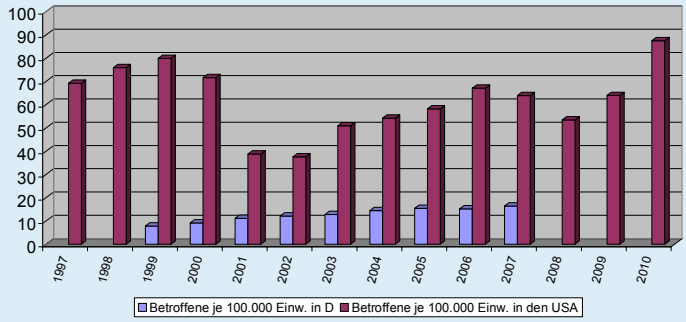
secorvo
security consulting

Secorvo Security News

Juli 2011

TK-Überwachung im Vergleich

Die heimliche Überwachung von Telekommunikationseinrichtungen ist ein Eingriff in das Fernmeldegeheimnis (Art. 10 GG) – und den Strafverfolgungsbehörden nur bei begründetem Tatverdacht, schweren Straftaten und als „ultima ratio“ (§ 100a StPO) erlaubt. Sie erfordert zudem eine richterliche Anordnung (§ 100b StPO). Anders als in den USA, die die Richter verpflichten, das Ergebnis der Überwachung in einem „Wiretap Report“ (Umfang, Anklagen und Verurteilungen) zu dokumentieren, unterliegt die TK-Überwachung in Deutschland keiner Erfolgskontrolle. Den tatsächlichen Umfang der Überwachung geben aber auch die amerikanischen Wiretap Reports nicht auf den ersten Blick preis. Im direkten Vergleich zeigt sich, dass die Zahl der von einer Überwachung Betroffenen je Einwohner und Jahr in den USA erheblich schwankt, während sie in Deutschland - auf niedrigerem Niveau - kontinuierlich wächst. Leider ist der deutschen Statistik die Zahl der Betroffenen nur bis 2007 zu entnehmen.



Bedenklicher stimmen die Ergebnisse empirischer Analysen, wie die von Dr. Jens Eckhardt (2009). Sein Fazit: „Die Erfolge stehen in keinem angemessen Verhältnis zu den damit verbundene Eingriffen.“ Und: „Eine substantiierte Begründung der Überwachung war nur in einem geringen Maß festzustellen.“

Inhalt

Security News

Böse Schnittstelle

USB-Sticks haben nicht erst seit Stuxnet (SSN 10/2010) anderen Speichermedien den Rang als verbreitetste „Gefährder“ abgelaufen. Nach Dumper, HackSaw und SwitchBlade hat nun die Firma Netragard dies im Rahmen eines Penetrationstests in besonders kreativer Weise unter Beweis gestellt: Sie verschickte eine „trojanisierte“ USB-Maus als Werbegeschenk getarnt an einen Mitarbeiter des Unternehmens.

Darin befanden sich zusätzlich ein USB-Hub, ein USB-Flash-Drive sowie ein Mikrocontroller, der nach dem Anstecken eine Tastatur emulieren und Tastatureingaben an den PC senden konnte – die Herstellung dieser Spezialmaus wurde detailliert beschrieben. Mit einer Standard-Remote-Shell aus dem Metasploit-Framework konnte damit der PC übernommen und in das Netzwerk eingedrungen werden.

Ein ähnlich kreativer Ansatz, per USB und einem Teensy Controller Systeme anzugreifen, wurde am 13.07.2011 von Didier Stevens vorgestellt: Mit vorprogrammierten Tastatureingaben wird ein Editor geöffnet, binärer Code eingetippt und dieser als PDF gespeichert. Wird das PDF geöffnet, führt das befallene System den Code aus.

In beiden Fällen rettet kein Virenschutz – höchstens eine Kontrollsoftware für angeschlossene USB-Geräte, die die Maus als Datenspeicher entlarvt hätte. Aber es geht auch nicht ohne Benutzersensibilisierung, denn bei allen unbekannten USB-Geräten ist Vorsicht geboten – auch Lautsprecher, Tassenwärmer oder Spaß-Geräte aus externer Quelle können solche Erweiterungen in sich bergen.

IMSI-Catcher für jedermann

In Großbritannien verkauft Vodafone als Femtozelle ein Gerät, das für UMTS eine ähnliche Funktion wie ein WLAN Access Point bietet: Das Handy des Kunden funkt zur Femtozelle, die über den heimischen Internet-Anschluss an das Vodafone Mobilfunknetz angebunden ist. Am 13.07.2011 publizierte nun die Gruppe THC Untersuchungen aus 2009/10, denen zufolge es gelang, dank eines schwachen Root-Passworts mittels Reverse-Engineering die Kontrolle über die Linux-basierten Zellen zu übernehmen. Nach Ausbau bzw. Deaktivieren einiger Sicherheitseinrichtungen konnten die Forscher dann – wie auch von anderen Experten erwartet – Gespräche abhören und auf fremde Kosten telefonieren.

Das gelang, weil die Femtozelle große Teile der Funktion eines UMTS Radio Network Controllers (RNC) wahrnimmt, darunter die Verschlüsselung der Funkstrecke, und die erforderlichen Schlüssel über die Internet-Anbindung aus dem Kern-Netz des Providers bezieht. In der ursprünglichen UMTS-Architektur ist der RNC eine Komponente des Providernetzes – nur autorisiertem Personal zugänglich und kein kleines Gerät im Kunststoffgehäuse, an das der zahlende Kunde Anschlüsse anlöten und „Man-in-the-Middle“ spielen kann.

Auch hier zeigt sich wieder wie wichtig es ist, zuerst die zu Grunde liegenden Sicherheitsannahmen zu hinterfragen, ehe man ein bewährtes Verfahren auf neue Szenarien überträgt.

Mit der Schrotflinte...

Auf Initiative Hessens hat der Bundesrat am 17.06. 2011 einen Entwurf zur Überarbeitung des Telemediengesetzes (TMG-E) vorgelegt. Darin findet sich in § 13 Abs. 8 – entsprechend Art. 2 Abs. 5 der Richtlinie 2009/136/EG, die eine entsprechende Regelung in die Datenschutzrichtlinie für elektronische Kommunikation einfügte und bis Mai 2011 umzusetzen war – die Festlegung, dass die Speicherung und der Abruf von Daten im Endgerät des Nutzers künftig nur mit Unterrichtung und vorheriger Einwilligung zulässig sein werden.

Betroffen hiervon sind sämtliche Cookies und automatischen Abfragen, bspw. durch Apps. Praktisch würde damit der Einsatz von Cookies unhandlich bis unmöglich. Die Ausnahme der „unbedingten Erforderlichkeit zur Dienstnutzung“ ist ungeeignet, diese Wirkung zu entschärfen, denn wie viel Bequemlichkeit ist unbedingt erforderlich?

In § 13a TMG-E werden Anbieter von Foren, Blogs, Social Networks und ähnlichen Diensten verpflichtet ihre – nicht näher definierten – höchsten Sicherheitseinstellungen als Default anzubieten. Einzige materielle Vorgabe ist die Unauffindbarkeit durch Suchmaschinen. Eine Herabsetzung der Einstellungen soll nur Nutzern über 16 Jahren möglich sein.

In beiden Fällen ist die Absicht zu begrüßen, Transparenz, Nutzerkontrolle und Nutzerschutz im Internet zu stärken - die derzeitige Fassung des Gesetzentwurfs erscheint jedoch wenig durchdacht und praxisuntauglich.

Hase ./. Igel

Der Wettlauf zwischen IT-Sicherheit und organisierter IT-Kriminalität geht in die nächste Runde. Da Nutzer der DHL Packstation als potentielle Zieladresse für online ergaunerte Waren ein beliebtes Phishing-Ziel darstellen, ist seit März 2011 eine Kunden-Magnetkarte erforderlich, um eine Sendung abzuholen. Am 25.06.2011 wurde nun gezeigt, wie

man sich zu jeder Packstation-Adresse eine passende Magnetstreifenkarte selbst kodieren kann.

Magnetstreifenkarten haben auch am Geldautomaten bald ausgedient. Die Schadensfälle durch Skimming nehmen dermaßen überhand, dass viele Banken, wie am 05.07.2011 bekannt wurde, die außereuropäische Nutzung der EC-Karte drastisch einschränken. Und beim Online-Banking schließlich wechseln viele Institute mittlerweile von der iTAN zu Verfahren mit Handheld-Kartenlesern (chipTAN oder SmartTAN genannt). Derweil warnte das BKA am 15.07.2011 vor Trojanern, die ihre Opfer ganz offen zu einer Überweisung auffordern – unter dem Vorwand, eine versehentliche Gutschrift rückgängig zu machen. Da hilft leichtgläubigen Kontoinhabern auch kein chipTAN-Verfahren mehr.

Es sieht also so aus, als ob uns dieser Wettlauf noch eine Weile erhalten bleibt. Noch ist allerdings unentschieden, welche Seite im Ziel der Igel ist.

Same procedure …

Bei der Durchsicht der am 27.06.2011 veröffentlichten CWE/SANS TOP 25 Most Dangerous Software Errors – ermittelt anhand des CWSS-Bewertungssystems, reduziert auf Tragweite, Verbreitung und Ausnutzbarkeit der Schwachstellen – fühlt man sich wie Miss Sophie an Sylvester: Seit Jahren finden sich dieselben Schwachstellen auf den Top-Positionen der Liste, darunter SQL-Injection, Command Injection und Cross-Site Scripting, obwohl seit längerem wirksame Ansätze zu deren Bekämpfung bekannt sind.

Die Liste findet ihre praktische Bestätigung in aktuellen Schwachstellenübersichten und Berichten über erfolgreiche Hacks (Citibank, MySQL, Barracuda, REWE, Schufa, …) und deckt sich größtenteils mit den weithin bekannten OWASP Top 10.

Sofern die Entwicklung sicherer Software nicht bald durchgängig ernster genommen wird, müssen wir uns wohl auch im nächsten Jahr auf eine ganz ähnliche Übersicht einstellen. „Cheerio, Sophie, mee girl!“

ShellBag Forensik

Seit dem 29.05.2011 liegt der Windows ShellBag Parser von TZ Works als stabile und skriptfähige 64-bit-Version vor, die auch mit den ShellBags von Windows 7 problemlos arbeitet – anders als etwa kommerzielle, forensische Suiten, bei denen die Auswertung von ShellBags z. T. noch in den Kinderschuhen steckt.

Damit kann aus vorliegenden benutzerspezifischen Profil-Dateien von Windows (NTUSER.DAT, UsrClass.DAT) eine Vielzahl von Informationen über das Laufzeitverhalten eines Windows-Benutzerkontos gewonnen werden. Mit diesen Informationen wird die Erstellung von aussagefähigen Zeitlinien und Nutzungsabfolgen aus Metadaten des NTFS-Dateisystems, gecarvten Dateifragmenten und Benutzerkonteninteraktionen deutlich besser interpretierbar.

Da die Aufrufreihenfolge der jeweils letzten Aktionen in den ShellBags von Windows automatisch festgehalten wird, können so z. B. auch Malwareaktivitäten identifiziert werden, die im Benutzerkontext gestartet wurden – oder auch versehentlich gelöschte Verlaufshistorien zurück gewonnen werden.

Secorvo News

TISP und mehr

Nach der Sommerpause startet Secorvo College zunächst mit dem Seminar „Sicherheitsmanagement heute“ vom 27.-29.09.2011. Es folgen die Seminare „Verlässliche Web-Anwendungs-Sicherheit“ (05.-06.10.2011), „IT-Sicherheitsaudit in der Praxis“ (10.-12.10.2011) und „Datenschutzaudit: Best Practice“ (13.-14.10.2011).

Die nächste Gelegenheit zur TISP-Zertifizierung bietet Secorvo College mit der T.I.S.P.-Schulung vom 17.-22.10.2011 (einschließlich Prüfung).

Die Programme aller Seminare und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Tag der IT-Sicherheit

Wer am 14.07.2011 den mit ca. 100 Besuchern hervorragend besuchten 3. Tag der IT-Sicherheit in der IHK Karlsruhe verpasst hat, findet die Unterlagen der Referenten auf den Webseiten der IHK unter der Dokumentennummer 83415 und eine Pressemitteilung der KA-IT-Si zum Download.

Zum Vormerken: Das nächste KA-IT-Si-Event findet am 22.09.2011 im Panoramasaal der IHK-Karlsruhe statt (Anmeldung).

Veranstaltungshinweise

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

August 2011	
04.-07.08.	DEFCON 19 (DEFCON, Las Vegas/US)
10.-12.08.	20th USENIX Security Symposium (Usenix, San Francisco/US)
14.-18.08.	Crypto 2011 (IACR, Santa Barbara/US)
September 2011	
13.-14.09.	Cybersecurity 2011 (Handelsblatt, EUROFORUM, Berlin)
19.-23.09.	OWASP Global AppSec North America (OWASP Foundation, Minneapolis/US)
27.-29.09.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Oktober 2011	
05.-06.10.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
24.-27.10.	it-sa (SecuMedia Verlag, Nürnberg)
26.-29.10.	hashdays security & risk conference 2011 (DEFCON Switzerland, Luzern/CH)

Fundsache

Das German Chapter des Berufsverbands ISACA hat am 17.05.2011 einen Prüfleitfaden zur Auftragsdatenverarbeitung (§ 11 BDSG) publiziert. Der knapp 40seitige Leitfaden enthält Prüffragen zu den acht in der Anlage zu § 9 BDSG geforderten Maßnahmenbereichen mit Bezügen zu COBIT (4.1), ISO 27xxx und BSI IT-Grundschutz.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, 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