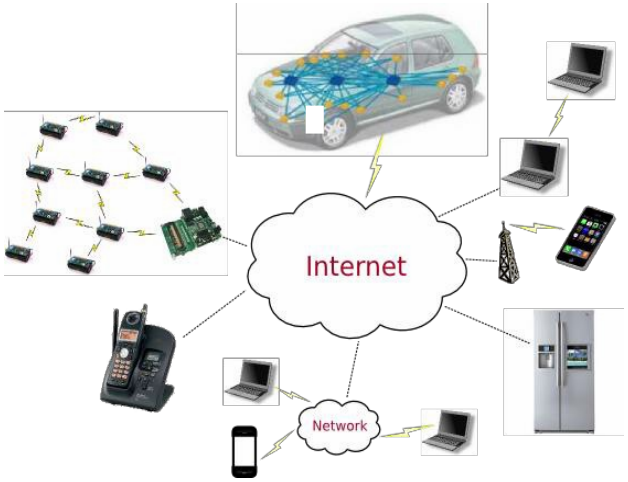
Wer sind Sie?

Bitte tragen Sie sich in ILIAS ein…

Passwort: **thiel17/18**

Motivation (I)

- IT-Trends:
  - Mobilität, Vernetzung, Miniaturisierung, Dienste-Orientierung
  - Internet der nächsten Generation:
    - Hochgradig verteilt und vernetzt
    - Heterogen, dynamisch und kooperativ
  - Internet der Dienste und Dinge
    - Ubiquitäre IT:
    - Durchdringung unseres Alltags mit IT



Quelle: TU München

- Konsequenz:
  - Anforderungen an Verlässlichkeit und Security steigen

Motivation (II)

**Thema: Wie kann man (ITK-)Systeme bauen,
die sicherer und verlässlicher arbeiten als die gegenwärtigen?**

Was bedeutet „Security“?

Was sind typische Gefahren, Bedrohungen, Schwachstellen?

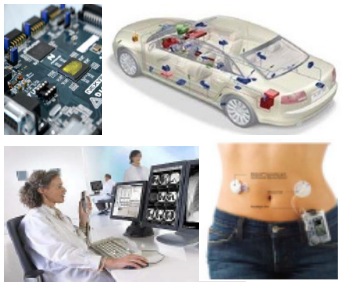
Wie erstellt man Risikoanalysen?

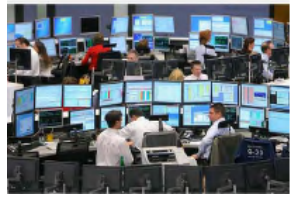
Welche Mechanismen gibt es, um Systeme „sicherer“ oder „verlässlicher“ zu machen?

Machen Firewalls ein Netz sicher?

Welche Angriffsarten gibt es?

Kann man „Sicherheit“ oder „Verlässlichkeit“ bewerten ,… und falls ja, wie ?





Gibt es sichere Verschlüsselungs-verfahren?

Wie sorgt man für Fehlertoleranz?

Inhalt der Vorlesung

- Grundlegende Begriffe und Definitionen
- Ziele und (semantische) Dimensionen der Verlässlichkeit und Security
- Risikoanalysen
- Sicherheitspläne/-konzepte
- Basisfunktionen für Verlässlichkeit und Security
- Mechanismen für Verlässlichkeit und Security
- SIcherheitsmanagement

FH Bielefeld
University of
Applied Sciences
Campus Minden

Grundlegende Begriffe und Definitionen

Begriffe (I)

- Unter einem verlässlichen und sicheren System verstehen wir im Rahmen der Vorlesung
  - ein System, dem man vertraut, dass es spezifizierte Dienste bzw. eine spezifizierte Funktionalität auch beim Auftreten von Störungen oder Fehlern korrekt und verlässlich erbringt.

- Ursache für Störungen/Fehler können sein:
  - (1) Security-Probleme*
  - (2) Dependability-Probleme (Verlässlichkeit)

*Im Rahmen dieser Vorlesung meint **Sicherheit** (sofern nicht explizit anders erwähnt) **Security**. Dagegen kann **Safety** als Teilaspekt der Verlässlichkeit betrachtet werden.

Begriffe (II)

- (1) Security-Probleme:
  - gezielte Störversuche (Angriffe) mit Schadensabsicht
  - vom Mensch verursacht und beabsichtigt
  - Angriffsmethoden:
    - Ausnutzen von Schwachstellen in Programmen: u.a. Buffer-Overflow, Cross-Site-Scripting, SQL-Injection, …
    - Ausnutzen von Design-Fehlern: u.a. Identitätsdiebstahl, Sniffing, Datenmanipulation, …
    - Ausnutzen des ‘Human Factor’: Social Engineering
  - Im Vordergrund bei Security stehen:
    - Konzepte und Verfahren, um die Schutzziele der Integrität, Vertraulichkeit, Verfügbarkeit, Authentizität und Privatheit zu erfüllen (später genauer)

Begriffe (III)

- (2) Dependability-Probleme (Verlässlichkeit)
  - fehlerhafte unzuverlässige funktionale Abläufe
    - meist von innen, durch das System selber durch inkorrekte Programmierung / Implementierung verursacht
  - unabsichtliche menschliche Fehler (human factor), meist ohne Schad-Absicht
  - Im Vordergrund bei Verlässlichkeit stehen Verfahren, um die Ziele der Zuverlässigkeit, Instandhaltbarkeit, Safety, …zu erreichen (später genauer)

Begriffe (IV)

- Beispiele
  - Security: Phishing-Angriff (Passwort Fishing)
    - Semantischer Angriff, der bestehende Geschäfts- und Vertrauens-beziehungen ausnutzt.
    - Vorgehen:
      - Benutzer werden getäuscht, um sie zur Eingabe vertraulicher Daten zu verleiten.
      - Angriffsziel: Stehlen der Identität (Authentizitätsproblem)
  - Dependability: Radio Failure at Palmdale (September 2004)
    - Fluglotsen verloren Sprachkontakt zu 400 Flugzeugen aufgrund eines Fehlers im Sprach- und Kontrollsystem
    - Human factor: Angestellter vergaß, das System zu re-booten. Software-Problem: Re-Boot war nach jeweils 30 Tagen notwendig. Der Zähler musste manuell gesetzt werden.

Begriffe (V)

- Unter einem verlässlichen und sicheren System verstehen wir im Rahmen der Vorlesung
  - ein System, dem man vertraut, dass es spezifizierte Dienste bzw. eine spezifizierte Funktionalität auch beim Auftreten von Störungen oder Fehlern korrekt und verlässlich erbringt.
- Vertrauen setzt voraus, dass das System nachweisbar
  - sicher arbeitet: Sicherheit (Security)
  - verlässlich arbeitet: Verlässlichkeit (Dependability)
  - (korrekt arbeitet: Verifizierbarkeit (Correctness))

Begriffe (VI)

- Wechselwirkungen: Verlässlichkeit und Sicherheit
  - Sicherheitsverletzungen können Verlässlichkeit gefährden: Beispiel?
  - Sicherheitsmaßnahmen können Verlässlichkeit gefährden: Beispiel?
  - Verlässlichkeitsverletzungen können die Sicherheit gefährden: Beispiel?

Begriffe (VII)

- Ausfall/Versagen (failure):
  - Ein System versagt, wenn der angebotene Service nicht mehr wie spezifiziert angeboten werden kann. Das System verhält sich nicht spezifikationskonform.
  - Beispiele für Failures sind: Absturz des Systems, das System berechnet etwas falsches, das System reagiert nicht auf Benutzereingaben.
- Eingetretener Fehler (error):
  - Teil eines unerlaubten Systemzustands, der zu einem Ausfall führen kann (falls nicht entsprechend behandelt).
- Fehlerursache (fault):
  - Ursache für einen eingetretenen Fehler.

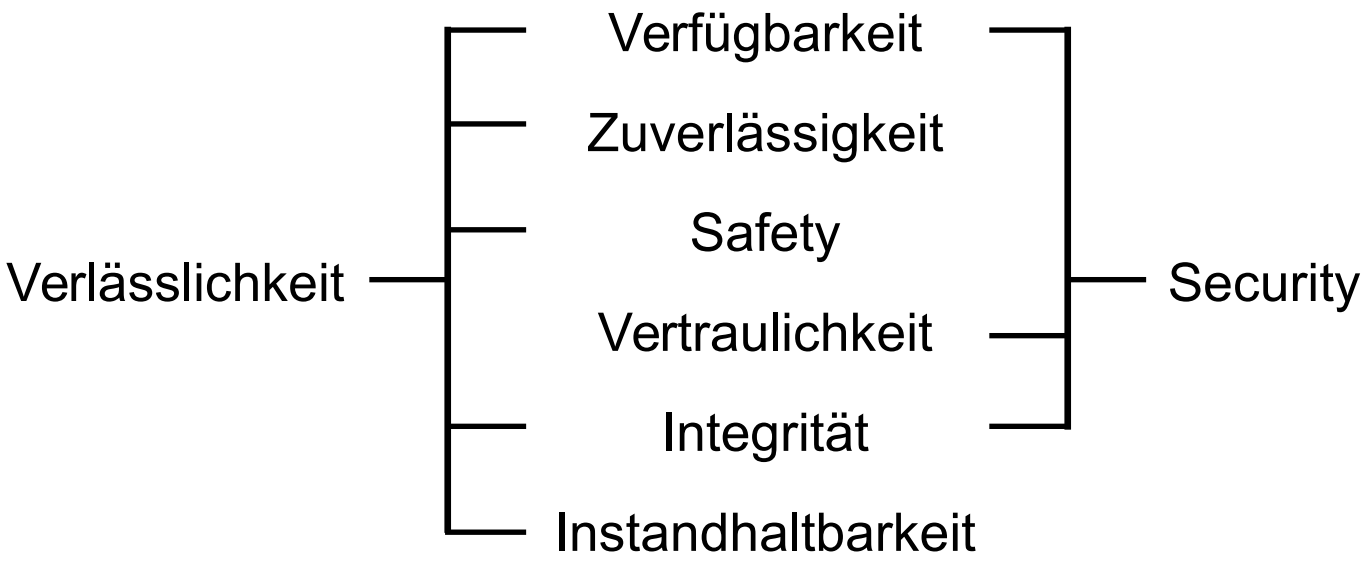
Begriffe (VIII)

- Beispiel:
  - Ein Fault in einer Robotersteuerungssoftware ist z.B. ein falsch gesetzter Punkt bei einer Dezimalzahl, welche die Koordinaten für die Bewegungen des Roboters darstellt. Durch diesen Fault wird ein Error verursacht, da sich der Roboterarm an den falschen Platz bewegt. Da sich der Roboterarm am falschen Platz befindet, kann er die geplante Arbeit nicht verrichten, was zu einem Failure führt.

FH Bielefeld
University of
Applied Sciences
Campus Minden

Ziele und (semantische) Dimensionen der Verlässlichkeit und Security

(Haupt-)Ziele der Verlässlichkeit und Security



Basic Concepts and Taxonomy of Dependable and Secure Computing
Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr,
IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 1, NO. 1,
JANUARY-MARCH 2004

Ziele der Security (I)

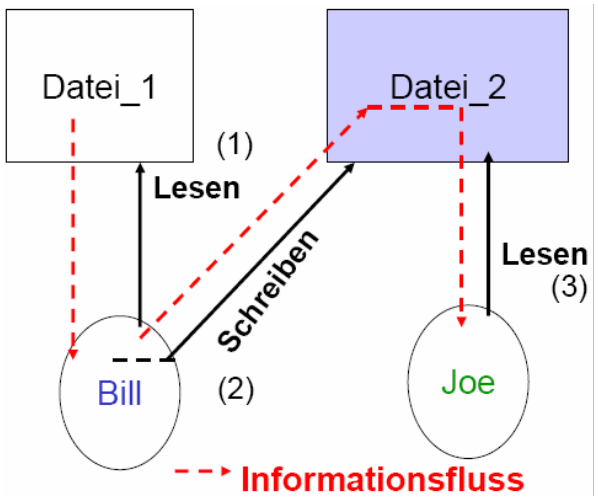
- Verfügbarkeit:
  Schutz vor unbefugter Beeinträchtigung der Funktionalität
  - Maßnahmen:
    - Festlegen und Kontrollieren von Regeln zur Aufzeichnung und Überwachung
      - Welche Zugriffe auf welche Objekte, wann mit welchem Ressourcenverbrauch (z.B. Speicher) aufzeichnen
      - Festlegen von Schwellwerten, z.B. wann ist die Netzlast zu hoch, welche Reaktionen sind einzuleiten
      - Bem.: Regelungen sind Verpflichtungen (obligation) etwas zu tun, (im Gegensatz zu den Berechtigungen/Verboten)
  - Schutzmechanismen: u.a.
    - Festlegen von Quotas (z.B. max. Anzahl von Prozessen)
    - Schreiben von Logdateien, Sichern der Logdateien
    - Intrusion Detection and Reaction Systeme (IDS)

Ziele der Security (II)

- Vertraulichkeit (bzgl. Informationen)
  Schutz vor unautorisierter Informationsgewinnung
  - Maßnahmen:
    - Festlegen und Kontrollieren von Regeln für zulässige/unzulässige Informationsflüsse
      - Wer darf auf welche Informationen zugreifen, bzw. davon Kenntnis erlangen
  - Beispiel: Prüfungsamt
    - Studierender mit Matrikelnummer X darf Kenntnis über seine Prüfungsnoten erlangen
    - Mitarbeiter im Prüfungsamt darf Kenntnis erlangen
    - Keine Kenntnis über die Prüfungsdaten für Unberechtigte
  - Frage: gleiche Regeln wie vorher oder doch Unterschied?

Ziele der Security (III)

- Bem.: Kontrolle der Objektzugriffe ≠ Kontrolle der Information!
  - Beispiel-Szenario:
    - Forderung: Subjekt Joe darf keine Kenntnis über vertrauliche Informationen erlangen, Bill aber sehr wohl!



Annahme:
Subjekt Chef schreibt vertrauliche Informationen in Datei_1 (Objekt)

Policy: Joe hat kein Recht, auf Datei_1 zuzugreifen!

Gut, aber reicht nicht, denn …

Annahme:
Bill liest die Information aus Datei_1 und schreibt sie in Datei_2 ⇒ Forderung verletzt

Ziele der Security (IV)

- Schutzmechanismen für Vertraulichkeit:
  - Verschlüsselung: symmetrisch oder asymmetrisch
    - Bem.: als Technik geeignet, aber Hauptsicherheitsprobleme liegen im korrekten Einsatz von Verschlüsselung:
      - Was (welche Information) soll verschlüsselt werden?
        Daten in Dateien, aber was ist mit der Metainformation?
      - Wo liegen Kopien entschlüsselter Daten?
        auf der Platte (nach Login)? Im Hauptspeicher? In Caches?
      - Wer kennt alles den Schlüssel: nur einer? Probleme?
  - Klassifizieren (labeling) von Objekten und Subjekten:
    z.B. vertraulich, geheim, streng-geheim
  - Kontrollierte Informationsweitergabe: z.B. no write down

Ziele der Security (V)

- Integrität (bzgl. Daten)
  Schutz vor unautorisierter und unbemerkter Modifikation

  - Maßnahmen:
    - Festlegen und Kontrollieren von Regeln für zulässige/unzulässige Datenänderungen
      - Wer (Subjekt) darf Was (Rechte) unter welchen Bedingungen mit welchem Objekt (Asset) tun?
  - Beispiel für Regeln im Prüfungsamt-Szenario
    - Studierender mit Matrikelnummer X darf nur lesend auf seine Prüfungsnoten in seiner Akte zugreifen
    - Mitarbeiter im Prüfungsamt darf lesen und schreiben, aber nur vom PC des Prüfungsamtes
    - Admin hat kein Schreibrecht auf die Prüfungsdaten

Ziele der Security (VI)

- Schutzmechanismen für Integrität:
  - Verschlüsselung (s. zukünftige Vorlesung)
  - Hashfunktionen und MACs? (s. zukünftige Vorlesung)
  - Vergabe von Zugriffsrechten: z.B. l, w, x
  - Schutzdomänen, Sandboxes: Isolierung von Prozesen
  - Firewall: Filtern von Datenpaketen, Intrusion Detection System

Weitere Ziele der Security (I)

- Die Ziele
  - Vertraulichkeit - **C**onfidentiality
  - Integrität - **I**ntegrity
  - Verfügbarkeit - **A**vailablility

  heißen auch CIA-Ziele oder Hauptziele der Security.

- Gibt es weitere sinnvolle Ziele der Security?

Weitere Ziele der Security (I)

- Verbindlichkeit:
  Schutz vor unzulässigem Abstreiten durchgeführter Handlungen
  - Maßnahmen: Festlegen, was verbindliche Aktionen sind
    - Festlegen, welche Nachweise, dass die Aktion verbindlich ist, zu erstellen sind
    - Beweissicherungen durchführen (ggf. bis hin zu Computer Forensik)
    - Beispiel Prüfungsamt:
      - Melden von Noten an das Prüfungsamt durch Prüfer?
  - Schutzmechanismen: u.a.
    - (qualifizierte) digitale Signaturen und Zertifikate
    - Änderungshistorien verwalten, Log-Bücher führen

Weitere Ziele der Security (II)

- Authentizität:
  Nachweis der Echtheit und Glaubwürdigkeit der Identität eines Objekts/Subjekts
  - Maßnahmen:
    - Festlegen und Kontrollieren von Regeln zu Vergabe von eindeutigen Identifikationen von Subjekten und Objekten und Verfahren zum Nachweis der Korrektheit der Identität
    - Beispiel Prüfungsamt:
      - Identität des Studierenden: Matrikelnummer
      - Nachweis der Identität: Kenntnis eines Passworts (?)
  - Schutzmechanismen: u.a.
    - Passworte, PINs, secret Keys, Biometrie
    - Smartcards, Security-Tokens
    - Signierter Code (was für eine Authentizität damit erreichbar?)

Weitere Ziele der Security (III)

- Beispiel: Identitätsfälschung
  - Mail mit gefälschter Mailadresse (mit Virus im Anhang)
    - Sehr geehrte Dame, sehr geehrter Herr,
      das Herunterladen von Filmen, Software und MP3s ist illegal und somit strafbar.
      Wir möchten Ihnen hiermit vorab mitteilen, dass Ihr Rechner unter der IP
      233.160.187.243 erfasst wurde. Der Inhalt Ihres Rechner wurde als
      Beweismittel sichergestellt und es wird ein Ermittlungs-verfahren gegen Sie
      eingeleitet. Die Strafanzeige und die Möglichkeit zur Stellungnahme wird Ihnen
      in den nächsten Tagen schriftlich zugestellt.

      Aktenzeichen NR.:#4621 (siehe Anhang)
      Hochachtungsvoll
      i.A. Jürgen Stock
      --- Bundeskriminalamt BKA
      --- Referat LS 2
      --- 65173 Wiesbaden
      --- Tel.: +49 (0)611 - 55 - 12331 oder --- Tel.: +49 (0)611 - 55 - 0

Weitere Ziele der Security (IV)

- Privatheit:
  Schutz der personenbezogenen Daten, Schutz der Privatsphäre, Gewährleistung des informationellen Selbstbestimmungsrechts
  - Maßnahmen: Regeln zu Datenvermeidung, zur
    - Datensparsamkeit
    - Festlegung der Zweckbindung der erhobenen Daten
    - Festlegen von ‚Verfallsdaten‘
  - Schutzmechanismen: u.a.
    - Pseudonyme anstelle von realen Identitäten
    - Verschlüsseln der Identitäten (Tunneln), z.B. Sendeadresse

Ziele der Dependability (I)

- Verfügbarkeit:
  Schutz vor unbeabsichtigter Beeinträchtigung der Funktionalität
  - Maßnahmen:
    - Festlegen und Kontrollieren von Regeln zur Kontrolle und zur Bereitstellung von Komponenten und Ersatz und Einsatz redundanter und diversitärer Komponenten
  - Schutzmechanismen: u.a.
    - Backups und Mirroring (Spiegeldateien)
    - Ersatzhardware und Clustersysteme,
    - Redundanz
    - Health-checks

Ziele der Dependability (II)

- Zuverlässigkeit:
  Schutz vor Fehlern in einem Zeitintervall
  - Maßnahmen:
    - Festlegen und Kontrollieren von Regeln zur Zuverlässigkeitsbewertung und Erkennung kritischer Komponenten und ständige Systemverbesserung über den Lebenszyklus
  - Schutzmechanismen: u.a.
    - Einsatz betriebsbewährter und qualifizierter Komponenten
    - Einsatz redundanter und diversitärer Komponenten
    - Maßnahmen der Fehlerselbsterkennung
    - Anwendung des Prinzips „Fail-Safe“

Ziele der Dependability (III)

- Safety:
  Schutz der Umgebung / des Menschen (vor katastrophalen Auswirkungen eines Systemversagens)
  - Maßnahmen:
    - Festlegen und Kontrollieren von Regeln zur Vermeidung, Erkennung, Beseitigung und Einschränkung katastrophaler Auswirkungen
  - Schutzmechanismen: u.a.
    - Verwendung betriebsbewährter und qualifizierter Komponenten
    - Maßnahmen der Fehlerselbsterkennung
    - Stress Testing
    - Anwendung des Prinzips „Fail-Safe“
    - Schulung der Nutzer und des Umfelds

Ziele der Dependability (IV)

- Instandhaltbarkeit:
  Fähigkeit eines Systems, unter gegebenen Anwendungsbedingungen in einem Zustand erhalten bzw. in ihn zurückversetzt werden zu können, in dem es eine geforderte Funktion erfüllen kann, wobei vorausgesetzt wird, dass die Instandhaltung unter den gegebenen Bedingungen mit den vorgeschriebenen Verfahren und Hilfsmitteln durchgeführt wird (DIN IEC 60300-3-10).

Ziele der Dependability (V)

- Instandhaltbarkeit:
  - Maßnahmen:
    - Verwendung von standardisierten Bauteilen,
    - Sicherstellung (im Lifecycle, bginnend bei der Konzeption)
      - einer leichten Zugänglichkeit der Komponenten, die häufiger repariert oder ausgetauscht werden müssen,
      - einer eichten Handhabbarkeit und Ersetzbarkeit von Komponenten sowie
      - einer einfachen und genau die Störung ermittelnde Prüfbarkeit.

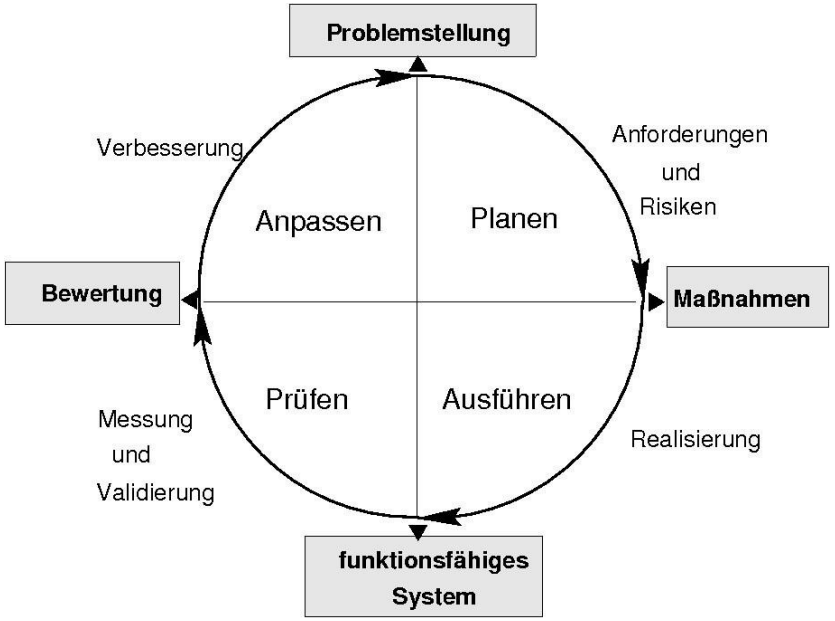
Schutzziele im Einzelnen

- Schutzziele sind abhängig von der zu schützenden Anwendung bzw. den Funktionen des zu schützenden Systems

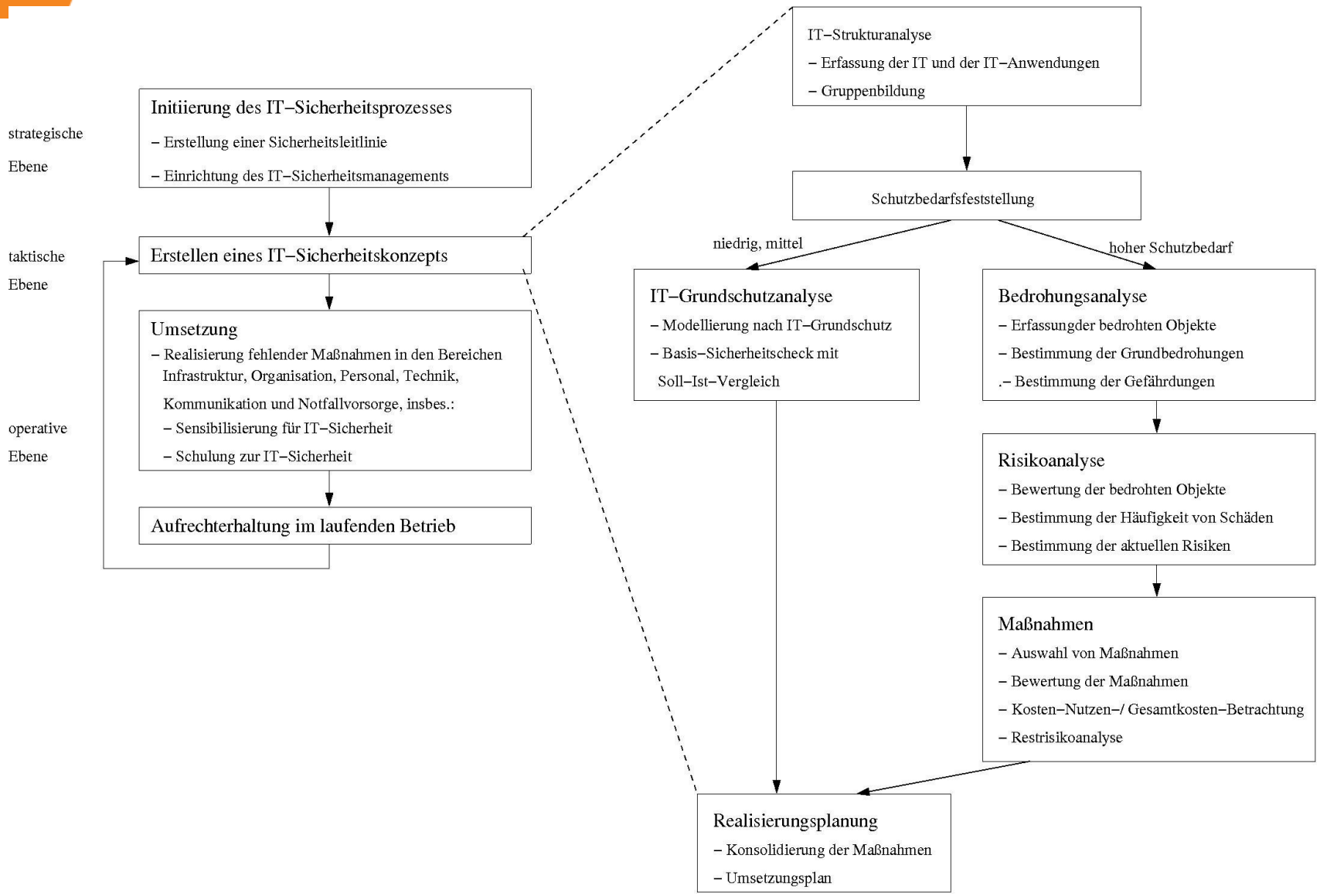
- Beispiel-Szenarien:
  - (1) Prüfungsamt-Szenario: Schutzziele?
  - (2) E-Bay-Verkaufs-Szenario: Schutzziele?

„Dependability & Security“-Engineering

- Strukturanalyse und Pflichtenheft
- Ermittlung des Schutzbedarfs
- Bedrohungsanalyse
- Risikoanalyse
- Erstellen einer Sicherheits-Policy
- Modellierung des Systems
- Entwurf einer Systemarchitektur
- Feinentwurf und Implementierung
- Validierung und Evaluierung des Systems
- Wartung und Überprüfung im laufenden Betrieb



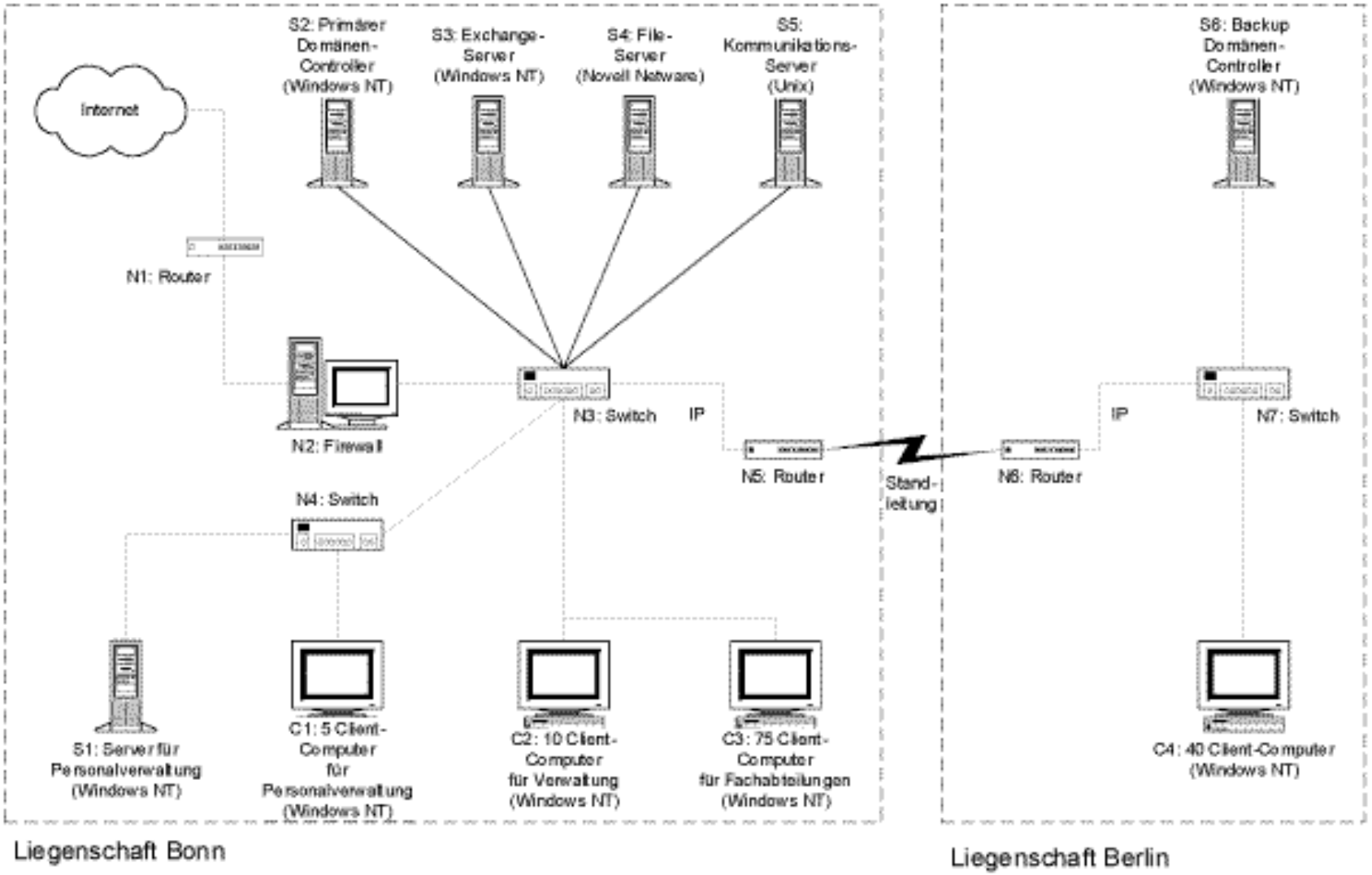
Beispiel „Dependability & Security“ Engineering
BSI Sicherheitsprozess



Strukturanalyse

- Beschreibung des (vorhandenen bzw. geplanten) Systems:
- Beschreibung der Systemfunktionalität
  - Beschreibung vorhandener bzw. einzusetzender
- Systemkomponenten u. -dienste
- Beschreibung des Pflichtenhefts
  - Systemanforderungen und Einsatzumgebung des Systems
- Erstellung eines Netztopologieplans
  - grafische Übersicht aller Teilkomponenten (z.B. PCs, Server, DBs, Hubs) und deren Verwendungszweck
  - Vorhandene Dienste u. Verbindungen (LAN, WLAN, ...)
  - Technische Details (z.B. Hardware, MAC-Adresse, ...)

Beispiel für Netztopologieplan



Beispiel für Übersicht der Komponenten

Nr.	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Anwender/ Admin.
S1	Server für Personalverwaltung	Windows NT-Server	1	Bonn, R 1.01	in Betrieb	Personalreferat
S2	Primärer Domänen-Controller	Windows NT-Server	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
C1	Gruppe von Clients der Personaldatenverarbeitung	Windows NT-Workstation	5	Bonn, R 1.02 - R 1.06	in Betrieb	Personalreferat
C2	Gruppe von Clients in der Verwaltungsabteilung	Windows NT-Workstation	10	Bonn, R 1.07 - R 1.16	in Betrieb	Verwaltungsabteilung
C6	Gruppe der Laptops für den Standort Berlin	Laptop unter Windows 95	2	Berlin, R 2.01	in Betrieb	alle IT-Anwender in der Außenstelle Berlin
N1	Router zum Internet-Zugang	Router	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N2	Firewall	Application Gateway auf Unix	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N3	Switch	Switch	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
T1	TK-Anlage für Bonn	ISDN-TK-Anlage	1	Bonn, B.02	in Betrieb	alle Mitarbeiter in der Hauptstelle Bonn

Schutzbedarfsermittlung

- Ziel:
  - Klären: Was sind schützenswerte Objekte, was sind die Schutzziele, wie wichtig sind sie?
  - Schutzbedarfsfeststellung anhand von Schadensszenarien, z.B. orientiert an Grundschutzhandbuch des BSI
  - meist nicht quantitative sondern qualitative Aussagen: niedriger bis mittlerer, hoher, sehr hoher Bedarf

niedrig bis mittel	Die Schadensauswirkungen sind begrenzt und überschaubar
hoch	Die Schadensauswirkungen können beträchtlich sein
sehr hoch	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß annehmen

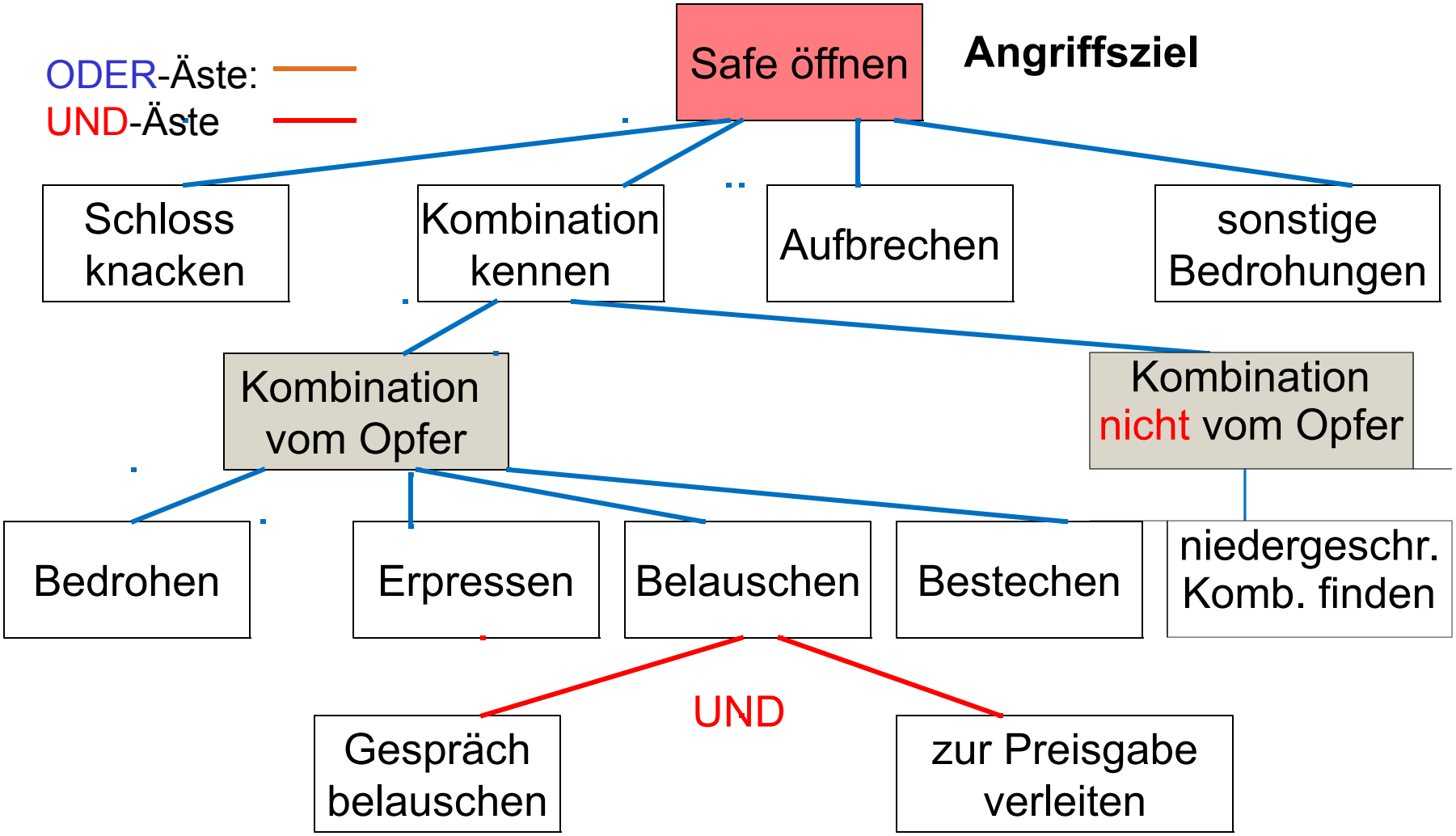
Bedrohungsanalyse & Risikoanalyse

- Was sind Risiken?
  - Kombination aus Bedrohungen (Threats) und Verwundbarkeiten (Schwachstellen, Vulnerabilities)
  - Schadenspotential
    - Monetär: finanzielle Schäden
    - Nicht monetär:
      - gesundheitliche Schäden
      - Gesetzesverstöße (Compliance),
      - Ruf- oder Ansehensschädigung
  - Schadenswahrscheinlichkait
    - Wahrscheinlichkeit dafür, dass ein Schaden eintritt

Bedrohungsanalyse (I)
Beispiel Bedrohungsbaum

- Methode: Strukturierte Analyse mittels Bedrohungsbäumen (attack tree)
  - Angelehnt an Fehlerbäumn, HAZARD-Analyse
  - Ziel: Modellierung verschiedener Angriffsmöglichkeiten
  - Pro Angriffsziel ein Baum:
    - Wurzel beschreibt ein Angriffsziel, z.B. Safe knacken
    - Blatt beschreibt einen einzelnen Angriffsschritt
    - Pfad von Blatt zur Wurzel: Angriff zum Erreichen des Ziels
  - Beschreibung von Situationen, in denen
    - mehrere Angriffsschritte zusammen notwendig sind: UND
    - alternative Angriffsschritte möglich sind: ODER-Äste (Teilbäume)
  - Zur systematischen Erstellung: Festlegen von Teilzielen

Bedrohungsanalyse (II)
Beispiel Bedrohungsbaum



Bedrohungsanalyse (III)
Beispiel Bedrohungsbaum

- Methode ist primär für die Analyse von aktiven Angriffen ausgelegt.
  - Technische Fehler / Naturkatastrophen etc. können nicht analysiert werden
- Methode hilft Systeme zu analysieren, für die es noch keine publizierten Analysen möglicher Angriffe bzw. Tabellen mit Risiken / Gefährdungslagen gibt.
- Auswirkung von Gegenmaßnahmen kann studiert werden.

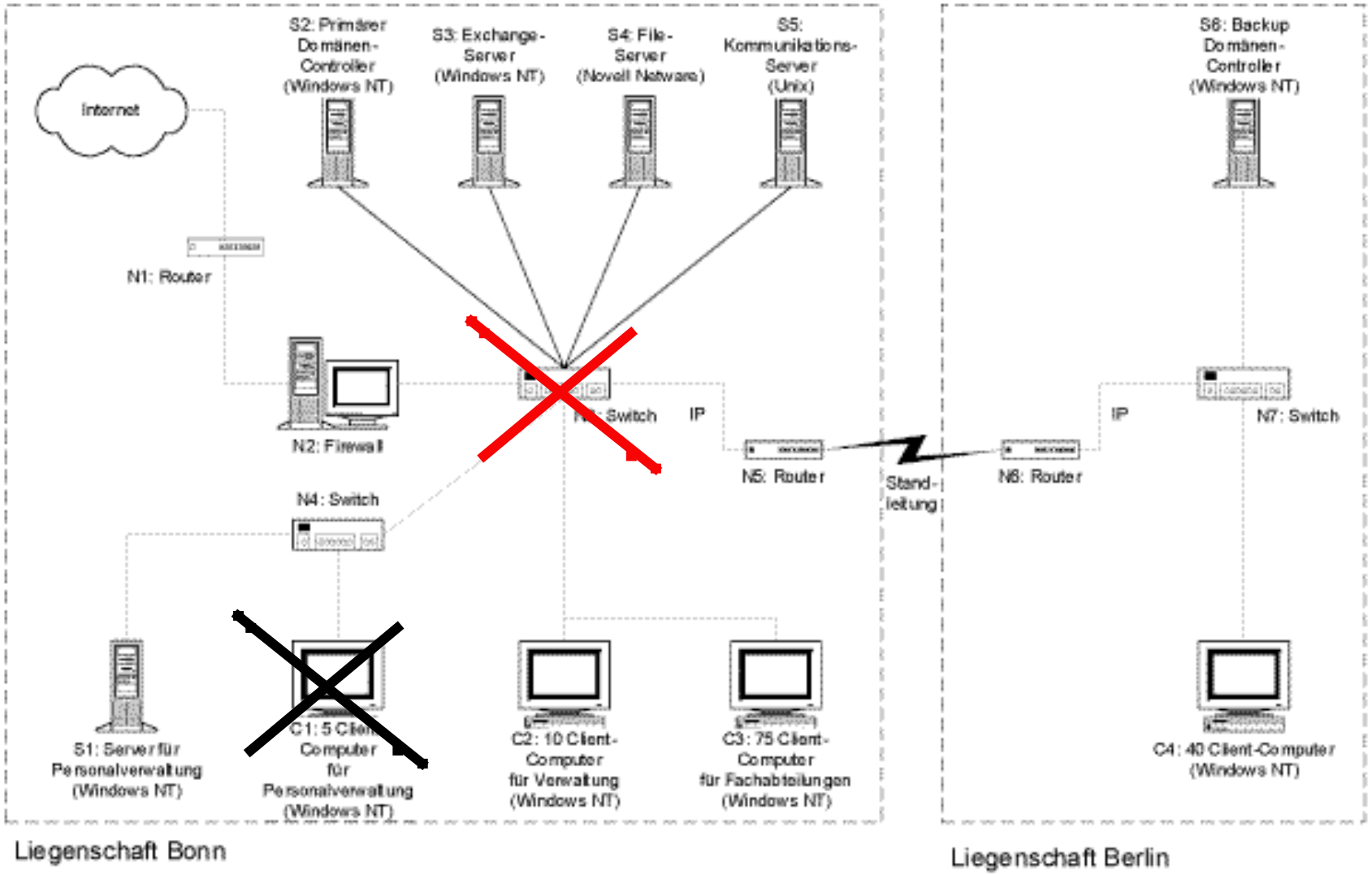
Bedrohungsanalyse (IV) Beispiel: STRIDE-Methode

- Methode, um STRIDE-Angriffe zu identifizieren, bewerten und Abwehrmaßnahmen festzulegen (insbes. für Consumer-Anwendungen)
  - S poofing Identity: Alle Arten von Maskierungsangriffen
  - T ampering with Data: Veränderung persistenter Daten und Integrität von Datenpaketen
  - R epudiation: Abstreiten von Aktionen
  - I nformation Disclosure: Unberechtigte Informationsweitergabe
  - D enial of Service: Überfluten, Fehlleiten, etc.
  - E levation of Privilege: Erhöhen der eigenen Berechtigungen
  - Für jede Angriffsklasse:
    - Festlegen von Best-Practice-Abwehrmaßnahmen
    - z.B. starke Mehrfaktor-Authentisierung, Verschlüsselung, …

Bedrohungsanalyse (V)
Beispiel: STRIDE-Methode

- Einsatz von STRIDE
  - Schwachstellen-Analyse der Software-Komponenten in Bezug auf die sechs Angriffsklassen (S,T, R, I, D und E)
  - Modellierung der Systeme und Komponenten, z.B. mit UML
    - mögliche Datenflüsse (u.a. Netzverbindungen),
    - Datenspeicher (u.a. Dateien, Datenbanken),
    - Prozesse (u.a. Benutzer, Server, Web-Dienste)
  - Für jedes Element: Prozesse, Datenspeicher, Datenflüsse:
    - Identifizierung der Bedrohungen der STRIDE-Klassen,
    - z.B. für Datenflüsse sind es Bedrohungen der Klassen Tampering, Disclosure oder auch Denial of Service
    - Identifikation von Abwehrmaßnahmen

Bedrohungsanalyse (VI)
Failure Impact Analysis



Bedrohungsanalyse (VII) Failure Impact Analysis

- Vorgehen und Ergebnis
  - Systematisches Probieren:
    - Wie wirken sich Verlust von
      - Vertraulichkeit
      - Verfügbarkeit
      - Integrität

      auf mein Verfahren aus?

- Ergebnis: Single Points of Failure (SPOF) werden rasch entdeckt

Bedrohungsanalyse (VIII)
Beispiel: Kataloge aus Standards

- Inspiration aus Standardrisiken nach ISO 27001
  - Abgeleitet aus den Control-Objectives:
    - Unzureichende Sicherheitspolitik
    - Mangelhafte interne (Sicherheits-) Organisation
    - Fehlende Sicherheit bei bzw. durch Externe
    - Unzureichendes Management der vorhandenen Werte
      - Personal mit seinen Beschäftigungszyklen nimmt hier breiten Raum ein
    - Unzureichende Raum- und Gebäudesicherheit (Physical and Environmental Security), Zutrittsschutz
    - Mangelhafte Regelungen im Umgang mit Ausstattung
    - Unzureichende Regelungen für die Planung und den IT-Betrieb (ITIL)
    - Fehlende Sicherheit bei Dienstleistern
    - Unzureichender Schutz gegen Schadcode und mobilen Code

Bedrohungsanalyse (IX)
Beispiel: Kataloge aus Standards

- Weitere Standardrisiken nach ISO 27001
  - Unzureichende Datensicherung
  - Unzureichende Netzwerksicherheit
  - Unzureichende Sicherheit im Umgang mit Speichermedien
  - Unzureichende Sicherheit bei Informationsaustausch
  - Unsichere eCommerce-Dienste
  - Fehlende Überwachung von Systemen, Nutzern und Administratoren
  - Unzureichender Zugangs- und Zugriffsschutz
    - Bezogen auf Systeme,
    - Betriebssysteme und
    - Netze
    - Anwendungen
  - Unzureichende Sicherheit bei Telearbeit
  - Unzuverlässige Datenverarbeitung in Anwendungen

Bedrohungsanalyse (X)
Beispiel: Kataloge aus Standards

- Weitere Standardrisiken nach ISO 27001
  - Fehlender oder unsicherer Einsatz von Kryptographie
  - Unsicherheit in Dateisystemen
  - Unzureichende Beachtung der Sicherheit bei Softwareentwicklung
  - Fehlendes oder unwirksames Management von Verwundbarkeiten
  - Unzureichendes oder fehlendes Management von sicherheitskritischen Ereignissen oder Sicherheitsvorfällen
  - Fehlende oder unzureichende Notfallvorsorge
  - Fehlende Compliance
  - Fehlende interne Compliance
  - Fehlende Auditierung und Optimierung des Sicherheitsmanagement-Systems

Bedrohungsanalyse (XI)
Beispiel: Kataloge aus Standards

- Inspiration aus Grundschutzkatalogen des BSI
  - Pauschalisierte Gefährdungen und Eintrittswahrscheinlichkeiten für typische Komponenten eines Systems (Server, Clients, Serverraum, E-Mail...)
  - Empfehlung von Standard-Sicherheitsmaßnahmen
  - Konkrete Maßnahmenbeschreibung

Risikoanalyse

- Wie kann man Risiken analysieren?
  - Quantitativ
  - Qualitativ
  - Grundschutzmethode

- Quelle: ISO TR 13335 Teil 3

Quantitative Bewertung von Risiken (I)

- Sicherheitsrisiko R = S · P mit:
  - Schadenshöhe (Schadenspotential) S
  - Eintrittswahrscheinlichkeit E
- Beispiele:

  S = 1.000.000 EUR; P = 0,01: R = 10.000 EUR

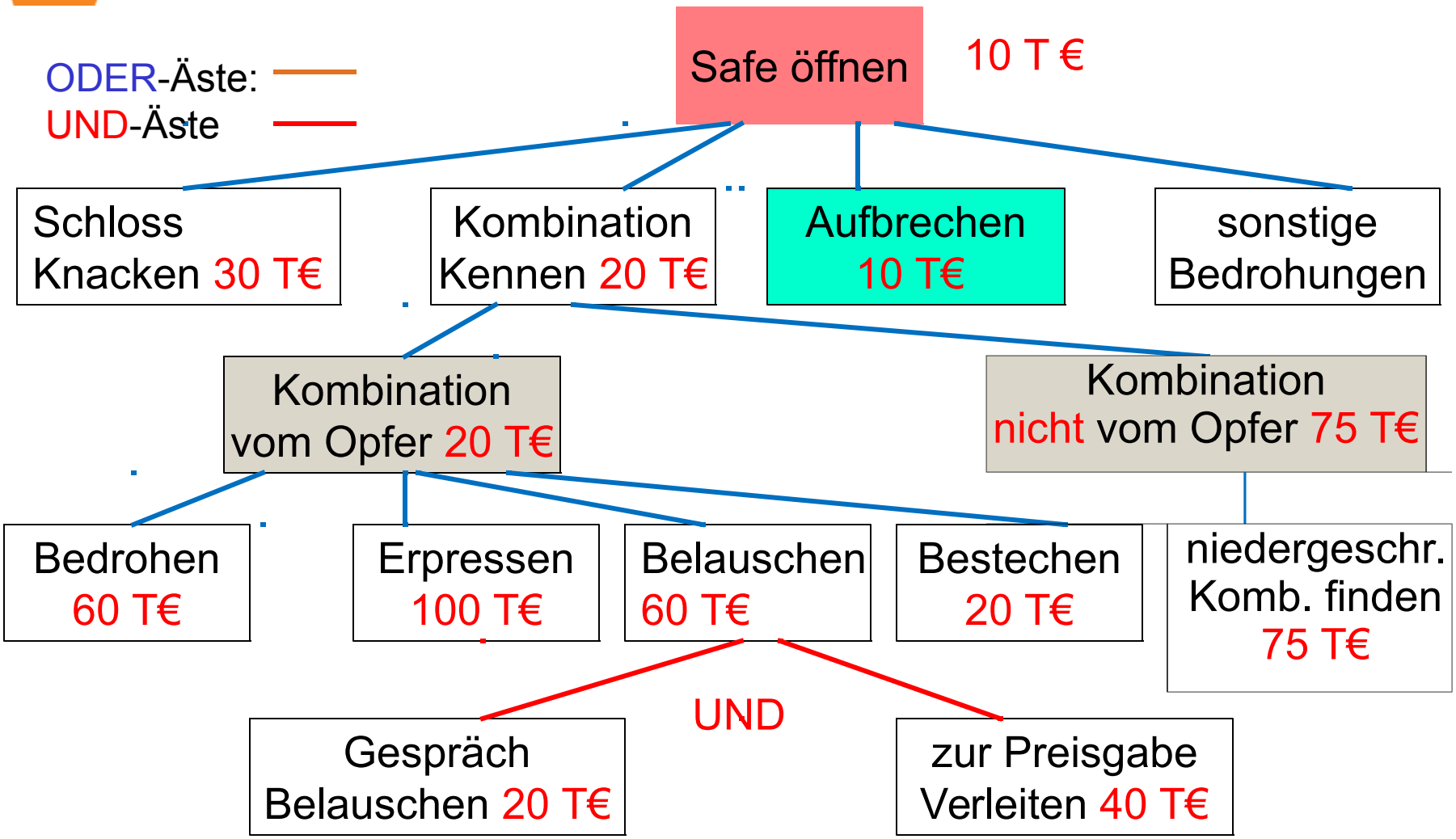
  S = 30.000 EUR; P = 0,5: R = 15.000 EUR

- Schadenshöhe S:
  - Primäre Schäden: Produktivitätsausfall, Wiederbeschaffungs-, Personalkosten, Wiederherstellungskosten, …
  - Sekundäre Schäden (schwer zu quantifizieren): Imageverlust, Vertrauensverlust bei Kunden, ….

Quantitative Bewertung von Risiken (II)

- Bestimmung der Eintrittswahrscheinlichkeit P (0 ≤ P ≤ 1):
  - Eigene Erfahrungen (z.B. aus Auditprozessen)
  - Öffentliche Statistiken
  - Einschätzung des Nutzens für den Angreifer und Einschätzung des Aufwands für erfolgreichen Angriff auf Basis von Angreifermodellen
    - Angreifermodell: beschreibt u.a.
      - Angreifertyp (Hacker, Spezialist, ...),
      - Budget (Unternehmen, Regierung, Privatperson, ...)
      - Kenntnisse (keine, Insider-Wissen, Expertenwissen, ...),
      - Ziele (Gewinn, Schaden, Rache, ...)
- Methodik: z.B. Attributierung des Baumes mit S und P-Werten

Quantitative Bewertung von Risiken (III)
Attributierung des Bedrohungsbaums



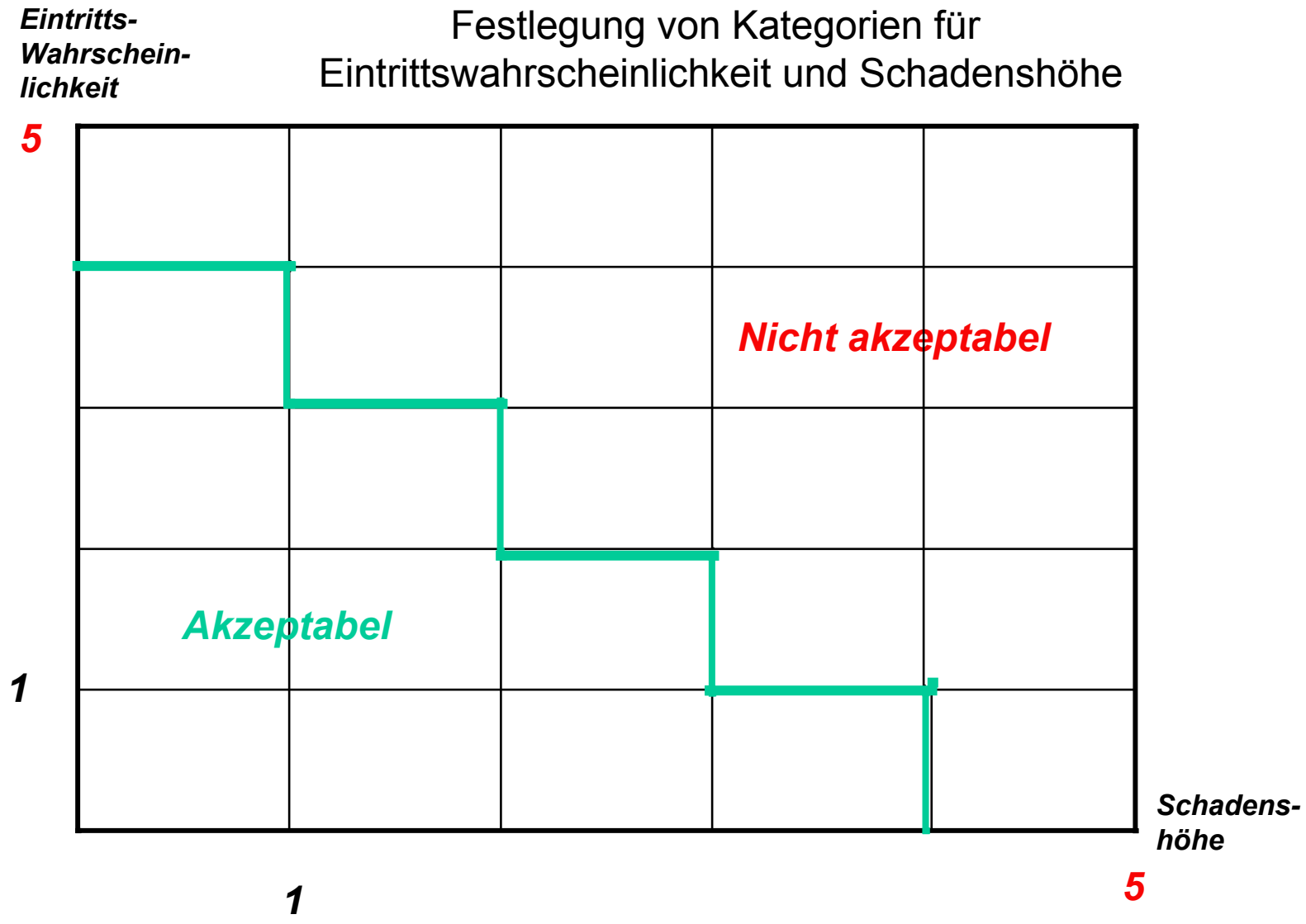
Ziel: Erkennen der „kritischen“ Pfade!

Quantitative Bewertung von Risiken (IV)

- Vorteile
  - Vergleichbarkeit der Ergebnisse
  - Methode in der Finanzwirtschaft etabliert und weit verbreitet
  - Gute Möglichkeit der Diskussion der Wirtschaftlichkeit von Maßnahmen
- Nachteile
  - Unschärfe bei Schadenshöhen (speziell bei sekundären Schäden)
  - Eintrittswahrscheinlichkeiten oft nicht genau bekannt
    - Wie oft und wie lange fällt ein Switch aus?
  - Wechselwirkungen können nicht einfach berücksichtigt werden.

Qualitative Bewertung von Risiken (I)

Festlegung von Kategorien für
Eintrittswahrscheinlichkeit und Schadenshöhe



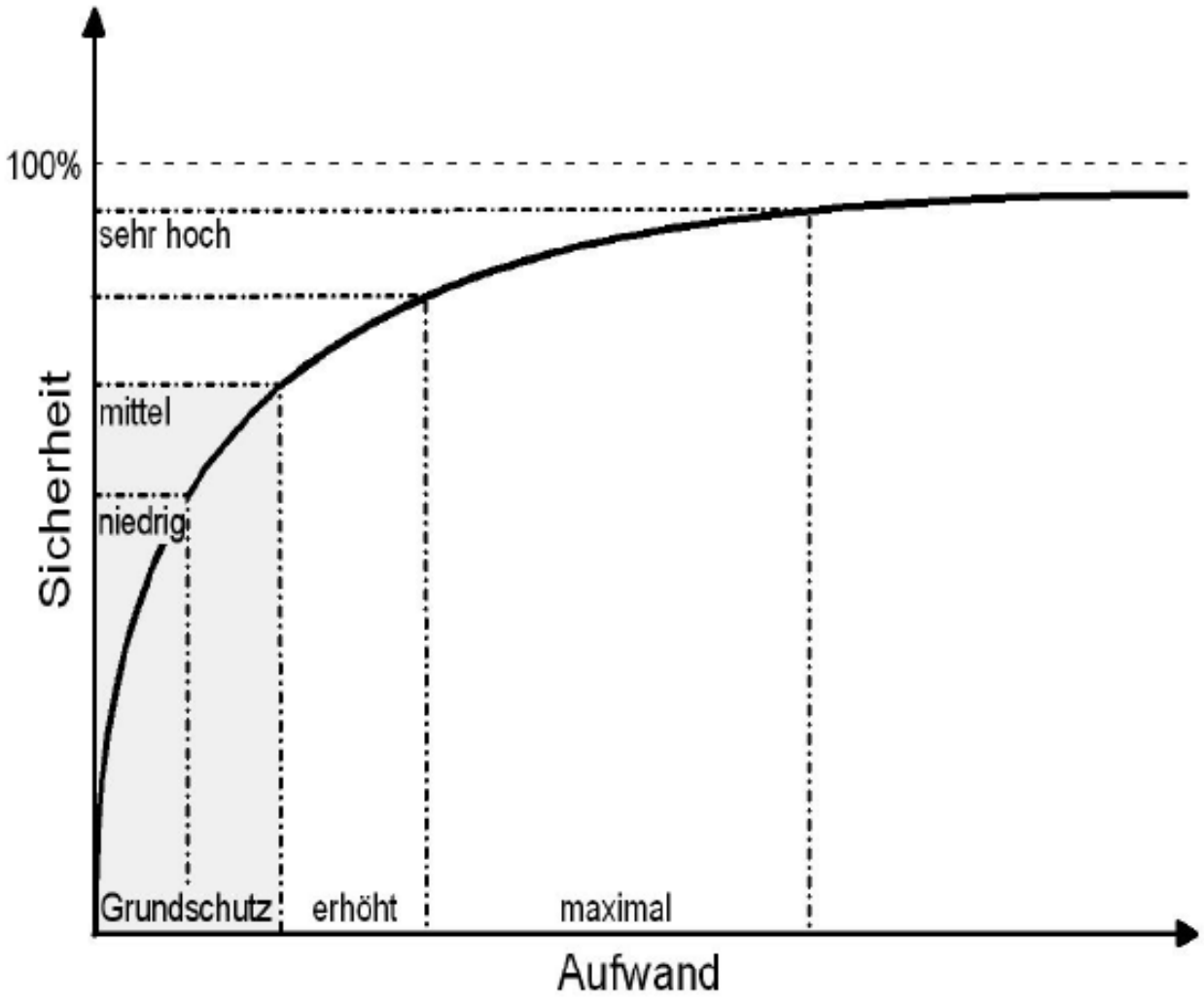
Qualitative Bewertung von Risiken (II)

- Vorteile
  - Anschaulichkeit
  - Gute Möglichkeit der Diskussion der Wirtschaftlichkeit von Maßnahmen
- Nachteile
  - Reproduzierbarkeit?
  - Einschätzung hängt stark von der Erfahrung der Beteiligten und von der „Risikokultur“ der Organisation ab.

Grundschutzmethode des BSI (I)

- These: Es gibt ein Sicherheitsniveau, das für durchschnittliche Verfahren ausreichend ist.
  - Dieses ist durch ein Set an Risiken und korrespondierenden Maßnahmen (in den Grundschutzkatalogen) beschrieben
  - Abweichungen in den Sicherheitsanforderungen werden relativ zu diesem Grundschutzniveau (baseline security level) beschrieben. (Vgl. Folie 37)

Grundschutzmethode des BSI (II)



Risikobehandlung (I)

- Umgang mit Risiken
  - Reduzierung
    - Durch technische und organisatorische Maßnahmen
  - Vermeidung
    - Durch Änderung in den Verfahren und der Infrastruktur
  - Verlagerung
    - Versichern
  - Tragen
    - Restrisiko
    - Residual Risk

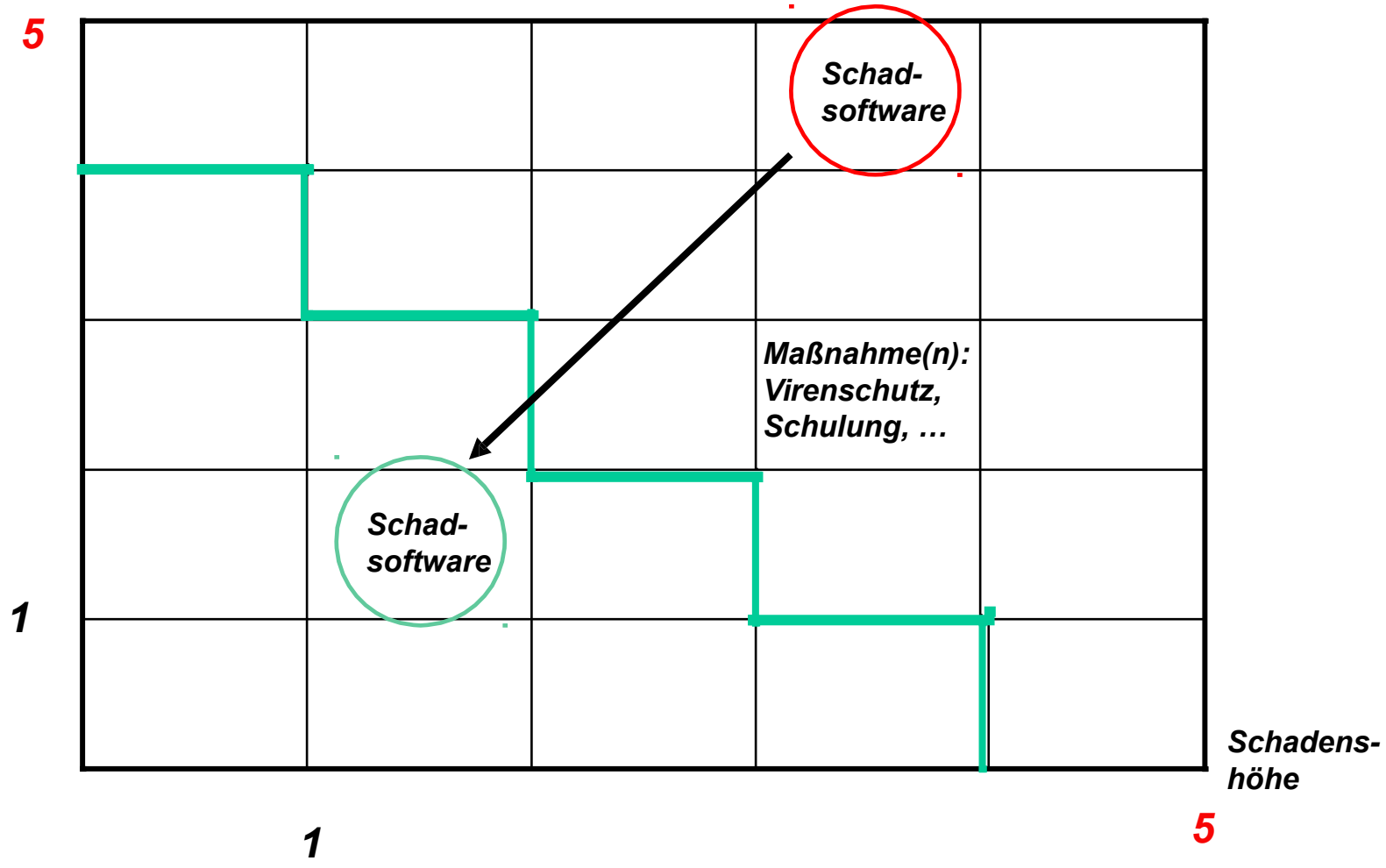
Risikobehandlung (II)

- Risikoreduzierung

  - Schritt 1: Zusammenstellen der zu reduzierenden Risiken
  - Schritt 2: Ermitteln geeigneter Maßnahmen
  - Schritt 3: Analyse der Wirkung von Maßnahmen

Risikobehandlung (II)

Festlegung von Kategorien für Eintrittswahrscheinlichkeit und Schadenshöhe



Risikobehandlung (III)

- Maßnahmentypen der Risikoreduzierung:
  - Maßnahmen zur
    - Verhinderung von Ursachen
    - Reduzierung von Schäden
    - Tolerierung von Schäden
    - Voraussage von Schäden
  - Analyse des neuen Systems (“Simulation”)

➡ Reduzierung des Gesamtrisikos

Maßnahmen und Schutzmechanismen aus der Kryptographie

- Zur Umsetzung der Ziele der Security und Dependability werden (jeweils) verschiedene Maßnahmen und die für sie geeigneten Schutzmechanismen angewendet.
- Für die Ziele Vertraulichkeit und Integrität (von Informationen) werden
  - als Maßnahmen das Festlegen und Kontrollieren von Regeln für zulässige/unzulässige Informationsflüsse und von Regeln für zulässige/unzulässige Datenänderungen angewendet;
  - u.a.Schutzmechanismen aus der Kryptographie (z.B. Verschlüsselung, Hashfunktionen etc). eingesetzt