

# Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 2)

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

## Teil 2: Grundlagen der IT-Sicherheit

### **1. Einflussfaktoren zur IT-Sicherheit**

#### **1.1 Einflussfaktor Recht**

- 1.1.1 Sorgfaltspflicht
- 1.1.2 Datenschutz & Fernmeldegeheimnis
- 1.1.3 spezialrechtliche Vorgaben & vertragsrechtliche Verpflichtungen

#### **1.2 Einflussfaktor Technik**

- 1.2.1 Bedeutung von Informationen & IuK-Technik
  - \* Eigenschaften des Rohstoffs „Information“
  - \* Fortentwicklung der Technik
- 1.2.2 Internationale Normen & best-practice-Standards

#### **1.3 Einflussfaktor Unternehmensspezifika**

- 1.3.1 Branchenzugehörigkeit & Marktstellung
- 1.3.2 innerbetriebliche Organisation

# Teil 2: Grundlagen der IT-Sicherheit

## 2. Mehrseitige IT-Sicherheit

### 2.1 Einordnung mehrseitiger IT-Sicherheit

2.1.1 Geschichte und Übersicht

2.1.2 Definition & Grundsätze mehrseitiger IT-Sicherheit

2.1.3 Ziele mehrseitiger IT-Sicherheit

- \* Verlässlichkeit von IT-Systemen (Verfügbarkeit, Integrität, Vertraulichkeit)

- \* Beherrschbarkeit von IT-Systemen (Zurechenbarkeit, Rechtsverbindlichkeit)

2.1.4 Unterscheidung zwischen Safety & Security

# Teil 2: Grundlagen der IT-Sicherheit

## 2. Mehrseitige IT-Sicherheit (Forts.)

### 2.2 Analyse mehrseitiger IT-Sicherheit

2.2.1 Berechnung der Verfügbarkeit

- \* Einzelverfügbarkeiten von IT-Komponenten & Diensten

- \* Verfügbarkeiten von IT-Systemen

- \* Verfügbarkeit redundanter IT-Systeme

2.2.2 Analyse von Ausfallzeiten

2.2.3 Verlust der Vertraulichkeit

2.2.4 Verschlüsselung

- \* Ende-zu-Ende-Verschlüsselung vs. Verbindungsverschlüsselung

- \* symmetrische Verschlüsselung vs. asymmetrische Verschlüsselung

2.2.5 Sicherung der Integrität

2.2.6 Authentifizierungsverfahren

# Teil 2: Grundlagen der IT-Sicherheit

## **3. Risiko-Management**

### **3.1 Risiko-Identifikation**

#### 3.1.1 Bedrohungsanalyse

- \* Beispiele für Bedrohungen der IT-Sicherheit
- \* Mögliche Gegenmaßnahmen
- \* Unterscheidung in aktive und passive Angriffe

### **3.2 Risiko-Analyse**

#### 3.2.1 Fehlerbaum-Analyse

#### 3.2.2 Angriffsbaum-Analyse

#### 3.2.3 Fehlermöglichkeits- und -einflussanalyse

#### 3.2.4 Ergebnis: Festlegung des Schutzbedarfs

# Teil 2: Grundlagen der IT-Sicherheit

## **3. Risiko-Management (Forts.)**

### **3.3 Risiko-Bewertung**

#### 3.3.1 Risikomatrix bzw. Risikotabelle

#### 3.3.2 Risikoportfolio bzw. Risk-Map

#### 3.3.3 SWOT-Analyse & Balanced Score Card

### **3.4 Risiko-Behandlung**

#### 3.4.1 Bestimmung der Akzeptanzlinie

#### 3.4.2 Bestimmung des Restrisikos

#### 3.4.3 Zusammenspiel mit IT-Sicherheits-Management

# Teil 2: Grundlagen der IT-Sicherheit

## 4. Konzeption von IT-Sicherheit

### 4.1 Erstellung sicherer IT-Systeme

#### 4.1.1 Software-Erstellung gemäß standardisierter Vorgehensweisen

- \* V-Modell XT
- \* Software-Qualität nach DIN 9126
- \* formaler Nachweis zur Korrektheit

#### 4.1.2 allgemeine Konstruktionsprinzipien

#### 4.1.3 Prinzipien für Sicherheitsprozesse

# Teil 2: Grundlagen der IT-Sicherheit

## 4. Konzeption von IT-Sicherheit (Forts.)

### 4.2 Gestaltung der IT-Infrastruktur

#### 4.2.1 Berücksichtigung gängiger Standards

- \* IT-Grundschutz-Kataloge des BSI
- \* Informationssicherheitsmanagement nach ISO/IEC 17799 & 27001
- \* ITIL

#### 4.2.2 Architektur von IT-Systemen

#### 4.2.3 Notfall-Vorsorge-Konzept

#### 4.2.4 laufender Betrieb von IT-Systemen

#### 4.2.5 Sicherheitsleitlinie

#### 4.2.6 Management der Netzwerksicherheit

#### 4.2.7 physischer Schutz & Sicherung der Authentisierung

# Teil 2: Grundlagen der IT-Sicherheit

## **4. Konzeption von IT-Sicherheit (1. Forts.)**

### **4.3 Praktische Anwendungen zur IT-Sicherheit**

4.3.1 Voice over IP

4.3.2 WLAN

4.3.3 DMZ

4.3.4 Sicherheitskonzept am Beispiel der Telearbeit

### **4.4 Datenschutzfreundliche Techniken**

4.4.1 Kennzeichen datenschutzfreundlicher Techniken

4.4.2 Prinzipien datenschutzfreundlicher Techniken

4.4.3 Beispiele für datenschutzfreundliche Techniken