Alexander Dix

# Privacy Respecting Incident Management - die Datenschutzsicht

*Überarbeitete Fassung des beim PRIMA-Workshop in Regensburg am 6.4.2005 gehaltenen Vortrags*

## Vorbemerkung

Der Begriff des „Privacy Respecting Incident Management“ verweist auf das Verhältnis zwischen Datenschutz und Datensicherheit. Dabei steht „Privacy“ für den deutschen Datenschutz (trotz ursprünglicher Bedeutungsunterschiede werden die beiden Begriffe inzwischen international weitgehend synonym verwendet). „Incident Management“ beschreibt dagegen den gesamten organisatorischen und technischen Prozess der *Reaktion auf* erkannte und vermutete *Sicherheitsvorfälle* in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse[1].

Zugleich verweist die Begriffsbildung „Privacy Respecting Incident Management“ darauf, dass Incident Management nicht per se datenschutzfreundlich ist. Demgegenüber steht die herkömmliche Sicht der deutschen Datenschutzgesetze, die Datensicherheit als zweites, „technisch-organisatorisches Standbein“ des Datenschutzes verstehen. Allerdings weisen alle Datenschutzgesetze des Bundes und der Länder insofern ein bemerkenswertes quantitatives Ungleichgewicht auf, als sie rund 40 Paragrafen mit datenschutzrechtlichen Regelungen, aber nur eine einzige mit dezidiert technisch- organisatorischem Inhalt vorsehen. Das verdeutlicht das traditionelle Übergewicht datenschutzrechtlicher Vorgaben (Wann ist die Verarbeitung welcher Daten zu welchem Zweck zulässig ?) gegenüber Regelungen technischen Inhalts (Wenn bestimmte Daten verarbeitet werden dürfen, wie ist der Verarbeitungsprozess technisch-organisatorisch zu sichern ?).

## Das „Security-Privacy Paradox“

[1] So die Definition der Fachgruppe SIDAR der Gesellschaft für Informatik, vgl. http://www.gi-fb-sicherheit.de/fg/sidar/incident-response.html

Das nicht immer konfliktfreie Verhältnis zwischen Datenschutz und Datensicherheit ist von der Informations- und Datenschutzbeauftragten der kanadischen Provinz Ontario treffend als „Security-Privacy Paradox“ bezeichnet worden[2]. Zwar gibt es zwischen den Prinzipien der Datensicherheit einerseits und des Datenschutzes andererseits zahlreiche Überlappungen. Dazu zählen die Vertraulichkeit, Integrität, Genauigkeit und Verfügbarkeit der Daten. Während aus der Sicht der Informationssicherheit aber Zugangs- und Zugriffskontrollen, Authentifizierung, Autorisierung und Nichtabstreitbarkeit (Non-repudiation) im Vordergrund stehen, sind gerade für den modernen Datenschutz Elemente des Systemschutzes (Datenvermeidung, Datenparsamkeit), Zweckbindung, Transparenz-, Kontroll- und Steuerungsrechte der Betroffenen maßgeblich.

Informationelle Selbstbestimmung steht insofern auch in einem Spannungsverhältnis zu Anforderungen des technisch - organisatorischen Datenschutzes, als diese unabhängig von der Einwilligung Betroffener zu berücksichtigen sind. Gerade der Arbeitnehmerdatenschutz ist ein klassisches Beispiel für dieses Spannungsverhältnis, insbesondere dann, wenn der Arbeitgeber den Beschäftigten die Nutzung dienstlicher Rechner zu privaten Zwecken gestattet. Der Betrieb von Firewalls und SPAM-Filtern, aber auch die Ausfilterung von e-mails, die an ehemalige Beschäftigte gerichtet werden[3], sind in diesem Zusammenhang beispielhaft zu nennen. Dass mangelhafte Datensicherheit, die primär (wenn auch nicht ausschließlich) der Arbeitgeber für die Computerarbeitsplätze in seinem Betrieb zu verantworten hat, sogar existenzvernichtend wirken kann, hat der Fall des schwedischen Universitätsmitarbeiters gezeigt, dem aufgrund des Vowurfs, kinderpornografische Bilder auf seinem Rechner gespeichert zu haben, gekündigt wurde. Seinen Arbeitsplatz erhielt er auch dann nicht zurück, als nach Jahren nachgewiesen worden war, dass die Bilder über einen Trojaner auf seiner Festplatte abgelegt und von ihm nie geöffnet worden waren. Sein Ruf war geschädigt, er musste ins Ausland gehen[4].

---

[2] Information and Privacy Commissioner/Ontario and Deloitte & Touche, The Security-Privacy Paradox: Issues, Misconceptions and Strategies, Joint Report, August 2003 (http://www.ipc.on.ca/docs/sec-priv.pdf)
[3] Dazu OLG Karlsruhe DuD 2005, 167 = MMR 2005, 178 m. Anm. Heidrich; Köcher DuD 2005, 163.
[4] Vgl. http://www.heise.de/newsticker/meldung/57030

Das mangelnde Verständnis des Security-Privacy-Paradoxons, insbesondere die Gleichsetzung von IT-Sicherheit und Datenschutz, führt häufig zu einem gerade in Wirtschaftsunternehmen folgenschweren Missverständnis: wenn die Unternehmensleitung glaubt, alles Nötige für die IT-Sicherheit getan zu haben, meint sie, damit auch den Anforderungen des Datenschutzes genügt zu haben (eben weil verkannt wird, dass IT-Sicherheit nur teilweise mit dem Datenschutz deckungsgleich ist). Abgesehen davon, dass IT-Sicherheit die gesamte (auch nicht-personenbezogene) Datenverarbeitung betrifft, muss sich häufig in vielen Unternehmen erst noch ein Gespür dafür herausbilden, dass Maßnahmen zur IT-Sicherheit nicht per se datenschutzkonform oder gar datenschutzfreundlich sind. Vielmehr bedarf es dazu einer Analyse und Bewertung der möglichen Maßnahmen zur Feststellung und Abwehr von sicherheitsrelevanten Vorfällen.

In der frühen Datenschutzdiskussion ist die Frage der Protokollierung in dieser Hinsicht kritisch erörtert worden. Die vom Datenschutzrecht vorgeschriebene Protokollierung zum Zweck der Eingabekontrolle kann als Vollprotokollierung oder als stichprobenbezogene Protokollierung betrieben werden. Erstere würde zwar (theoretisch) eine lückenlose Überprüfung aller Zugriffe auf ein Datenverarbeitungssystem ermöglichen, zugleich aber eine permanent anwachsende neue personenbezogene Datensammlung erzeugen. Eine stichprobenhafte Protokollierung würde gewisse Kontrolllücken in Kauf nehmen, zugleich aber der Datensparsamkeit besser Rechnung tragen. Unbefugte wüssten zudem nicht, wie sie der Stichprobenkontrolle entgehen könnten.

In beiden Fällen (bei der Voll- oder Stichprobenprotokollierung) muss die strikte Bindung an die Zwecke der Datenschutzkontrolle sicher gestellt werden, die das Gesetz (§§ 14 Abs. 4, 31 BDSG) vorschreibt. Wie weit diese Zweckbindung im Ernstfall juristisch trägt, ist aber noch ungeklärt. Das betrifft vor allem die Frage, inwieweit solche Protokolldateien dem Zugriff der Strafverfolgungsbehörden unterliegen. Das wird man jedenfalls insoweit bejahen müssen, als es um die Ahndung von Straftaten gegen den Datenschutz geht[5], denn gerade auch zu deren Aufklärung ist die Protokollierung erfolgt. Ob die Gerichte aber die Beschlagnahme von Protokolldateien ablehnen würden, wenn sie zur Aufklärung von anderen,

[5] Simitis/Dammann, Rdnr. 115 zu § 14 BDSG.

schweren Kriminalitätsformen beitragen könnten, ist ungewiss. Die Strafprozessordnung enthält jedenfalls bislang kein – wenn auch nur eingeschränktes – Beschlagnahmeverbot.

Welche Bedeutung die Dokumentation und Protokollierung für den Schutz des Rechts auf informationelle Selbst bestimmung wie auch für den Rechtsschutz allgemein haben kann, hat das Bundesverfassungsgericht in seiner Eilentscheidung zum zentralen Kontenzugriff nach dem Gesetz zur Förderung der Steuerehrlichkeit deutlich gemacht[6]. Da das Gesetz sowohl den Finanzämtern als auch – indirekt – allen anderen Behörden, die Voschriften unter Anknüpfung an das Einkommensteuergesetz anzuwenden haben (vor allem den Sozialbehörden), den heimlichen Zugriff auf alle Kontostammdaten erlaubt, muss den Betroffenen zumindest nachträglich eine Rechtmäßigkeitskontrolle dieser Zugriffe ermöglicht werden. Dies setzt aber eine Dokumentation bzw. Protokollierung der Zugriffe voraus.

Während das Kreditwesengesetz (§ 24 c Abs. 4) eine automatisierte Protokollierung durch die Bundesanstalt für Finanzdienstleistungsaufsicht vorschreibt, was entsprechend auch für Abrufe durch das Bundesamt für Finanzen gilt, hat das Bundesverfasssungsgericht darüber hinaus eine formularmäßige (wohl: papiergestützte) Dokumentation durch die ersuchende Behörde verlangt, die inzwischen durch den Anwendungserlass des Bundesfinanzministeriums vorgeschrieben ist. Dies war – neben der Festlegung, dass die Betroffenen in der Regel über die Abfrage zu informieren sind - ein wesentlicher Grund dafür, dass das Bundesverfassungsgericht den Erlass der einstweiligen Anordnung gegen das Inkrafttreten des Gesetzes zur Förderung der Steuerehrlichkeit abgelehnt hat[7]. Auch wenn die Entscheidung des Gerichts in der Hauptsache noch aussteht, gehört nicht viel Fantasie dazu vorausszusagen, dass diese Anforderungen auch Eingang in das Gesetz finden müssen. Protokollierung und Dokumentation sind wichtige Voraussetzungen für die Transparenz und Überprüfbarkeit von Datenerhebungen.

---

[6] Beschluss v. 22.3.2005, 1 BvR 2357/04.
**http://www.bverfg.de/entscheidungen/rs20050322_1bvr235704.html**

[7] Vgl. Rdnr. 67 des Beschlussumdrucks.

## Der Trend zur Vorratsdatenspeicherung

In diesem Zusammenhang ist auch der zunehmende Trend zur Vorratsdatenspeicherung zu sehen, und zwar aus zwei Gründen: zum einen gibt es starke Interessen insbesondere bei den Sicherheitsbehörden, anlassunabhängig und flächendeckend personenbezogene Daten speichern zu lassen; dazu könnten auch Daten gehören, die zur Feststellung und Abwehr von sicherheitsrelevanten Vorfällen im Sinne der IT-Sicherheit genutzt werden sollen. Es ist nicht auszuschließen, dass derartige Informationen auch Ermittlungsansätze für Strafverfolgungsbehörden in Verfahren liefern könnten, die nicht im Zusammenhang mit Datenschutzverstößen stehen. Zum anderen stellt sich erneut die bereits angesprochene Frage, auf welche Weise die Zweckbindung einmal angelegter personenbezogener Datenammlungen gesichert werden kann: letztlich nur durch strafbewehrte Zweckentfremdungs- und Beschlagnahmeverbote, die rechtspolitisch kaum durchsetzbar und überdies auch durch den Gesetzgeber jederzeit änderbar sein werden.

Nicht nur zur Bekämpfung der Cyberkriminalität, sondern auch zur Bekämpfung von Straftaten, die im Netz vorbereitet werden oder dort Spuren hinterlassen, fordern Strafverfolger seit langem die Einführung einer gesetzlichen Pflicht zur routinemäßigen, flächendeckenden, anlassunabhängigen Speicherung sämtlicher Verkehrsdaten (Verbindungsdaten) der Telekommunikation auf Vorrat. Dazu zählen neben den sog. Randdaten (so die euphemistische, in der Schweiz gebräuchliche Bezeichnung) der Telekommunikation (wer hat wann mit wem von wo aus wie lange via Fest- oder Mobilfunknetz per Fax oder im Internet kommuniziert) auch inhaltlich aufgeladene Verkehrsdaten wie URLs oder eindeutige Inhaltsdaten wie SMS- oder MMS-Nachrichten. Ins Visier einer solchen Maßnahme kämen ganz überwiegend unverdächtige Personen.

Diese Forderung der Sicherheitsbehörden hat Eingang gefunden in den Entwurf von vier EU-Regierungen für einen Rahmenbeschluss. Obwohl der Deutsche Bundestag mehrfach und zuletzt sogar einstimmig im Februar 2005 die Bundesregierung aufgefordert hat, diesen Rahmenbeschluss abzulehnen, ist keineswegs sicher, dass die Bundesregierung dieser Aufforderung Folge leistet. Vielmehr gibt es Anzeichen dafür, dass jedenfalls der Bundesinnenminister die europäische Ebene nutzt, um

nationale Widerstände zu umgehen. In den USA hat sich für etwas Ähnliches der Begriff der „Politikwäsche“ (policy laundering) durchgesetzt: die US-Regierung hat nach dem 11. September 2001 besonders einschneidende Beschränkungen der Bürgerrechte zunächst nur für Ausländer vorgesehen, um erst später (vielleicht sogar unter Rückgriff auf Gleichbehandlungsgesichtspunkte) ihre Erstreckung auf US-Bürger einzuleiten.

Gegenwärtig herrscht noch Streit zwischen dem Europäischen Rat der Justiz- und Innenminister einerseits und der Europäischen Kommission und dem Europäischen Parlament andererseits. Der Dissens zwischen Rat und Kommission scheint sich aber auf die Frage der Rechtsgrundlage zu beschränken, während das Parlament eine solche Maßnahme generell ablehnt. Der Rat vertritt den Standpunkt, der Rahmenbeschluss könne in der sogenannten Dritten Säule (Zusammenarbeit bei Justiz und Inneres) von den Regierungen allein (einstimmig) und ohne Mitwirkung des Europäischen Parlaments beschlossen werden. Demgegenüber vertritt die Kommission die Auffassung, es handle sich um eine Maßnahme auf dem Gebiet des Binnenmarktes (zumal die Provider in die Pflicht genommen werden sollen) und deshalb müssten Rat, Kommission und Parlament sich einigen (Mitentscheidungsverfahren).

Die Kommission arbeitet aber bereits selbst an einem eigenen Vorschlag, der wohl lediglich bei der Länge der Speicherverpflichtung hinter dem Ratsvorschlag zurückbleiben wird. Die Wahrscheinlichkeit ist hoch, dass der Streit ähnlich wie bei der Frage der Übermittlung von Flugpassagierdaten in die USA letztlich vom Europäischen Gerichtshof in Luxembourg entschieden werden muss. Sollte ein solcher Beschluss des Rates oder der drei EU-Organe vorher gefasst werden, wäre aber zu prüfen, ob der Gerichtshof die Wirksamkeit des Beschlusses vorläufig aussetzen könnte, weil sonst bis zu einer sehr viel späteren Entscheidung in der Hauptsache zulasten der Nutzerinnen und Nutzer von Kommunikationsnetzen Fakten geschaffen würden. Damit wäre – wie es der Bayerische Datenschutzbeauftragte Reinhard Vetter zutreffend formuliert hat – ein datenschutzpolitischer „Dammbruch“ verbunden.

In der Sache ist die Wahrscheinlichkeit hoch, dass der Gerichtshof einen solchen Rahmenbeschluss verwerfen würde, denn er hat in seiner Rechtsprechung stets die Bedeutung des Artikels 8 der Europäischen Menschenrechtskonvention betont, wonach Eingriffe in die Privatsphäre nicht schon dann zulässig sind, wenn sie dem Staat nützen, sondern erst, wenn ein zwingendes gesellschaftliches Bedürfnis für solche Eingriffe besteht und der Grundsatz der Verhältnismäßigkeit gewahrt bleibt. Das aber ist nicht erkennbar, denn es gibt weniger einschneidende, grundrechtskonforme Verfahren der Strafverfolgung.

Dazu zählt insbesondere das „fast freeze – quick thaw"-Verfahren, das zum einen in den USA praktiziert wird, wo es auch nach dem 11. September keine Pflicht zur Vorratsdatenspeicherung gegeben hat, und das zum anderen in der noch zu ratifizierenden Cybercrime-Konvention des Europarats vorgesehen ist. In diesem Verfahren sichern Polizei und Staatsanwaltschaft bei den Providern aus gegebenem Anlass, also wenn eine Straftat begangen worden ist oder unmittelbar bevorsteht, die vorhandenen Verkehrsdaten, indem sie sie vor Ort einfrieren lassen, um ihre regelmäßige Löschung zu verhindern. Anschließend entscheidet ein Gericht, ob die Daten für dieses konkrete Ermittlungsverfahren aufgetaut werden dürfen.

In diesem grundrechtskonformen Sinne sollten auch Daten zu Zwecken des Incident Management erhoben und verarbeitet werden: die Begriffsbestimmung hebt zu recht darauf ab, dass es sich um einen Prozess der *Reaktion auf* erkannte und vermutete *Sicherheitsvorfälle* in IT-Bereichen handelt. Ein Incident Management mit routinemäßiger Vorratsdatenspeicherung muss sich jedenfalls dann aus datenschutzrechtlicher Sicht kritische Fragen gefallen lassen, wenn es personenbezogene Daten registriert.

**Die Empfehlungen der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation**

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (wegen des Vorsitzlandes international als „Berlin Group" bekannt) hat sich 2003 mit

Intrusion Detection Systemen (einer bestimmten Form des Incident Management) befasst und eine Reihe von Empfehlungen[8] formuliert.

Danach muss Intrusion Detection den Zwecken der Datensicherheit und des Systemschutzes dienen, die Datenspeicherung muss dem Schutzzweck angemessen sein und es muss eine Festlegung (policy) im Unternehmen oder in der Dienststelle geben, die den Schutz personbezogener Daten regelt und deren Einhaltung zu überwachen ist.

Die Forderung nach Angemessenheit im Hinblick auf den Schutzzweck ist so zu verstehen, dass im Sinne des modernen Systemdatenschutzes immer zuerst nach Wegen gesucht werden sollte, wie Sicherheitsvorfälle ohne Erhebung personenbezogener Daten registriert werden können. Erst in einem zweiten Schritt könnten – bei Vorliegen entsprechender Anhaltspunkte – Daten der betroffenen Beschäftigten erhoben werden.

In jedem Fall sollten solche Maßnahmen nicht hinter dem Rücken der Betroffenen, sondern offen und transparent vorgenommen werden. Dabei ist allerdings sicherzustellen, dass böswillige Insider („disgruntled employees“) nicht die Aufklärung behindern. Letztlich ist dies auch eine Frage des Arbeitnehmerdatenschutzes, der in Deutschland noch immer nicht gesetzlich geregelt ist.

**Fazit**

Zusammenfassend lässt sich feststellen:

1. Datenschutz und IT-Sicherheit haben teilweise kongruente, aber auch widerstreitende Ziele.
2. Eine umfassende, anlassunabhängige Erhebung von personenbezogenen Daten auf Vorrat – zu welchen legitim erscheinenden Zwecken auch immer – ist abzulehnen.

[8] http://www.datenschutz-berlin.de/doc/int/iwgdpt/ids_de.pdf

3. Ein modernes Datenschutzrecht muss für einen grundrechtskonformen Ausgleich zwischen Datenschutz und IT-Sicherheit sorgen.
4. Auch Maßnahmen zur IT-Sicherheit dürfen nicht dazu führen, dass die Nutzung von Kommunikationsnetzen stets und von vornherein die personenbezogene Überwachung zur Folge hat, der einzelne Mensch sich dieser Überwachung also nur durch Technikabstinenz entziehen kann.