Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 1c)

Vorlesung im Sommersemester 2010

an der Universität Ulm

von Bernhard C. Witt

1. Grundlagen des Datenschutzes

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
✓	Geschichte des Datenschutzes		Anforderungen zur IT-Sicherheit
✓	Datenschutzrechtliche Prinzipien		Mehrseitige IT-Sicherheit
➔	Technischer Datenschutz		Risiko-Management
	Kundendatenschutz		Konzeption von IT-Sicherheit

- Daten, personenbezogene Daten und Informationen
- technische & organisatorische Maßnahmen
- Vorabkontrolle zu Datenschutzrisiken
- Abgrenzungen zur Datensicherheit
- datenschutzfreundliche Techniken

Daten vs Informationen

Grunddilemma: Uneinheitliche Begriffswelt (vor allem zwischen Informatik & Jura)

→**Lösung**: Festlegung von Definitionen!

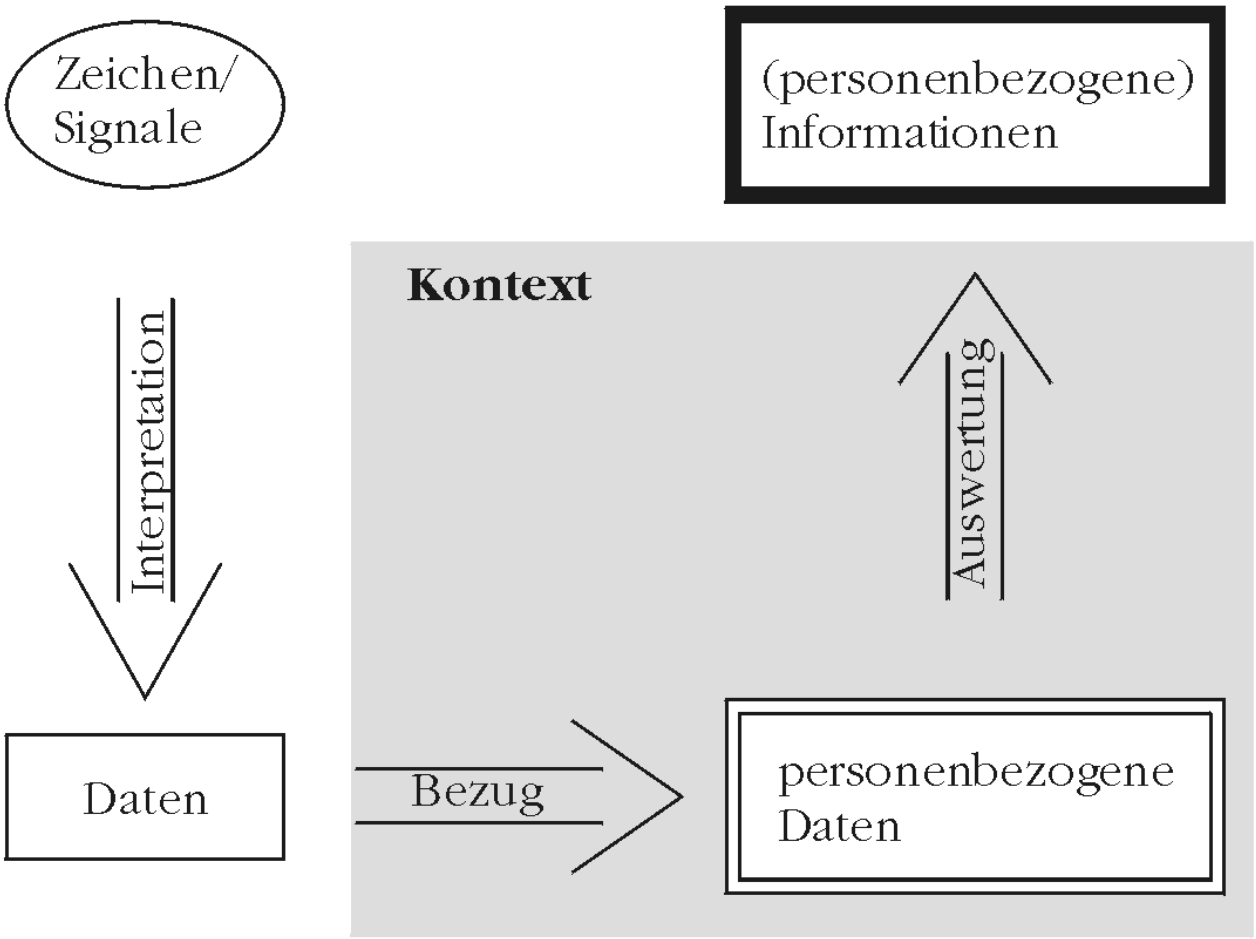
Definition 2: Daten

kontextfreie Angaben, die aus interpretierten Zeichen bzw. Signalen bestehen

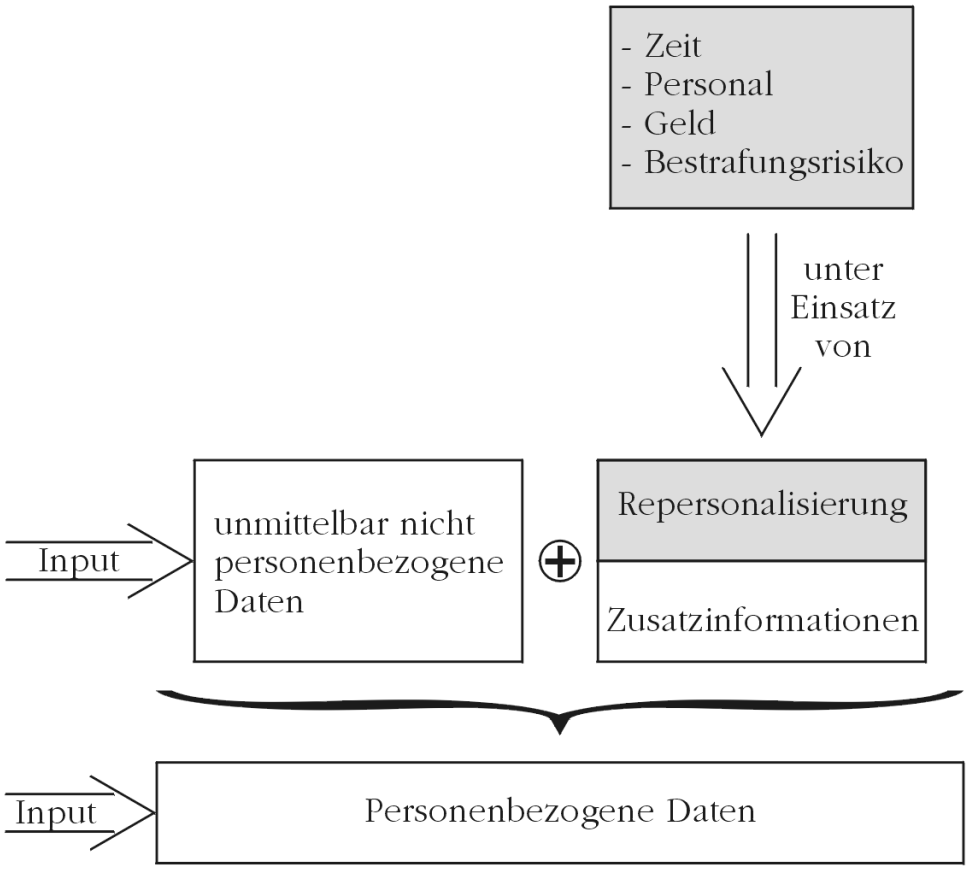
Definition 3: Informationen

Daten, die (durch den Menschen) kontextbezogen interpretiert werden und (prozesshaft) zu Erkenntnisgewinn führen

Vom Datum zur Information



Personenbezogene Daten vs Personenbeziehbare Daten



Technische & organisatorische Maßnahmen zum Datenschutz

- **Zutrittskontrolle**: Einrichtung physischer Schutzzonen
- **Zugangskontrolle**: Nutzung von IT-Systemen erst nach Authentifizierung
- **Zugriffskontrolle**: Zugriff gemäß begründetem Berechtigungs-konzept
- **Weitergabekontrolle**: Einrichtung von Perimeterschutz
- **Eingabekontrolle**: Zuordnung von Verantwortung
- **Auftragskontrolle**: Aufgabenerfüllung gemäß Weisungskette
- **Verfügbarkeitskontrolle**: Schutz der Daten vor Zerstörung oder Verlust
- **Datentrennungskontrolle**: Zweckgebundene & -getrennte Da-tenverarbeitung

→ **Angemessenheit nach Schutzgrad & Verletzlichkeit**

Beispiel für technische & organisatorische Maßnahmen (1)

- **Zutrittskontrolle**:
  - Gebäude nur mittels Chipkartenfreischaltung betretbar
  - Datenserver in besonders geschütztem Server-raum gespeichert, zu dem nur EDV-Personal Zutritt hat
- **Zugangskontrolle**:
  - System nur mittels Eingabe von Benutzerkennung und (regelmäßig zu änderndem) Passwort nutzbar
  - Sicherungsbänder werden im Tresor aufbewahrt (anderer Brandabschnitt)

Beispiel für technische & organisatorische Maßnahmen (2)

- **Zugriffskontrolle**:
  - Zugriffsberechtigt sind nur befugte Benutzer
  - Applikationspasswort weist ausreichende Komplexität auf (8 Stellen, Angabe von Buchstaben, Zeichen und Sonderzeichen obligatorisch)
- **Weitergabekontrolle**:
  - Datentransfer via Internet erfolgt mittels SSLv3
  - LAN durch DMZ vom Internet separiert
  - USB-Port nur für Befugte freigegeben
- **Eingabekontrolle**:
  - Protokollierung von Eingaben, Änderungen und Löschungen

Beispiel für technische & organisatorische Maßnahmen (3)

- **Auftragskontrolle**:
  - Auftragnehmer darf keine Subunternehmer einsetzen
  - Auftraggeber darf jederzeit ergriffene Maßnahmen des Auftragnehmers kontrollieren
- **Verfügbarkeitskontrolle**:
  - Datensätze werden täglich auf Band gesichert
  - Rückeinspielung von Bandsicherungen auch im Notfall erprobt
- **Datentrennungskontrolle**:
  - Applikation mehrmandantenfähig
  - logische Trennung der Datensätze realisiert

Vorabkontrolle

- Sofern automatisierte Verarbeitungen u.U. **besondere Risiken** für die Rechte und Freiheiten der Betroffenen erzeugen können, ist nach § 4d Abs. 5 BDSG eine Vorabkontrolle durchzuführen
- In erster Linie wird dabei die **Rechtmäßigkeit** der geplanten automatisierten Verarbeitung überprüft
- Ein besonderer Augenmerk gilt den vorgesehenen **technischen und organisatorischen Maßnahmen**, die wirksam ein besonderes Risiko vermeiden helfen

→ Vorabkontrolle = Instrument präventiver Compliance

Anlässe für Vorabkontrolle

Checkliste für Vorabkontrolle

- ☐ besondere Arten personenbezogener Daten?
- ☐ Leistungs- / Verhaltens- / Fähigkeitsbewertung?
- ☐ Erstellung Persönlichkeitsprofil?
- ☐ neu entwickelte bzw. hochkomplexe IuK-Technik?
- ☐ Medienwechsel bei vertraulichem Verfahren?
- ☐ gravierende Wirkung auf Betroffenen?
- ☐ verschiedene Zwecke mit einem IT-System?
- ☐ Daten verschiedener Auftraggeber auf einem IT-System?
- ☐ Daten mit Amtsgeheimnis?
- ☐ Personalplanungs-/-informationssystem?
- ☐ CRM-System mit ERP-System vernetzt?

Bestimmung des Datenschutzrisikos

Schutzgrad

Schutzgrad 1 (kein Schutzbedarf):
Daten weisen keinen Personenbezug auf

Schutzgrad 2 (niedriger Schutzbedarf):
ein Personenbezug kann nur mit erheblichem Aufwand hergestellt werden

Schutzgrad 3 (mittlerer Schutzbedarf):
Daten sind mit vertretbarem Aufwand repersonalisierbar oder stammen aus allgemein zugänglichen Quellen

Schutzgrad 4 (hoher Schutzbedarf):
ein Vertraulichkeitsverlust der Daten erzeugt bereits einen Schaden für den Betroffenen, z.B. aufgrund von Zusatzwissen

Schutzgrad 5 (sehr hoher Schutzbedarf):
besonders sensible bzw. aufgrund einer besonderen Schutzverpflichtung geschützte Daten

Eintrittsstufe

Eintrittsstufe 1:
mit einer an Sicherheit grenzenden Wahrscheinlichkeit erfolgt keine Kompromittierung

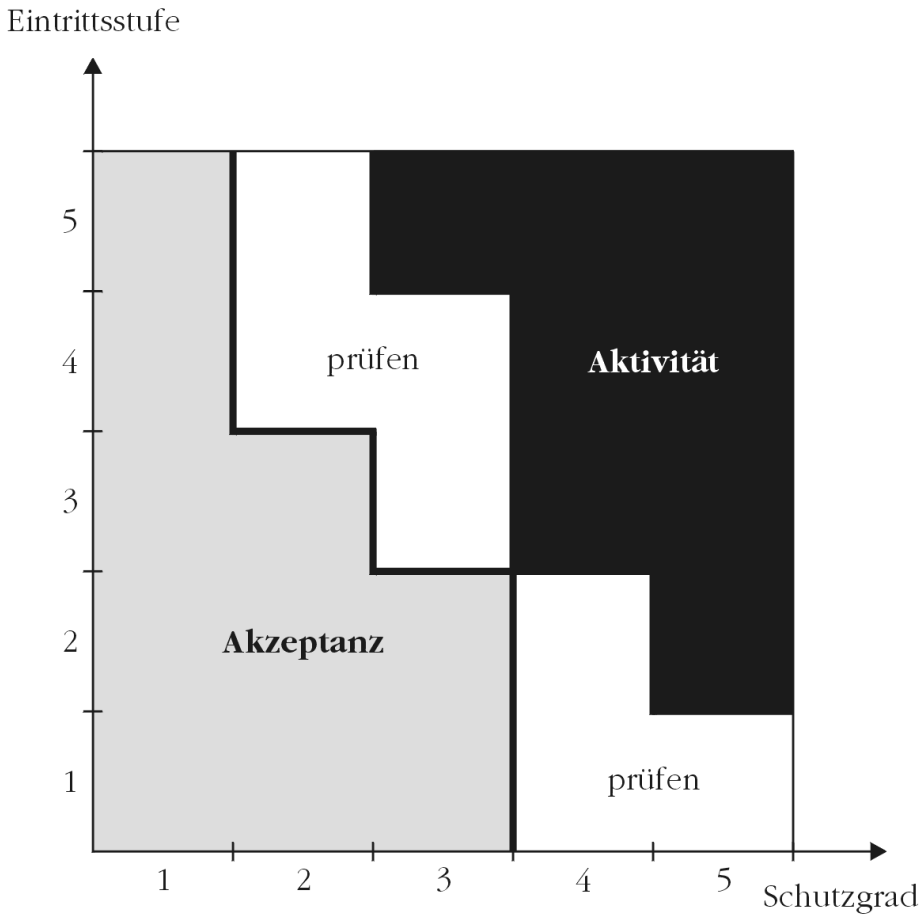
Eintrittsstufe 2:
ein Störer oder Angreifer muss über erhebliche Ressourcen oder Kenntnisse verfügen, um eine Kompromittierung erreichen zu können

Eintrittsstufe 3:
ein Störer oder Angreifer muss über begrenzte Ressourcen oder Kenntnisse verfügen, um eine Kompromittierung erreichen zu können

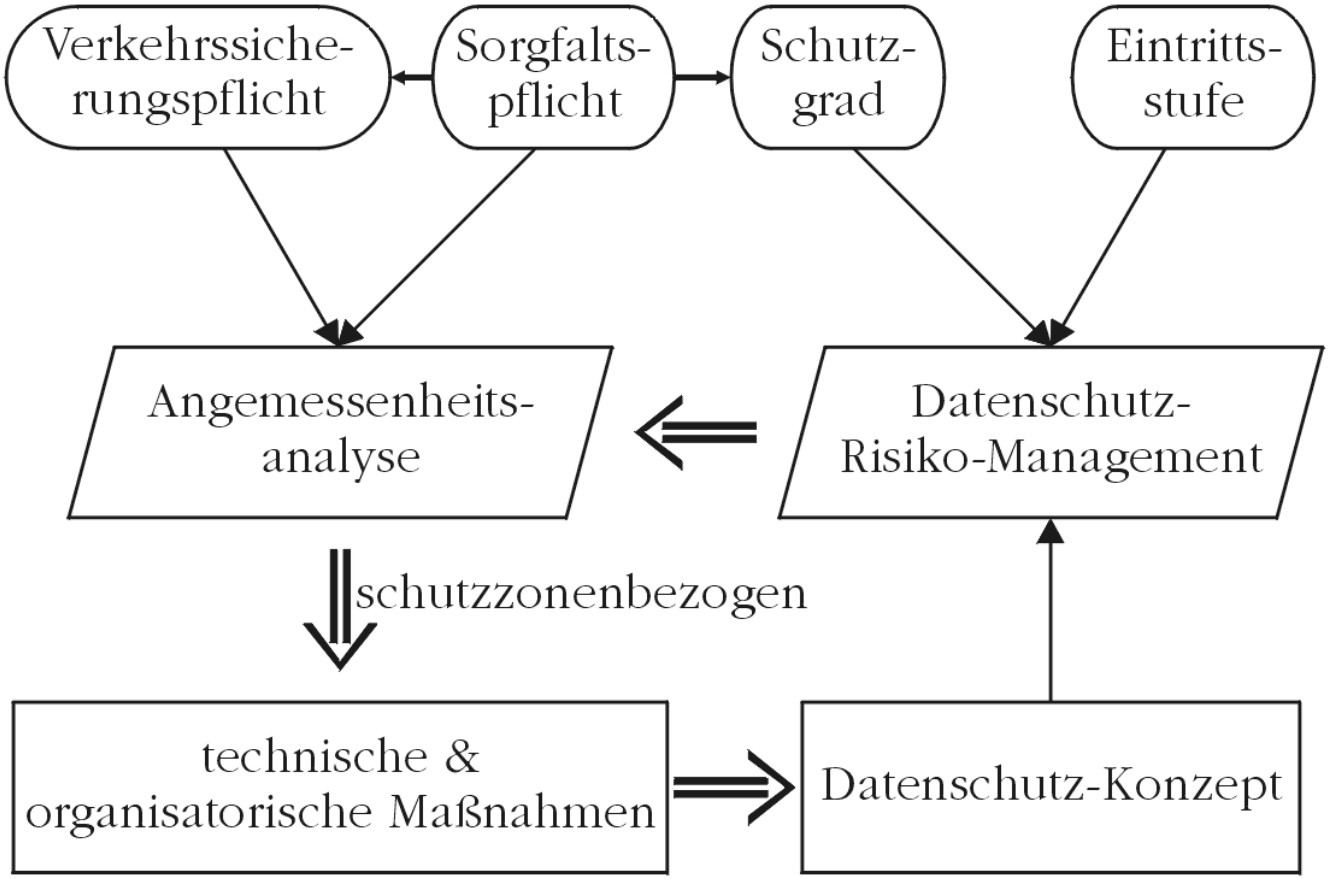
Eintrittsstufe 4:
für eine Kompromittierung sind keine Ressourcen oder Kenntnisse erforderlich, die nicht leicht zu beschaffen sind

Eintrittsstufe 5:
eine Kompromittierung kann bereits aufgrund üblicher Basisausstattungen stattfinden

Umgang mit Datenschutzrisiko



Datenschutzkonzept als Sammlung der Schutzvorkehrungen



Datensicherheit

Definition 4: Sicherheit

Abwesenheit von Gefahren

Definition 5: Datensicherung

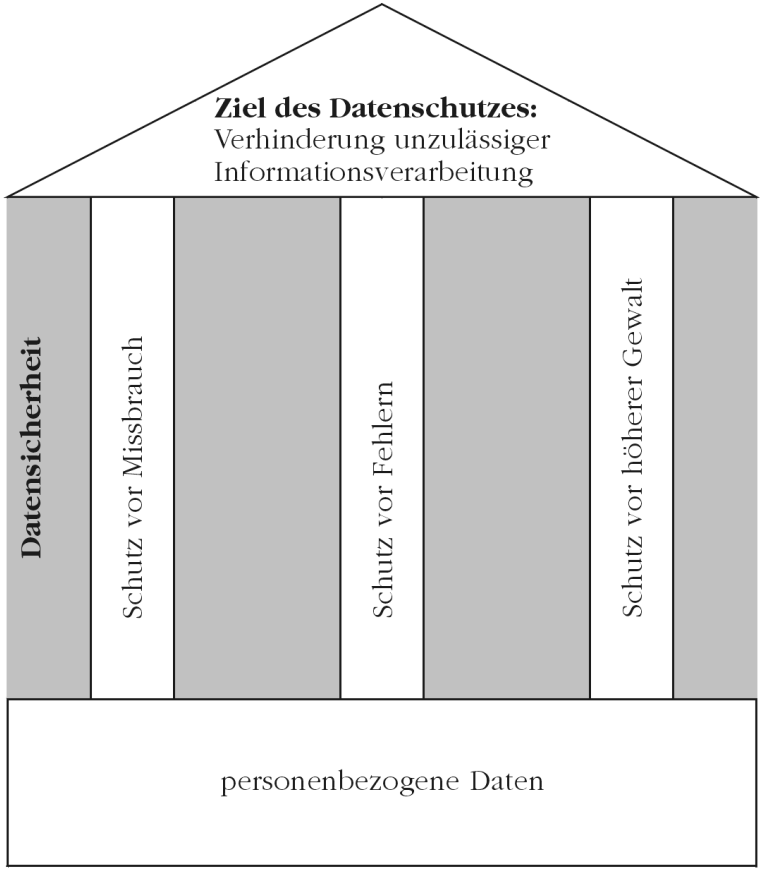
Maßnahmen zur Erhaltung und Sicherung des DV-Systems, der Daten und Datenträger vor Missbrauch, Fehler und höherer Gewalt

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

Definition 6: Datensicherheit

Schutz der gespeicherten Daten vor Beeinträchtigung durch Miss-brauch, menschliche oder technische Fehler und höhere Gewalt

Zusammenhang zwischen Datensicherheit und Datenschutz



Begriff der IT-Sicherheit

Definition 7: 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)
- → IT-Sicherheit zielt auf Schutz der Informationen ab
- → **technische & organisatorische Maßnahmen (= Schutzvorkehrungen) 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 (insbesondere Authentizität und Verbindlichkeit)

→ Berücksichtigung der Interessen aller Beteiligten

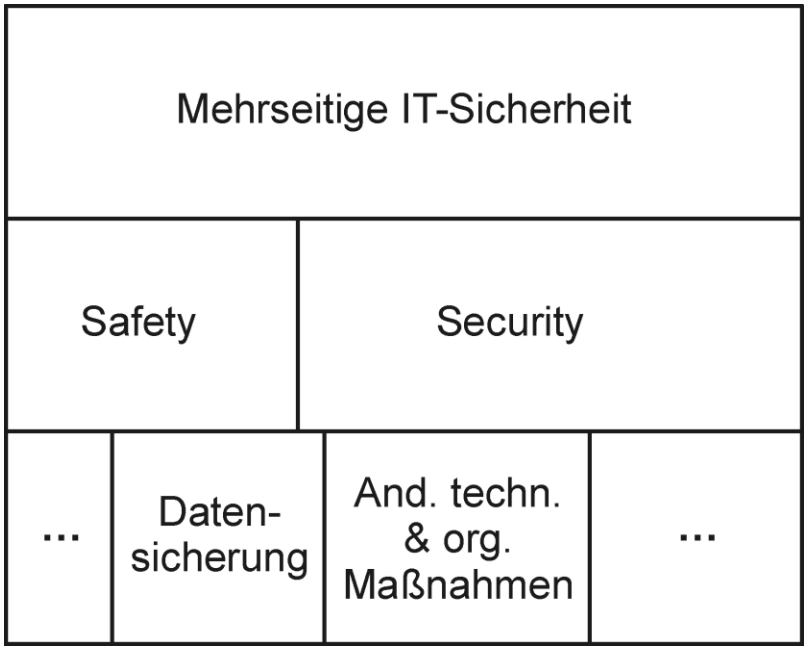
→ Verlässlichkeit und Beherrschbarkeit der IT-Systeme

→ Sicherheit der Systeme und vor den Systemen

Abgrenzung zwischen Datensicherheit & IT-Sicherheit

- Schutz vor unbeab-sichtigten Ereignissen: Safety
- Schutz gegen beabsich-tigte Angriffe: Security

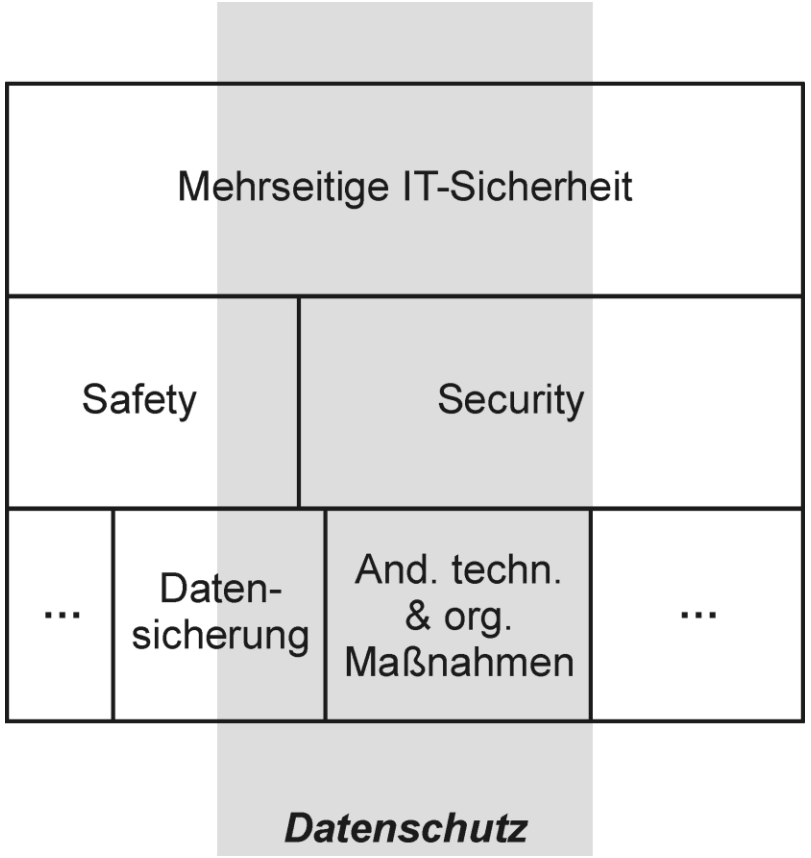
→ **IT-Sicherheit = Safety + Security**



Abgrenzung zwischen Datensicherheit & IT-Sicherheit

Zusammenhang zwischen mehrseitiger IT-Sicherheit und Datenschutz:

- Überschneidung bei der Verarbeitung personen-bezogener Daten
- Schwerpunkt liegt auf Security



Kennzeichen datenschutz-freundlicher Techniken

= Privacy Enhancing Technologies (PET; 1995)

- **Ziel**: weniger Risiken für die Privatsphäre der Betroffenen durch Ausgestaltung eingesetzter Informations- und Kommunikations-technik unter Reduktion des Personenbezugs (→ Anonymität)
- setzt bereits im **Vorfeld** der Verarbeitung personenbezogener Daten an → Datenvermeidung!
- wichtiges Hilfsmittel vorausschauender Technikgestaltung
- unabhängig von etwaigen Rechtsnormen
- Rückwirkung auf rechtliche Entwicklung („Stand der Technik“)
- frühere Bezeichnung: „**Systemdatenschutz**“ (Podlech)

→ datenschutzgerechte & datenschutzfördernde Technik zur strukturellen & systemanalytische Ergänzung des individuellen Rechtsschutzes der Betroffenen

Prinzipien datenschutz-freundlicher Techniken (1)

Datensparsamkeit & Systemdatenschutz

- je weniger personenbezogene Daten herausgegeben werden (müssen), desto leichter lassen sich entsprechende Techniken anwenden

→ nur erforderliche Daten verarbeiten

→ frühestmögliche Anonymisierung

→ frühestmögliche Löschung

→ Verschlüsselung bei Kommunikation

→ Beispiel: prepaid-Chipkarten, Mix-Netz, Transaktionspseudonym (z.B. mit verdeckter Zufallszahl bei elektronischem Geld)

Prinzipien datenschutz-freundlicher Techniken (2)

Selbstdatenschutz & Transparenz

- Selbstbestimmung und –steuerung des Nutzers

→ Nutzer entscheidet selbst, wie anonym er Dienste in Anspruch nimmt

→ Verarbeitung wird verständlich offengelegt (Verfahrensverzeichnis) und ist nachprüfbar (→ Identitätsmanagement)

→ Formulierung eigener Schutzziele

→ Nutzung vertrauenswürdiger Institutionen (Trust Center)

→ Unterstützung durch Anwendung der Betroffenenrechte

→ Beispiel: Platform for Privacy Preferences (P3P auf www.w3.org/P3P/)

Beispiel für datenschutzfreundliche Technik: DC-Netz (1)

Teilnehmer A	
Nachricht:	**1011**
Symm. Schlüssel mit B	1100
Symm. Schlüssel mit C	1001
Übertragung 1	**1110**

Teilnehmer B	
Nachricht:	**0000**
Symm. Schlüssel mit A	1100
Symm. Schlüssel mit C	0101
Übertragung 2	**1001**

Teilnehmer C	
Nachricht:	**0000**
Symm. Schlüssel mit A	1001
Symm. Schlüssel mit B	0101
Übertragung 3	**1100**

Übertragung 1	1110
Übertragung 2	1001
Übertragung 3	1100
Ergebnis:	**1011**

DC-Netz = Dining Cryptographers Network (David Chaum 1988)

- Verfahren zur Anonymität des Senders
- für jedes Nutzbit werden n Schlüsselbits bei n Teilnehmer über unsicheren Kanal gesandt und mittels Vernam-Chiffre (per XOR) summiert
- die Teilnehmer vereinbaren paarweise gemeinsame Schlüssel

Beispiel für datenschutzfreundliche Technik: DC-Netz (2)

Vorteile:

- Verfahren garantiert die Anonymität des Senders
- Vernam-Chiffre macht Verfahren mathematisch beweisbar sicher (nutzt one-time-pad-Eigenschaft)
- aktiver Angreifer kann aufgespürt werden, da der Sender den korrekten Wert der überlagerten Nachricht kennt und überprüfen kann

Nachteile:

- Austausch der paarweisen Schlüssel muss sicher erfolgen
- eignet sich nur für die Kommunikation einer beschränkten Gruppe, bei der alle Teilnehmer kommunizieren müssen
- Verfahren muss synchronisiert ablaufen

Andere datenschutz-freundliche Techniken

- **MIX-Netz**: Kommunikation wird über einen Nachrichtenvermittler (Zwischenknoten) abgewickelt, der genügend viele Datenpakete von genügend vielen Sendern sammelt und leitet diese so verändert weiter, dass außer Sender oder MIX-Station keiner die Pakete zuordnen kann. (Empfänger-Anonymität durch „anonyme Rückadressen“ realisierbar) → asynchrone Kommunikation
- anonymisierende Proxies (z.B. anonymizer.com, rewebber.com)
- Verfahren mit Berücksichtigung von Verkehrsanalysen (z.B. AN.ON/JAP = MIX-Netz unter JAP.inf.tu-dresden.de)
- Cookie-Austausch (z.B. CookieCooker.de) bzw. Cookie-Filter (z.B. webwasher.com)