secorvo
security consulting

Secorvo Security News

Oktober 2012

Grenzen der Kooperation

Im Februar 2004 wurde Facebook als Studentennetzwerk gegründet. Vier Jahre danach war Facebook bereits international, auch auf deutsch, verfügbar, und die Gründung von Facebook Ireland Ltd. wurde angekündigt. Weitere vier Jahre später ist Facebook die unumstrittene Nummer Eins der sozialen Netzwerke mit geschätzt einer Milliarde Mitglieder. Eine rasante Entwicklung.

Seit 2010 rücken jedoch vermehrt Datenschutzprobleme in den Fokus. Die Hamburgische und die Schleswig-Holsteinische Datenschutzaufsicht sind gegen Facebook bzw. Fanpage-Betreiber vorgegangen. Eine österreichische Studentengruppe hat eine Reihe von Beschwerdeverfahren bei der irischen Datenschutzaufsichtsbehörde DPC angestoßen. Sogar die US-amerikanische Federal Trade Commission (FTC), zuständig für das Safe Harbor-Abkommen, ist eingeschritten und hat jährliche Audits vereinbart. Hinzu kommen diverse Datenschutzpannen.

Dabei überwiegt ein kooperativer Ansatz, um dem neuen Phänomen „Soziale Netzwerke" Rechnung zu tragen. Ein solcher gestalterischer Ansatz hat den Vorteil, unter Nutzung gesetzlicher Auslegungsspielräume passende Regeln zu entwickeln, die das Geschäftsmodell nicht zerstören, aber Gemeinwohlinteressen durchsetzen.

Kooperation darf aber nicht zur Anbiederung werden, bei der staatliche Autoritäten sich lächerlich machen und ihre Autorität verlieren. Das Gutachten der DPC zu Facebook vollbringt dies jedoch schon im Vorwort: Facebook habe zur vollsten Zufriedenheit kooperiert, dabei Empfehlungen und Best Practices akzeptiert. Ein genauerer Blick zeigt, dass facebook vielen Empfehlungen gar nicht oder nur ungenügend nachgekommen ist. Hinweise auf die vorliegenden Rechtsverstöße fehlen völlig, Sanktionsandrohungen finden sich nicht.

Um Grenzen zu setzen, muss auch Kooperation Grenzen haben.

Inhalt

secorvo
security consulting

Security News

Unselbständig

Fast zwei Jahre nach Verabschiedung des unter Federführung des Bitkom entwickelten Datenschutzkodex für Geodatendienste am 01.12.2010 hat der Verein Selbstregulierung Informationswirtschaft e.V. Ende September die nach Abschnitt 6 des Kodex zu errichtende Website der zentralen Informations- und Widerspruchstelle vorgestellt. Sie bietet eine Suchmöglichkeit nach Geodaten anhand der Postanschrift und verweist auf die Widerspruchsverfahren der Anbieter (im Wesentlichen Google Streetview). Die gemeinsame telefonische Beratungsstelle (6.2) sucht man ebenso wie den Beschwerdeausschuss (8.2) und das Gremium zur Selbstkontrolle (7.2) vergeblich; dafür findet sich ein Einheits-Widerspruchformular.

Der Kodex selbst blieb bereits bezüglich der eingeräumten Betroffenenrechte hinter geltendem Datenschutzrecht zurück (Widerspruch erst nach Veröffentlichung). Und nennenswerte Bedeutung wird ihm offenbar seitens der Unterzeichner auch nicht eingeräumt – in den deutschsprachigen Datenschutzangaben zu Google Streetview wird er nicht einmal erwähnt.

Deutlicher als mit solcherlei Selbstregulierung kann man kaum nach einer Verschärfung des Datenschutzrechts rufen.

Ungebrochen

Am 02.10.2012 verkündete das NIST nach fünf Jahren den Gewinner des Wettbewerbs um den Hash-Standard SHA-3. Es ist der „Keccak"-Algorithmus, der sich vor allem durch zwei Eigenschaften gegenüber dem SHA-2 auszeichnet: Er beruht auf einem anderen Grundprinzip als die Familie der MD-Hashes bis einschließlich SHA-2, was zur Hoffnung berechtigt, dass sich mögliche künftige Angriffe auf SHA-2 nicht so einfach auf SHA-3 übertragen lassen. Und er lässt sich besonders effizient in Hardware realisieren – kaum verwunderlich, da die vier Keccak-Autoren, unter ihnen einer der Sieger des AES-Auswahlwettbewerbs, bei Halbleiterherstellern arbeiten, die beide Security-Chips im Portfolio haben.

Anders als beim AES ersetzt SHA-3 den Vorläufer nicht, sondern wird vom NIST als Ergänzung betrachtet, die für manche Einsatzfelder Vorteile bieten kann – und als Rückversicherung, falls SHA-2 eines Tages gebrochen werden sollte. Anwender des SHA-1 sollten nicht warten, bis SHA-3 in Produkten verfügbar ist: Der Sicherheitsgewinn durch den Wechsel zum SHA-2 (SSN 09/2002) ist deutlich größer als von SHA-2 zu SHA-3.

Unzufrieden

Auf Grundlage einer Rechtsprüfung der französischen Datenschutzaufsichtsbehörde (CNIL) hat die Art. 29 Gruppe (europäische Datenschutzaufsicht) Google am 16.10.2012 in einem offenen Schreiben zur Überarbeitung der Datenschutzerklärung und Nutzungsbedingungen vom 01.03.2012 aufgefordert. Im Anhang bescheinigen die Aufseher Google, dass die geltenden Richtlinien jegliche Begrenzung des Verarbeitungszwecks und des Gebrauchs personenbezogener Daten vermissen lassen.

Hauptkritikpunkte sind die mangelnde Transparenz Googles bezüglich der verarbeiteten Daten, die Verarbeitung und Zusammenführung von personenbezogenen Daten über Dienstgrenzen hinweg ohne Rechtsgrundlage oder Einwilligung, das Fehlen jeglicher Löschfristen und der Vorbehalt einer jederzeitigen Änderung der Richtlinien. Es folgen Empfehlungen zur besseren Gestaltung der Datenschutzrichtlinien, zur Einführung vereinfachter Opt-Out Mechanismen und zum Einholen von Einwilligungen in nicht offen ersichtliche Verarbeitungen. Die in Deutschland 2011 vereinbarten Regelungen zu Google Analytics (Ausschluss der dienstüberschreitenden Verwendung, Abschluss eines Auftragsdatenverarbeitungsvertrages und Anonymisierung der IP-Adressen) werden zur Nachahmung empfohlen – etwas voreilig vielleicht, tragen sie doch wenig zu mehr Transparenz der Verarbeitung bei. Sie stehen zudem unter dem Vorbehalt der Umsetzung der EU-Cookie-Richtlinie von 2009.

Unverändert

Das CA/Browser-Forum ist eine informelle Organisation von fünf Browser-Herstellern und ca. 30 kommerziellen CA-Betreibern, die u. a. das Prozedere festlegt, wie Root-Zertifikate in den Browsern vorinstalliert werden. Als eine Konsequenz aus den Trustcenter-Einbrüchen des vergangenen Jahres (SSN 09/2011) wurde diskutiert, das Forum zu reformieren und für interessierte Anwenderkreise zu öffnen, die darauf angewiesen sind, dass Vertrauensanker tatsächlich vertrauenswürdig sind. Wie am 05.10.2012 bekannt wurde, stimmten die Mitglieder jedoch für einen geschlossenen Club.

Die Browser-Hersteller haben die künftige Entwicklung ohnehin in der Hand: Im August 2012 trat der DANE/TLSA-RFC in Kraft, nach dem Serverbetreiber eigene SSL/TLS-Zertfikate im DNS publizieren und Clients sie per DNSSEC validieren können. Sobald die Browser- oder Plugin-Entwickler diese Alternative alltagstauglich umsetzen, dürften öffentliche Root-CAs an Stellenwert einbüßen.

Ungeeignet

Am 19.09.2012 beschloss die Bundesregierung einen Gesetzesentwurf zur Förderung der elektronischen Verwaltung, mit dem auf Bundesebene Hindernisse bei der Einführung elektronischer Verwaltungsverfahren beseitigt werden sollen. Neben der qualifizierten elektronischen Signatur sind nun auch De-Mail und elektronische Formulare unter Verwendung der eID-Funktion des Personalausweises als Ersatz für die Schriftform vorgesehen. Bundesbehörden werden verpflichtet, hierfür den Zugang zu eröffnen, und das De-Mail-Gesetz wird um die Möglichkeit ergänzt, über den Verzeichnisdienst die Zugangseröffnung gegenüber der Verwaltung zu erklären. Bundesbehörden sollen zudem zur elektronischen Aktenführung übergehen und Papierdokumente – wenn sie aus rechtlichen Gründen nicht weiter benötigt werden – entsorgen (sic!).

Es darf bezweifelt werden, dass dem E-Government auf diesem Weg messbare Impulse gegeben werden: fast jede Regelung des Gesetzes liefert den adressierten Behörden eine Ausnahme von der Umsetzungspflicht, die ergänzten Verfahren sind (wie die qualifizierte elektronische Signatur) wenig verbreitet, und ein Großteil der Regelungen hinkt bereits praktizierten Verfahren um Jahre hinterher. Da wirkt die Berechnung der Ersparnisse wie blanker Zweckoptimismus: In 82 Millionen Fällen pro Jahr soll die Bearbeitungszeit je Bürger um acht Minuten sinken – 10 Stunden in 75 Lebensjahren.

Unverzichtbar

Seit dem 02.10.2012 ist das automatisierte Sichtungs-Tool Forensic Scanner verfügbar. Es ist mit 44 Plugins für die Bereiche „System“ und „User“ vorkonfiguriert. Besonders bei Erstuntersuchungen von Windows-Domaincontrollern oder Terminalservern spielt dieses Werkzeug seine Stärken aus, da es sowohl einzelne als auch Gruppen von Benutzerkonten analysieren kann und die Ergebnisse in ASCII-Dateien ausgibt.

Die am 26.09.2012 stark erweiterten und überarbeiteten 243 Plugins des „großen Bruders“ RegRipper detaillieren die Bereiche „System“ (49) und „User“ (106) deutlich weiter, so dass die mit dem Forensic Scanner gelieferten Anhaltspunkte vertieft untersucht werden können. Doch Vorsicht – der korrekte Sicherheitskontext (psexec –s cmd.exe), in dem der Forensic Scanner zur Ausführung gebracht wird, entscheidet darüber, ob er auf die zu untersuchenden Daten zugreifen kann. (Das lässt sich einfach prüfen, indem man mit beiden Werkzeugen dasselbe Windows-Benutzerprofil analysiert und die Ergebnisse für identische Plugins vergleicht.)

Unumgänglich

Am 10.10.2012 ist auf THC die Version 2.0 des THC-IPv6-Toolkits veröffentlicht worden. Es enthält zahlreiche Tools, mit denen inhärente Schwachstellen von IPv6 demonstriert werden können, vor denen eine Personal Firewall für IPv4 nicht schützt. Für Administratoren ist es zugleich ein guter Werkzeugkasten, um die eigenen Netzwerke auf IPv6 zu untersuchen oder sie zu auditieren.

Das Toolkit belegt, dass die Hacker-Community ihre IPv6-Hausaufgaben gemacht hat: Zur Ausnutzung der inhärenten Schwachstellen von IPv6 stehen bereits alle Werkzeuge zur Verfügung. Zwar wird IPv6 nicht in einem „magischen Moment“ IPv4 ablösen. Dennoch: Selbst wenn die IPv6-Einführung im eigenen Netz noch nicht auf der Tagesordnung steht, wird es für Betreiber und Administratoren Zeit, sich mit IPv6 auseinanderzusetzen, um Angreifern im Verlauf einer Umstellung nicht blindlings ins Messer zu laufen – zumal in der Standard-Konfiguration von Windows IPv6 bereits aktiviert ist.

Secorvo News

… zum Dritten

Die dritte und letzte Gelegenheit für IT-Sicherheitsexperten, ihre Kenntnisse in diesem Jahr mit dem T.I.S.P.-Zertifikat zu krönen, bieten wir am **12.–16.11.** Allen Teilnehmern wird vor Seminarbeginn das von Secorvo verfasste 500seitige Begleitbuch zum T.I.S.P. (Zentrale Bausteine der IT-Sicherheit) zur Vorbereitung zugesandt.

Heute schon gefacebookt?

In vielen Unternehmen drängen Marketing- und Personalabteilung auf eine Unternehmenspräsenz bei Facebook & Co, und meist ist ein erheblicher Teil der Mitarbeiter bereits „drin". In den zum großen Teil von amerikanischen Anbietern betriebenen Social Networks lauern jedoch zahlreiche Fallen, wie Copyrightverletzungen, unkontrollierte Informationspreisgabe und Verstöße gegen Datenschutzbestimmungen.

Zu diesen Fragen gibt der Jurist Michael Knopp am **08.11.2012** beim letzten KA-IT-Si-Event dieses Jahres einen Überblick und praktische Tipps. Für ein besonderes Ambiente ist gesorgt: Erstmals ist die KA-IT-Si mit ihrer Veranstaltungsreihe in den stilvollen Räumlichkeiten der Buhlschen Mühle in Ettlingen zu Gast (Anfahrt; ca. 10-15 Minuten S-Bahn-Fahrt vom Karlsruher Hauptbahnhof). Beginn der Veranstaltung ist um 18 Uhr. Um Anmeldung wird gebeten. Wir freuen uns auf spannende Diskussionen und ein interessantes Networking!

Veranstaltungshinweise

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

Oktober 2012	
31.10.-03.11.	hashdays security & risk conference 2012 (DEFCON Switzerland, Luzern/CH)
November 2012	
05.-06.11.	TISP Community Meeting (TeleTrusT, Köln)
07.11.	German OWASP Day 2012 (OWASP Germany, München)
08.11.	Heute schon gefacebookt? (KA-IT-Si, Ettlingen)
09.11.	Zur Rolle des CISO/IT-Sicherheitsbeauftragten (GI-FG SECMGT, Frankfurt)
12.-17.11.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
22.-23.11.	36. DAFTA (GDD, Köln)
27.-30.11.	DeepSec 2012 (DeepSec, Wien)
Dezember 2012	
03.-04.12.	IsSec/ZertiFa 2012 (Computas, Berlin)

Fundsache

Am 30.07.2012 hat der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) die Ergebnisse einer Befragung von 1.000 Internet-Nutzern ab 14 Jahren und 800 IT-Leitern, CIOs, Datenschutzbeauftragten und Geschäftsführern zu Datenschutz und Informationssicherheit veröffentlicht. Die 30seitige Studie gibt nicht nur Einblick in Organisation, Kosten und Technik der Informationssicherheit in deutschen Unternehmen, sondern zeigt auch den großen Anteil von Internet-Nutzern, die aufgrund von Sicherheitsbedenken die Inanspruchnahme von Online-Diensten verweigern.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Knobloch, Michael Knopp (Editorial), 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