Personenbezogene Daten:

Data Breach Notification

Muss ein Unternehmen bei einem Sicherheitsvorfall seine Kunden von der möglichen Kompromittierung personenbezogener Daten informieren? Neue EU-Richtlinien sollen eine derartige Pflicht zur Data Breach Notification einführen. Das e-center informiert in Kooperation mit output.

Das Konzept der verpflichtenden Information bei Fällen der Verletzung der Vertraulichkeit oder Integrität personenbezogener Daten wurde erstmals 2002 in Kalifornien umgesetzt (California Civil Code §§ 1798.82 und 1798.29). In den folgenden Jahren haben 43 weitere Bundesstaaten der USA Data Breach Notification Laws erlassen.

Im November 2007 hat die Europäische Kommission einen Vorschlag zur Reform des Telekom-Rechtsrahmens erarbeitet, der eine Pflicht zur Data Breach Notification enthielt. Der Vorschlag der Kommission unterscheidet sich in zwei wesentlichen Punkten vom kalifornischen Vorbild. Zum einen sollen nicht alle Unternehmen, sondern nur Telekombetreiber und Internet Access Provider zur Information ihrer Kunden verpflichtet werden. Zum anderen sind nicht nur bestimmte Datenkategorien (z.B. Kreditkartendaten), sondern alle personenbezogenen Daten geschützt. Der europäische Ansatz ist im persönlichen Anwendungsbereich somit enger, im sachlichen jedoch weiter als das kalifornische Vorbild.

Der Vorschlag der Kommission wird derzeit im Europäischen Parlament behandelt. In den zuständigen Ausschüssen wurde bereits eine wesentliche Änderung des Vorschlags beschlossen: Im Fall der Kompromittierung personenbezogener Daten sollen nicht wie bisher vorgesehen die Betroffenen, sondern die nationalen Regulierungsbehörden informiert werden. Es soll dann den Regulierungsbehörden obliegen, die Schwere des Vorfalls zu beurteilen und gegebenenfalls die Information der Betroffenen bzw. der Öffentlichkeit anzuordnen.

Markttransparenz. Diese Abänderung verkennt die eigentliche Funktion der Data Breach Notification. Sie ermöglicht es den Konsumenten durch Information über vergangene Vorfälle Kenntnis über den Grad der Sicherheit eines Dienstes zu erlangen. Bei der Wahl eines bestimmten Dienstes kann so neben dem Preis und der Funktionalität auch der Grad der Sicherheit des Dienstes berücksichtigt werden. Data Breach Notifications sind daher ein wichtiges Mittel um auf dem Bereich der Datensicherheit eine gewisse Markttransparenz zu schaffen.

Risikoverlagerung. Ein weiterer Aspekt der Data Breach Notification ergibt sich aus einer risikobasierten Betrachtung. Derzeit wird das Risiko der Kompromittierung personenbezogener Daten vor allem vom Betroffenen getragen, dem jedoch kaum Möglichkeiten zur Minderung dieses Risikos offen stehen. Der Diensteanbieter, der die Möglichkeit hätte Sicherheitsvorkehrungen zu treffen, ist jedoch nur einem geringen Risiko ausgesetzt, denn wenn der Vorfall nicht bekannt wird, hat er keinen (Image-)Schaden zu tragen. Die Pflicht zur Data Breach Notification verlagert einen Teil des wirtschaftlichen und rechtlichen Risikos in die Sphäre des Diensteanbieters, d.h. in die Sphäre dessen, der in der Lage ist das Risiko tatsächlich zu mindern. Die Pflicht zur Data Breach Notification stellt einen vielversprechenden regulativen Ansatz dar. Der tatsächliche Erfolg wird jedoch von der konkreten Ausgestaltung auf europäischer und nationaler Ebene abhängen. Die Abstimmung im Plenum des Europäischen Parlaments ist für 3. September 2008 angesetzt.

Lukas Feiler

Steckbrief

Name: Lukas Feiler
Position: Vizedirektor des e-center
Organisation: europäisches zentrum für e-commerce und internetrecht
Tel.: (01) 535 46 60
Mail: office@e-center.eu
Web: www.e-center.eu

Who is who?

(e-center

Das »europäische zentrum für e-commerce und internetrecht« ist die größte europäische Plattform für Rechtsfragen der Informations- und Kommunikationstechnologie. Unter der Leitung von Univ.-Prof. Dr. Wolfgang Zankl sorgt es für Rechtssicherheit im E-Commerce und Mobile Business.
Partner des e-center sind: DAS, Deloitte, EMC, Erste Bank, First Data, Gassauer-Fleissner, Hutchison 3g, MBO Media (output), Microsoft, Mobilkom Austria, One, Raiffeisen Informatik, Siemens, Telekom Austria, Tele.ring, T-Mobile, Wolf Theiss. Näheres sowie profunde Rechtsinformation zu E-Commerce und IT-Law unter

WWW.E-CENTER.EU