secorvo
security consulting

Secorvo Security News

April 2011

Anonyme Kontrolle

Der eine oder andere „Datenschutzaufreger“ mutet schon etwas skurril an. So wissen wir jetzt, dass der Navigationsgerätehersteller TomTom Daten über Streckendurchschnittsgeschwindigkeiten (die aus den Fahrdaten von TomTom-Kunden errechnet werden, um möglichst realistische Fahrzeiten zu prognostizieren) niederländischen Behörden zugänglich macht, um diesen die Beseitigung von Engpässen und Stauabschnitten zu erleichtern. Die niederländische Polizei nutzte diese Daten unerwartet kreativ: Sie platzierte Radarfallen an Stellen, an denen die von TomTom bestimmten Durchschnittswerte über der örtlichen Geschwindigkeitsbegrenzung lagen. (Vielleicht hatte sie den Datenschutzbericht der Telekom gelesen.)

Aus der Perspektive des Steuerzahlers und Bürgers ist das eine sehr vernünftige Maßnahme: höchste Wirtschaftlichkeit der Geschwindigkeitskontrollen, wirksame Erhöhung der Verkehrssicherheit in kritischen Straßenabschnitten – und datenschutzrechtlich nicht zu beanstanden, da lediglich mit Zustimmung der Nutzer erstellte anonyme Statistiken verwendet wurden. Dennoch ist die Aufregung groß. Das mag daran liegen, dass TomTom-Nutzer den Eindruck gewonnen haben, dass sie mit ihrer Zustimmung zur Datenerhebung der Polizei die Ahndung eigener Verkehrsdelikte erleichtern.

Vielleicht aber versteckt sich hier ein sehr grundsätzliches Datenschutzproblem, das das geltende Recht nur unzureichend erfasst. Denn auch anonyme Statistiken – nach Definition gerade keine personenbezogenen Daten – können die freie Entfaltung beeinträchtigen. So könnten Stadtwerke in Abhängigkeit vom Mietniveau eines Wohnbezirks entscheiden, ob sie bei Zahlungsverzug den Kunden erst anrufen oder lieber gleich zwei kräftige Ableser vorbeischicken. Versandhändler könnten Bestellungen aus Städten mit hoher Arbeitslosigkeit ablehnen, um Zahlungsausfälle zu minimieren. Und Anbieter von Pillen gegen Harndrang könnten die Plakatierung in Gegenden verstärken, in denen die Smart Meter gehäuft nächtliche Toilettengänge registrieren. Schöne neue Welt.

Inhalt

secorvo
security consulting

Security News

Ein Goldchip ist keine Silberkugel

Zu Jahresbeginn forderte das BKA, zum Schutz gegen Skimming-Angriffe an Geldautomaten endlich komplett vom Magnetstreifen auf den EC-Karten-Chip umzusteigen. Bereits am 11.02.2010 hatten britische Forscher der BBC demonstriert, wie sich eine Schwäche im dort verwendeten „Chip&PIN" Verfahren am Point-of-Sale-Terminal ausnutzen lässt. Sie benötigten dazu allerdings einen Rucksack voller Elektronik und im Ärmel versteckte Kabel.

Am 10.03.2011 präsentierten amerikanische Wissenschaftler nun bei der CanSecWest Konferenz ein Skimming-Gerät, das vollständig im Schlitz eines Kartenlesers verschwindet und sich als ultraflacher Man-in-the-Middle zwischen die Kontakte des Lesers und der Karte setzt. Ohne starke Krypto-Protokolle schützt auch ein Sicherheitschip nicht vor Missbräuchen an der Automatenschnittstelle.

Erhöhtes Grundrauschen

Am 19.04.2011 veröffentlichte der Sicherheitsdienstleister Verizon Business seinen Data Breach Investigations Report für 2011. Danach hat die große Zahl externer Hacking-Angriffe auf Zufallsopfer den Anteil an Insiderattacken gegenüber dem Vorjahr zurück gedrängt - nicht jedoch deren absolute Zahl.

Diesen Trend bestätigt eine Meldung vom 16.04. 2011, nach der selbst von seriösen Webseiten wie den von Amnesty International aus Drive-By Downloads über die offenbar nicht auszurottenden Schwachstellen des Flash Players verteilt werden.

Die Empfehlung der Autoren des Reports für den Umgang mit dem damit verbundenen Risiko ist Wasser auf die Mühlen von Datenschützern: Man lösche alle nicht benötigten Daten, damit man die verbleibenden besser im Blick behalten kann.

Datenschutz zum Anfassen

Das Projekt „Autobahnmaut" des Betreibers Toll Collect stand vor Beginn des Wirkbetriebs am 01.01. 2005 wegen Startproblemen und der Erhebung der Mautdaten unter starker Kritik. Seither ist es ruhig geworden um Toll Collect - die Mauterhebung läuft reibungslos und der BfDI überzeugte sich 2006 von der Wirksamkeit des Daten-Löschkonzepts.

Am 25.02.2011 ging Toll Collect mit der Eröffnung einer Datenschutz-Ausstellung in die Öffentlichkeit: Spannungsfelder zwischen Techniknutzung und Datenschutz werden in fünf Installationen aufbereitet, z. B. in Form einer Datenspur über einen Tag – mit überraschenden Einsichten. Drei weitere Installationen beschäftigen sich mit der beschlagnahmefesten Zweckbindung der Mautdaten, der Löschkaskade für Kontrolldaten aus den Mautbrücken und den Löschfristen für Daten im Lebenszyklus eines Mautbenutzers. Die Besichtigung der Berliner Ausstellung ist nach Anmeldung möglich.

Bleibt zu wünschen, dass sich solche Best Practice in andere Unternehmen verbreitet – und der Gesetzgeber die strenge Zweckbindung der Mautdaten auch in der Zukunft aufrecht erhält.

Virencheck-Check

Viele IT-Nutzer erleben IT-Sicherheit vor allem beim Viren-Scan – häufig allerdings eher als (vermeintliche) Ursache für Performance- oder Funktionalitätseinschränkungen denn als wirksamen Schutz.

Am 14.04.2011 veröffentlichte nun das renommierte unabhängige Magdeburger AV-Testlabor aktuelle Prüfergebnisse für 22 führende Anti-Virus-Produkte. Seit Mitte 2010 erhalten Produkte, die 11 der maximal 18 zu vergebenden Testpunkte erreichen, von AV-Test ein Zertifikat. Ein zugehöriger Test-Report weist die vom Produkt für die Erkennung und Beseitigung von Viren sowie den Bedienkomfort erreichten Punkte aus.

Zwar kann man geteilter Meinung darüber sein, ob ein umfassender Client-Virenschutz auf rein geschäftlich genutzten Systemen noch zeitgemäß ist – denn eingehende E-Mails und Internet-Downloads lassen sich zentral wirksamer prüfen. Damit bleibt wenig mehr als das Einfallstörchen USB-Stick.

Bei privaten Systemen hingegen, die in der Regel durch keine Firewall und keinen zentralen Virenscanner geschützt sind, sind Anti-Viren-Produkte nach wie vor unverzichtbar – da kann es lohnen, vor der nächsten Verlängerung der Produktlizenz einen Blick auf die Testergebnisse zu werfen.

GPS-Daten in Smartphones

Der am 20.04.2011 publizierte „iPhone Tracker" von Alasdair Allan und Pete Warden, der die im iPhone gespeicherten GPS-Informationen eines Nutzers visualisiert, hat großen Wirbel ausgelöst – dabei ist die Speicherung von GPS-Daten auf dem iPhone lange bekannt. Auch der primäre Zweck der Speicherung ist leicht zu raten: Da präzise GPS-Lokalisierungen zeit- und rechenintensiv (und damit auch energiehungrig) sind, suchen alle Smartphone-Hersteller nach Optimierungen – z. B. durch die Speicherung „bekannter Wege", denn Menschen neigen dazu, bestimmte Wege immer wieder zu nutzen. Nicht auszuschließen allerdings, dass Apple mit den Daten zukünftig auch anderes im Sinn hatte: Erst

im Juni 2010 hatte Apple in seine Datenschutzrichtlinie die Nutzung und Weitergabe (anonymisierter) Standortdaten aufgenommen.

Andere Anbieter haben sich da geschickter angestellt. So erzeugt Vodafone mit seinem Ortungsservice „Vodafone Locate“ zur Handyortung, Routen- und Terminplanung Umsatz – statt eines Datenschutzskandals.

Personalausweis im Test

Am 21.04.2011 hat die Stiftung Warentest die Ergebnisse des Schnelltests der Einsatzmöglichkeiten des neuen Personalausweises veröffentlicht. Ganze 18 Angebote für die Online-Identifikation mit der eID zählten die Tester – davon ist ein Teil nur für registrierte Kunden nutzbar. Die Testseite des „Kompetenzzentrums neuer Personalausweis“ erzeugte z. T. merkwürdige Fehlermeldungen. Und einzig beim Angebot der Schufa erhält man bei deaktivierten Cookies eine aussagekräftige Meldung – alle anderen Angebote stellen sich „tot“.

Das nüchterne Fazit: Der praktische Nutzen der eID-Funktion hält sich (noch) stark in Grenzen, die wenigen Anwendungen gehören zudem zum Teil in die Kategorie „Bananen-Software“: Reift beim Kunden.

Smart Meter – mit Sicherheit

Seit Anfang 2010 ist der Einbau von Smart Metern in Neubauten und bei Renovierungen nach § 21b Abs. 3a/b Energiewirtschaftsgesetz (EnWG) vorgeschrieben. Dass Sicherheitsprobleme in diesen Geräten weit reichende Auswirkungen haben können, ist keine neue Erkenntnis. Daher wird derzeit unter der Federführung des BSI ein passendes Schutzprofil nach Common Criteria für die zugehörige Kommunikationseinheit (auch „Multi Utility Communication Controller“ oder „MUC“ genannt) erarbeitet.

Am 26.04.2011 führte das BSI einen Workshop durch, bei dem die Gerätehersteller den Autoren des Schutzprofils Fragen stellen konnten. Offen blieb dabei, wie im Falle des Bekanntwerdens einer sicherheitsrelevanten Schwachstelle in zertifizierten Geräten vorzugehen ist. Denn bei einem MUC verbietet sich das schnelle Ausbringen einer neuen Version, da die bevorstehende Novelle des EnWG voraussichtlich den Betrieb von nicht-zertifizierten Systemen untersagen wird. Der Einsatz einer fehlerbereinigten, aber noch nicht nachzertifizierten Geräteversion würde also gegen geltendes Recht verstoßen. Denkbar wäre eine definierte Notfallstrategie mit einer Ad-hoc-Freigabe durch das BSI.

Während die für Mitte 2011 angekündigte endgültige Version des Schutzprofils inhaltlich wohl nur marginal von der aktuellen Vorversion abweichen dürfte, bleibt diese Nuss bis zur Markteinführung der Geräte noch zu knacken. Da die Hersteller vorher allerdings noch die Zertifizierung durchlaufen müssen, ist damit allerdings kaum vor Mitte 2012 zu rechnen.

Secorvo News

Lizenz zum Entwickeln

Software ohne Schwachstellen schützt Kunden und Anbieter: Vom 24.-27.05.2011 bieten wir mit dem Seminar „Certified Professional for Secure Software Engineering (CPSSE)“ eine praxisorientierte Einführung in die sichere Softwareentwicklung. Mit der sich anschließenden Prüfung können Sie das international anerkannte Qualifikations-Zertifikat zum CPSSE erwerben.

Security News Symposium 2011

Am 31.05.-01.06.2011 ist es wieder soweit – wir laden Sie herzlich ein zum zweiten „Security News Symposium“ in das Tagungszentrum Buhlsche Mühle in Karlsruhe/Ettlingen. Auch in diesem Jahr werden wir aktuelle Security- und Datenschutzfragen aufgreifen, die uns bereits in den SSN beschäftigt haben, und gemeinsam mit Ihnen in Vortrag und Diskussion vertiefen. Zusammen mit weiteren Fachexperten bieten wir Ihnen ein spannendes Programm rund um VoIP, IPv6, Webtracking, Skimming und Online-Banking - und freuen uns auf Ihre Teilnahme!

DuD 2011

Am 05.-06.06.2011 findet die 13. Fachkonferenz „Datenschutz und Datensicherheit“ (DuD 2011) in Berlin unter der fachlichen Leitung der Herausgeber der Fachzeitschrift DuD statt. Das Programm umfasst eine breite Themenpalette: von der Datenschutzaufsicht über aktuelle Entwicklungen im EU-Datenschutzrecht hin zu aktuellen Datenschutzfragen des Cloud Computing, Smart Metering, Sozialer Netzwerke, forensischer Analysen und der Videoüberwachung – einschließlich einer Führung durch die Datenschutz-Ausstellung von Toll Collect.

College-Seminare

Eine sehr praxis- und anwendungsorientierte Einführung in die Computer-Forensik bieten wir vom 28.-30.06.2011 mit dem Seminar „Forensik – Verfahren, Tools, Praxiserfahrung“.

Die nächste Gelegenheit zur T.I.S.P.-Zertifizierung (TeleTrusT Information Security Professional) bietet Secorvo College vom 06.-11.06.2011.

Veranstaltungshinweise

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

Mai 2011	
10.-12.05.	12. Deutscher IT-Sicherheitskongress (BSI, Bonn)
12.-15.05.	Swiss Cyber Storm 3 Security Conference (Compass Security AG, Rapperswil/CH)
17.-20.05.	12. Datenschutzkongress (Euroforum, Berlin)
24.-27.05.	Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
31.05.-01.06.	2. Security News Symposium (Secorvo, Karlsruhe/Ettlingen)
Juni 2011	
06.-07.06.	DuD 2011 (Computas, Berlin)
06.-11.06.	T.I.S.P.-Schulung und -Prüfung (Secorvo College)
06.-11.06.	OWASP Global AppSec Europe (OWASP Foundation, Dublin/IE)
28.-30.06.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
Juli 2011	
14.07.	3. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum und KA-IT-Si, Karlsruhe)

Fundsache

Satire findet sich bisweilen an Stellen, wo man sie am wenigsten erwartet. So z. B. in Bugzilla, dem Bug-Tracking-System von Firefox & Co. Ähnlichkeiten des dort am 06.04.2011 eingereichten Antrags auf Aufnahme einer weiteren Root-CA mit den Geschäftsmodellen real existierender Trustcenter sind bestimmt rein zufällig.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

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