Datenschutz Datensicherheit

Definition

- Datenschutz:
  unbefugtes Bearbeiten von Daten verhindern
  (Verantworlichkeit liegt beim Datenherrn
  = Inhaber der Datensammlung)
- Datensicherheit:
  Verfügbarkeit, Integrität und
  Vertraulichkeit garantieren
  (Verantwortung liegt beim
  Datenaufbewahrer)

Technisch organisatorische Massnahmen (VDSG Art 8-10&20)

VDSG
Verordnung zum BG über den Datenschutz

- allgemeine Massnahmen
  - Zugangskontrolle
  - Datenträgerkontrolle
  - Transportkontrolle
  - Bekanntgabekontrolle
    (Datenempfänger muss
    autentifiziert werden können)
  - Speicherkontrolle
    (z.B. Arbeitsspeicher)
  - Benutzerkontrolle
    (Wer darf welche Applikation nutzen)
  - Zugriffskontrolle
    (Wer darf welche Daten bearbeiten)
  - Eingabekontrolle
    (wer hat wan was wo geändert)
- Abgangskontrolle
  (Wer nimmt was mit raus)
- Uebermittlungskontrolle
  (wer darf was wohin versenden)
- Auftragskontrolle
  (wurde nur gemacht, was im Auftrag steht)
- Organisationskontrolle
  (Datenschutz/-sicherungsstelle schaffen)

Vorgehen bei der Systemgestaltung

- Risikoerkennung
- Risikobewertung
- Planung, Entscheidung und Realisierung
  von Schutz- und Sicherheitsstufen
  1 - minimales Risiko
  2 - mittleres Risiko
  3 - hohes Risiko
  (4) - sehr hohes Risiko
- Kontrolle

Risiken / Gefahren

- Mensch
  - zufälliger Verlust (z.B.Handling-Fehler)
  - unbefugte oder zufällige Vernichtung
  - technischer Fehler
    (z.B. Bit-Fehler auf Disk)
  - Fälschung, Diebstahl oder
    widerrechtliche Verwendung
  - unbefugtes Aendern, Kopieren,
    Zugreifen oder anderes Bearbeiten
- Natur
  - Feurer
  - Wasser, Lawinen
  - Sturm
  - Erdbeben
  - schlechte Bausubstanz
  - Krieg, Unruhen, Terrorismus
  - Diebstahl

rechtliche Kontrolle

- Kontrollierbarkeit:
  Je sensitiver ein Informationssystem ist,
  desto detaillierter ist die Aufbau- und
  Ablauforganisation festzuhalten.
  => revisionsfähige Protokollierung
- Der Zweck der Datenverarbeitung
  ist verbindlich und darf nicht abgeändert werden
- Art und Umfang der Datenverarbeitung
  - manuell oder mit IT-Sachmitteln
  - Anzahl Aufgabenträger
  - Anzahl und Art der Berechtigungen
- Einschätzen des Risikopotentials
  - Risikoanalyse => Unternehmen kennt mögliche Gefahren
- Gegenwärtiger Stand der Technik
  - regelmässige Kontrolle der Massnahmen,
    da neue Technologien neue Risiken
    bergen