Grundlagen des Datenschutzes und der IT-Sicherheit (5)

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)

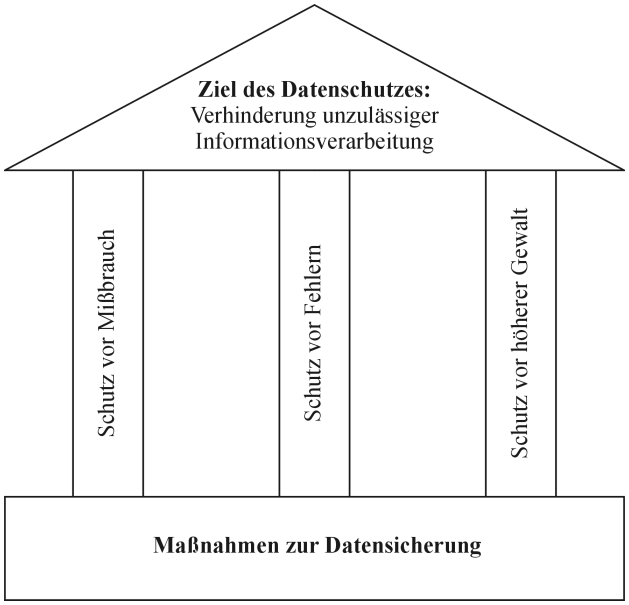
Datensicherheit (1): Begriffsdefinitionen (1)

Definition 4: Sicherheit
Abwesenheit von Gefahren

Definition 5: Datensicherung
Maßnahmen zur Erhaltung und Sicherung des DV-Systems, der Daten und Datenträger vor Fehler, Missbrauch und höherer Gewalt

→ Datensicherung zielt insb. auf **Ausfallsicherheit** ab!

Datensicherheit (2): Verhältnis Datenschutz zu Datensicherung



Datensicherheit (3): Begriffsdefinitionen (2)

Definition 6: IT-Sicherheit nach § 2 Abs. 2 BSIG

Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in oder bei der Anwendung von informationstechnischen Systemen/Komponenten

- → Datensicherung nur Teil der Verfügbarkeit: Ausfallsicherheit
- → Datensicherheit nur Spezialfall der IT-Sicherheit hinsichtlich der Daten (statt informationstechnischer Systeme/Komponenten)
- → **technische & organisatorische Maßnahmen dienen Datenschutz und IT-Sicherheit**

Klassische IT-Sicherheit vs Mehrseitige IT-Sicherheit

Klassische IT-Sicherheit:

- Verfügbarkeit
- Unversehrtheit = Integrität
- Vertraulichkeit

→ Vermeidung unzureichender Beeinträchtigungen der IT-Systeme, Daten, Funktionen und Prozesse in Bestand, Nutzung oder Verfügbarkeit

→ Verlässlichkeit der IT-Systeme

→ Sicherheit der Systeme

Mehrseitige IT-Sicherheit:

- klassische IT-Sicherheit
- ergänzt um weitere Sicherheitsziele (insb. Authentizität und Verbindlichkeit)

→ Berücksichtigung der Interessen aller Beteiligten

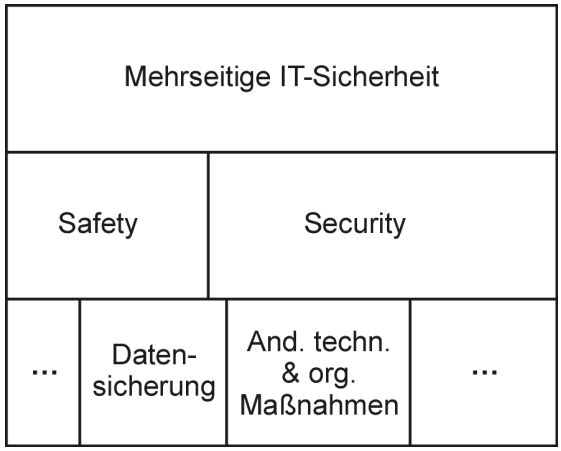
→ Verlässlichkeit und Beherrschbarkeit der IT-Systeme

→ Sicherheit der Systeme und vor den Systemen

Datensicherheit (4): Abgrenzungen

- Schutz vor unbeabsichtigten Ereignissen: Safety
- Schutz gegen beabsichtigte Angriffe: Security

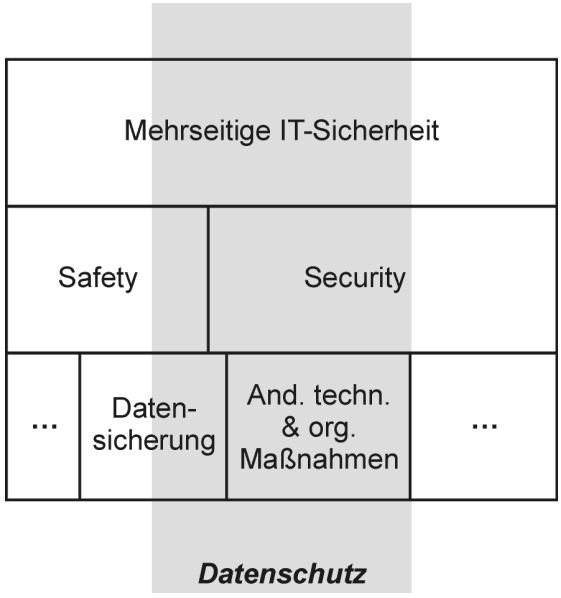
→ **IT-Sicherheit = Safety + Security**



Datensicherheit (5): Abgrenzungen

Zusammenhang zwischen mehrseitiger IT-Sicherheit und Datenschutz:

- Überschneidung bei der Verarbeitung personenbezogener Daten
- Schwerpunkt liegt auf Security



Kundendatenschutz

- **Kunden** der Unternehmen können sein:
  - ° **juristische Personen** (Kapitalgesellschaften, Mehrpersonengesellschaften, Personenvereinigungen)
  - ° **natürliche Personen** (Einpersonengesellschaften, Privatpersonen)
- Datenschutz in der BRD nur für natürliche Personen relevant!
- Vertreter juristischer Personen werden i.d.R. als juristische Person „gewertet“, sofern es nicht um die Person als solche geht

→ bei Kundendatenverwaltung zu ermitteln, ob Datenschutz überhaupt relevant ist

→ Aber: Einpersonengesellschaften nicht immer leicht zu erkennen

Kundendatenverwaltung

- **Vertrieb** befasst mit:
  - ° Werbung (→ Kundengewinnung)
    → vertragsähnliches Vertrauensverhältnis
  - ° Bestandspflege (→ Kundenbindung)
    → Vertragsverhältnis
- **Finanzbuchhaltung** befasst mit:
  - ° Verwaltung der Zahlungsströme
    → Vertragsverhältnis
  - ° Umgang mit Zahlungsverzug
    → Vertragsverhältnis
- Besonderheiten:
  - ° **Mitarbeiter** als Kunden → Vertragsverhältnis
  - ° **RFID** zur Warenkennzeichnung kann zu personenbezogenem Datum mutieren! → vertragsähnliches Vertrauensverhältnis

Kundengewinnung (1)

- Erhebung von **Interessentendaten** (z.B. via Web-Formular unter Beachtung von Telemedienrecht)
- Abgabe einer „**invitatio ad offerendum**“
- Einkauf (Adresshandel) oder Nutzung (Lettershop) von **listenmäßig** zusammengefassten Daten (Zugehörigkeit zu einer Personengruppe, Berufs- / Branchen- / Geschäftsbeziehung, Namen, Titel, akademische Grade, Anschrift, Geburtsjahr) nach § 28 Abs. 3 Nr. 3 BDSG i.V.m. § 29 BDSG
  ~ Auszug aus Melderegister gem. jeweiligem Meldegesetz (Gruppenauskunft ohne Angabe der Staatsangehörigkeit, Geschlecht und evtl. relevante gesetzliche Vertreter bzw. einfache Melderegisterauskunft mit Titel und Geburtsjahr)
- Auswertung von **Veröffentlichungen**

→ **Angabe der Quelle bei Speicherung erforderlich!**

Kundengewinnung (2)

- bei **Werbung** außerdem zu beachten: [siehe insb. 3. Übung]
  - ° unlautere Werbung (Kaltaquise am Telefon, unverlangte Werbung per Fax/E-Mail...) → UWG
  - ° SPAM → TMG
  - ° Widerspruchsrecht des Betroffenen → BDSG (z.B. via Robinsonliste beim Direktmarketing)
  - ° Einwilligung (elektronisch → TMG; sonst → BDSG)
  - ° Auswertung von Todesanzeigen wäre sittenwidrig!

→ Datenschutz und Verbraucherschutz konvergieren

- Bei Erhebungen personenbezogener Daten via Telemedien sind die **Impressumpflichten** zu beachten
- Abgabe einer **Visitenkarte** begründet zwar vertragsähnliches Vertrauensverhältnis, berechtigt aber noch nicht zur Werbung (→ Kontext beachten!)

Zur elektronischen Einwilligung

- eindeutige und bewußte Handlung des Telemedien-Nutzers (z.B. durch gesonderte Bestätigung der Eingabe → „opt-in“ mit Bestätigung)
- mit Protokollierung (zur Nachprüfbarkeit)
- jederzeitige Abrufbarkeit und Widerrufbarkeit der Einwilligung durch den Telemedien-Nutzer
- keine Kopplung an andere Rechtsgeschäfte zulässig
- Telemedien-Nutzer ist vor der Erhebung personenbezogener Daten über Art, Umfang und Zweck der geplanten Verarbeitung verständlich zu informieren

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

→ **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)