Sicherheit aus Unternehmenssicht

Prof. Dr.-Ing. Heinz Thielmann

Münchner Kreis Kongress

18. September 2003

Fraunhofer Institut
Sichere Telekooperation

Sicherheit aus Unternehmenssicht

Übersicht:

1. **Aufgabe des Unternehmens / Unternehmers / der Organe**
2. **Die Bedrohungen und deren Auswirkungen**
3. **Die Haftungs-Fragen für das Management**
4. **Die ganzheitliche Sicherheit**
5. **Die Infrastruktur-Sicherheit**
6. **Die Geschäftsprozess-Sicherheit**
7. **Sicherheits-Policies / Total Security Management**
8. **Business Continuity Management**

Fraunhofer Institut
Sichere Telekooperation

Sicherheit aus Unternehmenssicht

Übersicht:

1. **Aufgabe des Unternehmens / Unternehmers / der Organe**
2. **Die Bedrohungen und deren Auswirkungen**
3. **Die Haftungs-Fragen für das Management**
4. **Die ganzheitliche Sicherheit**
5. **Die Infrastruktur-Sicherheit**
6. **Die Geschäftsprozess-Sicherheit**
7. **Sicherheits-Policies / Total Security Management**
8. **Business Continuity Management**

Die Aufgaben des Unternehmens / Unternehmers / der Organe (I)

- **Operativen Betrieb sicherstellen**
- **Wettbewerbsfähigkeit sicherstellen**
- **Wachstum sicherstellen**
- **Ertragssituation optimieren**
- **Kernkompetenzen optimieren**
- **Effizienz steigern**
- **Strategien entwickeln und umsetzen**
- **Personal-Ressourcen entwickeln und pflegen**
- **Kundenbestand entwickeln und pflegen**
- **.....**

Die Aufgaben des Unternehmens / Unternehmers / der Organe (II)

- **Unternehmenswerte sichern**
- **Physische Werte als „assets“ schützen**
- **Immaterielle Werte als „e-Güter“ schützen**
  - **Dokumente, Verträge, Geschäftsprozesse**
  - **Kundenbestände, Software, sonstige Geschäftsinhalte**
- **Risiken abwenden bzw. minimieren**
  - **Verlust der „e-Güter“ verhindern**
  - **Manipulation der „e-Güter“ verhindern**
  - **externe und interne Angriffe verhindern**

Die Aufgaben des Unternehmens / Unternehmers / der Organe (III)

- **Die Management-Sicht**

  - Geschäftsprozess-Sicherung

- **Die Shareholder-Sicht**

  - Ertrags-Sicherung, Werte-Sicherung

  - „e-Güter“ bilanziert ?, „e-Risiken“ bekannt und bewertet ?

- **Die Kunden-Sicht**

  - Geschäftspartner nachhaltig zuverlässig ?

- **Die Mitarbeiter-Sicht**

  - Arbeitgeber nachhaltig zuverlässig ?

SIT
Fraunhofer Institut
Sichere Telekooperation

Sicherheit aus Unternehmenssicht

Übersicht:

1. **Aufgabe des Unternehmens / Unternehmers / der Organe**
2. **Die Bedrohungen und deren Auswirkungen**
3. **Die Haftungs-Fragen für das Management**
4. **Die ganzheitliche Sicherheit**
5. **Die Infrastruktur-Sicherheit**
6. **Die Geschäftsprozess-Sicherheit**
7. **Sicherheits-Policies / Total Security Management**
8. **Business Continuity Management**

Fraunhofer Institut
Sichere Telekooperation

Die Bedrohungen und deren Auswirkungen (I)

- über 50% aller Angriffe durch Mitarbeiter: Innentäter

  Ursache häufig Nachlässigkeit, Unwissenheit der Benutzer
- Hacker: versierte Spezialisten,

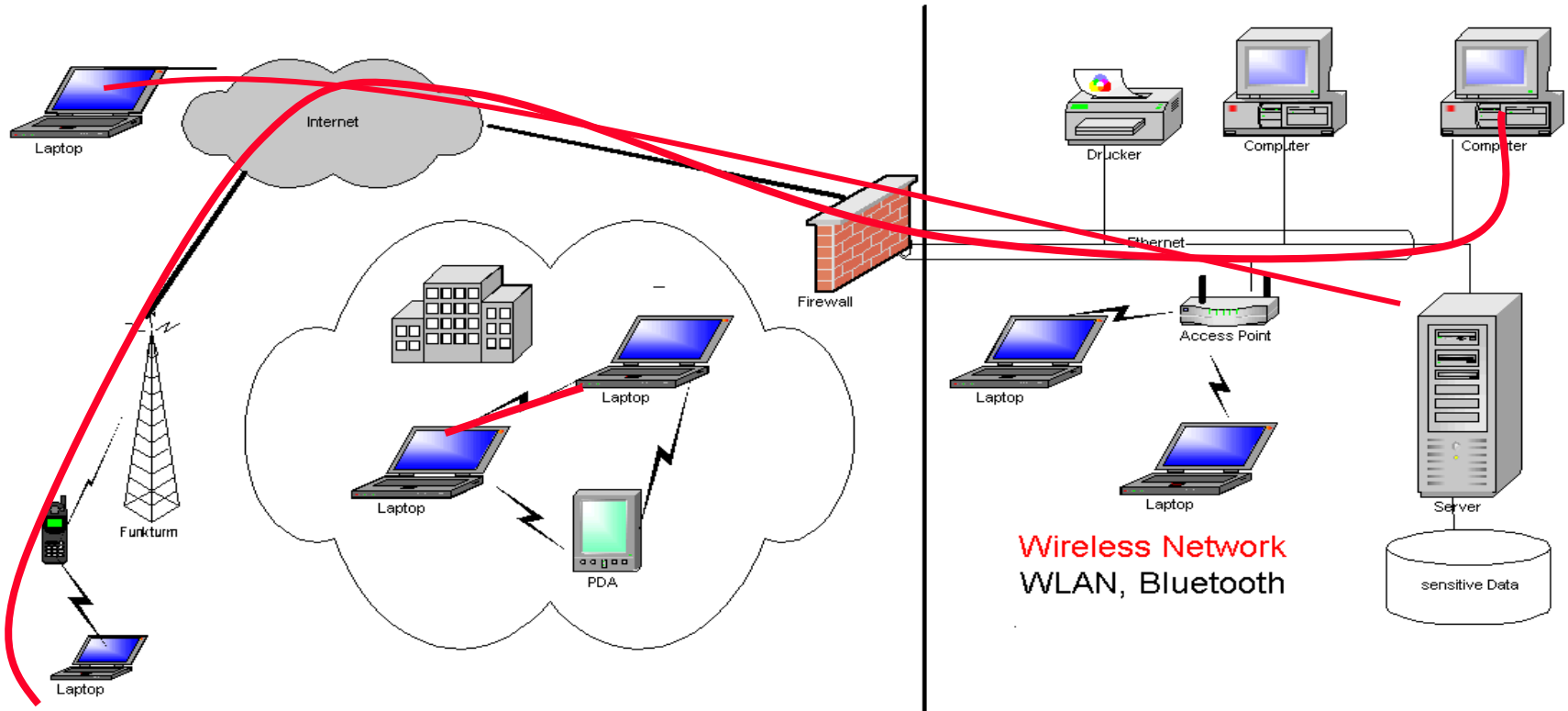
  Ziel: Lücken auffinden, warnen, selten Missbrauchsabsicht
- Cracker: versierte Spezialisten i.d.R. mit Missbrauchsabsicht

  Ziel: Angriffe auf schlecht geschützte Unternehmen, Behörden,...
- Skript Kiddie: nutzt fertige Angriffe, i.d.R. wenige Kenntnisse, viel Zeit

  Sehr großes Potential an Angreifern (u.a. Schüler, Spieler-Naturen ..)!
- Zunehmend Wirtschaftsspione und Kriminelle

→ **Jede(r) kann Ziel eines Sicherheitsangriffs werden!**

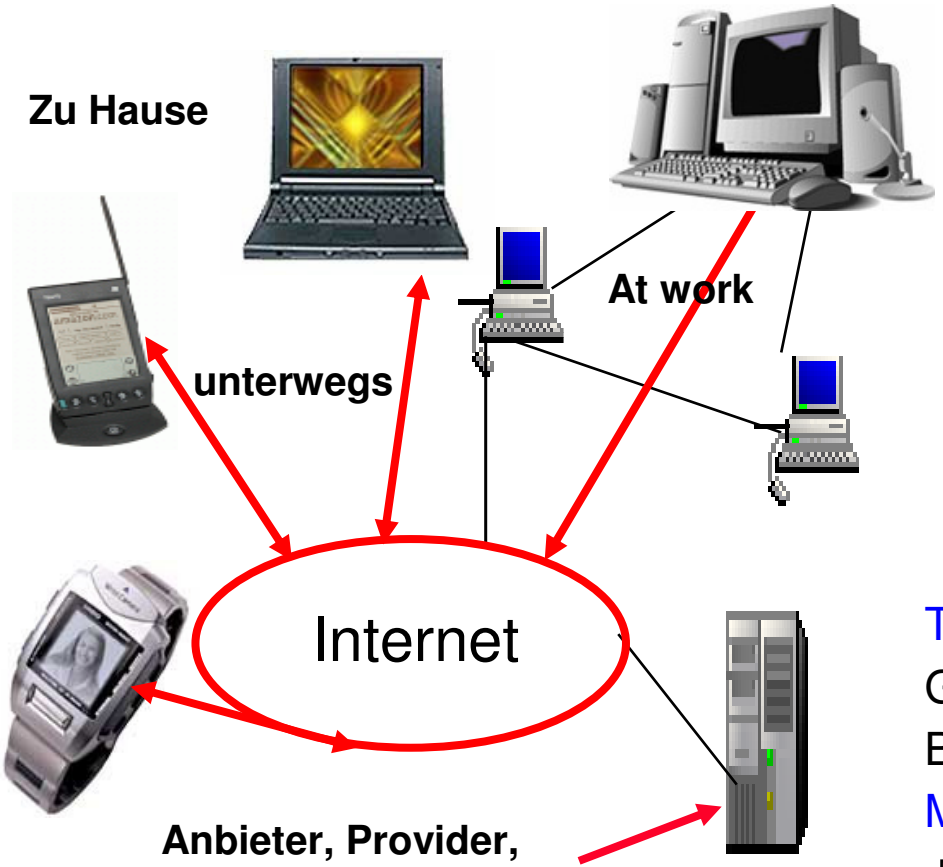
Die Bedrohungen und deren Auswirkungen (II)



Fraunhofer Institut
Sichere Telekooperation

Die Bedrohungen und deren Auswirkungen (III)

Nutzung der IT-Systeme:



Klassisch, wohlbekannt

Mails: Versenden/Empfangen

Web-Dienste: Informationen

anbieten, sammeln

Download von Software

Spiele, Musik, Updates ...

Einkaufen über das Netz

Bücher, Tickets

Trend:

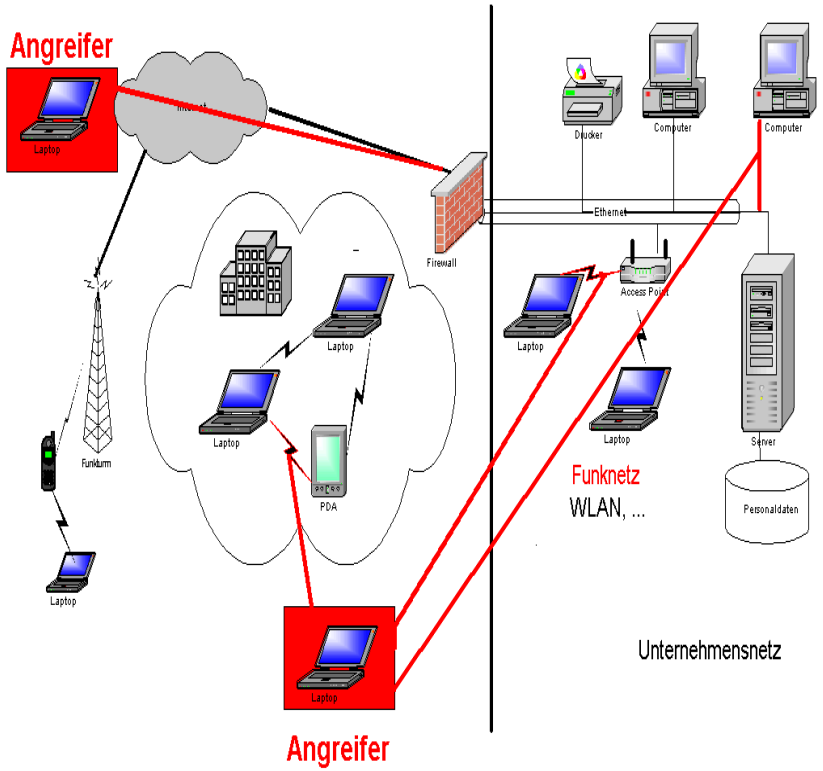
Geschäfte über das Internet B2B, C2B,...

Behördengänge, Anträge, C2G, B2G,...

Medienbruchfreies Arbeiten: effizient, effektiv

Aber sicher! Sicher?

Die Bedrohungen und deren Auswirkungen (IV)



Abhören von E-Mails, Nachrichten
E-Mail ist wie eine Postkarte
keine Vertraulichkeit

Verändern von Nachrichten, ...
Falsche Daten (z.B. Überweisung)
keine Integrität

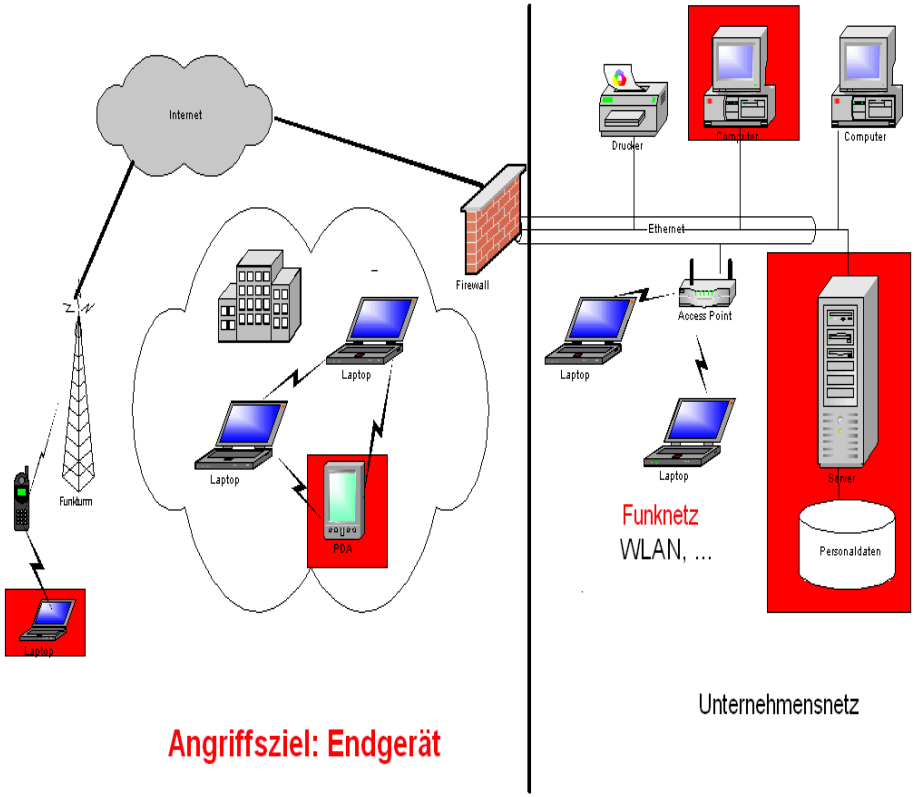
Gefälschte Absender-Adresse
Falsche E-Mail, falscher Käufer, ...
keine Authentizität

Cookies, Surfen, Mailen
Datenspuren, Zugriffsprofile
keine Privatheit

Abstreiten von gesendeten Daten
keine Verbindlichkeit

Die Bedrohungen und deren Auswirkungen (V)

Endgeräte



Angriffe: u.a. durch

Verseuchte E-Mails

Viren, Würmer, ...

- Daten zerstören, System-Absturz, ...

Verseuchte Web-Seiten

JavaScript, VBScript, ...

- Daten lesen, zerstören

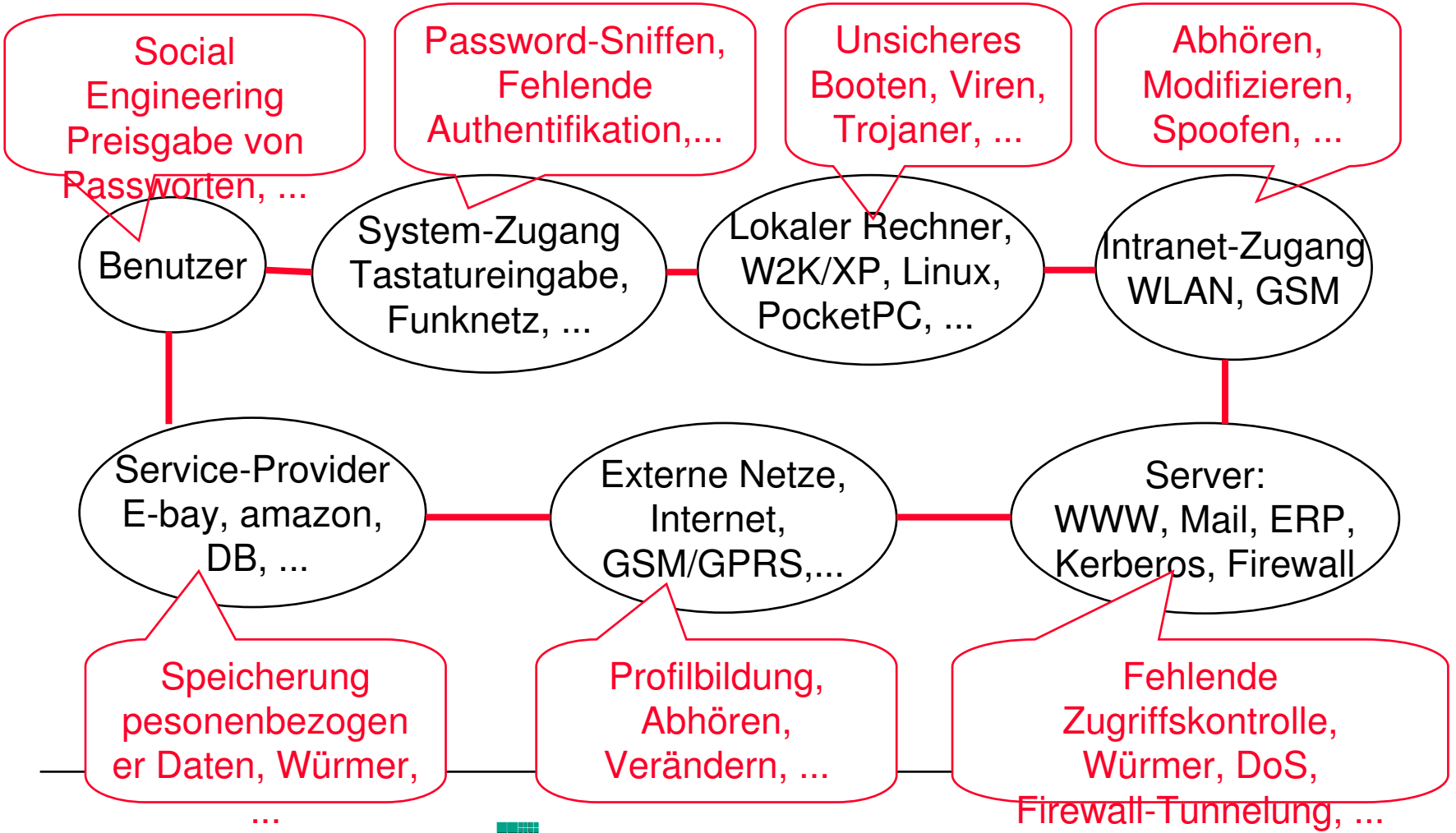
Passwort-Cracking

- Rechte-Aneignung

Denial of Service (DoS)

Fraunhofer SIT Institut Sichere Telekooperation

Die Bedrohungen und deren Auswirkungen (VI)



Die Bedrohungen und deren Auswirkungen (VII)

Direkte Schäden

- Wiederbeschaffungskosten,....
- Wiederherstellungs- und Reparaturkosten
- Schäden durch Verlust der Geheimhaltung und Integrität

Folgeschäden

- Stillstandskosten
- Auswirkungen auf andere Geschäftsprozesse
- Anspruchskosten

Strategische Kosten

- Imageverlust,....

Die Bedrohungen und deren Auswirkungen (VIII)

- Internet-Wurm Code Red [Computer Economics]
  - Bekämpfung des Virus: 1,1 Mrd. $
  - Produktionsausfälle: 1,5 Mrd. $
- Slammer Wurm: 750 Mio. und 1,2 Mrd. $
- „I LOVE YOU“-Virus [Heise Online News im Mai 2000]
  - Gesamtschaden weltweit bis zu 30 Mrd. $
- Studien von Hewlett-Packard zur Datensicherheit (1999):
  - Kosten des Stillstandes, Wiederbeschaffung, entstandene Wettbewerbsnachteile, etc.
    bis zu 7,3 Mill. US$ / Stunde Tendenz steigend!

  - 94 % der Unternehmen überleben bei einem Totalausfall ihrer Daten die nächsten zwei Geschäftsjahre nicht !!!

Die Bedrohungen und deren Auswirkungen (IX)

Spezielle Probleme bei mobilen Geräten:

- **Mobile Endgeräte: Laptops, PDAs, Mobiltelefone**
- **Schwachstelle: Verlieren, vergessen, stehlen**
- **Klassische Antwort: „Das passiert mir doch nicht?“**

Wirklichkeit: Statistik: Londoner Taxen, erstes Halbjahr 2001

- **2900 Laptops vergessen!**
- **1300 PDAs vergessen und**
- **63 000 Mobiltelefone vergessen!**

Problem: private und geschäftliche Daten auf mobilen Geräten!

Die Bedrohungen und deren Auswirkungen (IX)

Was soll man tun? Einige Weisheiten zum Thema:

Zitat von Bruce Schneier: (ein ‚Sicherheitspapst')
„ The only secure Computer is one that's turned off, locked in a safe, and buried 20 feet down in a secret location – and I'm not completely confident of that one either"
Fazit: ist sowieso nichts zu machen, also Augen zu und durch?

Nein, halten wir uns lieber an Erich Kästner:
„ An allem Unfug, der passiert, sind nicht etwa nur die Schuld, die ihn tun, sondern auch die, die ihn nicht verhindern!"
Fazit: wir sollten und wir können auch was tun, aber.....

Zitat von J. Ringelnatz:
„ Sicher ist, dass nichts sicher ist. Selbst das ist nicht sicher."
Fazit: Perfekte Sicherheit ist nicht erreichbar, das ist ja normal

Sicherheit aus Unternehmenssicht

Übersicht:

1. **Aufgabe des Unternehmens / Unternehmers / der Organe**
2. **Die Bedrohungen und deren Auswirkungen**
3. **Die Haftungs-Fragen für das Management**
4. **Die ganzheitliche Sicherheit**
5. **Die Infrastruktur-Sicherheit**
6. **Die Geschäftsprozess-Sicherheit**
7. **Sicherheits-Policies / Total Security Management**
8. **Business Continuity Management**

Die Haftungs-Fragen für das Management (I)

- **Kritische Ereignisse führen immer häufiger zu Ansprüchen (Mitarbeiter, Dritte) an das Unternehmen**

- **Versicherungen handeln in jüngster Zeit restriktiv: nicht mehr alle Risiken sind versicherbar, Prämien sind teils prohibitiv teuer**

- **Haftung des Fachverantwortlichen ist beschränkt: Schaden kann durch „symbolische Pfändung“ selten abgewendet werden**

Fraunhofer Institut
Sichere Telekooperation

Die Haftungs-Fragen für das Management (II)

- **Mittelbar greift die Vorstands- / Geschäftsführerhaftung (AktG/GmbHG - kaufm. Sorgfalt, Pflicht zur Voraussicht, Pflicht zur Schadensabwendung), in Deutschland sogar mit Beweislastumkehr**
- **„Schuldhaftes Unterlassen“ ist strafbar**
  .....geeigneter Absicherungsmaßnahmen...“ ?
  .....wider besseres Wissen“ (Vorsatz) ??
  .....ohne sich rechtzeitig informiert zu haben (Fahrlässigk.) ???
- **Das Management und die Organe des Unternehmens sind verpflichtet, die Kontinuität und die Werte zu sichern.**

Fraunhofer Institut
Sichere Telekooperation

Die Haftungs-Fragen für das Management (III)

- KonTraG 1998 – Frühwarn- und Früherkennungssystem
- Deutscher / österr. Corporate Governance Kodex
- Spezielle Anforderungen im Finanzsektor
- Basel II Dokumentation
- ISO 17799, BS 7799 (2002);....
- NFPA 1600, HIPAA (USA)
- Fed / SEC Interagency Paper zur Kontinuität (Aug. 2002)
- FSA Working Papers zur Kontinuität (2002)
- .....

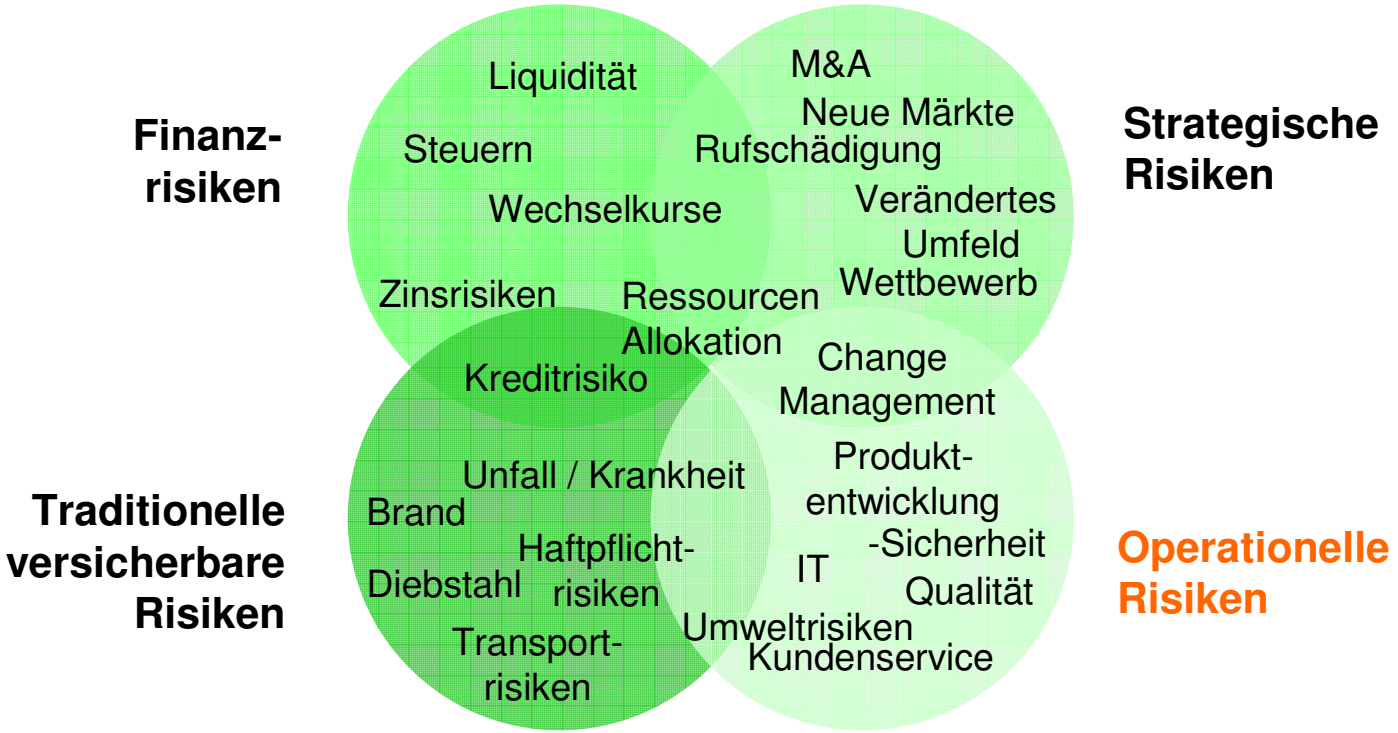
Sicherheit aus Unternehmenssicht

Übersicht:

1. **Aufgabe des Unternehmens / Unternehmers / der Organe**
2. **Die Bedrohungen und deren Auswirkungen**
3. **Die Haftungs-Fragen für das Management**
4. **Die ganzheitliche Sicherheit**
5. **Die Infrastruktur-Sicherheit**
6. **Die Geschäftsprozess-Sicherheit**
7. **Sicherheits-Policies / Total Security Management**
8. **Business Continuity Management**

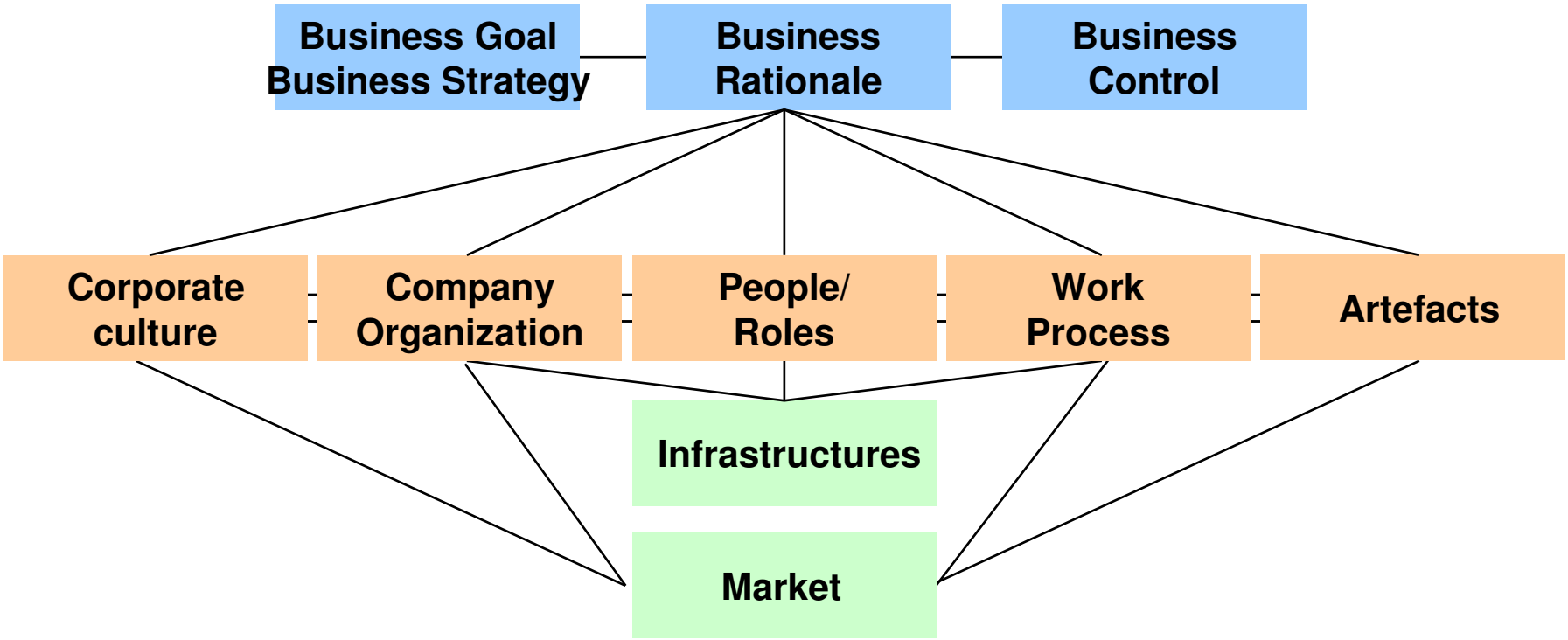
Die ganzheitliche Sicherheit (I)

Zustand eines Unternehmens, in dem es alle Anforderungen erfüllt, welche eine beurteilende Person an es stellt, d.h. in dem alle Risiken auf ein tragfähiges Maß reduziert sind. (Quelle: FhG-ISST)



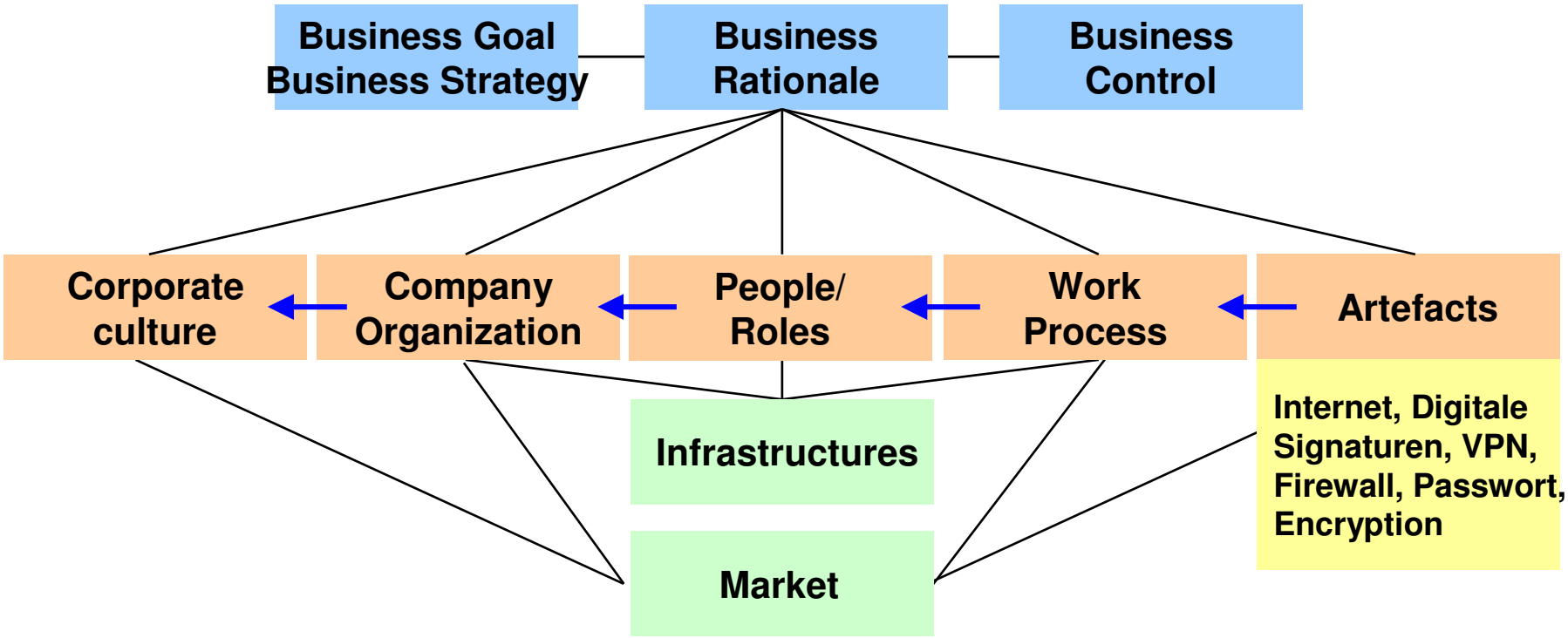
Die ganzheitliche Sicherheit (II)

.....umfasst alle Aktivitäten und Maßnahmen zum Erreichen von Business Security, betrifft also alle Unternehmensbestandteile und –sichten.....



Die ganzheitliche Sicherheit (III)

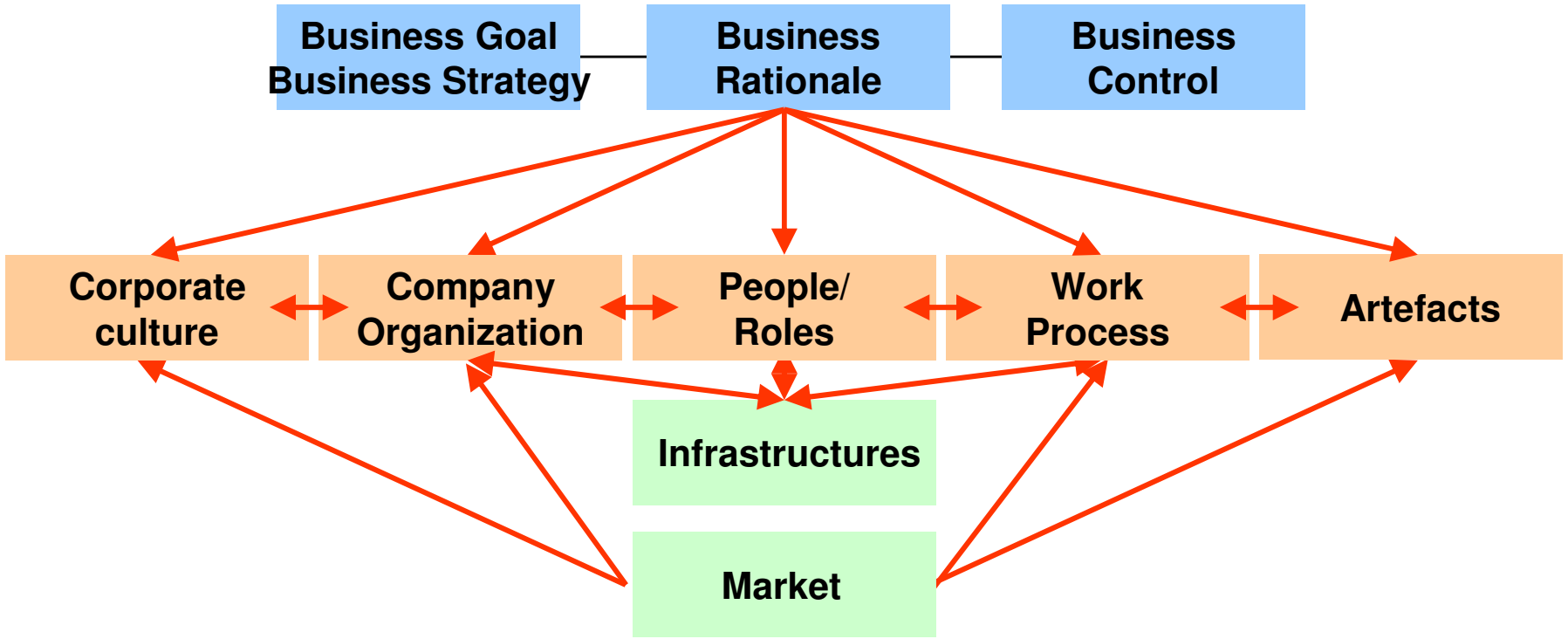
Sicherheitstechnik ist der entscheidende Baustein, aber nicht alles !



Fraunhofer SIT Institut Sichere Telekooperation

Die ganzheitliche Sicherheit (VI)

Unternehmenskultur, -organisation, -rollen und –prozesse sind wesentliche Bausteine und haben direkt oder indirekt Einfluss auf die Sicherheitstechnik!

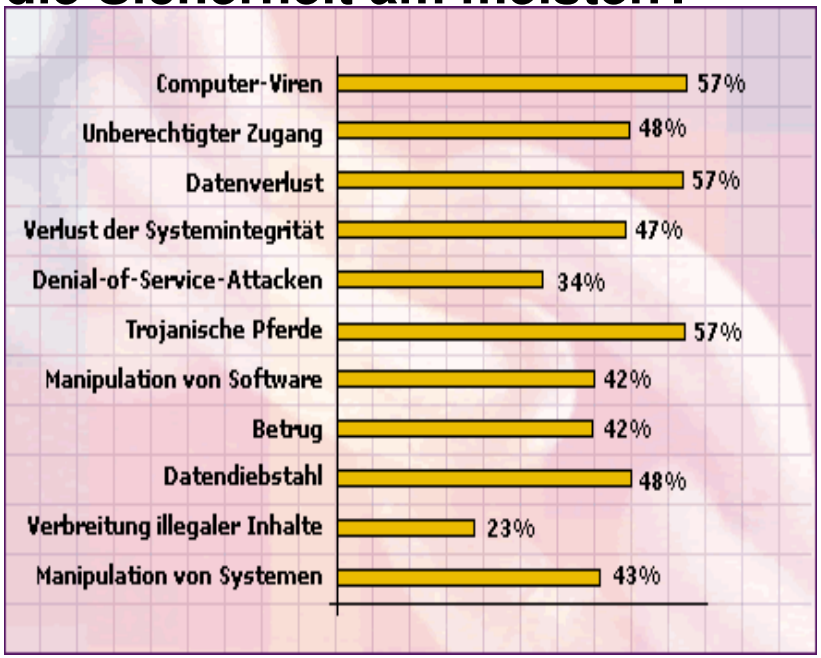


Fraunhofer SIT Institut Sichere Telekooperation

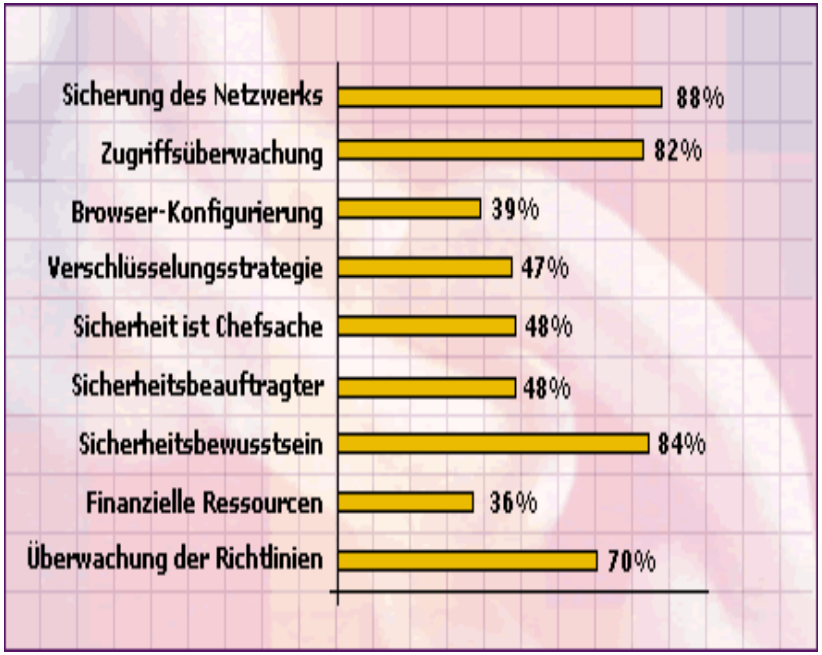
Die ganzheitliche Sicherheit (V)

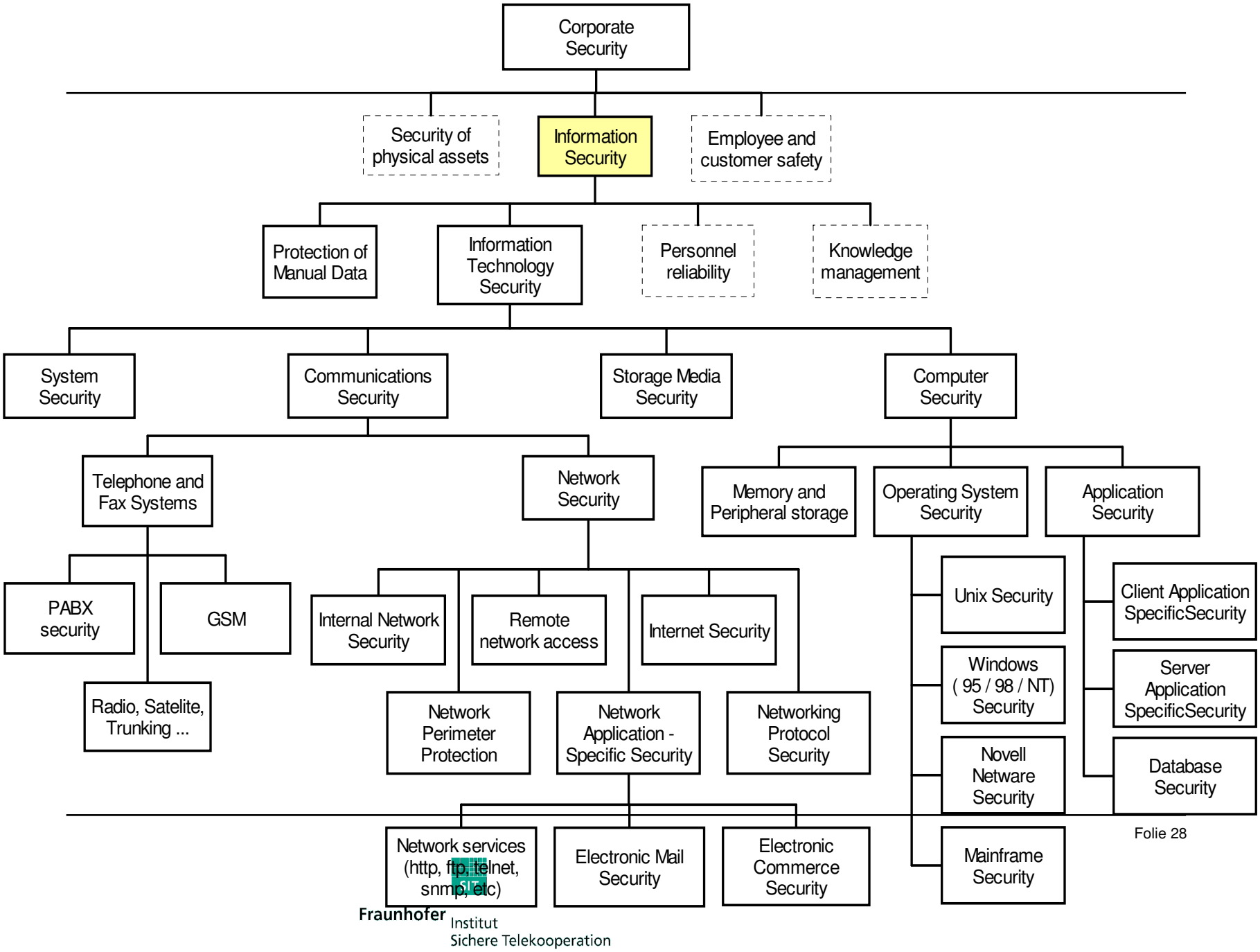
Was sind die größten Sicherheitsprobleme? Ergebnisse einer Studie/Umfrage in 2002, 483 KMUs

Frage 1: was gefährdet die Sicherheit am meisten?



Frage 2: was sind die wichtigsten Faktoren für die Sicherheit?





Folie 28

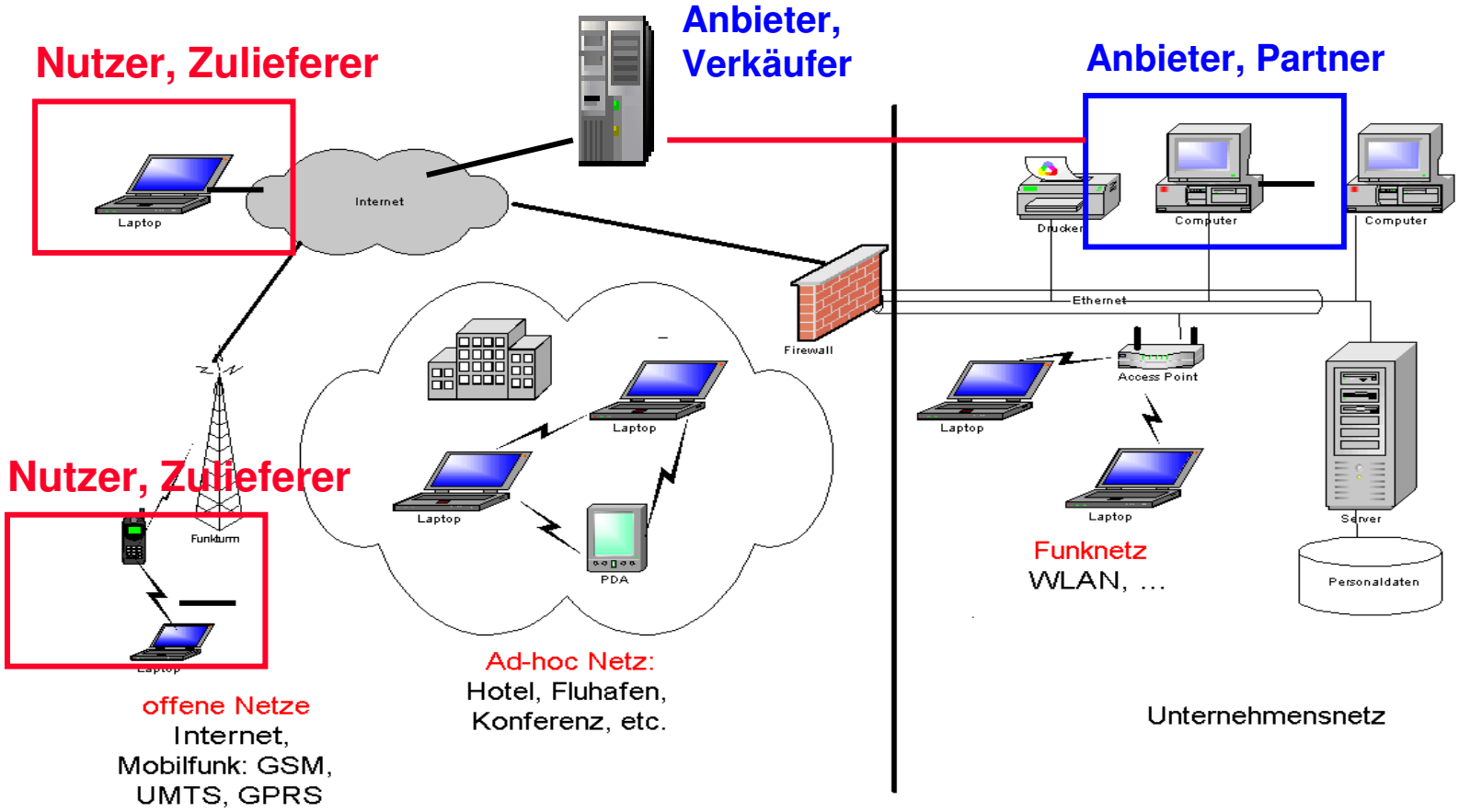
Fraunhofer Institut Sichere Telekooperation

Sicherheit aus Unternehmenssicht

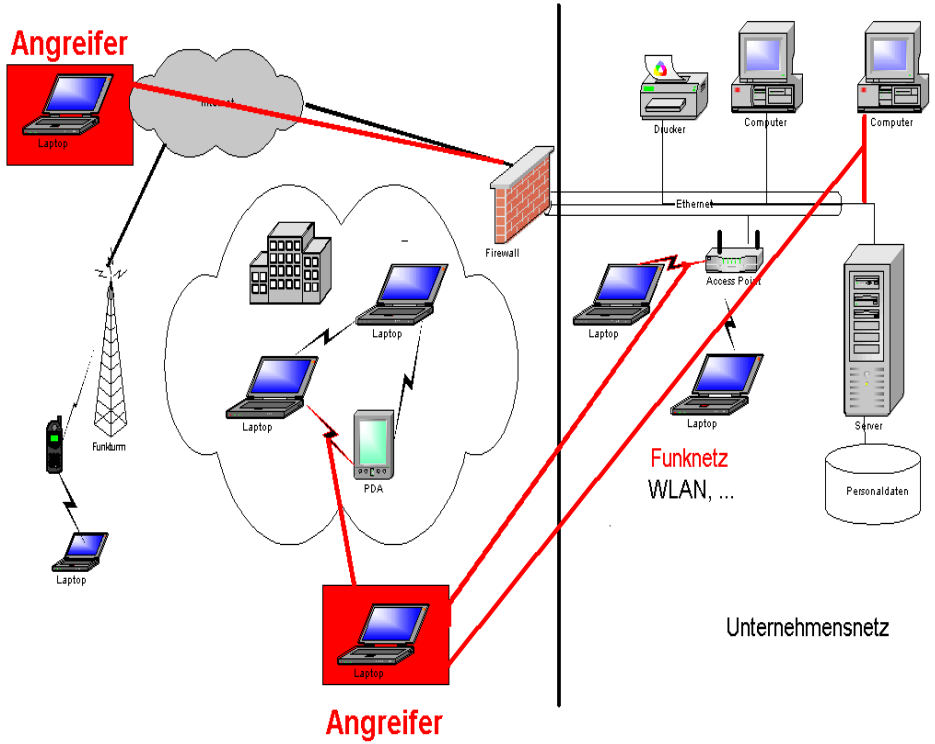
Übersicht:

1. **Aufgabe des Unternehmens / Unternehmers / der Organe**
2. **Die Bedrohungen und deren Auswirkungen**
3. **Die Haftungs-Fragen für das Management**
4. **Die ganzheitliche Sicherheit**
5. **Die Infrastruktur-Sicherheit**
6. **Die Geschäftsprozess-Sicherheit**
7. **Sicherheits-Policies / Total Security Management**
8. **Business Continuity Management**

Die Infrastruktur-Sicherheit (I)



Die Infrastruktur-Sicherheit (II)



Schlechte Nachricht:

Viele Bedrohungen:

Abhören!

Verändern!

Maskieren!

Abstreiten!

Profilbildung!

Behinderung! (DoS)

Gute Nachricht:
Standardtechniken zur Abwehr stehen bereit!

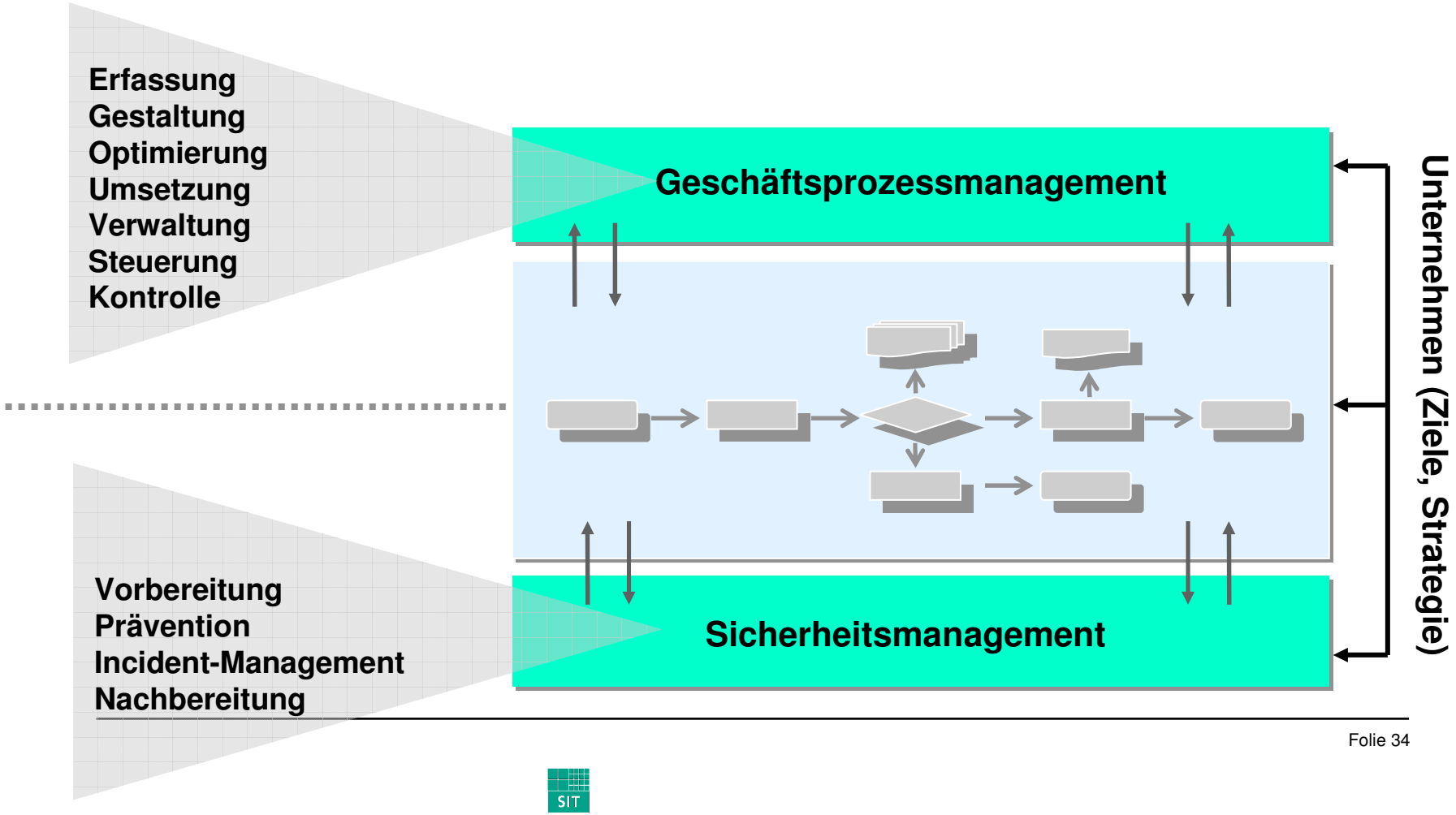
Sicherheit aus Unternehmenssicht

Übersicht:

1. **Aufgabe des Unternehmens / Unternehmers / der Organe**
2. **Die Bedrohungen und deren Auswirkungen**
3. **Die Haftungs-Fragen für das Management**
4. **Die ganzheitliche Sicherheit**
5. **Die Infrastruktur-Sicherheit**
6. **Die Geschäftsprozess-Sicherheit**
7. **Sicherheits-Policies / Total Security Management**
8. **Business Continuity Management**

Die Geschäftsprozess-Sicherheit (I): (Quelle E&Y)

Die Geschäftsprozess-Sicherheit (II): (Quelle FhG-IAO)



Fraunhofer Institut Sichere Telekooperation

Sicherheit aus Unternehmenssicht

Übersicht:

1. **Aufgabe des Unternehmens / Unternehmers / der Organe**
2. **Die Bedrohungen und deren Auswirkungen**
3. **Die Haftungs-Fragen für das Management**
4. **Die ganzheitliche Sicherheit**
5. **Die Infrastruktur-Sicherheit**
6. **Die Geschäftsprozess-Sicherheit**
7. **Sicherheits-Policies / Total Security Management**
8. **Business Continuity Management**

Sicherheits-Policies / Total Security Management (I)

- **Konzentration auf das Kerngeschäft, nicht auf Technik**
- **Kritikalität ermitteln und definieren**
- **Abtrennung technischer Einzeldisziplinen wie IT-Sicherheit, Hochverfügbarkeit und Neueinordnung im Hinblick auf Ertrag / Schaden**

Sicherheits-Policies / Total Security Management (II)

- **Abkehr von der Kostensicht hin zur Betrachtung des Unternehmenserfolgs !!!**

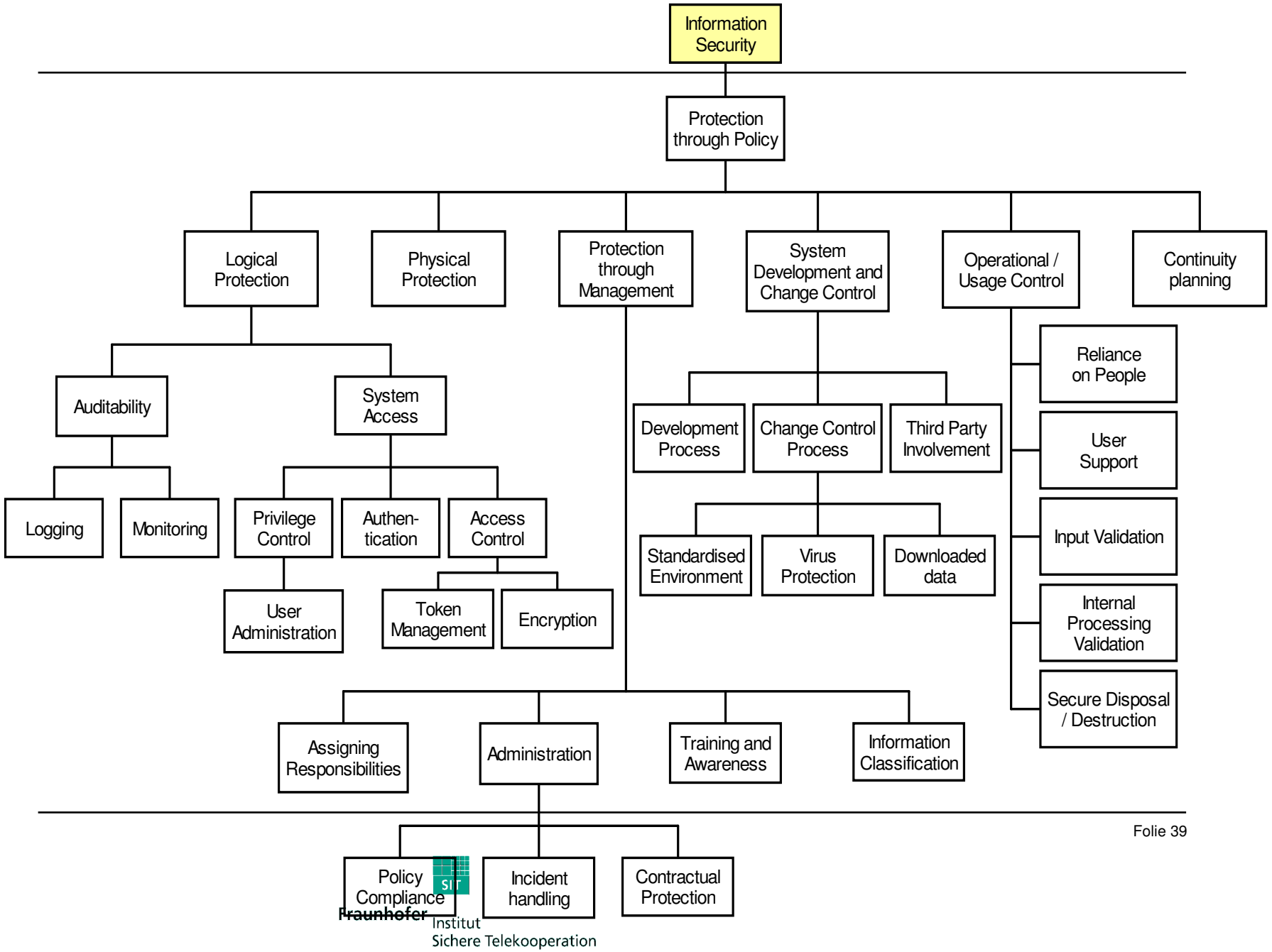
- **Grundlegende Schaffung einer Robustheit, Reduzierung der zunehmenden Anfälligkeit der Unternehmen**

- **Konzentration auf Fortführung der Geschäftstätigkeit im Krisenfall, Abkehr vom Konzept der vollständigen Prävention**

Sicherheits-Policies / Total Security Management (III)

- **Organisations-Sicherheit: Risiko-Management umsetzen**
- **Bedrohungen und Risiken ganzheitlich definieren**
- **IT-Sicherheit + Verfügbarkeit definieren**
- **Datenschutz; Schutz der „e-Güter**
- **Business-Modelle für Sicherheits-Policies entwickeln (ROSI)**

Fraunhofer SIT Institut Sichere Telekooperation



Fraunhofer SIT Institut Sichere Telekooperation

Sicherheit aus Unternehmenssicht

Übersicht:

1. **Aufgabe des Unternehmens / Unternehmers / der Organe**
2. **Die Bedrohungen und deren Auswirkungen**
3. **Die Haftungs-Fragen für das Management**
4. **Die ganzheitliche Sicherheit**
5. **Die Infrastruktur-Sicherheit**
6. **Die Geschäftsprozess-Sicherheit**
7. **Sicherheits-Policies / Total Security Management**
8. **Business Continuity Management**

Business Continuity Management (I)

Definition

IT-Sicherheitsmanagement ist ein kontinuierlicher Prozess, der die Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Authentizität und Zuverlässigkeit von Systemen der Informationstechnik (IT-Systemen) innerhalb einer Organisation gewährleisten soll. (Quelle: Österreichisches IT-Management Handbuch, 2001)

Bestandteile

- **Vorbereitende Maßnahmen**
- **Prävention**
- **IT-Incident-Management**
- **Nachbereitung**

Inhalte

- **Politik**
- **Ziele**
- **Strategie**
- **Organisation**
- **Verantwortlichkeiten**
- **Sicherheitsniveau**

Business Continuity Management (II)

Definition

Vorfälle (IT incidents) sind Ereignisse, die den normalen Betrieb stören und die eine gewisse Krisensituation auslösen. Das IT-Incident-Management befasst sich mit der Behandlung von Vorfällen, um den Schaden zu begrenzen, indem zügig und effizient nach gewissen Vorgaben vorgegangen wird (in Anlehnung an das BSI IT Grundschutzhandbuch, 2002).

Business Continuity Management (III)

Bestandteile

Vorbereitung auf einen Vorfall

Erkennung des Vorfalls

Erste Reaktion / Basisanalyse

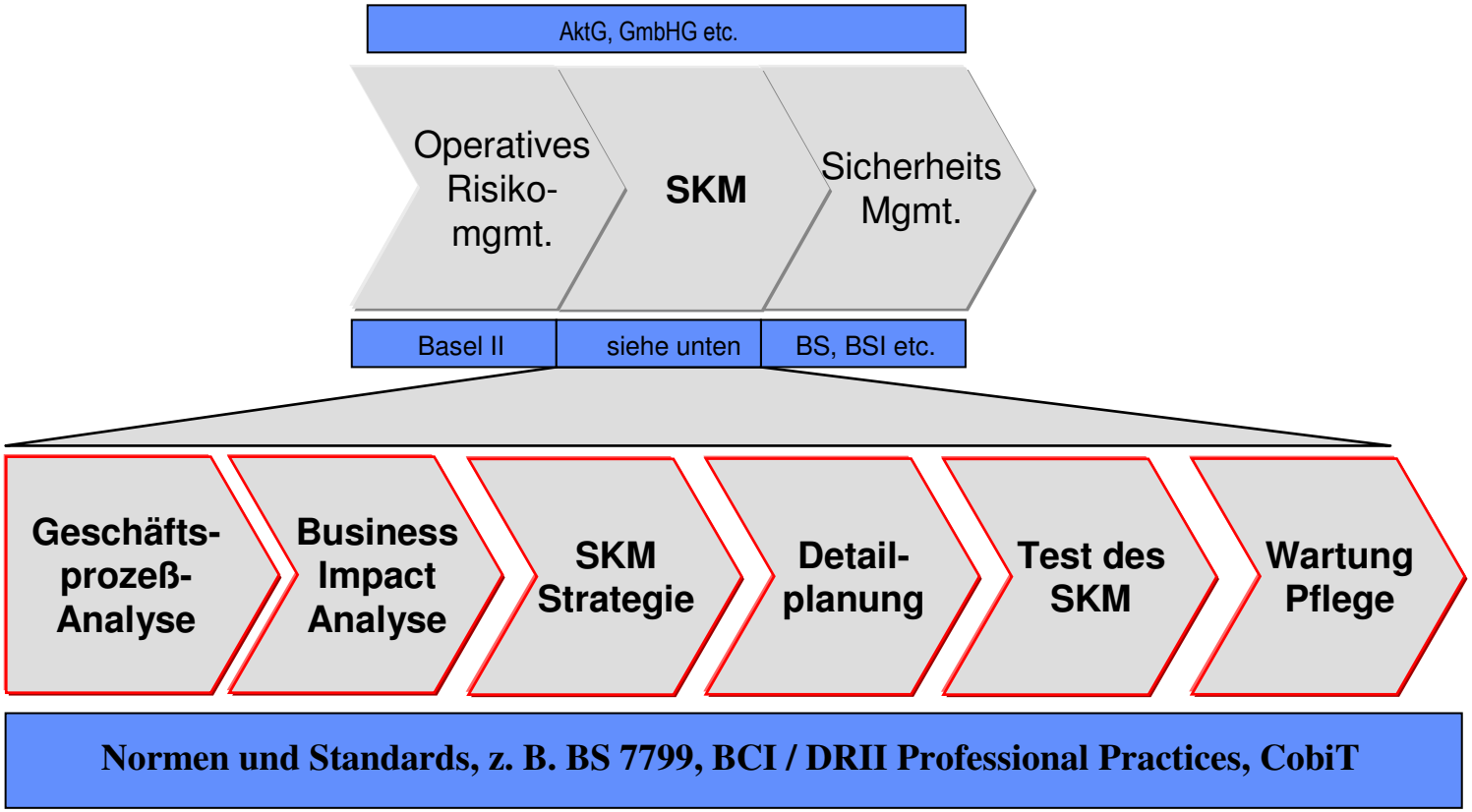
Formulierung einer Reaktionsstrategie

Duplikation relevanter Daten

Ermittlung

- **Durchführung von Sicherheitsmaßnahmen**
- **Netzwerkbeobachtung**
- **Wiederherstellung**
- **Dokumentation**
- **Nachbereitung**

Business Continuity Management (IV): (Quelle E&Y)



> Herausforderung <

Ganzheitliches
Sicherheits-Management
für
Management-Sicherheit !!!

Fraunhofer Institut
Sichere Telekooperation