Secorvo Security News

Juli 2013

Vertrauen verspielt

Das Konstrukt ist sehr elegant. Lässt ein Unternehmen personenbezogene Daten seiner Kunden oder Mitarbeiter durch einen Dritten verarbeiten – Lettershop, CRM-Anbieter, Rechenzentrum oder IT-Dienstleister – wird dies als „Auftragsdatenverarbeitung“ geregelt: Die Verantwortung für den Schutz und die ausschließlich zweckbezogene Verarbeitung bleibt beim Unternehmen, der Auftragnehmer erhält konkrete vertragliche Weisungen, wie die Verarbeitung zu erfolgen hat, der Auftraggeber überzeugt sich davon, dass diese auch umgesetzt werden - und der Gesetzgeber behandelt die Verarbeitung so, als ob sie im Unternehmen verbleiben würde.

Kommt das nichteuropäische Ausland ins Spiel wird es kompliziert. Denn dort entspricht das Schutzniveau nicht überall dem der EU. Um das Konzept zu retten, wurden Ende des letzten Jahrtausends mit den USA die „Safe Harbor Principles“ vereinbart. Am 26.07.2000 von der EU-Kommission in Kraft gesetzt postulieren sie bei US-Unternehmen, die dieser Selbstverpflichtung beitreten, ein ausreichendes Datenschutzniveau.

Doch die eleganteste Konstruktion hilft nichts, wenn sie mit der Wirklichkeit wenig zu tun hat. Schon im April 2010 meldeten die Datenschutz-Aufsichtsbehörden Zweifel an und verpflichteten deutsche Unternehmen, die die Verarbeitung personenbezogener Daten an amerikanische Unternehmen auslagern, Nachweise für die Einhaltung der Grundsätze einzufordern.

Da die nach deutschem Recht unzulässige Datenweitergabe an Nachrichtendienste nun amtlich ist, haben die Aufsichtsbehörden der EU-Kommission eine Aufkündigung des Abkommens empfohlen (siehe ‚Unsicherer Hafen'). So schmerzlich das insbesondere für internationale Unternehmen sein dürfte: Es ist sehr zu hoffen, dass die EU diesmal Rückgrat zeigt – und die Persönlichkeitsrechte nicht auf demselben Altar opfert, auf dem sie bereits Flugpassagierdaten und Bankdaten (SWIFT) dem Großen Bruder dargebracht hat.

Inhalt

Security News

Recht auf Verschlüsselung

Der BGH hat in einem Beschluss vom 26.02.2013 festgestellt, dass Behörden nicht verlangen können, dass Unternehmen interne Informationen mittels unverschlüsselter E-Mail an sie weitergeben. Die Behörde muss wenigstens alternative Kommunikationswege zulassen. Dabei komme es nicht darauf an, ob die Mitteilung tatsächlich Betriebs- oder Geschäftsgeheimnisse umfasst. Der BGH geht damit über ein Urteil des Brandenburgischen Oberlandesgerichts vom 11.09.2012 hinaus, das noch auf das Vorliegen von Geschäftsgeheimnissen abgestellt hatte.

Auch wenn das Urteil zunächst nur auf Behörden Anwendung findet, die eine ausschließlich elektronische Übermittlung von Informationen fordern, wertet es den Schutz elektronischer Kommunikation deutlich auf und trägt der Tatsache Rechnung, dass unverschlüsselte E-Mails keinen technischen oder organisatorischen Schutz vor unberechtigter Kenntnisnahme genießen.

Datenschutz abmahnfähig

Das OLG Hamburg hat in einem Urteil vom 27.06.2013 der datenschutzrechtlichen Informationspflicht aus § 13 Abs. 1 S. 1 TMG den Status einer das Marktverhalten regelnden Norm zugesprochen. Es widerspricht damit dem von Datenschützern kritisierten Urteil des KG Berlin vom 29.04.2011.

Bei § 13 Abs. 1 TMG handelt es sich um die Pflicht von Telemediendiensteanbietern, vor allem also Betreibern von Websites oder Apps, zu Beginn der Nutzung über Art, Umfang und Zwecke einer Verwendung personenbezogener Daten oder deren Verarbeitung außerhalb der Europäischen Union zu informieren, in der Regel in einer von jeder Seite aus erreichbaren Datenschutzerklärung.

Konsequenz des Urteils ist die Möglichkeit für Mitbewerber, Interessensverbände, Verbraucherschutzverbände sowie die Industrie- und Handelskammern, Unterlassungstäter nach § 8 Abs. 1 UWG wegen einer unlauteren Wettbewerbshandlung nach § 4 Nr. 11 UWG abzumahnen, wie es für Verletzungen der Impressumspflicht schon lange möglich ist.

Die Entscheidung stützt sich hauptsächlich auf die durch das KG Berlin vernachlässigten Erwägungsgründe der europäischen Datenschutzrichtlinie, die auch das Ziel der Wettbewerbergleichstellung als Begründung angeben.

Obgleich eine weitere Abmahnwelle aus überwiegend datenschutzfernen Interessen sicher nicht wünschenswert ist, dürfte das sich abzeichnende Risiko effektiver als das Bußgeld nach § 16 Abs. 2 Nr. 1 TMG zur Durchsetzung der Informationspflicht verhelfen und Bewegung in die hiermit verbundenen Fragen wie die Aufklärung über die Datenverarbeitung beim Einsatz von Webtracking-Tools oder die Datennutzung durch die Betreiber sozialer Netzwerke bringen.

Unsicherer Hafen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte als Konsequenz der umfassenden Kommunikationsüberwachung der NSA am 24.07.2013 von der EU-Kommission die Aussetzung des Safe-Harbor-Abkommens – der Selbstverpflichtung zahlreicher amerikanischer Unternehmen auf das europäische Datenschutzniveau. In der Liste des US-Handelsministeriums finden sich so klangvolle Namen wie Microsoft, Apple, Facebook, Google, Yahoo und AOL – hinreichend bekannt aus einschlägigen Veröffentlichungen zur Prism-Affäre. Ebenso soll die Anerkennung eines angemessenen Datenschutzniveaus auf Grundlage der EU-Standardvertragsklauseln mit Blick auf die USA eingestellt werden.

Die Konferenz sieht die Ausnahmeregelung des Safe Harbor-Abkommens für Maßnahmen zur nationalen Sicherheit oder auf Grundlage entsprechender Gesetze durch die verdachtsunabhängige, flächendeckende Überwachung als überschritten an. Die Vorgaben der Standardvertragsklauseln, die die Zusicherung enthalten, dass die jeweiligen nationalen Gesetze des Staates des Datenempfängers keine Regelungen enthalten, die den Datenschutz gravierend beeinträchtigen (Klausel 5 b), könnten ebenfalls unter den gegenwärtigen Bedingungen in den USA nicht eingehalten werden. Art. 4 des Kommissionsbeschlusses zu den Standardvertragsklauseln erlaubt den Aufsichtsbehörden unter diesen Umständen die Aussetzung.

Sollten sowohl das Safe-Harbor-Abkommen als auch die Standardvertragsklauseln als Möglichkeit zur Sicherung eines angemessenen Datenschutzniveaus wegfallen, würde ein großer Teil der derzeitigen Datenübermittlungen in die USA, bspw. im Rahmen der Cloud-Nutzung oder durch deutsch-amerikanische Unternehmensverbünde rechtswidrig. Betroffen sind von dieser Maßnahme allerdings nicht nur amerikanische Anbieter, sondern auch deutschen Unternehmen, die auf der Grundlage von Safe Harbor personenbezogene Daten übermitteln: sie handeln ordnungswidrig.

NTFS-Analysen

Mit der am 08.07.2013 veröffentlichten graphischen Oberfläche gnea von TZWorks lassen sich forensische Analysen von NTFS-Dateistrukturen sehr effizient durchzuführen. gnea baut auf den Werkzeugen ntfswalker und wisp auf und kann auch Skripte mit spezifischen Einstellungen und Filterparametern für eine vollautomatische Erhebung erzeugen.

Als statische Datenquellen können sowohl DD- und VMware-Images sowie extrahierte $MFT-Dateien genutzt werden. Sogar im laufenden Betrieb kann auf NTFS-Laufwerke zugegriffen werden – wichtig vor allem für die *in vivo*-Analyse von Servern.

Besonders empfiehlt sich gnea für die Hashwertprüfung von Dateiobjekten in NTFS-Dateisystemen, da ntfswalker die MD5- und SHA1-Hashwerte direkt und ohne Nutzung einer Windows-API errechnet – ein unschätzbarer Vorteil, wenn Schadsoftware im Spiel ist und nichts so ist wie es scheint.

Secorvo News

Anti-Prism-Party

Nach dem ungeplanten *Coming out* der US-Geheimdienste starren viele Nutzer wie das Kaninchen auf die Schlange. Dabei gibt es – wie Sie wissen – zahlreiche Schutzmaßnahmen, die ausländischen Nachrichtendiensten das Datensammeln wenigstens erschweren.

Um dieses Wissen allen zugänglich zu machen, die sich angesichts der aktuellen Nachrichten um den Schutz ihrer Daten sorgen, veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem Cyberforum und dem IT-Sicherheits-Kompetenzzentrum KASTEL am **05.09.2013** im Karlsruher Zentrum für Medientechnologie (ZKM) eine öffentliche Anti-Prism-Party. Zahlreiche Sicherheitsexperten werden erläutern, wie sich E-Mails und Festplatten verschlüsseln, Surfspuren vermeiden sowie Online-Banking und Filesharing sichern lassen. Schicken Sie Verwandte, Freunde und Bekannte! Beginn ist um 18 Uhr, der Eintritt ist frei. Für gute Stimmung sorgen die Curbside Prophets, bekannt von ihren Auftritten 2012 und 2013 auf Das Fest.

Informationen rund um die Anti-Prism-Party gibt es in den kommenden Wochen in einem wöchentlichen Newsletter und auf Twitter.

Expertenwissen

Die Quelle der meisten Sicherheitsschwachstellen findet sich im Entwicklungsprozess. Mit dem Prinzip „Security by Design“ soll das Übel an der Wurzel gepackt werden, um bereits bei der Konzeption und Implementierung von IT-Lösungen Sicherheitsziele wie Verfügbarkeit, Vertraulichkeit, Integrität und Datenschutz in Architektur und Umsetzung zu integrieren.

Wie „Security by Design“ bei der Systementwicklung wirksam umgesetzt werden kann, lernen Sie auf der Zertifikatsschulung "Security Engineering – Sichere Systeme durch Security by Design" vom 23.-26.09.2013, die Sie mit dem Zertifikat T.E.S.S. (TeleTrusT Engineer for Systems Security) abschließen können.

Vom 21.-25.10.2013 können Sie Ihr Expertenwissen und Ihre Berufserfahrung in Informationssicherheit mit der T.I.S.P.-Schulung und einem T.I.S.P.-Zertifikat krönen. Zur Vorbereitung erhalten Sie nach Ihrer Anmeldung das T.I.S.P.-Begleitbuch „Zentrale Bausteine der Informationssicherheit“.

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

Rückblick 5. Tag der IT-Sicherheit

Wer den wieder sehr gut besuchten 5. Tag der IT-Sicherheit bei der IHK Karlsruhe am **04.07.2013** verpasst hat, findet die Presseberichte und alle Vortragsunterlagen (zu den Themen Smartphone-Sicherheit, Cybersicherheit und Grundschutz, Umgang mit Sozialen Netwerken und IT-Security Management Strategie) ab sofort auf http://www.tag-der-it-sicherheit.de.

Wie ich lernte, Malware zu lieben

Seit Jahren nimmt die Verbreitung von Malware zu und täglich kommen neu Arten von Viren, Würmern und Trojanern hinzu. Bedingt durch das immer bessere Sicherheitsbewusstsein der Benutzer und bessere Erkennungsraten von Antivirensoftware ändert Malware ständig die Infektionswege.

Einen Einblick in die Arbeitsweise von moderner Malware gibt Dr. Matthias Schmidt (1&1 Internet AG) mit seinem Vortrag beim KA-IT-Si Event „Dr. Seltsam, oder wie ich lernte, Malware zu lieben“ am **19.09.2013** ab 18 Uhr im Panoramasaal der IHK Karlsruhe. Anhand praktischer Beispiele werden neue Infektionswege aufgezeigt und mobile Malware beleuchtet, die sprunghaft an Zuwachs gewinnt.

Im Anschluss an den Vortrag haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking".
Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

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

August 2013	
01.-04.08.	DEF CON 21 (DEFCON, Las Vegas/US)
04.-07.08.	13th Annual DFRWS Conference 2013 (DFRWS, Monterey/US)
14.-16.08.	22nd USENIX Security Symposium (USENIX, Washington/US)
18.-22.08.	Crypto 2013 (IACR, Santa Barbara/US)
20.-23.08.	OWASP AppSec Europe Research 2013 (OWASP Foundation, Hamburg)
26.08.	Sommerakademie 2013 (ULD Hamburg, Kiel)
September 2013	
02.-06.09.	SecSE2013 (SINTEF, Regensburg)
05.09.	Anti-Prism-Party, (KA-IT-Si, ZKM Karlsruhe)
16.-20.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
17.-18.09.	D A CH Security (GI/OCG/BITKOM/TeleTrusT, Nürnberg)
19.09.	Dr. Seltsam, oder wie ich lernte, Malware zu lieben (KA-IT-Si, IHK Karlsruhe)
23.-26.09.	Security Engineering (Secorvo College, Karlsruhe)

Fundsache

Am 13.03.2013 veröffentlichte der BITKOM den Leitfaden „Sicheres Cloud Computing". Das eine oder andere klang schon im März befremdlich: „... wer Cloud Computing nutze, verliere die Kontrolle über seine Daten. Diese Befürchtungen sind unberechtigt." Angesichts der jüngsten Erkenntnisse ist eine Überarbeitung nun dringend anzuraten...

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, 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