secorvo
security consulting

Secorvo Security News

Februar 2015

Why privacy matters.

Der Amerikaner *Glenn Greenwald*, Jurist, Blogger und seit Juni 2012 Journalist der britischen Tageszeitung The Guardian, bekam als einer der ersten Edward Snowdens Materialien zu Gesicht.

Snowden hatte ihn mit Bedacht gewählt: 2009 war Greenwald mit dem Izzy Award for Independent Journalism ausgezeichnet worden, 2010 erhielt er den Online Journalism Award for Best Commentary für seinen damaligen Blog Salon.com.

Anfang 2014 initiierte er mit finanzieller Unterstützung des Ebay-Gründers *Pierre Omidyar* das Portal „The Intercept", dessen Ziel es ist, „*auf Pressefreiheit zu bestehen und sie gegenüber denjenigen zu verteidigen, die diese verletzen.*"

Am 07.10.2014 hielt Glenn Greenwald eine Rede auf der Konferenz TEDGlobal 2014 in Rio de Janeiro. Sein Titel: „Why privacy matters".

Es ist eine brilliante Rede: Ein Muss für jeden, der meint, Datenschutz sei wohl eher etwas für diejenigen, die etwas zu verbergen haben. Und für alle anderen ebenfalls. Zum Nachlesen existiert eine deutsche Übersetzung.

Es ist eine Rede, bei der sich jeder weitere Kommentar erübrigt.

Inhalt

secorvo
security consulting

Security News

ISO-Norm für Datenschutz

Am 30.07.2014 wurde die ISO/IEC 27018 als neuer internationaler Standard für den Datenschutz in der Cloud veröffentlicht. Der Standard orientiert sich im Wesentlichen an den Schutz- und Überwachungspflichten des europäischen Datenschutzrechts. Wie das Bundesdatenschutzgesetz fordert er die sorgfältige Auswahl des Dienstleisters. Auch Anforderungen an die Auftragsdatenverarbeitung aus § 11 BDSG sind bereits enthalten; beispielsweise dürfen personenbezogene Daten ausschließlich nach den Vorgaben des Kunden verarbeitet werden und es muss transparent sein, in welchen Ländern die Verarbeitung erfolgt.

Am 16.02.2015 ging Microsoft in die Offensive und gab bekannt, dass das British Standards Institute (BSI) die ISO-27018-Konformität der Cloud-Services Azure, Office 365 und Dynamics CRM Online bestätigt hat. Die Beauftragung eines nach ISO/IEC 27018 zertifizierten Dienstleisters bestätigt – unabhängig von der unklaren Perspektive der EU-Datenschutz-Grundverordnung – zumindest die unternehmerische Sorgfalt bei der Auswahl.

Libellen im Kraftwerk

Schon seit 2013 sind Industrieanlagen der Pharmabranche Ziel der Malware Dragonfly, Warnmeldungen gibt es jedoch erst seit dem vergangenen Jahr. Dragonfly nutzt Spear-Phishing-E-Mails mit viralen Anhängen gefolgt von Malware-Ködern auf Branchen-Webseiten – kombiniert mit infizierten Software-Updates auf Webseiten vertrauter Produkt-Lieferanten wie dem Routerhersteller eWON. In einem Whitepaper vom 09.12.2014 analysiert Joel Langill die Wirksamkeit üblicher Schutzmaßnahmen gegen Dragonfly. Nach bisherigen Erkenntnissen sind Patch-Management, Application-Listing oder VPNs nutzlos. Der Bericht stellt sieben wirksame Techniken vor, die gegen solche Angriffe in der Lieferkette helfen. Zwei der wichtigsten sind:

- Detaillierte Sicherheitsanforderungen an alle Lieferanten, insbesondere bei Fernwartung – Dragonfly attackiert gezielt kleine Dienstleister, die IT-Sicherheit eher ‚pragmatisch' sehen.
- Nutzung von Industrie-Sicherheitsstandards und Isolation durch Netzwerksegmentierung – Dragonfly sucht nach erreichbaren OPC-Servern, die den Datenaustausch zwischen Automatisierungsanwendungen steuern.

Der Angriff zeigt, wie gefährlich es inzwischen ist, „Legacy"-Systeme z. B. im Anlagenbereich von strikten Sicherheitsvorgaben auszunehmen.

Outsourcing und Berufsgeheimnis

Auch Rechtsanwälte, Steuerberater und Ärzte setzen zunehmend Dienstleister ein, um personenbezogene Daten zu verarbeiten. Zu den datenschutzrechtlichen Anforderungen der Auftragsdatenverarbeitung (§ 11 BDSG) kommen hier die strengen Regeln des Berufsgeheimnisses hinzu (§ 203 StGB).

Dennoch finden sich in der Presse regelmäßig Berichte über sensible Daten im Altpapier. Besonders schwer wiegt dies bei Patientendaten wie jüngst in Bayern, wo Röntgenbilder am Straßenrand entdeckt wurden, mit deren Entsorgung ein Krankenhaus einen Dienstleister beauftragt hatte. Die Bayerische Datenschutz-Aufsichtsbehörde äußerte sich am 19.02.2015 unmissverständlich zum Outsourcing im Krankenhaus: Im Regelfall sei das unzulässig. Nach Auffassung der baden-württembergischen Datenschutzaufsicht gibt es nur zwei Lösungen für die Auslagerung der Datenlöschung: Der Dienstleister vernichtet mit einem mobilen Schredder vor Ort oder ein Mitarbeiter des Krankenhauses begleitet den Transport und überwacht die Vernichtung.

Zu beachten ist: Was für Krankenhäuser gilt, müssen auch Rechtsanwälte und Steuerberater beachten. Dienstleister mit der Verarbeitung personenbezogener Daten zu beauftragen ist bei Berufsgeheimnisträgern – wenn überhaupt – nur sehr eingeschränkt zulässig.

Klare Vorgaben für Cookies gefordert

Bereits im Mai 2011 hätte Deutschland die Neufassung der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG („Cookie-Richtlinie") in deutsches Recht umsetzen müssen. Wesentliche Änderung war die Ersetzung der bisherigen Opt-out-Regelung für den Einsatz von Cookies auf Webseiten durch ein Opt-in: „(...) die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, [ist] nur gestattet (...), wenn der betreffende Teilnehmer oder Nutzer (...) seine Einwilligung gegeben hat."

Die Bundesregierung vertritt bisher die Auffassung, dass die Regelungen des § 13 Abs. 1 S. 2 TMG ausreichen. Das sehen die Datenschutz-Aufsichtsbehörden anders: Mit ihrer Entschließung vom 05.02.2015 stellen sie fest, dass Cookies nur mit Einwilligung der Internetnutzer eingesetzt werden dürfen. Im Telemediengesetz sei die Richtlinie nur unzureichend umgesetzt.

Insecure by Default

Schon am 21.09.2014 wurde berichtet, dass Lenovo Notebooks für Endverbraucher ab Werk mit der Adware Superfish ausliefert. Superfish schleust Werbung in verschlüsselte HTTPS-Verbindungen ein und registriert sich dazu ungefragt im Zertifikatsspeicher von Windows als Root-CA. Der private Schlüssel für das Superfish-Zertifikat liegt dabei quasi ungeschützt auf der Festplatte.

Gefährlicher als die störende Werbung durch Superfish ist die Möglichkeit für Angreifer, damit Man-in-the-Middle-Angriffe auf beliebige HTTPS-Verbindungen durchzuführen. Dafür stellen diese sich mit dem Superfish-Schlüssel Zertifikate für beliebige Domänen aus. Inzwischen konnten derartige Angriffe bei mehr als einem Dutzend verschiedener Malware-Typen beobachtet werden.

Lenovo hat inzwischen angekündigt, künftig nur noch erforderliche Programme vorzuinstallieren. Der Vorfall zeigt jedoch, dass einer Betriebssysteminstallation im Auslieferungszustand besser nicht vertraut werden sollte. Darin findet sich oft ab Werk Zusatzsoftware, die im normalen Betrieb nicht benötigt wird und die Angriffsfläche vergrößert. Gelegentlich erkaufen sich sogar Softwarehersteller ihren Platz in der Standardinstallation. Bei der Beschaffung eines neuen Geräts sollte daher immer zuerst eine Neuinstallation des Betriebssystems durchgeführt werden, die nur die betrieblich benötigten Softwarepakete einschließt.

Immer wieder Facebook

Mit Wirkung zum 30.01.2015 hat Facebook erneut seine Datenschutzrichtlinie, seine Cookie-Richtlinie, die Nutzungsbedingungen sowie weitere Hinweise zum Datenschutz geändert. Die Zustimmung des Nutzers soll ohne ausdrückliche Zustimmung per Login erfolgen. Nach Darstellung von Facebook erleichtert die Änderung das Verständnis der Funktionsweise von Facebook und verbessert die Nutzerkontrolle. Neu eingeführt wurden Lokalisierungsdienste, Einkaufsmöglichkeiten direkt aus Facebook heraus, neue Erläuterungen zu Privatsphäreneinstellungen, eine engere Verknüpfung der Facebook-Dienste sowie die Auswertung von App-Nutzungen. Werbetreibende Dritte sollen Informationen zur Individualisierung von Werbung ohne die Möglichkeit zur Identifizierung des Nutzers erhalten.

Eine Studie im Auftrag der belgischen Datenschutzaufsichtsbehörde kommt zu einem anderen Ergebnis: Bereits die Praxis, die Nutzung von Facebook als Einwilligung zu interpretieren, sei ebenso rechtswidrig wie das Fehlen einer effektiven Opt-out-Möglichkeit. Dasselbe gelte für die Zusammenführung der Daten unterschiedlicher Dienste. Facebook dehne durch die Änderungen seine Datenverwendungen ohne Rechtsgrundlage aus. Am 23.02.2015 hat daher der Bundesverband der Verbraucherzentralen ein Unterlassungsverfahren eingeleitet und Facebook abgemahnt.

Oldie but Goldie

Bereits am 03.11.2014 erschien Version 3.1.1 des bewährten Forensik-Werkzeugs Autopsy. Hinzu gekommen ist die lange ersehnte automatoische Identifikation von Dateitypen. Sehr praktisch ist die neue skriptgesteuerte Reporterstellung, die auch für mehrere Festplattenimages übergreifend funktioniert. Dank einer Multi-Thread-Verarbeitung für beliebig viele CPU-Kerne sinkt die Bearbeitungszeit effektiv um die Hälfte. Hilfreichste Neuerung ist die überarbeitete grafische Zeitlinie: Man kann nun ein Analyse-Zeitfenster bis auf Millisekunden festlegen und die Ergebnisse aus allen verfügbaren Metadaten parallel darstellen.

Secorvo News

Ei des Kolumbus oder Kuckucksei?

Kann man das Microsoft-Cloud-Angebot Office 365 Datenschutz konform einsetzen? Welche Hürden sind dabei zu bewältigen? Diese Fragen wird *Christoph Schäfer* auf der kommenden KA-IT-Si Veranstaltung am **19.03.2015** im CyberForum e.V. beantworten. Nach dem Vortrag gibt es Gelegenheit zum „Buffet-Networking". **Anmeldung** unter www.ka-it-si.de (nur noch wenige Plätze!).

Kompetenz, wo sie gebraucht wird

Als Datenschutzbeauftragter in einem großen Unternehmen benötigen Sie Datenschutzkoordinatoren mit solidem Basiswissen im Datenschutz. Unsere zweitägige Schulung „Geprüfter Datenschutzkoordinator im Unternehmen" vom **28. bis 29.04.2015** hilft Ihnen dabei, Ihren Kollegen die erforderlichen Grundkenntnisse zu vermitteln.

Viele Angriffsszenarien gäbe es gar nicht, wenn bei der Code-Entwicklung Schwachstellen systematisch vermieden würden. Wie man etablierte Verfahren der sicheren Softwareentwicklung in den gesamten Software-Lifecycle einbindet, zeigt die Schulung CPSSE – Certified Professional for Secure Software Engineering vom **04. bis 07.05.2015**.

Die nächste Möglichkeit zur T.I.S.P.-Zertifizierung bieten wir vom **09. bis 13.03.2015**.

Alle Termine und Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/college.

Veranstaltungshinweise

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

März 2015	
03.-05.03.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen und Schutzmechanismen (Secorvo, Karlsruhe)
09.-13.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
19.03.	Ei des Kolumbus – oder Kuckucksei? (KA-IT-Si, Karlsruhe)
23.-26.03.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)
April 2015	
14.-15.04.	Datenschutztage 2015 (FFD Forum für Datenschutz, Wiesbaden)
21.-24.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
22.-23.04.	Security Forum 2015 (Hagenberger Kreis, Hagenberg/AT)
23.-24.04.	8. GDD-Fachtagung „Datenschutz International“ (GDD e.V., Berlin)
26.-30.04.	Eurocrypt 2015 (IACR, Sifia/BG)
Mai 2015	
04.-07.05.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
06.-07.05.	16. Datenschutzkongress (EUROFORUM, Berlin)
11.-12.05.	BvD Verbandstag 2015 (BvD e. V., Berlin)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Michael Knopp, Sven Köhler, Christoph Schäfer, 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