VON IDG COMPUTERWOCHE VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/schaar-schaerfere-sanktionen-bei-datenpannen,2531198

Telekom, Sony, Lidl

Schaar - Schärfere Sanktionen bei Datenpannen

Datum: 25.01.2013
Autor(en): Johannes Klostermeier

Im Interview mit unserer Schwesterpublikation CIO fordert der Datenschützer von Firmen mehr Sicherheitsausgaben, kritisiert Billig-Gütesiegel und erklärt die Kooperation mit Behörden im Ausland.

CIO.de: **Sie**[1] haben neulich mit der kanadischen Datenschutzbeauftragten ein **Memorandum**[2] für eine verstärkte Zusammenarbeit unterschrieben. Ist das der Auftakt für weitere ähnliche Abkommen gegen globale Firmen wie Google und Co?

Bundesdatenschutzbeauftragter Peter Schaar in seinem Berliner Büro. Seit 2003 ist Schaar im Amt.
Foto: REGIERUNGonline/Denzel

Peter Schaar: Das Abkommen geht auf die Initiative der kanadischen Datenschutzbeauftragten zurück. Nach dem kanadischen Recht ist es für den grenzüberschreitenden Austausch von Informationen notwendig, dass ein entsprechendes Abkommen besteht. Wir haben deshalb ein Cooperation Arrangement verhandelt, das eine enge Kooperation vereinbart. Es gibt vergleichbare Abkommen mit anderen Datenschutzbehörden in und außerhalb Europas.

Dies ist nur ein Element einer verstärkten internationalen **Kooperation**[3]. In Europa haben wir in allen EU-Mitgliedstaaten schon lange ein System der gegenseitigen Zusammenarbeit. Mit Drittstaaten oder etwa auch der US-amerikanischen Aufsichtsbehörde, der Federal Trade Commission (FTC), ist es aufgrund dortiger Geheimhaltungsvorschriften bisweilen schwierig, im Detail Informationen auszutauschen. Wir beabsichtigen daher, auch mit der FTC eine Vereinbarung abschließen. Das 2008 eingerichtete GPEN-Netzwerk (Global Privacy Enforcement Network) soll zusätzlich dafür sorgen, dass Informationen zwischen den Datenschutzbehörden ausgetauscht werden können.

"Weiße Flecken auf der Weltkarte des Datenschutzes"

CIO.de: Firmen arbeiten globalisiert. Es ist schwer datenschutzrechtlich hinterherzukommen. Ist das ein Schritt in die richtige Richtung?

Schaar: Es ist ein Schritt in die richtige Richtung, dass auch Datenschutzbehörden datenschutzrechtlich miteinander kooperieren und dafür sorgen, dass sich Unternehmen den Datenschutzbestimmungen nicht entziehen können, indem sie einfach in andere Länder ausweichen.

Diese Kooperation ist allerdings, auch wenn sie gut funktioniert, nur eine notwendige aber keine hinreichende Bedingung dafür, dass wir einen wirksamen weltweiten Datenschutz haben. Zum einen gibt es noch bedeutende weiße Flecken auf der Weltkarte des Datenschutzes. Zum anderen ist das Datenschutzrecht nicht harmonisiert, es weicht voneinander ab. Etwa in den Fragen, für welche Bereiche es gilt, was personenbezogene Daten eigentlich sind und was man mit den Informationen machen darf. Hier muss man zu einem gemeinsamen Verständnis kommen.

CIO.de: Wird das mittelfristig passieren?

Schaar: Es ist ja in vollem Gang. Auf europäischer Ebene haben wir seit 1995 ein gemeinsames Verständnis durch den laufenden **Reformprozess**[4]. Die Harmonisierung wird weiter voran schreiten. Durch die neue **Verordnung**[5], die die EU-Kommission vorgeschlagen hat, soll sich die Kooperation zwischen den Datenschutzbehörden verbessern.

Auf der anderen Seite gibt es viele Bemühungen, international auf einen gemeinsamen Nenner zu kommen. 2011 ist die FTC erstmals als Vollmitglied in der internationalen Datenschutzkonferenz akzeptiert worden. Auf allen Ebenen wird diskutiert. Ob wir auch eine UN-Konvention zum Datenschutz bekommen, steht allerdings noch nicht fest. Die Vorarbeit hierzu wurde bereits 2009 auf der Internationalen Datenschutzkonferenz in Madrid geleistet.

In den USA fehlt ein generelles Datenschutzgesetz

CIO.de: Wo gibt es noch weiße Flecken auf der Karte des Datenschutzes?

Schaar: Bei großen Unternehmen haben sich verbindliche Unternehmensregelungen, BCRs, bewährt.

Schaar: Das sind zum einen Staaten, die keine Rechtsstaaten sind. Dort ist jegliche Form des Datenschutzes, wie wir ihn verstehen, noch nicht einmal rudimentär gewährleistet, weil es eben keinerlei Rechtsschutz gibt. Selbst wenn ein autoritärer Staat ein Datenschutzgesetz erlässt, bietet das keine Gewähr, dass die Rechte auch wirklich durchgesetzt werden können. Datenschutz setzt rechtsstaatliche Verhältnisse voraus.

Zum anderen gibt es Staaten, die keine Datenschutzgesetze haben oder in denen sich diese nur auf bestimmte Bereiche beschränken. In den USA etwa gibt es nur drei bereichsspezifische Regeln zum Datenschutz - im Bereich des Bankensektors, der Gesundheitsinformationen und des Kinderschutzes. Ein generelles Datenschutzgesetz fehlt. Dafür existiert dort die Vorstellung von „fair information practices". Danach dürfen Unternehmen nicht von dem abweichen, was sie ihren Kunden versprochen haben.

CIO.de: Sind Sie zufrieden damit, wie deutsche CIOs mit den Daten in ihren Unternehmen umgehen?

Schaar: Gerade bei Datenübermittlungen außerhalb Europas sind die CIOs gefordert, ein angemessenes **Schutzniveau**[6] der personenbezogenen Daten in ihrem Unternehmen sicherzustellen. Hier haben sich verbindliche Unternehmensregelungen, sogenannte **Binding Corporate Rules**[7] (BCR), als praktikabel erwiesen.

Auf ihrer Basis ist es möglich, weltweit Informationen etwa über Beschäftigte innerhalb eines Konzerns auszutauschen. Die Unternehmen müssen garantieren, dass die Informationen nach diesen Vorgaben verarbeitet werden und dass es auch Kontrollmechanismen gibt. Die Einzelnen müssen ebenfalls die Möglichkeit haben, das durchzusetzen.

CIO.de: Was machen kleinere Firmen?

Schaar: Da gibt es so genannte Standardverträge, die von der Europäischen Kommission genehmigt worden sind. Bei Anwendung dieser Standardverträge ist man auf der sicheren Seite. Zudem besteht die Möglichkeit individualrechtliche Vereinbarungen zu treffen, um den Datenschutz zu gewährleisten.

CIO.de: Die Stiftung Datenschutz sei eine gute Sache, weil Firmen damit ein Datenschutz-Zertifikat bekommen können, sagte eine Rechtsanwältin im **Interview**[8] mit CIO.de. Sie finden die Stiftung nicht so gut.

"Es darf keine Billig-Gütesiegel geben"

Schaar: Schon seit 2001 steht die Möglichkeit eines Datenschutz-Audits im Bundesdatenschutzgesetz. Allerdings hat die Bundesregierung die notwendigen gesetzlichen Präzisierungen nicht vorgelegt – ein unter dem damaligen Innenminister Wolfgang Schäuble ausgearbeiteter erster Entwurf eines Auditgesetzes war noch stark verbesserungsbedürftig und wurde vom Kabinett nicht beschlossen. Jetzt beabsichtigt die Bundesregierung die Stiftung Datenschutz als Plattform der Audits zu etablieren.

Aber so wie die **Stiftung**[9] aktuell ausgestaltet ist, ist sie eher eine Wirtschaftsstiftung, die sehr stark von dem Geld und dem Einfluss der Wirtschaftsvertreter bestimmt wird. Auf Grund dieser **Konstruktionsfehler**[10] wird die Stiftung Datenschutz den Datenschutz nicht so voran bringen, wie ich es mir gewünscht hätte. Ob es der Stiftung gelingt, die erforderlichen Kriterien für die Auditierung zu erarbeiten und auf dieser Basis Audits zu realisieren, wird sich zeigen. Es darf keine Billig-Gütesiegel geben. Das werde ich kritisch beobachten.

CIO.de: In einer Umfrage von D21 hat die Mehrheit der befragten Bürger das Thema mangelnde Datensicherheit als Haupthinderungsgrund für E-Government angegeben.

Schaar: Auch deswegen brauchen wir ein verbessertes und durchsetzungsfähigeres Datenschutzrecht. Dieses Anliegen teilen auch die Europäische Kommission und das Europäische Parlament mit dem Entwurf einer Datenschutzgrundverordnung. Datenschutz darf aber nicht nur auf dem Papier verbessert werden, sondern muss auch gelebt werden. Die Unternehmen müssen Datenschutz ernster nehmen und dafür gegebenenfalls auch Geld ausgeben. Allerdings ist dieses Geld gut angelegt, denn Datenskandale kosten das Unternehmen unter dem Strich mehr.

CIO.de: Nehmen Firmen Datenschutz nur ernst, wenn es ums Geld geht?

Schaar: Da ist etwas dran. Hier spielen Sie auf die geplante Verschärfung der Sanktionsmöglichkeiten der Datenschutzaufsichtsbehörden an. Der Verordnungsentwurf der Europäischen Kommission sieht Bußgelder von bis zu einer Million Euro oder zwei Prozent des weltweiten Jahresumsatzes vor. Ich unterstütze diese geplante Verschärfung. Zu den Bußgeldern kommen aber auch immense Kosten auf die Unternehmen zu, um ihr ramponiertes Image wieder aufzupolieren.

"Skandalöse Datenschutzlücken beim Online-Reisevermittler Unister"

CIO.de: Da gibt es ja einige aktuelle Beispiele...

Schaar: Der Sony-Fall etwa. In **Deutschland**[11] hatten wir bei der Deutschen Bahn, bei der Deutschen Telekom und bei Lidl schwerwiegende Vorfälle. Oder denken Sie an die kürzlich bekannt gewordenen skandalösen Datenschutzlücken beim Online-Reisevermittler Unister. Da wurde viel Lehrgeld bezahlt. Ich denke, die Unternehmen wären gut beraten, zu handeln, bevor ein Schaden entsteht.

CIO.de: Sie helfen Unternehmen auch, wenn Sie Fragen haben?

Schaar: Ja, die Datenschutzaufsichtsbehörden sind auch beratend tätig. Die **Firmen**[12] stehen aber selbst in der Verantwortung, sich so aufzustellen, dass der **Datenschutz**[13] gewährleistet ist. Eine zentrale Rolle spielt hierbei der betriebliche Datenschutzbeauftragte. Von der Bundesregierung erwarte ich in diesem Punkt, dass sie sich für eine umfassendere Bestellungspflicht und eine bessere Rechtsstellung der Beauftragten in den Unternehmen einsetzt, wenn sie die Brüsseler Gesetzesvorschläge mit den anderen EU-Mitgliedstaaten verhandelt.

CIO.de: Wo steht Deutschland weltweit?

Schaar: Das ist schwer zu sagen. Die meisten Ranking-Versuche sind methodisch eher zweifelhaft. Deutschland hat aber ein sehr hohes Maß an ‚Awareness'. Deutsche Firmen sind weltweit gut aufgestellt, was die Entwicklung von IT-Sicherheits- und Datenschutzsystemen angeht. Man sollte sich darauf aber nicht ausruhen, sondern weiter vorangehen. Bei Smart Meters können deutsche Firmen beispielsweise sichere Lösungen gewährleisten, während viele Firmen, insbesondere aus Fernost, diese Features derzeit nicht anbieten. Das ist auch eine Chance für deutsche Firmen, ihr Know-how weltweit zu vermarkten.

Dieser Artikel basiert auf einem Beitrag der CW-Schwesterpublikation **CIO**[14].

Links im Artikel:

[1] **http://www.bfdi.bund.de/DE/Home/homepage_node.html;jsessionid=FFBD1482167B4A5AEB25C30840C4E10E.1_cid344**
[2] **http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2012/21_DCANDSBehoerdenSchaffenGrundlageZurZusammenarbeit.html**
[3] **https://www.computerwoche.de/a/europaeische-datenschuetzer-legen-sich-gemeinsam-mit-google-an,2525227**
[4] **https://www.computerwoche.de/a/eu-datenschutz-als-vorbild,2522928**
[5] **http://www.bfdi.bund.de/DE/EuropaUndInternationales/EUInt_node.html**
[6] **https://www.cio.de/public-ict/datenschutz/2886484/index2.html**
[7] **http://www.bfdi.bund.de/cln_134/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/5_BCRUebergabeAnDPAG.html?nn=408920**
[8] **https://www.cio.de/public-ict/datenschutz/2888554/index.html**
[9] **https://www.cio.de/public-ict/datenschutz/2888554/index.html**
[10] **http://www.zeit.de/digital/datenschutz/2012-11/stiftung-datenschutz-scheitern**
[11] **https://www.cio.de/public-ict/datenschutz/2271682/index.html**
[12] **https://www.cio.de/knowledgecenter/security/2884665/index.html**
[13] **https://www.cio.de/knowledgecenter/security/**
[14] **https://www.cio.de/public-ict/datenschutz/2904023/index.html**
