secorvo
security consulting

Secorvo Security News

Mai 2008

Editorial: Geistige Brandstifter

Der 11. September 2001 wird uns nicht nur als der Tag eines schockierenden Massenmords in Erinnerung bleiben. Er wird auch als Wendepunkt in die Annalen der Inneren Sicherheit eingehen. Mit beispielloser Geschwindigkeit zauberten Sicherheitsbehörden westlicher Regierungen gleich welcher politischen Couleur in den darauffolgenden Monaten neue Sicherheitsgesetze aus den Schubladen, die ohne nennenswerten politischen oder öffentlichen Widerstand die demokratischen Entscheidungsgremien passierten. Auch bestehende Befugnisse wurden ausgeweitet. In Deutschland stieg die ohnehin schon rekordverdächtig hohe Zahl angeordneter Telekommunikationsüberwachungen rapide: sie verdoppelte sich seit 2001 auf knapp 45.000 Fälle. 2007 war es für einen Bundesbürger 74 mal so wahrscheinlich, abgehört zu werden, wie für einen Nordamerikaner.

Erst in den vergangenen Monaten regt sich nennenswerter öffentlicher Widerstand – gegen die Pläne einer Online-Durchsuchung, den biometrischen Personalausweis und die Vorratsdatenspeicherung; ermutigt vom Bundesverfassungsgericht, das die rechtsstaatlichen Grenzen staatlicher Überwachung in Erinnerung gebracht hat.

Schlimmer noch als die schleichende Ausdehnung von Überwachungsbefugnissen ist jedoch der Geist, den die scheinbar widerspruchsfreie Beschränkung bürgerlicher Freiheitsrechte gesät hat. So sollte es eigentlich niemanden wundern, dass in der herrschenden Atmosphäre des Misstrauens Verantwortliche in Unternehmen auf die Idee kommen, Mitarbeiter, Aufsichtsräte und Investoren zu überwachen. Das Bewusstsein der Strafbarkeit solcher Maßnahmen kann in einem politischen Kontext abhanden kommen, in dem Datenschutz als „Täterschutz“ diffamiert wird, Abschüsse von Linienflugzeugen, Online-Überwachung und Vorratsdatenspeicherung ohne Rücksicht auf elementare Grundrechte in Gesetze gegossen werden und Nachrichtendienste rechtswidrig Journalisten bespitzeln. Die geistigen Brandstifter – die sitzen in den Innenministerien.

Inhalt

secorvo
security consulting

Security News

WLAN-Missbrauch strafbar

Erstmalig hat ein deutsches Gericht den Missbrauch eines ungeschützten privaten WLANs als Straftatbestand gewertet: Das Amtsgericht Wuppertal verurteilte in einem am 03.04.2008 publizierten Urteil (Az. 22 Ds 70 Js 6906/06) den „Schwarzsurfer" wegen unerlaubten Abhörens eines Funknetzes (§ 89 TKG) sowie nach § 44 BDSG wegen der widerrechtlichen Aneignung einer privaten IP-Adresse – die ihm der Router zugeteilt hatte. Die Strafe (20 Tagessätze) wurde zur Bewährung ausgesetzt, der Laptop des Täters jedoch als „Tatwerkzeug" eingezogen (NStZ 03/2008, S. 161 ff.). Auch wenn Kritik an der Rechtsauffassung des Gerichts angebracht erscheint, sollte man von der ungenehmigten Nutzung fremder WLANs tunlichst Abstand nehmen.

Botnetz-Analyse

Vitaly Kamluk, Virenanalyst bei Kaspersky Lab, veröffentlichte am 13.05.2008 eine lesenswerte Analyse über Botnetze. Neben einer systematischen Klassifizierung nach Architektur und verwendeten Netzprotokollen und einer anschaulichen Darstellung der Entwicklung der Botnetz-Technologie beleuchtet der Autor den gefährlichen Trend zu Peer-to-Peer-Botnetzen. Diese kommen ohne eine zentrale Kommandostelle aus, indem sie Befehle mit ihren „Nachbarn" austauschen. Besonders das „Sturmwurm"-Botnetz (SSN 08/2007) stellt eine erhebliche Bedrohung dar, da es sich über stündlich neue Mutationen verbreitet und bis zu seinem Einsatz unauffällig und „ruhig" verhält.

Die Analyse, die bei Kaspersky Lab auch als pdf-Datei heruntergeladen werden kann, schließt mit der Veranschaulichung einiger Geschäftsmodelle der „Botnetz-Industrie". Die zunehmende Professionalisierung von Konzeption, Infizierung und Steuerung von Zombie-PCs über Botnetze belegt, dass mit der Nutzung von Bots Geld verdient werden kann. Austrocknen lässt sich dieser Cyber-Sumpf nur an den Wurzeln: den Löchern in Systemen, die die Einnistung von Bots erst ermöglichen.

Schwerer Lotus Domino Bug

Am 20.05.2008 meldete MWR InfoSecurity einen Stack Overflow für IBMs Lotus Domino Web Server, der einem Angreifer die Ausführung beliebigen Codes unter System-Privilegien erlaubt – und der via Fernzugriff ausgelöst werden kann. Nachgewiesen wurde der Bug für die Versionen 7.0.3 und 8.0; mit hoher Wahrscheinlichkeit sind auch ältere Versionen betroffen. IBM hat passende Update-Patches bereitgestellt. Wer einen Lotus Domino Web Server im Internet betreibt sollte schnell reagieren.

Verbindungsdatenauskünfte

Neben den Inhalten unterliegen auch die „näheren Umstände" der Telekommunikation (Wer? Wo? Mit wem? Wann? Wie lange?), „Verbindungsdaten" genannt, dem Fernmeldegeheimnis (§ 88 TKG). Dessen Verletzung ist eine Straftat (§ 206 StGB) und kann mit bis zu fünf Jahren Freiheitsstrafe geahndet werden. Ausnahme: Strafverfolgungsbehörden dürfen im Zusammenhang mit Straftaten von „im Einzelfall erheblicher Bedeutung" (insbesondere die „Katalogstraftaten" des § 100a Abs. 2 StPO) auch ohne Wissen des Betroffenen Verkehrsdaten erheben (§ 100g StPO).

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat am 13.02.2008 ihre knapp 500 Seiten starke, im Auftrag des BMJ erstellte Langzeitstudie zur „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO" vorgelegt. Danach ist die Zahl der Verkehrsdatenabfragen in den vergangenen Jahren explodiert: Waren es im Jahr 2000 noch 5.000, stieg die Anzahl 2005 auf das Achtfache (40.000 Abfragen). Eine wachsende Rolle spielen dabei offenbar Standort- und Funkzellenabfragen (18% bzw. 10%), mit denen der Aufenthaltsort Verdächtiger ermittelt werden kann – oder auch alle Personen, die sich zum Tatzeitpunkt mit eingeschaltetem Handy in einer bestimmten Funkzelle aufhielten.

Mängel stellt die Untersuchung insbesondere bei der Benachrichtigung der Betroffenen fest: lediglich in 4% der Fälle war die Benachrichtigung in den Akten dokumentiert; die Vernichtung der Daten konnte nur in 3% der untersuchten Verfahren den Akten entnommen werden. Wer mag sich da noch wundern, dass die derzeit vor dem Bundesverfassungsgericht verhandelte Vorratsdatenspeicherung von Verbindungsdaten Befürchtungen weckt?

Pseudozufall

Am 13.05.2008 veröffentliche das Debian Projekt eine korrigierte Version des OpenSSL-Packets, da alle OpenSSL-Versionen seit September 2006 (Versionen 0.9.8c-1 bis 0.9.8g-9) auf Debian-Distributionen wie Ubuntu kompromittierbare kryptografische Schlüssel erzeugen. Ursache: Die Funktion, die für zufällige Startwerte im Zufallszahlengenerator sorgen sollte, war im Quellcode auskommentiert. Der Zufallszahlengenerator nutzte daher die Linux Prozess ID als Zufallswert, die nur 32.767 mögliche

Werte annehmen kann. Daher lassen sich die geheimen Schlüssel von u.a. SSL, SSH, DNSSEC sowie X.509-Zertifikaten via Brute-Force-Angriff finden. Betroffen sind alle Programme, die OpenSSL zur Erzeugung kryptografischer Schlüssel verwenden, darunter Apache, Sendmail, Exim und OpenVPN.

Zweck der nicht mit dem OpenSSL-Entwicklungsteam abgestimmten Auskommentierung durch den Debian OpenSSL Maintainer war die Unterdrückung von Fehlermeldungen, die das Softwareanalysewerkzeug valgrind festgestellt und fälschlich als Softwarefehler interpretiert hatte. Da kommt der Draft der NIST-Publikation SP 800-108 „Recommendation for Key Derivation Using Pseudorandom Functions“ vom 01.05.2008 leider zu spät: Jetzt müssen zahlreiche Schlüssel getauscht werden – ein gutes Geschäft für Certificate Authorities.

Leitfäden zum “Hackerparagraf”

Am 17.04.2008 hatte die EICAR einen von Christian Hawellek und Dennis Jlussi von der Universität Hannover entwickelten Leitfaden zur strafrechtlichen Relevanz von IT-Sicherheitsaudits veröffentlicht, der Empfehlungen zur Durchführung von Audits im Kontext des neuen § 202c StGB (der „Hackerparagraf“, siehe SSN 07/2007) zusammenfasst. Er geht unter anderem ausführlich auf die Gestaltung von Einverständniserklärungen zur Vermeidung von Strafbarkeitsrisiken ein. Ebenfalls 16 Seiten umfasst der am 23.05.2008 vom Bitkom publizierte Praktische Leitfaden für die Bewertung von Software im Hinblick auf den § 202c, StGB. Neben einer Kriterienliste zur Beurteilung, ob eine Software unter die Bestimmungen des § 202c fällt, schlägt der Leitfaden „Best Practice“-Regelungen für den Umgang mit „Dual-Use“-Software im Unternehmen vor. Beide enthalten vernünftige Empfehlungen zur Absicherung, insbesondere im Falle einer externen Durchführung von IT-Sicherheitsaudits.

Malware mit Copyright

Am 25.04.2008 veröffentlichte Liam O. Murchu im Symantec Security Response Blog beispielhaft die Copyright- und Lizenzhinweise der ZeuS-Crimeware – eines russischen Malware-Construction-Kits zum Aufbau von Botnetzen. Darin droht der „Anbieter“ damit, jede nicht vertragskonforme Nutzung durch die Versendung der Signatur der spezifischen Binärdatei an führende Antiviren-Hersteller zu unterbinden. Eine interessante Rolle für die AV-Industrie – Copyright Enforcement für Schadsoftware-Baukästen. Möglicherweise kann sie sich dieser Rollenzuweisung nicht einmal entziehen.

Firewire macht Feuer

In der Theorie ist es ein alter Hut: Schon am 30.09.2006 hatte Adam Boileau auf der damaligen Ruxcon über Angriffe via Firewire vorgetragen. Seine ausführliche Präsentation „Hit by a bus: Physical Attacks with Firewire“ wurde damals von einer Live-Demo begleitet. Knapp zwei Jahre später nun unterlegt er seine akademische Attacke mit einem „Proof of concept“: Anfang März 2008 stellte Boileau das Tool winlockpwn auf seiner Website zur Verfügung. Mit diesem Tool kann von einem via Firewire verbundenen Computer ein Login an einem Rechner unter Windows XP (SP2) als Administrator erzwungen werden. Die erschreckende Eleganz dieses Angriffs lässt sich auf YouTube bewundern. Boileau nutzt dabei die Eigenschaft der Firewire-Schnittstelle, den Speicher des angeschlossenen Rechners direkt zu adressieren – und ihm so z.B. eine modifizierte DLL unterzuschieben.

Die Existenz von winlockpwn fordert in vielen Bereichen das Überdenken existierender Sicherheitskonzepte. Beispielhaft sei hier der – nicht zu empfehlende – Einsatz von Festplattenvollverschlüsselungslösungen ohne „Pre Boot Authentication“ genannt.

Secorvo News

Secorvo College aktuell

Die Nachfrage nach dem TISP-Zertifikat wächst ungebrochen: Schon weit über 200 deutsche Security Professionals dürfen sich mit diesem Titel schmücken, und 2008 werden voraussichtlich weitere 100 Absolventen das Zertifikat erwerben. Noch zwei letzte freie Plätze für Kurzentschlossene gibt es auf dem TISP-Seminar am **02.-06.06.2008**.

Die nächste Gelegenheit zur TISP-Zertifizierung bietet College nach der Sommerpause vom **08.-12.09.2008**. Vorher führt College vom **01.-03.07.2008** noch mit einem dreitägigen Seminar in die Durchführung von forensischen Analysen ein.

Security Awareness Symposium

Vom 17.-18.06.2008 findet das sechste „Security Awareness Symposium“ statt, das sich zum jährlichen Treffpunkt von Security-Awareness-Verantwortlichen entwickelt hat. Auf dem von Secorvo zusammen mit den E-Learning-Experten von digital spirit und der Agentur DauthKaun veranstalten Symposium in den stilvollen Räumen der Buhlschen Mühle in Ettlingen werden unter anderem die Erfahrungen der Münchener Rück, SAP, T-Systems und MDS vorgestellt und diskutiert.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2008	
29.05.	Pimp your web (KA-IT-Si, Karlsruhe)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College)
09.-10.06.	DuD 2008 (Computas, Berlin)
17.-18.06.	6. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)
24.-25.06.	D-A-CH Security 2008 (GI/OCG/Bitkom/TTT, Berlin)
24.-26.06.	Sichere Softwareentwicklung (Secorvo College)
Juli 2008	
01.-03.07.	Forensik (Secorvo College)
10.-11.07.	DIMVA 2008 (GI)
28.07.-1.08.	17th USENIX Security Symposium 2008 (San José/US)
August 2008	
17.-21.08.	Crypto 2008 (IACR, Santa Barbara/US)

Fundsache

Symantec hat am 08.04.2008 den 13. „Global Internet Thread Report" für den Sechsmonatszeitraum Juli bis Dezember 2007 publiziert. Er enthält eine umfangreiche Analyse der Entwicklung aktueller Bedrohungen durch Malware, Botnetze und sicherheitskritische Softwarefehler. Explodiert ist die Menge bösartigen „Malicious Code": Gegenüber dem Vorjahreszeitraum hat sich deren Zahl auf 500.000 mehr als versechsfacht.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Kai Jendrian, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

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

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