

Marit Hansen

Informationen bei Datenschutzvorfällen: Ja, bitte!

Nach den Datenschutzgesetzen sind Daten verarbeitende Stellen für die von ihnen verarbeiteten personenbezogenen Daten verantwortlich. Ziel der Datenschutzgesetzgebung in Deutschland ist die Gewährleistung des Rechts auf informationelle Selbstbestimmung für jeden Menschen: Jeder soll wissen können, wer was wann über ihn weiß (BVerfG 1983). Dies ist nur möglich, wenn die geforderte Transparenz nicht nur die planmäßige Datenverarbeitung betrifft, sondern auch im Fall von Sicherheitsvorfällen und Datenschutzpannen die Information darüber umfasst, welche der eigenen Daten in unberechtigte Hände gelangt sind.

So forderte im November 2008 die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, „alle verantwortlichen Stellen – grundsätzlich auch alle öffentlichen Stellen – gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen.“ (DSB-Konferenz 2008).

Dass eine solche Informationspflicht nicht unrealistisch ist, zeigen die Erfahrungen aus den USA, wo sog. „Security Breach Notification Laws“ in der Mehrheit der Staaten gelten, die die Unternehmen verpflichten, bei Datenschutzpannen die Betroffenen – oder falls dies nicht möglich ist, die Öffentlichkeit – zeitnah zu informieren. Dabei wirkt diese Verpflichtung nicht nur im nachgelagerten Bereich, sondern sie motiviert Unternehmen dazu, durch Datensparsamkeit sowie techni-

sche und organisatorische Maßnahmen Datenschutzpannen bereits im Vorfeld zu verhindern (Schneier 2009). Um im Fall einer Datenschutzpanne sowie der verpflichtenden Benachrichtigung den Vertrauensverlust bei den Kunden zu minimieren, werden in zahlreichen Unternehmen präventiv Notfallpläne erarbeitet. Statistiken aus den USA zeigen übrigens, dass mehr Kunden abwandern, wenn ein Datenskandal ungesteuert durch die Medien veröffentlicht wird (Hanloser 2009).

Auch für Deutschland, wo im Entwurf zur Novelle des Bundesdatenschutzgesetzes ebenso wie bei der Umsetzung der EU-Vorgabe im Medienrecht Informationspflichten bei Datenschutzpannen vorgesehen sind, wird eine solche bußgeldbewehrte Verpflichtung Wirkung in vermutlich zwei Richtungen entfalten: Erstens werden Unternehmen stärker versuchen, gar nicht erst Datenschutzpannen entstehen zu lassen – in vielen der jüngsten Datenskandale waren die Datensicherheitsmaßnahmen mangelhaft gewesen. Und zweitens wird weniger vertuscht werden, weil dies ein erhebliches Bußgeld nach sich ziehen kann – hier sind die Aufsichtsbehörden gefragt.

Die für Deutschland diskutierten Mitteilungs- und Benachrichtigungspflichten sollen zunächst auf besonders sensible Daten, z.B. im Bereich Medizin oder bei Bank- und Kreditkarteninformationen, beschränkt werden, da man bei einer Ausdehnung auf weniger sensible Fälle einen kontraproduktiven Abstumpfungseffekt bei den Betroffenen fürchtet. Wichtig ist bei dem Umfang der Benachrichtigung von Betroffenen, dass sie nach Möglichkeit abschätzen können sollen, von wem welche rechtswidrige Nutzung ihrer Daten droht und ob gegenwärtig eine konkrete Gefahr besteht (Hanloser 2009). Ebenso sollen den Betroffenen

konkrete Handlungsempfehlungen zur Schadensminimierung gegeben werden.

Ähnliche Überlegungen stammen auch aus der Arbeit in den EU-Projekten „PRIME – Privacy and Identity Management for Europe“¹ (2004-2008) und PrimeLife² (2008-2011), in denen Konzepte und Prototypen für ein nutzergesteuertes Identitätsmanagement entwickelt wurden und werden:

Herzstück des PRIME-Identitätsmanagementsystems ist nutzerseitig der sogenannte „Data Track“, in dem mitgespeichert wird, welche Transaktionen der Nutzer abgewickelt hat, bei denen seine personenbezogenen Daten eine Rolle spielten. Der „Data Track“ gibt also Anhaltspunkte darüber, was der Transaktionspartner über einen weiß. Diese Grundfunktionalität wurde nicht nur um einen Abgleich mit den serverseitigen Datenschutz-Policies und erste Ansätze zur automatisierten Rechtswahrnehmung erweitert, sondern es wurde auch ein „Security Feed“ integriert, mit dem sich Sicherheitsvorfälle melden und an den Nutzer kommunizieren ließen (Nageler 2006, Hansen et al. 2007), siehe Abb. 1.

In der Praxis könnte es diverse Newsfeeds mit Informationen zu Datenschutzpannen und Sicherheitsrisiken geben, die in einem standardisierten Format Meldungen an diejenigen Nutzer weiterleiten würden, die den jeweiligen Newsfeed abonniert hätten. Verfasser dieser Meldungen könnten beispielsweise die verantwortlichen Daten verarbeitenden Stellen, Computer Emergency Response Teams, Online-Redaktionen oder beliebige Organisationen oder Einzelpersonen sein, die mit einer digitalen Signatur die Authentizität der Meldungen bestätigten würden. Das Identitätsmanagementsystem des

1 <http://www.prime-project.eu/>

2 <http://www.primelife.eu/>

Nutzers würde dann die abonnierten Newsfeeds auslesen und lokal aus den Meldungen diejenigen ausfiltern, die für den Nutzer bedeutsam sind, z.B. weil sie Transaktionspartner des Nutzers oder von ihm eingesetzte Technik betreffen. Bei dem im Projekt entwickelten XML-Format wurde u.a. berücksichtigt, zu welchem Zeitpunkt ein Vorfall bemerkt wurde und ab welchem früheren Zeitpunkt das Problem vermutlich schon Bestand hatte. Außerdem war ein Feld vorgesehen, um den Nutzer darüber zu informieren, welche Aktivitäten er entfalten könnte, um das Risiko für seinen Datenschutz zu minimieren: Im Kontodatenskandal 2008 hätte man z.B. auf die Möglichkeit des Wechsels der Kontonummer oder auf das regelmäßige Kontrollieren der Kontoauszüge hinweisen können; bei einem Datenleck, das pseudonyme Profile betrifft, wäre ein möglicher Ratschlag, nicht mehr das entsprechende Pseudonym zu verwenden.

Wichtig ist eine für den Betroffenen verständliche Art der Information. Identitätsmanagementsysteme können ihn bei der Interpretation der Benachrichtigungen ebenso unterstützen wie Datenschutzbehörden, Verbraucherschützer oder andere Organisationen seines Vertrauens.

Fazit:

Eine Informationspflicht bei Datenschutzpannen ist notwendig, damit Bürgerinnen und Bürger ihr Recht auf informationelle Selbstbestimmung ausüben können. Voraussichtlich wird daneben der Grad der Datensicherheit in Unternehmen steigen. Insgesamt wird sich daraus eine Kultur für mehr Datenschutzbewusstsein und einen faireren Umgang mit Daten entwickeln.

Literatur

BVerfG 1983
Bundesverfassungsgericht: Urteil vom 15. Dezember 1983, BVerfGE 65, 1

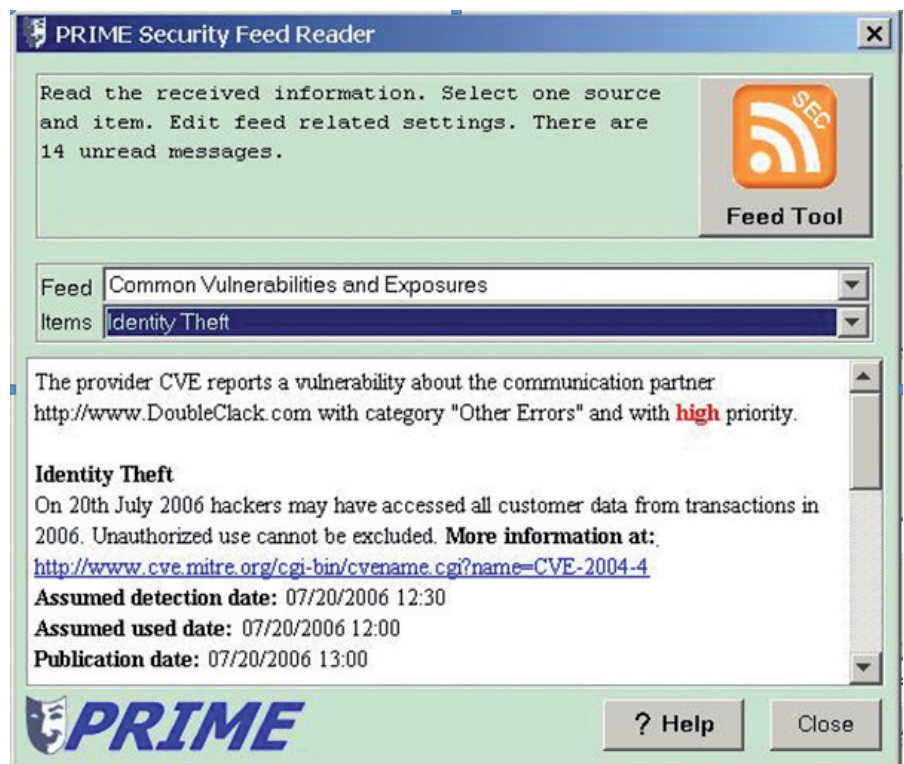


Abb. 1: Beispiel-Meldung im PRIME Security Feed

DSB-Konferenz 2008
Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Mehr Transparenz durch Informationspflichten bei Datenschutzpannen; Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn (abrufbar beim Punkt „Entschließungen“ unter <http://www.bfdi.bund.de/>)

Hanloser 2009
Stefan Hanloser: Opt-out ist demnächst absolut out; InformationWeek, Ausgabe 1, 29. Januar 2009, S. 10-12

Hansen et al. 2007
Marit Hansen, Simone Fischer-Hübner, John Sören Pettersson, Mike Bergmann: Transparency Tools for User-controlled Identity Management; in: Paul Cunningham, Miriam Cunningham (Hrsg.): Expanding the Knowledge

Economy: Issues, Applications, Case Studies; Proceedings of eChallenges 2007; IOS Press, Amsterdam 2007; S. 1360-1367

Nageler 2006
Antje Nageler: Integration von sicherheitsrelevanten Informationen in ein Identitätsmanagementsystem; Diplomarbeit am Institut für Informatik der Christian-Albrechts-Universität zu Kiel; Mai 2006

Schneier 2009
Bruce Schneier: Why security breach notification laws are a good thing, OUTLAW News 17.02.2009; <http://www.out-law.com/default.aspx?page=9800>

Karin Schuler

Pseudo-Transparenz bei Datenschutzvorfällen: Nein, danke!

Auch wenn der vorliegende Text sich kritisch mit einer Meldepflicht für Datenschutzverstöße auseinandersetzt, soll keineswegs der falsche Eindruck entstehen, derartige Verstöße sollen bagatellisiert oder gar als nicht sanktionswürdig eingestuft werden. Das Gegenteil ist der Fall. Sanktionierung ist in weit höherem Maße erforderlich, als dies derzeit der Fall ist. Die Ursachen hierfür werden von Datenschützern seit langem öffentlich benannt und beklagt: Die abgrundtief schlechte Ausstattung der Aufsichtsbehörden und der für den öffentlichen Bereich zuständigen Beauftragten, die daher lächerlich lückenhaften Kontrollen, die halbherzige Absicherung betrieblicher Datenschutzbeauftragter und die putzigen, zu geringen Geldstrafen, die manches Unternehmen aus der Portokasse begleicht – wenn es denn überhaupt jemals auffällt.

Maßnahmen, die größere Gesetzestreue zum Schutz und Nutzen der Betroffenen erreichen, sind ohne Zweifel dringend erforderlich. Darunter fallen beispielsweise verbindliche Vorgaben für Schutz- und Schulungsmaßnahmen und die Stärkung des Datenschutzmanagements. Was ich allerdings für nicht wünschenswert halte, wären Maßnahmen, die entweder diesen Zweck verfehlen, gar kontraproduktiv wirken oder beim Gesetzgeber Ressourcen binden, die für wichtigere gesetzgeberische Maßnahmen gebraucht würden. Inwieweit eine formalisierte Meldepflicht Unternehmen animiert, datenschutzgerechter zu agieren und dadurch die Betroffenenrechte stärkt, wird seit einiger Zeit diskutiert. Meine Bedenken gegen eine Meldepflicht resultieren im Wesentlichen aus der Befürchtung, ein inhaltlich richtiges Anliegen würde durch ein in der Praxis schwaches Instrument diskreditiert. Dies nicht zuletzt deshalb, weil von den wirklich dringenden Gestaltungserfordernissen im Datenschutz abgelenkt wird und,

im Vergleich zu anderen, dringenderen Maßnahmen, nur ein schlechtes Kosten-Nutzen-Verhältnis erzielt würde.

Zu spät, zu teuer

Meldepflichten sind immer nachlaufende „Schadensbegrenzung“ und daher schlechter als jede vorbeugende Maßnahme. Mit begrenzten Ressourcen investiert man besser und effizienter in letzteres.

Datenschutz kämpft seit Jahrzehnten mit dem Mangel. Die Ausstattung betrieblicher Datenschützer und staatlicher Kontrollbehörden ist gleichermaßen schlecht. Für jede substantielle Verbesserung müssen Verteilungskämpfe um bessere personelle und finanzielle Ausstattung gefochten werden. Es wäre daher strategisch geschickt, mit den begrenzten Ressourcen (Zeit, Geld, Personal, Einfluss) vorrangig für Datenschutz-Maßnahmen zu streiten, die möglichst frühzeitig und effizient in betrieblichen und behördlichen Abläufen wirken, wie z. B. der vernünftigen Organisation des Kontrollwesens.

Zu theoretisch, zu kompliziert

Meldepflichten nutzen den Betroffenen nur, wenn diese mit der Meldung auch tatsächlich etwas anfangen können (ganz praktisch, nicht nur in der grauen Theorie). Dafür müssten sie die Meldung a) mitbekommen, b) verstehen, c) persönliche Konsequenzen abschätzen können und d) geeignete Maßnahmen ergreifen können. Wenig davon trifft für die Mehrzahl der Betroffenen zu. Verfügbare Schutzvorkehrungen im Internet (z. B. Mail-Verschlüsselung) sind bis heute ein Spielzeug für Spezialisten, was aus meiner Sicht beispielhaft den Kenntnisstand und das Bewusstsein der meisten Betroffenen widerspiegelt. Mit der Pseudo-Offenheit,

mit der Datenschutzvorfälle bekannt gegeben würden, könnten ohne massive Sensibilisierungsbemühungen voraussichtlich nur wenige Betroffene etwas anfangen.

Zu nebulös, zu ungenau

Meldepflichten nutzen nur dann, wenn ihre Voraussetzungen eindeutig benennbar sind. So ist zum Beispiel ein meldepflichtiger Arbeitsunfall nachvollziehbar und eindeutig: Unfälle mit körperlichen Schäden während der Arbeitszeit lassen sich zweifelsfrei erkennen. Für Datenschutzvorfälle jedoch ergeben sich in der Praxis massive Abgrenzungsprobleme. Wie wird ein meldepflichtiger Vorfall definiert, wie also die Meldepflicht ausgelöst? Wer ist meldepflichtig (verantwortliche Stelle? Entdecker/Hacker? Aufsichtsbehörde?) und wie kann der meldepflichtigen Stelle nachgewiesen werden, dass sie Kenntnis hatte? Wie verhindert man, dass durch eine schlecht kontrollierte Meldepflicht letztlich die Vogel-Strauß-Politiker gewinnen (weil sie nicht öffentlich auffallen, weil sie keine aktive Fehlersuche betreiben) und sicherheitsbewusste Unternehmen durch aktives Sicherheitsmanagement evtl. Lecks entdecken, die ihnen dann öffentliche Aufmerksamkeit sichern?

Wenn sicherheits- und datenschutzbewusste Unternehmen jedoch die Dummen sind, wird ein Interesse ganz sicher weiter zunehmen: nämlich Vorfälle möglichst unter dem Deckel zu halten. Wie weit dieser Reflex schon heute verbreitet ist, lässt sich zum Beispiel daran ablesen, dass es keine seriösen, halbwegs repräsentativen Statistiken über Sicherheitsvorfälle gibt, die den Namen verdient hätten.

Die Meldung datenschutzrelevanter Vorfälle muss einen definierten, konkreten Nutzen für die Betroffenen haben, der über Schadenfreude, das Füllen von Zeitungsspalten, Datenschutzberichten

und Statistiken hinausgeht. Wie bereits dargestellt, ist ein wirklicher Nutzen für Betroffene fraglich. Die medialen Nebenwirkungen allerdings sind mit Sicherheit enorm und verstärken Vertuschungstendenzen.

Zu Wirklichkeitsfern

Meldepflichten können nur dann wirken, wenn ein Verstoß dagegen ernsthaft strafbewehrt ist. Voraussetzung hierfür ist allerdings, dass Verstöße überhaupt bemerkt werden. Dies wiederum setzt in erster Linie ausreichende Ressourcen für die Überwachung/Aufsicht voraus. Wie soll die Einhaltung der Meldepflicht durch Aufsichtsbehörden kontrolliert werden, die heute noch nicht mal bemerken (wenn man von der Zahl von Unternehmen ohne

Datenschutzbeauftragten ausgeht), wenn Unternehmen ihrer Meldepflicht gem. § 4 d BDSG nicht nachkommen? Und selbst wenn es gelänge, den jahrzehntelangen Kampf um mehr Ressourcen für die Aufsichtsbehörden positiv zu wenden, wären zuvörderst die bekannten und grundlegenden Missstände wirksam und flächendeckend zu kontrollieren: Missachtung der Pflichten zur Bestellung eines Datenschutzbeauftragten, zur Durchführung und Dokumentation innerbetrieblicher Vorabkontrollen, zur Erstellung eines Verfahrenszeichnisses usw.

Kontraproduktiv

Sind Eindeutigkeit und Durchsetzbarkeit nicht gegeben, mutieren

Meldepflichten zu einem Kampfinstrument im Wettbewerb. Das Ergebnis ist ein in höchstem Maße unfairer Zustand: Nicht diejenigen haben Vorteile, die die wenigsten Verstöße begehen bzw. erleiden, sondern diejenigen, die die besten Verschleierungstaktiken entwickeln. Und das erscheint aufgrund absolut mangelhafter Kontrollmöglichkeiten nicht schwer. Ein unerwünschtes Ergebnis könnte darin bestehen, dass Unternehmen zusätzlich in Verschleierungsmaßnahmen investieren und so die ohnehin schon schwierige Verfolgung von Verstößen zusätzlich erschweren.

Werner Hülsmann

EG-Richtlinie zur Vorratsdatenspeicherung ist auf eine geeignete Rechtsgrundlage gestützt

Am 10. Februar 2009 hat der Gerichtshof der Europäischen Gemeinschaften (EuGH) mit seinem Urteil die Nichtigkeitsklage Irlands und Sloweniens gegen die EG-Richtlinie zur Vorratsdatenspeicherung (Richtlinie 2006/24/EG) abgewiesen: „Der Gerichtshof stellt zunächst klar, dass sich die von Irland erhobene Klage allein auf die Wahl der Rechtsgrundlage bezieht und nicht auf eine eventuelle Verletzung der Grundrechte als Folge von mit der Richtlinie verbundenen Eingriffen in das Recht auf Privatsphäre.“¹

Der Gerichtshof stellt fest, dass die Richtlinie auf einer geeigneten Rechtsgrundlage erlassen worden ist.¹

Die Entscheidung betrifft – wie das Gericht selbst betont – nur die formale Frage der einschlägigen Rechtsgrundlage und hat die Verletzung der Grundrechte durch die anlasslose Erfassung des Telekommunikations- und Bewegungsverhaltens der gesamten Bevölkerung nicht zum Gegenstand.

Die mehr als 34.000 deutschen Beschwerdeführer/innen haben bereits beantragt, dass das Bundesverfassungsgericht den Europäischen Gerichtshof in einem zweiten Verfahren über die Vereinbarkeit der verdachtslosen Vorratsdatenspeicherung mit unseren Grundrechten entscheiden lässt. Daher ist das Urteil vom 10. Februar 2009 vermutlich nicht das letzte EUGH-Urteil in Sachen Vorratsdatenspeicherung.

¹ Pressemitteilung des EuGH vom 10.02.2009 - <http://curia.europa.eu/de/actu/communiqués/cp09/aff/cp090011de.pdf>