Grundlagen des Datenschutzes und der IT-Sicherheit (8)

Vorlesung im Sommersemester 2007
an der Universität Ulm
von Bernhard C. Witt

Grob-Gliederung zur Vorlesung

Topics zum Datenschutz:
- Geschichte des Datenschutzes
- Datenschutzrechtliche Prinzipien

→ **Vertiefung in ausgewählten Bereichen**

- Verwandte Gebiete zum Datenschutz

Topics zur IT-Sicherheit:
- Einflussfaktoren zur IT-Sicherheit
- Mehrseitige IT-Sicherheit
- Risiko-Management
- Konzeption von IT-Sicherheit

Datenschutzrechtliche Vertiefung

- Allgemein gültige Regelungen
- Datensicherheit
- Kundendatenschutz (Wahlthema)
- Datenschutz bei Sicherheitsbehörden (Wahlthema)

Kundenbindung (1)

- zur Vertragsabwicklung personenbezogene Daten i.d.R. unerlässlich
- **Formen** der Kundenbindung:
  - produkt-/dienstleistungsbezogene Folgeaufträge
  - Rabatt-Systeme (z.B. Kundenkarten)
  - gezielte Ansprache der Kunden (auch unter Berücksichtigung „weicher“ Informationen)
  - Einrichtung von Warndateien vor „faulen“ Kunden
- **Umsetzung** mittels:
  - Customer-Relationship-Management-Systeme
  - Data-Mining (z.B. via Business Intelligence Tools) / Data-Warehousing (z.B. mittels Online Analytical Processing) zur Kundendatenanalyse
  - Call-Center zur Kundenbetreuung

→ **i.d.R. Vorabkontrolle (insb. wg. Profilbildung) erforderlich!**

Kundenbindung (2)

- **Zweckbestimmung** der Vertragsbeziehung berücksichtigen!
- **Löschungsfristen** & **Sperrungsanforderungen** berücksichtigen!
- Problem: Manche Datenbanken „kennen“ keine Löschung wg. **Datenqualität**
- **Perspektivwechsel** bei CRM-Systemen oder Data Warehouses auch bei Vertretern juristischer Personen möglich → Grenzen setzen!

Finanzstromüberwachung

- ggf. fallen neben Barzahlungen oder EC-Kartenzahlungen auch Lastschriftermächtigungen, Kreditkartenzahlungen, eCash-Zahlungen oder Kundenkredite an
  → Vielzahl zu prüfender Formulare
  → Zweckbestimmung beachten
- auf Übermittlung von Adressdaten zum Forderungseinzug säumiger Zahler an Inkassounternehmen ist Betroffene hinzuweisen
- Übermittlung von Angaben zur Zahlungsunfähigkeit bzw. -unwilligkeit zur Wahrung berechtigter Interessen Dritter zulässig! (§ 28 Abs. 3 Nr. 1 BDSG)
- Finanzbuchhaltung i.d.R. in Enterprise-Resource-Planning-Systemen (ERP-Systemen) integriert!
- Archivierung unter Berücksichtigung von GoBS & GDPdU

Übersicht Sicherheitsbehörden

Zuständigkeit des Bundes:

- Bundesamt für Verfassungsschutz
  → Beobachtung verfassungsfeindlicher Bestrebungen
- Bundesnachrichtendienst
  → Auslandsaufklärung
- Militärischer Abschirmdienst
  → Geheimschutz für die Bundeswehr
- Bundeskriminalamt
  → Bekämpfung internationaler Straftäter
- Bundespolizei
  → grenzpolizeiliche Kontrolle

Zuständigkeit der Länder:

- Landesamt für Verfassungsschutz
  → Beobachtung verfassungsfeindlicher Bestrebungen
- Polizeibehörden
  → Gefahrenabwehr

Grundsätzlich sind die jeweiligen Landesämter zuständig, sofern es nicht ausdrücklich den Bund betrifft oder länderübergreifend ist

Grundsätze Sicherheitsbehörden

Abgrenzung zwischen Sicherheitsbehörden:

- Trennung zwischen Nachrichtendiensten und Polizeibehörden [Ziffer 2 im Polizeibrief der alliierten Militärgouverneure vom 14.04.1949 an den Parlamentarischen Rat]
- nachrichtendienstliche Methoden dürfen aber von Polizeibehörden angewandt werden (verdeckte Ermittlung)
- auch bei Amtshilfe stets Datenerhebungszulässigkeit zu prüfen [vollziehende Gewalt an Recht & Gesetz gebunden; Art. 20 Abs. 3 GG]
  → Kennzeichnungspflicht der Datenherkunft
- Unterscheidung bei Zwangsdurchsetzung von Maßnahmen

Unterscheidung Strafprävention & Strafverfolgung:

- Strafprävention → Polizeirecht [konkrete Gefahr]
- Strafverfolgung → Strafprozessordnung [konkreter Anfangsverdacht]

Hinweis: Hinsichtlich Datenschutz tritt teilweise das anzuwendende Datenschutzgesetz ergänzend hinzu!

Zur Gefahrenabwehr

- **konkrete Gefahr**

= mit hinreichender Wahrscheinlichkeit führt ein Sachverhalt an einem konkreten Ort bzw. zu einer konkreten Zeit zu einem Schaden für Schutzgüter der öffentlichen Sicherheit bzw. freiheitlich-demokratischen Grundordnung

→ Einschreiten durch Sicherheitsbehörde zur Abwehr geboten

- **abstrakte Gefahr**

= Eintritt einer konkreten Gefahr mit überwiegender Wahrscheinlichkeit aufgrund von Erfahrungswerten

- **allgemeine Gefahr**

= möglicher Schadenseintritt anhand bestimmbarer Geschehnisse

- **gegenwärtige Gefahr**

= Schadenseintritt bereits gegeben oder unmittelbar bevorstehend

→ **Eingriffsrecht der Sicherheitsbehörde hängt insb. von der Konkretion der vorliegenden Gefahr von Rechtsgütern ab!**

Vorratsspeicherung

- Grundlage: EU-Vorratsspeicherungs-RL 2006/24/EG vom 15.03.2006
- betrifft „nur“ Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste bzw. Betreiber eines öffentlichen Kommunikationsnetzes
- dient der Ermittlung, Feststellung und Verfolgung schwerer Straftaten (national unterschiedlich definiert!)
- Vorratsspeicherung der Verkehrs- und Standortdaten auf wenigstens 6 Monate (max. 2 Jahre) zu Telefonnetz, Mobilfunk, Internet-Zugang, Internet-E-Mail und Internet-Telefonie
- Umsetzung bis spätestens 15.09.2007 in EU-Mitgliedsstaaten, die Anwendung kann aber bis 15.03.2009 aufgeschoben werden

Computerstrafrecht

§ 201 StGB: Verletzung der Vertraulichkeit des Wortes
§ 201a StGB: Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen
§ 202 StGB: Verletzung des Briefgeheimnisses
§ 202a StGB: Ausspähen von Daten
§ 203 StGB: Verletzung von Privatgeheimnissen
§ 206 StGB: Verletzung des Post- oder Fernmeldegeheimnisses
§ 263a StGB: Computerbetrug
§ 267 StGB: Urkundenfälschung
§ 268 StGB: Fälschung technischer Aufzeichnungen
§ 269 StGB: Fälschung beweiserheblicher Aufzeichnungen
§ 270 StGB: Täuschung im Rechtsverkehr bei Datenverarbeitung
§ 271 StGB: Mittelbare Falschbeurkundung
§ 274 StGB: Urkundenunterdrückung
§ 303a StGB: Datenveränderung
§ 303b StGB: Computersabotage
§ 305a StGB: Zerstörung wichtiger Arbeitsmittel
§ 317 StGB: Störung von Telekommunikationsanlagen

Statistik Computerkriminalität

Computerkriminalität	**2002**	**2003**	**2004**	**2005**	**2006**
Scheckkartenbetrug	36.969	35.954	36.088	32.232	27.347
Computerbetrug	9.531	11.388	14.186	15.875	16.211
Dienstezugangsbetrug	5.902	7.003	7.357	5.788	5.822
Datenausspähung	806	781	1.743	2.366	2.990
DV-techn. Fälschungen	228	237	570	1.012	2.460
Datenveränderung	1.327	1.705	3.130	1.609	1.672
Softwarepiraterie (priv.)	1.947	2.053	2.782	2.667	1.920
Softwarepiraterie (gew.)	780	570	1.117	637	727

Quelle: BKA – polizeiliche Kriminalstatistik (erfasste Fälle zur Computerkriminalität im gesamten Bundesgebiet)