Kundeninformation Februar 2013

Sehr geehrte Damen und Herren,

wir wünschen Ihnen eine spannende Lektüre mit unserer Kundeninformation mit aktuellen Informationen und Entwicklungen im Datenschutz und Datenschutzrecht.

Ihre SaphirIT

Manuel J. Heinemann

Diplom-Kaufmann (FH)
Rechtsanwalt
Fachanwalt für Arbeitsrecht
Datenschutzbeauftragter (TÜV)
Datenschutzauditor (TÜV)
Geschäftsführer

Datenschutzniveau in Neuseeland erfüllt

EU-Kommission gibt grünes Licht für Datenübermittlung nach Neuseeland

Personenbezogene Daten aus den EU-Mitgliedsstaaten dürfen in Drittstaaten nur dann übertragen werden, wenn diese ein vergleichbar hohes Datenschutzniveau garantieren können, wie in den EU-Staaten selbst.
Dies kann aufgrund eines Vertrages oder sogenannter Binding Corporate Rules (BCR), Verwendung durch von der EU-Kommission vorgegebenen Standardvertragsklauseln oder aber durch eine Entscheidung der EU-Kommission, dass das betreffende Land grundsätzlich die Anforderungen an den Datenschutz erfüllt, geschehen.

Neuseeland erfüllt nach Ansicht der EU-Kommission nunmehr die geforderten Voraussetzungen.

Ebenfalls anerkannt ist ein ausreichendes Datenschutzniveau für Andorra, Argentinien, Australien, die Färöer-Inseln, die Isle of Man, Israel, Kanada, Schweiz, Uruguay sowie die Kanalinseln Jersey und Guernsey. Unter der Voraussetzung der Einhaltung des Safe-Harbour-System gilt dies auch für Firmen in den USA.

Praxistipp:

Bevor Sie eine Übermittlung von personenbezogenen Daten in einen Staat außerhalb der EU bzw. des EWR vornehmen, sollten Sie unbedingt überprüfen, ob und unter welchen Voraussetzungen dies zulässig ist.

Dies gilt nicht nur für Datenübermittlung an Fremdfirmen oder Dienstleister, sondern auch bei Übermittlungen an Tochter- oder Muttergesellschaften im Konzern.

EU-Datenschutzgrundverordnung schreitet voran

Änderungsvorschläge werden beraten. Inkrafttreten 2014 möglich.

In den Entwurf der neuen EU-Datenschutzgrundverordnung sind noch zahlreiche Änderungsvorschläge aufgenommen. So sollen beispielsweise IP-Adressen, Standortdaten und andere Online-Identifizierungsmerkmale auch als personenbezogene Daten eingestuft werden. Abschließende Beratungen in den Arbeitsgruppen stehen jedoch noch an.

Die EU-Datenschutzgrundverordnung wird nach ihrer Ratifizierung ohne weitere staatliche Umsetzung für alle Mitgliedsstaaten unmittelbares zwingendes Recht werden.

Neben dem EU-Parlament müssen auch noch die EU-Kommission und der Rat der Mitgliedsstaaten der Reform zustimmen. Frühestens 2014 könnten die neuen Datenschutzregelungen in Kraft treten.

SaphirIT GmbH
Sutthauser Straße 285 www.saphirit.de Oldenburgische Landesbank AG Telefon 0541/60079296
49080 Osnabrück USt.-ID DE 268765300 BLZ 280 200 50 Telefax 0541/60079297
Geschäftsführer Manuel J. Calvo Fernandez Kto.-Nr. 504 282 0000 datenschutz@saphirit.de
Amtsgericht Osnabrück HRB 203854

Ebook-reader Nutzerdaten auf Abwegen

Die „Daten-Sammelwut“ der Anbieter

Die Bürgerrechtsorganisation Electronic Frontier Foundation (EFF) prangert in ihrem “E-Book Buyer’s Guide to Privacy” die Verfehlungen der Ebook-reader-Anbieter an. Die Privacy Policy von Google Books erlaube dem Suchmaschinenspezialisten die Erhebung umfangreicher Nutzungsstatistiken, kritisieren die Datenschützer.

Die Kindle-Reader tracken “Informationen im Zusammenhang mit Inhalten auf Ihrem Device und Ihren Gebrauch” (Geschäftsbedinungen), senden via Wispernet regelmäßig entsprechende Berichte an Amazon. Was für Daten konkret übertragen werden, bleibt unklar – die EFF mutmaßt, Amazon könnte auch Informationen über außerhalb des Kindle Store besorgte Literatur übermitteln.

Die Sammelwut der eBook-Player ist natürlich nicht Selbstzweck, sondern dient allein wirtschaftlichen Interessen. Features wie Amazons “Was kaufen Kunden, nachdem sie diesen Artikel angesehen haben?” erhöhen die Umsätze, stellen für die Kundschaft durchaus auch einen Mehrwert dar. Auch für die Werbewirtschaft ist immer an Nutzungsdaten ihrer Kontakte interessiert – für Werbung in eBooks hält Amazon bereits Patente.

Quelle: www.eff.org/

Warnung vor „Schnüffel-Apps“

Landesdatenschutzbeauftragter empfiehlt App-Guard

Smartphones sind die Standbeine der mobilen Internet-Nutzung. Mit Hilfe von Apps erlangen sie Kenntnis über ihre Besitzer und deren soziales Umfeld. Kontaktdaten, Termine, Kommunikations- und Nutzungsverhalten, Aufenthaltsorte, Konsumgewohnheiten, Interessen und Vorlieben, zu allem speichern Smartphones Daten. Oft ist nicht klar, was die Apps damit anstellen. Eine Reihe von Untersuchungen, u.a. der Stiftung Warentest belegt außerdem, dass diese Daten vielfach ohne Einwilligung der Nutzer weitergegeben werden.

Von Mitarbeitern der Universität Saarbrücken wurde jetzt für Smartphones mit dem Betriebssystem Android ein Programm entwickelt, mit dem Datenzugriffe durch "neugierige" Apps unterbunden werden können. Mit diesem "App Guard" lässt sich verhindern, dass Apps auf Standortdaten, auf Kontakte, das Surf-Verhalten oder auf Kamerafunktionen zugreifen können. Die Applikation kann unter folgender Internet-Adresse bezogen werden:

http://www.backes-srt.de/produkte/srt-appguard/

"Die Nutzer gewinnen mit solchen Datenschutz-Apps einen Teil der Souveränität zurück, die das Internet und seine Dienste ihnen vielfach genommen haben", so der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz, Edgar Wagner. "Das Recht, selbst über die Preisgabe und Verwendung eigener Daten entscheiden zu können, muss auch im Internet gelten und die Nutzer brauchen dafür Steuerungs- und Kontrollmöglichkeiten. Schnüffel-Apps muss man ausbremsen können!"

Quelle: www.datenschutz.rlp.de

Botnetz stiehlt 36 Millionen Euro per mTAN

Banktransaktionen werden gezielt auf fremde Konten umgeleitet

Dazu infizierten Kriminelle PCs und Smartphones der Opfer, um per SMS verschickte TANs abzufangen und selbst zu nutzen. Bei der nächsten Transaktion über den PC schlagen beide Trojaner zu: Die Buchung wird nicht mit dem gewünschten Ziel und der richtigen Summe ausgeführt, sondern für ein Konto der Kriminellen vorbereitet.

Das System des Onlinebankings wird damit also nicht direkt angegriffen, aus Sicht der Bank sind alle Daten in Ordnung. Sie wurden nur von den Trojanern so manipuliert, dass das Geld woanders ankommt. Wie viel der Anwender am PC davon mitbekommt, schreiben die Sicherheitsexperten leider nicht. Denkbar ist aber, dass auch die eigentlich gewünschte Buchung als bestätigt angezeigt wird, da sich die Ausgaben der Bank ohnehin fälschen lassen. Das Login für das Konto kennt der Trojaner zu diesem Zeitpunkt ohnehin schon. Das Verfahren ist schon länger bekannt, im November 2012 warnte beispielsweise die Berliner Polizei vor Missbrauch von mTANs.

Vor allem italienische Konten wurden von den Angriffen betroffen, 20 Prozent der geschädigten Nutzer stammen aber aus Deutschland, weitere Fälle gab es in Spanien und den Niederlanden. Neben der technisch ausgefeilten Attacke setzt das Verfahren des Eurograbber auf die Gutgläubigkeit von Anwendern:

Banken fordern **nicht** zum Download von Software per Mail auf, weder an PCs noch an Smartphones. Wer solchen Hinweisen dennoch folgt, kann nur Glück haben, wenn sein Virenscanner die sich ständig verändernden Trojaner erkennt.

Quelle: www.golem.de