows 2000 dazu, dass das komplette System instabil wird:



1.3 Security Focus: Apple

Seit dem 31.05.2006 gibt es nun auch eine Mailingsliste zur Diskussion von Sicherheitsfragestellungen zu Apple's Hard- und Software. Durch eine E-Mail an focus-apple-subscribe@securityfocus.com kann die Aufnahme in den Verteiler initiiert werden. Sicherheitsschwachstellen werden weiterhin über Bugtraq gemeldet.

1.4 Datenklau bei US-Armee

Am 22.05.2006 hat das US-amerikanische Department of Veterans Affairs (zuständig für die medizinische und finanzielle Versorgung von Veteranen) die Serie peinlicher und brisanter Sicherheitsvorfälle in amerikanischen Bundesbehörden (siehe SSN 05/2006) um ein weiteres Highlight ergänzt.

Danach wurde einem Mitarbeiter zu Hause ein Laptop mit über 26 Millionen unge-

schützten Datensätzen von Militärangehörigen (9 % der US-Bevölkerung, davon ca. 2,2 Millionen Aktive) entwendet. Die Daten umfassen Name, Social Security Number und Geburtsdatum – alles, was in den USA zum Identitätsmissbrauch benötigt wird.

Die private Aufbewahrung des Laptop verstieß gegen die Security Policy. Daher wurden nach diesem Vorfall alle Mitarbeiter per Direktive zu einem jährlichen Privacy and Security Training verpflichtet. Denn neben geeigneten technischen und organisatorischen Maßnahmen ist auch ein hohes Sicherheitsbewusstsein im Umgang mit sensiblen Daten unverzichtbar.

1.5 Office im Visier

Am 10.05.2006 meldete Microsoft eine MS-Word Schwachstelle im Microsoft Security Advisory (919637). Sie ermöglicht einem Angreifer, der sein Opfer zum Öffnen präparierter Word-Dokumente verleiten kann, beliebigen Code mit den Berechtigungen des Opfers zur Ausführung zu bringen. Das ist an sich nichts grundsätzlich Neues – allerdings dauerte es über einen Monat, bis Microsoft am 13.06.2006 mit einem Patch im Microsoft Security Bulletin MS06-027 eine zielgruppengerechte Lösung veröffentlichte. Alle zuvor publizierten Workarounds von Trendmicro, Microsoft, US-CERT u. a. setzen zu viel Detailwissen voraus oder sind für den Arbeitsalltag nicht geeignet (Einsatz von WordViewer). Microsoft bewertete die Schwachstelle als „nicht kritisch“; erst im aktuellen Bulletin wurde die Bewertung auf „kritisch“ korrigiert.

Es ist dringend angeraten, den Patch einzuspielen und sich nicht nur auf den aktuellen Virenschutz zu verlassen.

Übrigens: Nicht nur Microsofts Office-Suite steht im Fokus. Am 31.05.2006 hat Kaspersky einen Proof-of-Concept Virus für StarOffice/OpenOffice veröffentlicht. In einer Stellungnahme relativierte das OpenOffice-Team am 02.06.2006 die Bedrohung durch diesen Virus.

1.6 ... back to the Future

BackTrack 1.0, eine Live-Linux-Distribution auf einer bootfähigen CD (oder einem USB-Stick) enthält eine umfassende Sammlung von Netzwerksicherheits- sowie Penetration-Testing-Tools und Exploits. Die neue, am 26.05.2006 freigegebene Distribution enthält sehr aktuelle Programmversionen dieser Werkzeuge (z. B. Metasploit 2.6). Darin laufen die Entwicklungslinien von Auditor Security Linux und WHAX (davor Whoppix) zusammen. Erstmals wurde auch ein eigener Bereich für Datenbankscanner integriert. Ob die Distribution auch die bewährte Robustheit und Funktionsfähigkeit ihrer Vorgänger erreicht, muss sich noch in der Praxis erweisen.

1.7 Big Brother Awards

Ganz ohne Fernsehen und Container werden seit 1998 in inzwischen 17 Ländern jährlich die Big Brother Awards für besondere Verdienste um Datenschutz feindliche Techniken und Datenerhebungen verliehen. In Deutschland organisiert seit dem Jahr 2000 der FoeBuD e. V. in Bielefeld die Nominierung der Preisträger und die Verleihung der „Oscars für Datenkraken“.

Die Nominierung von Preisverdächtigen ist noch bis zum 31.07.2006 möglich. Die diesjährige Verleihung der Awards erfolgt am 20.10.2006 im historischen Saal der Ravensberger Spinnerei im Zentrum von Bielefeld.

2 Secorvo News

2.1 Secorvo College aktuell

Nach der Sommerpause startet Secorvo College im September mit

- dem aktuellen Grundlagenseminar IT-Sicherheit heute (**19.-21.09.2006**) und
- einem Intensivseminar zu Public Key Infrastrukturen (PKI) (**26.-29.09.2006**).

Programme, weitere Seminarangebote, Preise und Online-Anmeldung unter http://www.secorvo.de/college

2.2 Gemalte Städte

Der Künstler Thitz, einigen von Ihnen durch Secorvo-Weihnachtskarten oder einem Besuch in Karlsruhe bekannt, zeigt seine „Gemalten Städte“ noch bis zum 29.10. 2006 in der Staatlichen Kunsthalle Karlsruhe.

2.3 KA-IT-Si @ Midvision

Die Karlsruher IT-Sicherheitsinitiative ist auf der Midvision 2006 am 21. und 22.06.2006 in der Messe Karlsruhe mit einem eigenen Stand vertreten. Auch die KA-IT-Si-Partner AMEC SPIE System Integration und Lampertz sind dabei und zeigen aktuelle Sicherheitslösungen.

Am **21.06.2006** wird um 18:30 Uhr Herr Professor Dr. Bartsch von der renommierten, auf IT-Recht spezialisierten Karlsruher Kanzlei Bartsch und Partner im Foyer der Messe über „Risiken, Pannen, Schäden – und wer haftet?“ sprechen. Anmeldung zu diesem KA-IT-Si-Event bitte über die Webseite (Anfahrtskizze).

Zum Vormerken: Ihren fünften Geburtstag wird Deutschlands älteste IT-Sicherheitsinitiative am **18.10.2006** im Saal Baden der IHK Karlsruhe angemessen feiern. Die Key Note wird Herr Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) halten.

3 Veranstaltungshinweise

Juni 2006	
21.06.	"Risiken, Pannen, Schäden – und wer haftet?" (KA-IT-Si, Messe Karlsruhe)
21.-22.06.	Midvision 2006 (Messe Karlsruhe)
25.-30.06.	18th Annual FIRST Conference (FIRST, Baltimore/USA)
Juli 2006	
13.-14.07.	DIMVA 2006 (GI, Berlin)
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/CA)
August 2006	
02.-03.08.	Black Hat USA 2006 (Black Hat, Las Vegas/USA)
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/US)
September 2006	
19.-21.09.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
26.-29.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2006	
18.10.	KA-IT-Si-Jubiläumsfeier (KA-IT-Si, IHK Karlsruhe)
23.-27.10.	Systems 2006 (Messe München, München)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

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