Privacy Respecting Incident Management - die Datenschutzsicht

Dr. Alexander Dix, LL.M.

LAND BRANDENBURG
LDA
Schutz der
• Persönlichkeitsrechte
• Informationsfreiheit

Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Übersicht

- **Datenschutz und Datensicherheit**
- **The Security-Privacy Paradox**
- **Was sind „Incidents“ ?**
- **Trend zur Vorratsdatenspeicherung**
- **Datenschutzgerechte Alternativen**
- **Fazit**

Datenschutz und Datensicherheit (1)

- **Verhältnis: Komplementär oder konflikthaft ?**
- **Herkömmliche Datenschutzgesetze betrachten die Datensicherheit als 2. Bein des Datenschutzes**
- **Aber: durchschnittl. 40 §§ zum Datenschutz, 1 § zur Datensicherheit**
- **Traditionelles Übergewicht rechtlicher Regelungen**

The Security-Privacy Paradox (1)

Informationssicherheit:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Unabstreitbarkeit

The Security-Privacy Paradox (2)

Datenschutz:

- Datenvermeidung, -sparsamkeit (Systemdatenschutz)
- Zweckbindung
- Transparenz
- Betroffenenrechte
- Ordnungsmäßigkeit der DV

Überschneidungen, Konflikte

- *Überschneidungen*
  Ordnungsmäßigkeit der DV, technisch-organisatorische Maßnahmen des DS-Rechts dienen der IT-Sicherheit
- *Konflikte*
  Z.B. beim Arbeitnehmerdatenschutz
  Überwachungseignung u. –wirkung von IT-Sicherheitsmaßnahmen gegen Insider-Angriffe („disgruntled employees“)

Grundmissverständnis

- Informationssicherheit (IT-Security) wird vor allem in der Wirtschaft vielfach mit dem Datenschutz gleichgesetzt
- Dem Datenschutz wird kein eigener Stellenwert eingeräumt

Protokollierung

- **Diskussion um Vollprotokollierung, Stichproben**
- **Personenbezogene Protokollierung Teil der vorgeschriebenen Eingabekontrolle nach § 9 BDSG**
- **Ausweg aus dem Dilemma: strikte Zweckbindung ? (§ 14 Abs. 4 BDSG)**
- **Beispiel: Eilentscheidung des BVerfG zum kontenübergeifenden Zugriff der Finanzverwaltung v. 22.3.2005**

Protokollierung zur Eingabekontrolle

Bei der automatisierten Verarbeitung personenbezogener Daten müssen u.a. Maßnahmen getroffen werden, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind. *(Eingabekontrolle) - Anlage zu § 9 BDSG*

Zweckbindung von Protokolldaten

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer DV-Anlage gespeichert werden, *dürfen nur für diese Zwecke verwendet werden*.
(§ 14 Abs.4 BDSG)

Grenzen der Zweckbindung ?

- Durchbrechung der Zweckbindung durch Beschlagnahme von Protokolldaten ?
- Konsequent wäre die Begrenzung der Beschlagnahme auf die Verfolgung von Datenschutzdelikten
- Aber: Was passiert bei Kapitalverbrechen und anderen Schwerstdelikten ?
- Bisher keine Rechtsprechung

Incident Management

- Welche Incidents ?
- Incident Management: der gesamte organisatorische und technische Prozess der *Reaktion auf* erkannte und vermutete *Sicherheitsvorfälle* in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse. (SIDAR-GI)

Verhältnis Protokollierung – Incident Management

- Protokollierungspflicht soll Umgang mit pb. Daten datenschutzrechtlich überprüfbar machen
- Incident Management soll Angriffe von innen und außen feststellen und abwehren, um Systemsicherheit zu gewährleisten

Was sind „Incidents“ ?

- Erkannte und vermutete Sicherheitsvorfälle = Bedrohungen der IT-Sicherheit
- Netzkriminalität (gegen und über Netze), „Cyberterrorismus“ gegen kritische Infrastrukturen
- Allgemeine Kriminalität ?

Maßnahmen gegen Computer-, Cyberkriminalität

- Cybercrime-Konvention des Europarats (seinerzeit mit Hochdruck ausgehandelt, Ratifikation durch die wichtigsten Länder bisher: Fehlanzeige) verlangt *Einfrieren* vorhandener Datenbestände bei Bedarf (fast freeze – quick thaw, keine Vorratsdatenspeicherung)
- EU-Rahmenbeschluss v. 24.2.2005 über Angriffe auf Informationssysteme

Trend zur Vorratsdatenspeicherung (1)

- **Nicht nur zur Bekämpfung von Cyberkriminalität, sondern ganz allgemein zur Verbrechensbekämpfung verlangen Strafverfolger immer wieder die anlass- und verdachtsunabhängige Speicherung von Verkehrsdaten in TK-Netzen auf Vorrat**

- **Der Bundestag hat dies mehrfach (zuletzt im Frühjahr 2005 einstimmig) abgelehnt, aber...**

Trend zur Vorratsdatenspeicherung (2)

- **Im Europäischen Rat (Justiz- und Innenminister) wird weiter über den Entwurf eines Rahmenbeschlusses zur Vorratsdatenspeicherung beraten**

- **Nach dem neuesten Entwurf ist vorgesehen, alle „Kommunikationsdaten" der Telefon-, SMS-, MMS-, Fax-, Mobil- u. Internetkommunikation für mindestens 6 Monate u. höchstens 3 Jahre zu speichern.**

Trend zur Vorratsdatenspeicherung (3)

- **EU-Parlament lehnt den Vorschlag ab**

- **Streit über Rechtsgrundlage u. Verfahren: Kommission u. Parlament halten dies für eine Binnenmarktregelung (*1. Säule*) – Mehrheitsprinzip im Rat u. Beteiligung des Parlaments**
  Rat hält dies für eine Regelung der *3. Säule* (Justiz/Inneres) – Einstimmigkeitsprinzip, keine Beteiligung des Parlaments

Trend zur Vorratsdatenspeicherung (4)

- **Wenn der Rat gegen den Widerstand von Parlament u. Kommission Vorratsdatenspeicherung beschließt, wird der EuGH zu entscheiden haben**

- **Zwingende Vorratsdatenspeicherung wäre ein Dammbruch zulasten des Datenschutzes (R. Vetter)**

Speicherung von IP-Adressen

- **Entscheidung des RP Darmstadt zur Speicherung von dynamischen IP-Adressen bei T-Online (2003):**

  Zulässig zu Abrechnungszwecken und erforderlich zur Gewährleistung der Datensicherheit nach § 9 BDSG

  Nahezu einhellige Ablehnung durch die anderen Aufsichtsbehörden und Datenschutzbeauftragten

Datenschutzgerechte Alternativen

- Incident Management muss auf Anlässe reagieren
- Generelle (routinemäßige, anlassunabhängige) präventive Speicherung von personenbezogenen Daten ist grundsätzlich abzulehnen
- Hersteller und Anwender müssen vorrangig die Systemsicherheit erhöhen

Datenschutzgerechte Alternativen (2)

- Allerdings: absolut sichere DV-Systeme wird es nicht geben
- Deshalb kann die stufenweise Erhebung personenbezogener Daten und ihr Einfrieren zur Feststellung und Aufklärung von konkreten Sicherheitsvorfällen notwendig sein.

Empfehlungen der International Working Group on Data Protection in Telecommunications (1)

Arbeitspapier zu Intrusion Detection Systemen (2003):

- Strikte Begrenzung der Erhebung von pb Daten auf das zwingend Erforderliche (Datenvermeidung)
- Transparenz gegenüber Arbeitnehmern, Nutzern, Kunden

Empfehlungen der International Working Group on Data Protection in Telecommunications (2)

- Schutz der gespeicherten Daten vor unbefugtem Zugriff und Zweckentfremdung
- Entwicklung spezieller gesetzlicher Regelungen für einen angemessenen Ausgleich zwischen Datenschutz und IT-Sicherheit

Fazit (1)

- **Datenschutz und IT-Sicherheit haben teilweise kongruente, aber auch widerstreitende Ziele**
- **Eine umfassende, anlassunabhängige Erhebung von personenbezogenen Daten auf Vorrat – zu welchen Zwecken auch immer – ist abzulehnen.**
- **Ein modernes Datenschutzrecht muss für einen grundrechtskonformen Ausgleich zwischen Datenschutz und IT-Sicherheit sorgen.**

Fazit (2)

Auch Maßnahmen zur IT-Sicherheit dürfen nicht dazu führen, dass die Nutzung von Kommunikationsnetzen stets die personenbezogene Überwachung zur Folge hat, der Einzelne sich dieser Überwachung also nur durch Technikabstinenz entziehen kann.

- Kontakt: Dix@LDA.brandenburg.de
- Arbeitspapier der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation zu Intrusion Detection Systemen (September 2003) http://www.datenschutz-berlin.de/doc/int/iwgdpt/
- Beschluss des Bundesverfassungsgerichts zum kontenübergreifenden Zugriff der Finanzverwaltung v. 22. März 2005 http://www.bverfg.de/entscheidungen/rs20050322_1bvr235704.html