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

Gliederung zur Vorlesung im
Sommersemester 2008
an der Universität Ulm
von Bernhard C. Witt

Teil 2: Grundlagen der IT-Sicherheit

1. Anforderungen 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 Eigenschaften des Rohstoffs „Information“

1.2.2 Fortentwicklung der Technik

1.2.3 Stand der Technik

1.2.4 Relevanz internationaler 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
* Verfügbarkeit redundanter IT-Systeme
* Verfügbarkeiten gesamter 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 vs. asymmetrische Verschlüsselung

2.2.5 Sicherung der Integrität

2.2.6 Authentifizierungsverfahren

Teil 2: Grundlagen der IT-Sicherheit

Teil 2: Grundlagen der IT-Sicherheit

3. Risiko-Management (Forts.)

3.3 Risiko-Analyse

3.3.1 Fehlerbaum-Analyse

3.3.2 Angriffsbaum-Analyse

3.3.3 Fehlermöglichkeits- und -einflussanalyse

3.3.4 Ergebnis: Festlegung des Schutzbedarfs

3.4 Risiko-Bewertung

3.4.1 Risikomatrix bzw. Risikotabelle

3.4.2 Risikoportfolio bzw. Risk-Map

3.4.3 SWOT-Analyse & Balanced Score Card

Teil 2: Grundlagen der IT-Sicherheit

3. Risiko-Management (2. Forts.)

3.5 Risiko-Behandlung

3.5.1 Bestimmung der Akzeptanzlinie

3.5.2 Bestimmung des Restrisikos

3.5.3 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 von 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 2700x
* Business Continuity Management nach BS 25999
* ITIL v2

4.2.2 Architektur der IT-Infrastruktur

4.2.3 Erstellung eines Notfall-Vorsorge-Konzepts

4.2.4 Erstellung eines Notfallplans

4.2.5 IT-Sicherheit im laufenden Betrieb

4.2.6 Erstellung einer Sicherheitsleitlinie (security policy)
* Allgemeines Sicherheitskonzept
* Spezifisches Sicherheitskonzept (am Beispiel Telearbeit)

Teil 2: Grundlagen der IT-Sicherheit

4. Konzeption von IT-Sicherheit (2. Forts.)

4.2 Gestaltung der IT-Infrastruktur

4.2.7 Management der Netzwerksicherheit
* ISO 7498-2
* ISO/IEC 18028-1
* Gestaltung von Firewalls

4.2.8 physischer Schutz & Sicherung der Authentisierung
* Password
* Chipkarte
* Biometrie

4.2.9 Zugriffskontrolle
* Access Control List
* Capability List

4.2.10 Folgen des § 202c StGB