Netzwerksicherheit

Risikoanalysen und Sicherheitspolitiken

Stephen Wolthusen

Fraunhofer IGD Institut Graphische Datenverarbeitung

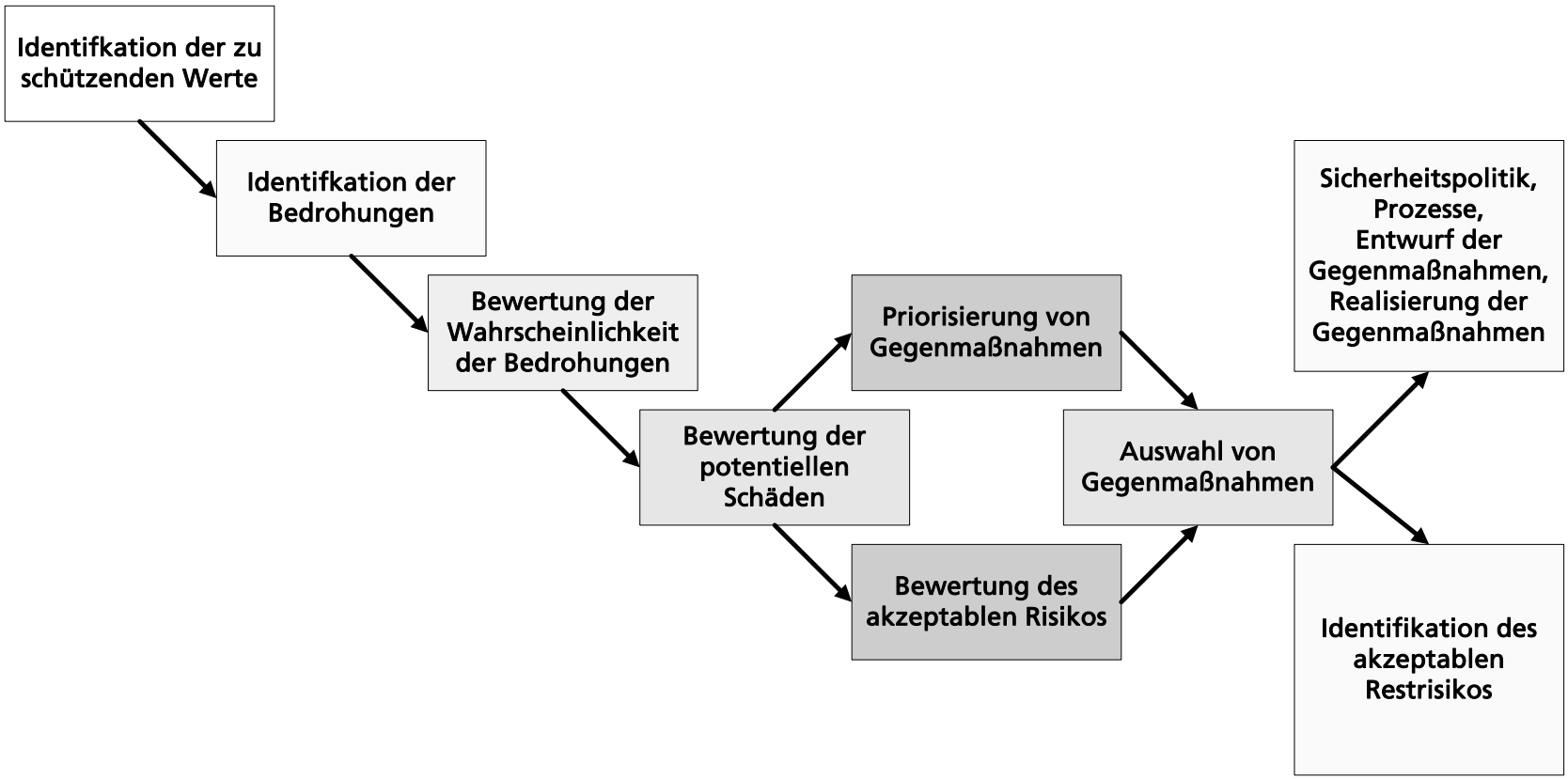
Themen

- Risikoanalyse
  - Methodik
  - Verfahren für Risikoanalysen
- Organisatorische Sicherheitspolitiken
  - Notwendigkeit
  - Einflußbereich
- Rechtliche Aspekte
  - Einschränkungen des technisch Machbaren
  - Verfolgungsmöglichkeiten

If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization

(Gerald M. Weinberg)

Methodik für Risikoanalysen



Identifikation von Werten: Kategorien

- Vertrauliche Informationen
- Verfügbarkeit von Diensten und Ressourcen (z.B. Geschäftsprozesse)
- Integrität von Informationen
- Ausrüstung
- Personal
- Problem: Identifikation von Abläufen, Informations- und Interaktionsbeziehungen ist meist unzureichend bekannt
- Gefahren durch übersehene Abhängigkeiten

Bedrohungen und Eintrittswahrscheinlichkeiten

- Identifikation der Charakteristiken, Quellen, Wahrscheinlichkeiten von Bedrohungen
  - Rückkoppelung durch Einführung von Gegenmaßnahmen
- Bedrohungswahrscheinlichkeit ist Maß für Wahrscheinlichkeit, daß Bedrohung in konkreten Angriff umgesetzt wird
- Quelle muß Fähigkeiten, Motivation potentieller Angreifer berücksichtigen
- Quantitative Bewertung analog zur Versicherungsmathematik:

  r = p • s (Risiko = Eintrittswahrscheinlichkeit • Schadenswert)

Qualitative Bewertung von Bedrohungen

- Quantitative Bewertung häufig schwierig, daher besser explizit qualitativ bewerten.
- Erfordert Dokumentation für Wahrscheinlichkeitsbänder, z.B.:
  - Vernachlässigbar (nicht plausibel)
  - Sehr niedrig (2-3 Ereignisse/Jahr)
  - Niedrig (Seltener als 1 Ereignis/Jahr)
  - Mittel (Seltener als 1 Ereignis in 6 Monaten)
  - Hoch (Seltener als 1 Ereignis/Monat)
  - Sehr Hoch (Mehrere Ereignisse/Monat)
  - Extrem (Mehrere Ereignisse/Tag)

Qualitative Bewertung: Folgenabschätzung

- Schäden müssen getrennt von Eintrittswahrscheinlichkeit bewertet werden. Qualitative Aussagen sind auch hier möglich:
  - Gering (kaum erkennbare Beeinträchtigung)
  - Signifikant (meßbare Schäden, Kreis der Betroffenen begrenzt)
  - Erheblich (Beseitigung erfordert erhebliche Mittel, Reputation der Systemverwaltung/der Organisation wird beeinträchtigt)
  - Ernst (dauerhafte Ausfälle, Zerstörung von Ressourcen, Kompromittierung sensibler Informationen, Vertrauensverlust)
  - Katastrophal (vollständiger Ausfall, Kompromittierung kritischer Informationen, dauerhafter Verlust von Ressourcen)

Restrisiko und Gegenmaßnahmen

- Restrisiko
  - Risiko, daß verantwortliche Stelle zu tragen bereit ist
- Erforderliche Aufwendungen für Gegenmaßnahmen vs. Schäden bei Eintritt des Ereignisses
  - Gegenmaßnahmen müssen auf Effizienz und Effektivität regelmäßig geprüft werden
- Bei Bedrohungen mit hohen Folgekosten und geringer Eintrittswahrscheinlichkeit kann eine Versicherungspolice günstig sein

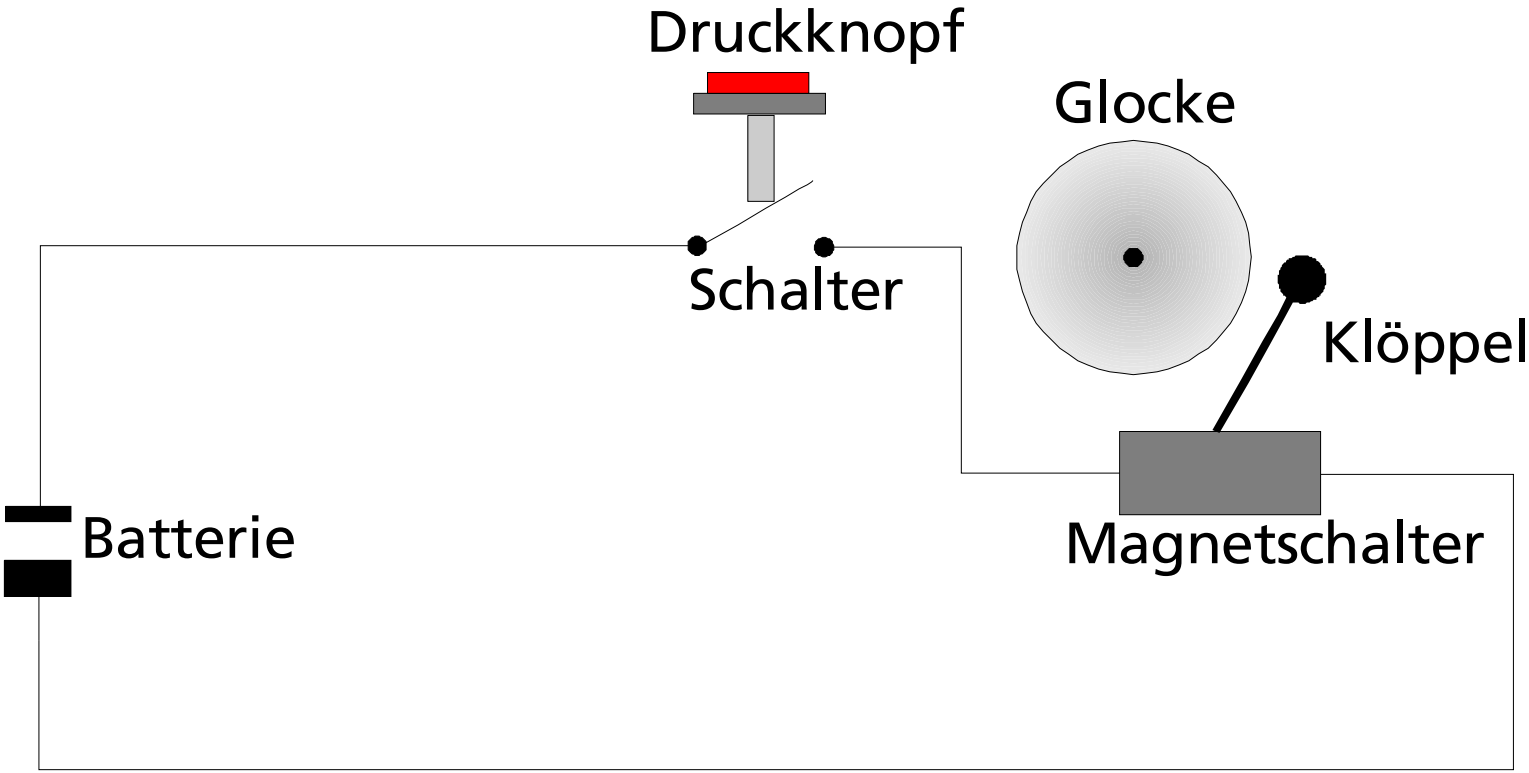
Techniken für die Durchführung von Risikoanalysen

- Techniken sind seit langem bekannt und werden in anderen Ingenieursdisziplinen angewandt
  - FTA (Fault Tree Analysis)
  - FMEA (Failure Mode and Effects Analysis)
  - HAZOP (Hazard and Operability Analysis)
  - CCA (Cause Consequence Analysis)
  - MORT (Management Oversight Risk Tree)
  - FIPS 191 (Guidelines for the Analysis of Local Area Network Security)

Begriffe der Fehleranalyse

- Fehlermechanismus
  - Art, in der ein Fehlermodus eintreten kann, evtl. auch Eintrittswahrscheinlichkeit
- Fehlermodus
  - Teilaspekte von Komponentenfehlern, die von Interesse für den betrachteten Fehler sind
- Fehlereffekt
  - Auswirkungen eines Fehlers auf das System

Beispiel: Klingel



Fehlermodi des Systems

- Klingel läutet nicht, wenn Knopf gedrückt wird
- Klingel läutet, obwohl Knopf nicht gedrückt ist
- Klingel läutet weiter, nachdem Knopf losgelassen wurde
- Reduktion der Fehlermechanismen des Systems auf Fehlermodi der Subsysteme:
  - Druckknopf
  - Klingel
  - Magnetschalter
  - Batterie
  - Verdrahtung

Fehlermodi der Subsysteme

- Druckknopf
  - Stromkreis wird bei Betätigung nicht geschlossen
  - Stromkreis wird bei Loslassen nicht unterbrochen
  - Stromkreis schließt ohne Betätigung
- Klingel und Magnetschalter läuten nicht, obwohl Stromzufuhr gegeben ist (auch: Läuten wird bei anhaltender Stromzufuhr unterbrochen)
- Batteriespannung zu niedrig
- Stromkreisunterbrechung, Kurzschluß

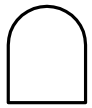
Analyse der Fehlermechanismen

Fehlereffekt	Fehlermodus	Fehlermechanismus
Stromkreis wird bei Betätigung des Knopfs nicht geschlossen	Kontaktpunkte defekt Kontaktwiderstand zu hoch	Mechanischer Schock Korrosion
Klingel, Magnetschalter läuten nicht	Schalter defekt, hängt Klöppel defekt Klöppel hängt Magnet zu schwach	Offener Schaltkreis in Magnetschalter Mechanischer Schock Korrosion Kurzschluß in Magnet-schalter
Batteriespannung zu niedrig	Kein Elektrolyt Positiver Pol defekt	Defektes Gehäuse Mechanischer Schock

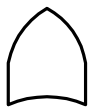
Fehlerbäume: Konstruktionsregeln

- System-Fehlermodi werden als „Top Events“ bezeichnet
- Wähle ein Top-Event aus, untersuche **unmittelbare** Ursachen für das Eintreten
  - Ursachen sind unmittelbare Fehlermechanismen für den ausgewählten Systemfehler (i.d.R. Subsystemfehler)
    - Unmittelbare, notwendige, hinreichende Gründe
  - Dies sind Fehlermodi der Subsysteme, d.h. 2. Ebene des Fehlerbaumes etc.
  - Unterste Ebene: Komponentenfehler (atomare Elemente)

Fehlerbäume: Elemente 1

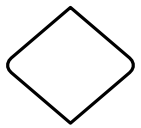


- Logisches AND
  - Alle Ereignisse an den Eingängen müssen gleichzeitig stattfinden



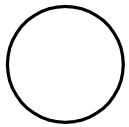
- Logisches OR
  - Mindestens ein Ereignis muß eintreffen

- Hauptereignis
  - Entstehen durch Verknüpfung elementarer Ereignisse

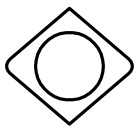


- Grundereignis 1
  - Element wird nicht weiter ausgearbeitet, maximale Betrachtungstiefe ist erreicht

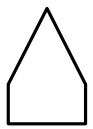
Fehlerbäume: Elemente 2



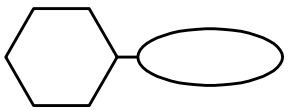
- Grundereignis 2
  - Wird nicht weiter ausgearbeitet, elementares Ereignis



- Teilbaum
  - Hier nicht weiter ausgearbeitet; Kreis im Inneren gibt an, daß dies in separatem Diagramm geschieht

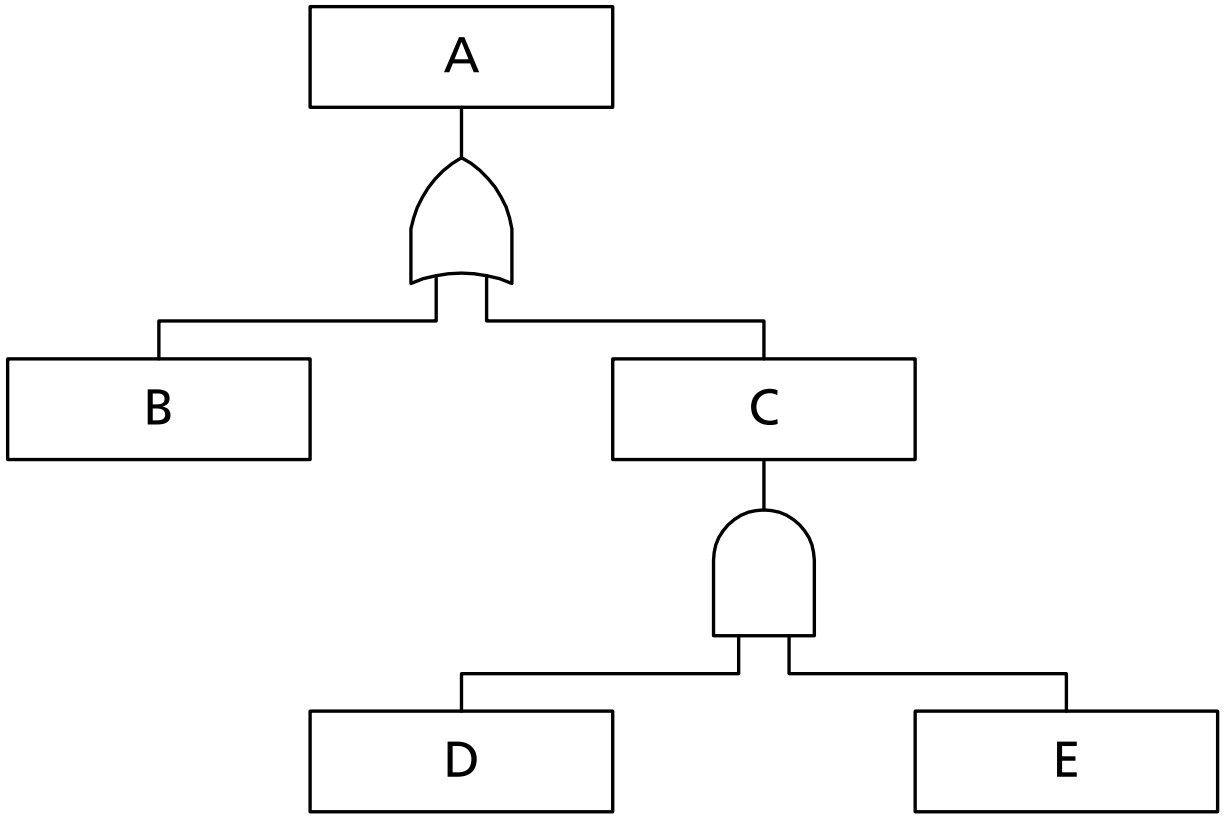


- Switch
  - Selektive Aktivierung eines Fehlerbaums



- Inhibit
  - Kausalzusammenhang: Ereignis wenn Bedingung

Fehlerbaum: Beispiel



Die Sicherheitspolitik: Umfang und Elemente

- Erforderlich u.a. aufgrund rechtlicher Rahmenbedingungen
- Problem: Balance zwischen Abstraktion und Umsetzbarkeit
- Inhalt:
  - Definition der Zielsetzungen, Umfang
  - Aussage über Zielsetzung der Geschäftsführung
  - Erläuterungen der Sicherheitspolitik, Richtlinien, Standards
    - Einhaltung vertraglicher Verpflichtungen
    - Einhaltung gesetzlicher Bestimmungen
    - Aus-, Fortbildung der Mitarbeiter

Die Sicherheitspolitik: Inhalt

- Inhalt (fortges.):
  - Vorbeugung, Erkennung von Viren, Trojanern
  - Verfügbarkeitsplanung
  - Konsequenzen und Sanktionen bei Verletzung der Politik
  - Bestimmung der Verantwortung für Sicherstellung der IT-Sicherheit
  - Verweise auf weiterführende Dokumente
    - Bereichsspezifische Sicherheitspolitiken
    - Technische Realisierung

Organisation und Verantwortung

- Spezifische Rollen, Verantwortung einzelner Stellen und Personen für Sicherheit
- Festlegung von Methoden und Verfahren (z.B. für Risikoanalyse)
- Weiterführende Maßnahmen (Mitarbeiter-Schulungen)
- Fortschreibungs-Mechanismen für neue IT-Vorhaben
- Mechanismen für Bewertung von technischen Umsetzungen der Sicherheitspolitik
- Verfahren für Umsetzung, Beurteilung der Wirksamkeit
- Vorgehen für Aufnahme, Analyse von Sicherheitsvorfällen

Klassifizierungsmechanismen

- Identifikation einzelner Werte, Zuweisung von Verantwortlichen
  - Informations-Werte
  - Software
  - Physische Werte
  - Externe Dienstleistungen
- Klassifizierung von Werten (Information) nach Sensibilität
  - Umgang mit Daten, Datenträgern nach Grad der Klassifizierung (nicht nur Geheimschutz!)
  - Verwahrdauer, Sicherstellung der Datenintegrität
  - Deklassifizierungsrichtlinien

Personal

- Richtlinien zur IT-Sicherheit müssen Bestandteil des Arbeitsvertrages werden.
  - Regeln zur privaten Nutzung von Rechnern, Netzwerk
- Bei Vertrauenspositionen (System-, Netzwerk, FW-Administrator)
  - Prüfung der Angaben von Bewerbern, Referenzen
  - Prüfung der finanziellen Verhältnisse (unregelmäßig)
- Einbeziehung aller Mitarbeiter
  - Nicht nur Verbote, auch Begründung für Regeln
  - Benachrichtigung bei Anomalien durch Mitarbeiter

Physische Sicherheit

- Geschichtete Struktur, Tiefenstaffelung
- Regelungen für Zugang durch Dritte (Wartung, Reinigung, Mitarbeiter anderer Unternehmen)
- Position, Zugriffsregeln für bei ISP positionierte Infrastruktur
- Schutz von Versorgungsdienstleistungen (Strom, Klima)
- Handhabung mobiler Geräte
- Schutz vor direktem Zugriff auf Netzwerkverkabelung, drahtlose Netzwerke
  - WLANs, Bluetooth etc. ermöglichen auf Sichtlinie Angriffe

Laufender Betrieb (1)

- Dokumentation von Betriebsvorgängen
  - Verarbeitung von Daten, insbesondere personenbezogene
  - Abhängigkeiten von Systemkomponenten untereinander
  - Zeitfenster für Wartungsarbeiten
  - Handlungsanweisungen für Fehler, Ausnahmebedingungen
  - Kontaktinformationen für Mitarbeiter, auch im Urlaubsfall
  - Handhabung der Ausgaben des Systems
    - Ausdrucke, Datenträger, Altsysteme
    - Richtlinien für Vernichtung sensibler Daten

Laufender Betrieb (2)

- Formalisierung der Verfolgung von Änderungen am System
  - Identifikation, Protokollierung signifikanter Änderungen
  - Prüfung der Auswirkung auf andere Komponenten
  - Formale Abnahme vorgeschlagener Änderungen
  - Mitteilung über zu erfolgende Änderungen an alle (vorab) identifizierten Betroffenen
  - Vorgehen, Verantwortung für den Fall, daß Änderung rückgängig gemacht werden muß

Laufender Betrieb (3)

- Formalisierung der Vorgehensweise bei Ausfällen, Sicherheitsproblemen
  - Art der zu erfassenden Vorfälle
  - Planung für Wiederaufnahme des Normalbetriebes
    - Analyse der Ursache
    - Vermeidung von Wiederholungen
    - Benachrichtigung von Aufsichts-, Strafverfolgungsbehörden
  - Sicherung von Protokoll- und Revisionsdaten
  - Vorgehen bei Maßnahme für Wiederaufnahme

Zugriffskontrollmechanismen

- Zugriffsrechte sollen nur aus operativen Anforderungen heraus vergeben werden
  - Notwendigkeit der Identifikation von Geschäftsprozessen
- Einrichtung neuer Nutzerkennungen nur mit Zustimmung des Verantwortlichen für den Nutzer
  - Protokollierung von Anlegen, Sperren, Löschen
- Hinweis auf Sicherheitsrichtlinien, Protokollierung, Untersagung der Nutzung von Gruppenkennungen
- (Netzwerk-)Dienste nur auf explizite operative Anforderung

Rechtliche Aspekte

- Die Administration der IT-Systemsicherheit erfolgt nicht in einem rechtlichen Vakuum
  - Sowohl das Unternehmen als auch Einzelpersonen obliegen Sorgfaltspflichten
  - Insbesondere bei Revisionsdaten sind in Deutschland (noch?) enge Grenzen für personenbezogene Daten gesetzt
  - Die Verfolgungsmöglichkeiten bei Angriffen oder auch internen Vergehen im Strafrecht sind Antragsdelikte
- Hier werden nur für Deutschland relevante Bestimmungen vorgestellt; bei multinationalen Netzwerken müssen u.U. auch darüber hinaus örtliche Bestimmungen beachtet werden

Das KonTraG

- „Artikel-Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“: Im April 1998 verabschiedet
  - Setzt OECD-Richtlinie „Principles of Corporate Governance“ um
  - Verschärft die Sorgfaltspflichten von Vorständen und Ge-schäftsführern, das bereits im AktG (§93 Abs. 1) enthalten ist
  - Das Aktiengesetz regelte bereits:
    - Festlegung der Unternehmenspolitik, Implementierung einer funktionsfähigen Unternehmensüberwachung
  - GmbHs, OHGs, KGs sind AGs aufgrund KapCoRiLiG „Kapital-gesellschaften und Co-Richtlinie-Gesetz“ gleichgestellt
- Ähnliche Auswirkungen gehen auch von den neuen EU-weiten Kreditvergaberichtlinien („Basel II“) aus

KonTraG: Anwendungsbereich

- Betroffen sind AGs und Gesellschaften, die mindestens zwei von drei Kriterien erfüllen:
  - Bilanzsumme größer 3.44 Mio. Euro
  - Umsätze größer 6.87 Mio. Euro
  - Mehr als 50 Mitarbeiter
- Mit dem KonTraG werden Gesellschaften verpflichtet,
- „... geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig erkannt werden“ (§91 Abs. 2)

Risikomanagementsystem gemäß KonTraG

- Umsetzung wird von unabhängigen Wirtschaftsprüfern im Rahmen des Jahresabschlusses geprüft
- Phasenmodell für Umsetzung:
  - Bestimmung der Beobachtungsbereiche
  - Risikoanalyse
  - Risikoaggregation
  - Risikobewältigung
  - Systemarchitektur
  - Systemgestaltung und Implementierung

Das Bundesdatenschutzgesetz

- Auffanggesetz, gilt für öffentliche Stellen und Private
- Erste Gesetzgebung 1970 in Hessen; erste Fassung des BDSG im Januar 1977.
- Erste Novellierung 1990 aufgrund des BVerfG-Urteils zur Volkszählung: „Recht auf informationelle Selbstbestimmung“, Änderungen durch Begleitgesetz zum Telekommunikations-gesetz
- 2. Novellierung im Mai 2001 aufgrund der EU-Datenschutz-richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom Oktober 1995 (Ergänzung EU-Datenschutzkonvention 1981)

Allgemeine Bestimmungen des BDSG

- Erhebung personenbezogener Daten:
  - Verbot mit Erlaubnisvorbehalt
  - erfordert Rechtsvorschrift oder Zustimmung des Betroffenen
  - Einwilligung hat in Schriftform zu erfolgen
    - z.B. besonders hervorgehobener Abschnitt in Nutzungsbedingungen
  - Es besteht Meldepflicht für die Einrichtung „automatisierter Verarbeitungseinrichtungen“ bzw. Bestellung eines Daten-schutzbeauftragten
  - Bei Mißachtung besteht u.a. Schadensersatzpflicht

Datenverarbeitung öffentlicher Stellen

- Rechte der Betroffenen
  - Auskunftsrecht, Recht auf Berichtigung, Löschung, Sperrung
    - Auskunftsrecht nicht bei Verarbeitung durch Dienste, bei Gefährdung ordnungsgemäßer Erfüllung der Aufgaben
  - Benachrichtigungspflicht
    - Betroffene müssen von Speicherung, Identität der verantwortlichen Stelle, Zweckbestimmung benachrichtigt werden
- Einrichtung des Bundesdatenschutzbeauftragten
  - Kontrolle öffentlicher Stellen, vom Bundestag bestellt

Datenverarbeitung nichtöffentlicher Stellen

- Erhebung, Verarbeitung, und Datennutzung für eigene Zwecke sind nur zur Erfüllung von vertragsähnlichen Vertrauens-verhältnissen oder zur Wahrung berechtigter Interessen gestattet
- §31 erlaubt Verarbeitung und Erfassung personenbezogener Daten, um Datenschutzkontrolle, Datensicherung, oder um den ordnungsgemäßen Betrieb des IT-Systems zu ermöglichen
- Betroffene haben ein Recht auf
  - Benachrichtigung bei Erhebung
  - Auskunft: Herkunft, Empfänger, Zweck der Speicherung
  - Berichtigung, Sperrung, Löschung (Korrekturpflicht)

Bußgeld- und Strafvorschriften

- §43: Zuwiderhandlungen werden als Ordnungswidrigkeiten aufgefaßt; Obergrenze in schweren Fällen liegt bei DM 200,000
- §44: Vorsätzliche Zuwiderhandlungen gegen Entgelt oder mit Bereicherungsabsicht oder der Absicht einen anderen zu schädi-gen kann mit Freiheitsstrafe bis zwei Jahren bestraft werden
- Straftaten nach §44 werden nur auf Antrag (von Betroffenem, verantwortlicher Stelle, Aufsichtsbehörde, oder Bundesbeauftragtem für den Datenschutz) verfolgt

Telekommunikationsgesetz (TKG)

- Verabschiedet im Juli 1996, zuletzt 2004 geändert
  - Novelle 2004 integriert bisheriges TKDSG, mit §91-§107 werden nun auch Datenschutz-Belange gesetzlich geschützt (bisher: Verordnung)
- §85 regelt Fernmeldegeheimnis
  - Nicht nur Inhalt, sondern auch Umstände (Beteiligte, nicht erfolgreiche Vermittlungsversuche) fallen hierunter
- Erbringung von TK-Diensten erzwingt technische Schutzmaß-nahmen (§87):
  - „Wer TK-Anlagen betreibt, die dem geschäftsmäßigen Erbringen von TK-Diensten dienen, hat bei den zu diesem Zweck betriebenen TK- und DV-Systemen angemessene technische Vorkehrungen oder sonstige Maßnahmen (...) zu treffen.“

Schutzvorschriften im TKG

- Zu schützen sind:
  - Fernmeldegeheimnis und personenbezogene Daten
  - programmgesteuerte TK- und DV-Systeme gegen unerlaubte Zugriffe
  - TK/DV-Systeme vor Störungen die zu erheblichen Beeinträchtigungen des Netzes führen
  - TK/DV-Systeme vor äußeren Angriffen und Einwirkungen von Katastrophen
  - Aber: Verkehrsdaten müssen vollständig gespeichert werden, Standortdaten brauchen jedoch Einverständnis des Kunden
- Die Anforderungen des TKG gehen dabei über die des BDSG hinaus - werden aber durch TKÜV u.a. teilweise konterkariert

TDG und TDDSG

- Das häufige Konstrukt der IT-Dienstleistung über Konzernunternehmen fällt unter die Kontrolle des TDG und TDDG.
- Konzernunternehmen darf Mitarbeiterdaten des Beschäftigungsunternehmens verarbeiten; zunächst auch zur Verhaltens- und Leistungskontrolle
  - Auftragsdatenverarbeitung im Sinne von §11 BDSG
  - Das Beschäftigungsunternehmen ist für Rechtmäßigkeit der Auftragsdatenverarbeitung verantwortlich
- Für Konzernmitarbeiter gelten die Datenschutzbestimmungen des TDDSG nur eingeschränkt

Pflichten des Dienstleisters nach TDDSG

- Gewährleistung der technischen Systemsicherheit
- Wenn private Nutzung gestattet ist sind jedoch Mitarbeiter Nutzer im Sinne des TDDSG!
  - private Nutzung muß klar von betrieblicher zu trennen sein
  - derartige Daten müssen frühestmöglich gelöscht werden
  - nur essentielle Abrechnungsdaten dürfen erfaßt werden
  - trägt das Beschäftigungsunternehmen die Kosten, so dürfen nur aggregierte, anonymisierte Daten übermittelt werden

E-Mails in Dienstleistungsverhältnissen

- Geschäftliche E-Mails und damit zusammenhängende Daten stehen dem Konzernunternehmen zu, gegenüber Dritten ist der Dienstleister nach TDG zur Sorgfalt verpflichtet
- Gegenüber Dritten (auch der Konzernmutter!) gilt nach §85 TKG das Fernmeldegeheimnis
  - Personenbezogene Daten dürfen an Konzernunternehmen nur mit Einverständnis des Betroffenen weitergeleitet werden
- Private E-Mails müssen klar von geschäftlichen zu trennen sein
  - vom Inhalt dürfen sich weder Dienstleister noch Beschäftigungsunternehmen Kenntnis verschaffen

Betriebsverfassungsgesetz (BetrVerfG)

- Nach §80 Abs. 1 Satz 1 ist es Aufgabe des Betriebsrates „darüber zu wachen, daß die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, (...) durchgeführt werden“
- Zur Durchführung der Aufgaben ist der BR rechtzeitig und umfassend zu informieren.
- §80 Abs. 2 Satz 1 verpflichtet den Arbeitgeber zur Unterrichtung des BR über alle Formen der Verarbeitung personenbezogener Daten der Arbeitnehmer.
  - Dies gilt nicht nur bei vermuteten Verletzungen der Bestimmungen des BDSG!

Einflußnahme durch BetrVerfG

- §87 Abs. 1 Nr. 6 räumt dem BR ein Mitbestimmungsrecht ein bei „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“
- Nach einem Urteil des BAG ist dieser Tatbestand selbst dann gegeben, wenn die Einrichtung auch nur dazu geeignet ist, Überwachungen durchzuführen - auch indirekt
- Nach §90 Abs. 2, 3 muß der BR bei neuen technischen Einrichtungen unter Vorlage der „erforderlichen Unterlagen“ unterrichtet werden

Relevante Bestimmungen des StGB

- 1986 wurden mit dem 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität Bestimmungen zur „Computerkriminalität“ aufgenommen.
- Alle Delikte sind Antragsdelikte; bei §303a, 303b und 303c können auch von Strafverfolgungsbehörden Verfahren eingeleitet werden
- §17 UWG regelt die Strafbarkeit des Verrats von Betriebsgeheimnissen (bis zu 3 Jahre Freiheitsstrafe)
- Verbreitung und Speicherung verbotener (pornographische und Propaganda-) Schriften sind nach §184, §86 verboten
  - Trotz Ausschluß nach §5 TDG kann ein Unternehmen aufgrund der Wissensvermutung haftbar sein

Bestimmungen des StGB (1)

- § 202a: Ausspähen von Daten
  - Die „besondere Sicherung“ ist jede Zugriffskontrolle
- § 263a: Computerbetrug
- § 268: Fälschung technischer Aufzeichnungen
  - Dies trifft insbesondere für Revisionsdaten zu
- § 269: Fälschung beweiserheblicher Daten
- § 270: Täuschung im Rechtsverkehr bei Datenverarbeitung

Bestimmungen des StGB (2)

- § 303a: Datenveränderung
- § 303b: Computersabotage
  - DDoS-Angriffe sollten unter §303b fallen.
- § 316b: Störung öffentlicher Betriebe
- § 317: Störung von Telekommunikationsanlagen
- § 274: Urkundenunterdrückung