Gut gemeint…

Kommentar zu den Änderungen des BDSG

Diplom-Informatikerin Karin Schuler

Nach zahlreichen Datenschutzverletzungen bei großen deutschen Unternehmen im vergangenen Jahr, wurden die Stimmen nach gesetzlichen Konsequenzen immer lauter. Dezember 2008 wurde das Bundesdatenschutzgesetz novelliert – die Kritik daran reißt aber nicht ab.

IT-Fachleute, Revisoren und Wirtschaftsprüfer kennen den Vorgang: Jahrelang hat man auf Missstände hingewiesen und Verbesserungsvorschläge gemacht – ohne Erfolg. „Zu teuer, zu umständlich, nicht durchsetzbar" schallte es einem von den Verantwortlichen entgegen. Schließlich kommt es, wie es kommen musste: der Misstand produziert einen kleinen oder größeren Skandal und plötzlich wimmelt es nur so von Einsichtigen. Hektische Betriebsamkeit wird öffentlich zelebriert und weder Geld noch Aufwand werden gescheut, um den entstandenen Schaden so schnell wie möglich zu begrenzen und für die Zukunft Vergleichbares auszuschließen.

Auch Datenschützer haben seit langem mit diesem Muster zu kämpfen. Die heftigen Datenschutzskandale der letzten Zeit haben im Sommer 2008 sogar das Bundesministerium des Innern (BMI) zu öffentlich demonstrierter Betriebsamkeit gezwungen. Leider weiß man, dass hektische Betriebsamkeit nach Skandalen und großem öffentlichem Druck meist nicht zu den besten, effizientesten und angemessensten Maßnahmen führt. Auch das BMI bildet da keine Ausnahme, wie man den verschiedenen Stadien der Referentenentwürfe und den heißen Diskussionen entnehmen konnte. Selbst nach mehreren Kommentierungs- und Nachbesserungsrunden stellt der Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften vom 10.12.2008 ein wildes Flickwerk dar.

Fast kann man sich schon gar nicht mehr erinnern, dass es einst eine Initiative zur Modernisierung des Datenschutzrechts gab. Der heutige unzumutbare und für Normalbürger völlig unverständliche gesetzliche Flickenteppich sollte in ein modernes Datenschutzrecht aus einem Guss überführt werden. Der Gesetzgeber hat in mehr als einer Legislaturperiode Versprechungen zur Umsetzung gemacht. Geschehen ist bis heute jedoch nichts. Stattdessen werden nun am alten Flickwerk weitere Läppchen angenäht, um die immer größer werdenden dünnen Stellen und Löcher notdürftig zu stopfen.

Flickwerk BDSG

Immerhin sind diese Flicken an der richtigen Stelle angebracht, sie betreffen die am lautesten in der Öffentlichkeit beklagten Kritikpunkte. So wird endlich der Kündigungsschutz des betrieblichen Datenschutzbeauftragten (bDSB) verbessert, um diesen in seiner Weisungsfreiheit und fachlichen Unabhängigkeit zu stärken. Das ist durchaus zu begrüßen, auch wenn nach Meinung vieler Fachleute die jetzt vereinbarten Änderungen in der Stellung des bDSB bei weitem noch nicht ausreichen.Das bisher in den Bereichen Werbung, Adresshandel und Markt- und Meinungsforschung vorherrschende Widerspruchsprinzip (opt out: solange der Betroffene nicht widersprach, durften seine Daten genutzt werden), soll grundsätzlich dem Einwilligungsprinzip weichen (opt in: Daten des Betroffenen dürfen nur nach und mit seiner ausdrücklichen Einwilligung verwendet werden). Die Qualität der endgültigen Regelung wird nur dann akzeptabel sein, wenn der Gesetzgeber sich nicht wieder von den erbosten Adresshandels- und Werbeverbänden vielfältige Ausnahmen vom Grundprinzip abschwatzen lässt. Ein Novum im deutschen Datenschutzrecht stellt das Vorhaben einer Meldepflicht dar. Hierdurch wird bei Datenschutzverstößen die verantwortliche Stelle verpflichtet, Aufsichtsbehörde und Betroffene zu informieren. Diese Pflicht soll auch im Geltungsbereich des Telemediengesetzes und des Telekommunikationsgesetzes Anwendung finden. Vorbilder für diese Regelung finden sich vor allem in US-amerikanischen Staaten. Es gibt allerdings unter Datenschützern einen Dissens darüber, wie wirksam diese Maßnahme die Folgen von Datenschutzverstößen mildern kann.

Die vorgesehene Erhöhung der Bußgelder geht einher mit einer Erweiterung des Bußgeldkatalogs, der nun beispielsweise auch die fehlende, unvollständige oder fehlerhafte Auftragserteilung bei Outsourcing

Karin Schuler ist Diplom-Informatikerin und Beraterin für Datenschutz und IT-Sicherheit. Sie fungiert als anerkannte Sachverständige für IT-Produkte (rechtlich/technisch) beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein und ist Mitglied des Leitungsgremiums der Fachgruppe Privacy Enhancing Technologies (PET) der Gesellschaft für Informatik e. V. (GI). Darüber hinaus ist Frau Schuler stellvertretende Vorsitzende der Deutschen Vereinigung für Datenschutz e.V.

(Auftrags-DV) mit Bußgeld belegt. Die vorgesehenen Bußgeldbeträge werden etwas erhöht – der eigentliche Qualitätsgewinn besteht allerdings in der vorgesehenen Option, diese Beträge weiter zu erhöhen, wenn nur so der durch den Verstoß erlangte Gewinn abgeschöpft werden kann.

Das ebenfalls in der Novellierung untergebrachte Datenschutzauditgesetz wird weniger in der Öffentlichkeit als in der Fachwelt diskutiert. Grundsätzlich ist zu begrüßen, dass das seit Jahren im § 9a des BDSG angelegte Gesetz nun doch endlich noch initiiert wurde. Analysiert man jedoch, was nach Jahren der Fachdiskussion und Erfahrungen mit privaten und öffentlichen Datenschutzaudits in diesen Entwurf eingeflossen ist, kann man nur ernüchtert sein. Der Text trägt mehr als deutlich die Handschrift eines Autors, der weder praktische Erfahrung mit Audits noch Kenntnis über die in den letzten Jahren geführten Fachdiskussionen hat: vermutlich eine der typischen Auswirkungen des eingangs beschriebenen Schnellschusseffekts.

Ungeeigneter Gegenstand

Beispielhaft seien zwei wesentliche Kritikpunkte herausgegriffen: Gegenstand des Audits sollen sowohl Datenschutzkonzepte verantwortlicher Stellen als auch informationstechnische Einrichtungen von Anbietern sein. Damit ist der mögliche Gegenstand eines Audits jedoch inhaltlich nicht annähernd ausreichend definiert. Wegen der Einschränkung auf Datenschutzkonzept und informationstechnische Einrichtungen ließen sich weder Webportale noch Online-Shops auditieren – Anwendungen, deren Datenschutzstandard Verbraucher heutzutage ganz besonders interessiert. Auch mindert die Einschränkung auf das Audit des Datenschutzkonzepts – ohne eine zumindest stichprobenartige Überprüfung der Umsetzung – den Wert des erteilten Zertifikats immens: Papier ist geduldig und das wahre Datenschutzniveau zeigt sich in der betrieblichen Umsetzung.

Insbesondere ist fragwürdig, dass der vorliegende Entwurf vorsieht, das freiwillige Zertifikat bereits für die eigentlich selbstverständliche, bloße Gesetzeseinhaltung zu erteilen. Dies transportiert nicht nur eine falsche Botschaft, sondern stellt auch keinen Wert für Verbraucher dar. Der Gesetzentwurf sieht vor, dass in einem bürokratisch aufwändigen, inhaltlich jedoch wirkungslosen Verfahren eine verantwortliche Stelle das Führen eines Auditsiegels anmelden kann. Eine Überprüfung durch die zuständige Kontrollstelle erfolgt erst nachträglich und richtet sich nicht zuletzt nach deren Arbeitsbelastung und der Einschätzung der Sensibilität der verwendeten Daten. Die Kontrollstelle soll dafür einerseits „angemessen“ von der verantwortlichen Stelle bezahlt werden, hat aber andererseits die Verpflichtung, jede Stelle zu auditieren, die dies wünscht. Gleichzeitig soll sie den Kunden, der sie für diese Leistung bezahlt hat, unabhängig und sachlich korrekt prüfen. Man darf sich fragen, ob es wohl häufig vorkommen wird, dass eine vom Kunden bezahlte Kontrollstelle im Falle unzureichenden Datenschutzniveaus ein Siegel versagt. Das gewählte einstufige Konstrukt, bei dem keine Trennung zwischen Sachverständigen und der auditierenden Stelle besteht, hat nicht zu Unrecht in Fachkreisen den Ruf eines leicht korrumpierbaren und daher letztlich wertlosen Modells.

Anforderungen

Besser wäre es, nach bewährtem Modell und an internationalen Zertifizierungsnormen ausgerichtet, in einem zweistufigen Verfahren eine unabhängige Zertifizierungsstelle auf der Grundlage eines Sachverständigengutachtens über die Zertifikatsvergabe entscheiden zu lassen. Wenn es nicht gelingt, mit einem Auditgesetz der Sache angemessene Rahmenbedingungen zu schaffen, so scheint die Gefahr groß, dass ein resultierendes Zertifikat in der Öffentlichkeit als nicht aussagekräftig wahrgenommen wird. Ein solches Gesetz sollte folgende Vorgaben umsetzen:

- Der Gegenstand des Audits, also das Prüfobjekt, sollte vorrangig die Datenschutzorganisation der datenverarbeitenden Stelle sein.
- Ein Zertifikat (als Bescheinigung eines erfolgreichen Audits) darf nur bei Erreichen eines hohen Datenschutzniveaus erteilt werden. Die alleinige Erfüllung der gesetzlichen Vorgaben ist nicht zertifizierungsfähig.
- Die Durchführung eines Datenschutzaudits ist für die datenverarbeitende Stelle freiwillig.
- Die Zertifizierung einzelner Organisationseinheiten oder Anwendungen der datenverarbeitenden Stelle ist nicht wünschenswert, weil die Aussagekraft

sehr begrenzt ist und die Gefahr besteht, dass das Zertifikat für ein bestimmtes System missbräuchlich für die datenverarbeitende Stelle insgesamt genutzt wird.

- Erteilte Zertifikate müssen ein Mindestmaß an Vergleichbarkeit zulassen, da sie sonst für Verbraucher oder sonstige Interessenten nur von geringem Wert sind.
- Es sollte ein einziges, gleiches Zertifikat für alle Arten von datenverarbeitenden Stellen geben, das eine gute Datenschutzorganisation und ein hohes Datenschutzniveau bescheinigt. Eine Aufteilung von Zertifikaten nach Branchen, Größe der Stelle oder Art der Datenverarbeitung würde eine für den Verbraucher nicht überblickbare Zersplitterung zur Folge haben.
- Bei der Gestaltung eines Datenschutzaudits sollten bisherige systematische und strukturierende Arbeiten (z. B. Rossnagel, Rechtgutachten zum Datenschutzaudit 1999) berücksichtigt werden.
- Sowohl die Durchführung der Zertifizierung als auch die Akkreditierung der Gutachter sollte durch eine Stelle erfolgen, die Erfahrung in der internationalen Normierung von Zertifizierungsprozessen mitbringt, aber nicht selbst am Wettbewerb teilnimmt.
- Begutachtung und Zertifizierung sollen durch voneinander unabhängige Instanzen erfolgen (zweistufiges Modell).

Da ein schludriges und unambitioniertes Gesetz die Idee eines Datenschutzaudits in der Öffentlichkeit dauerhaft diskreditieren wird, erscheint derzeit ein vorläufiger Verzicht auf ein Auditgesetz als die bessere Lösung.

Veranstaltungen

Messen Kongresse

ITSIFA 2009 - IT-Sicherheitsfachtagung
CBT Training & Consulting GmbH
25.03.2009 - 26.03.2009 München
www.cbt-training.de

Fraud Management & Datensicherheit Forum 2009
INFORMA Group
30.03.2009 - 31.03.2009 Frankfurt a. Main
www.iir.de

ediscovery 2009
IQPC
30.03.2009 - 01.04.2009 Zürich
www.iqpc.de

IT-Trends Sicherheit
ruhr networker e.V.
31.03.2009 - 31.03.2009 Bochum
www.networker-nrw.de

CeBIT
Deutsche Messe AG
19.03.2009 - 25.03.2009 Hannover
www.cebit.de

Seminare

Virus/Trojan/Backdoor Security Lab
ITACS Training AG
16.03.2009 - 18.03.2009 Zürich
www.itacs.com

16. DFN Workshop - Sicherheit in vernetzten Systemen
DFN-CERT Services GmbH
17.03.2009 - 18.03.2009 CCH Hamburg
www.dfn-cert.de/

Praxis des betrieblichen Datenschutzbeauftragten
FFD Forum für Datenschutz
18.03.2009 - 19.03.2009 München
www.ffd-seminare.de

E-Discovery
management forum starnberg
18.03.2009 - 18.03.2009 Frankfurt a. Main
www.management-forum-starnberg.de

Dokumentation und Test von Notfall- und Business-Continuity-Plänen
IIR Technology
23.03.2009 - 24.03.2009 Hamburg
www.iir.de

Risikoanalyse in der IT-Sicherheit
Integrata AG
23.03.2009 - 24.03.2009 München
www.integrata.de

ISO 27001: 2005 - Lead Auditor Kurs (IRCA)
qSkills GmbH & Co. KG
23.03.2009 - 27.03.2009 Nürnberg
www.qskills.com

Informationssicherheit als Managementaufgabe
Fraunhofer-Institut für Sicherer Informationstechnologie SIT
25.03.2009 - 26.03.2009 Sankt Augustin
www.sit.fraunhofer.de

Haftungsrisiken für IT-Verantwortliche
Forum für Führungskräfte
26.03.2009 - 26.03.2009 in Mainz
www.fff-online.com

Revision Datenschutzgesetz DSG
Swiss Infosec AG
26.03.2009 - 27.03.2009 Olten
www.infosec.ch

Datenschutzbeauftragter
TÜV Akademie GmbH TÜV Thüringen
30.03.2009 - 04.03.2009 Berlin
www.die-tuev-akademie.de

Datenschutz in medizinischen Einrichtungen
TÜV Rheinland Akademie GmbH
30.03.2009 - 31.03.2009 Berlin-Spandau
www.tuev-akademie.com

Revision des Risikomanagements
Haub + Partner GmbH
31.03.2009 - 01.04.2009 München
www.haub-seminare.de

Forensik - Verfahren, Tools, Praxiserfahrung
Secorvo Security Consulting GmbH
31.03.2009 - 03.04.2009 Karlsruhe
www.secorvo.de/college/

BSI IT-Grundschutz
BSP. SECURITY
01.04.2009 - 03.04.2009 Regensburg
www.bsp-security.de

Awareness Management - Sicherheit braucht System - Sensibilisierung im Unternehmen
CBT Training & Consulting GmbH
01.04.2009 - 01.04.2009 München
www.cbt-training.de

Kryptographie - eine Schlüsseltechnik zur Gestaltung zukünftiger Informationstechnik
CCG Carl-Granz-Gesellschaft e.V.
01.04.2009 - 02.04.2009 Oberpfaffenhofen
www.ccg-ev.de

IT-Notfallplanung
Management Circle AG
01.04.2009 - 02.04.2009 Frankfurt
www.managementcircle.de

Das Datenschutzhandbuch als Dokumentation des betrieblichen Datenschutzbeauftragten
Deutsches Institut für Betriebswirtschaft (dib) GmbH
02.04.2009 - 02.04.2009 Frankfurt a. Main
www.dib.de/

Business Continuity Management 2009
marcusevans
02.04.2009 - 03.04.2009 Bad Homburg
www.marcusevansde.com

Datenschutz Kompakt
GDD - Gesellschaft für Datenschutz und Datensicherung e.V.
06.04.2009 - 07.04.2009 Köln
www.gdd.de

ITC: Einführung in das IT-Recht für IT-Verantwortliche, Mitarbeiter und Berater
PROKODA GmbH
06.04.2009 - 06.04.2009 Berlin
www.prokoda.de