Einführung

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

- Reale Welt versus elektronische Welt
- Die Begriffe Sicherheit und IT-Sicherheit
- Bedeutungswandel der IT-Systeme
- IT-Sicherheit als Wirkungs- und Handlungszusammenhang
- Angriffsmöglichkeiten in Kommunikationssystemen
- Schäden
- Wer kümmert sich in Deutschland um die IT-Sicherheit?
- Zusammenfassung

Inhalt

- **Reale Welt versus elektronische Welt**
- Die Begriffe Sicherheit und IT-Sicherheit
- Bedeutungswandel der IT-Systeme
- IT-Sicherheit als Wirkungs- und Handlungszusammenhang
- Angriffsmöglichkeiten in Kommunikationssystemen
- Schäden
- Wer kümmert sich in Deutschland um die IT-Sicherheit?
- Zusammenfassung

In einer perfekten Welt

- ... regieren Vertrauen und Freundlichkeit.
- ... sind alle Informationen frei verfügbar und kostenlos.
- ... bereichert sich niemand zu Lasten anderer.
- ... zahlen alle Kunden gerne den gewünschten Preis.
- ... ist Wettbewerb transparent, fair und ausgeglichen.

Eine perfekte Welt gibt es nicht

Wie sieht die reale Welt aus?

- Informationen und Wissen (also Macht) sind ungleich verteilt
- Einbruch und Diebstahl gefährden Eigentum
- Betrug und Verrat beeinflussen das Geschäftsleben
- Anschläge und Terror zählen zum Alltag

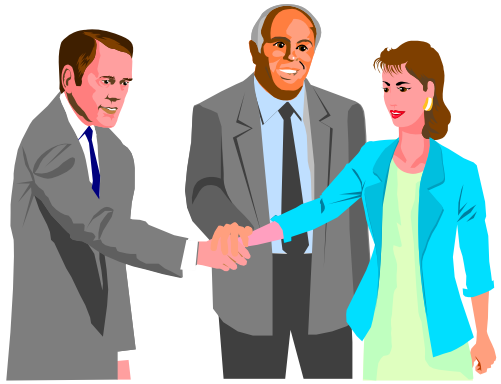
Wie schützen wir uns in einer realen Welt?

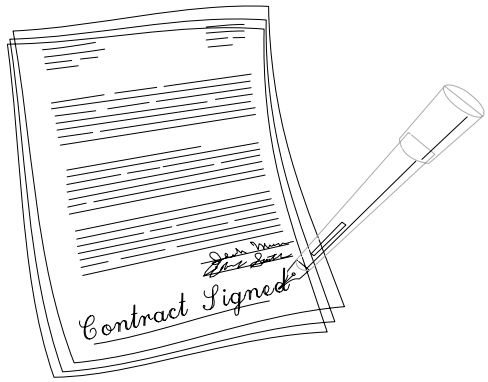
- **Pförtner**
  sorgt dafür, dass kein Unbefugter das Unternehmensgebäude betritt
- **Sicherheitstransporter**
  sichert den Transport der Unternehmenswerte
- **Standesamt/Einwohnermeldeamt**
  sichert die eindeutige Identität und deren Überprüfbarkeit
- **Briefe/Handgeschriebene Unterschrift**
  sorgt für den vertraulichen Austausch von Informationen und die Verbindlichkeit der damit verbundenen Aktionen
- **Safe/abschließbare Schränke**
  sorgt für eine sichere Aufbewahrung der Werte (Informationen, Strategiepapiere, Bürgerdaten etc.)

Reale versus elektronische Welt

„Vertrauenswürdigkeit in der elektronischen Welt”

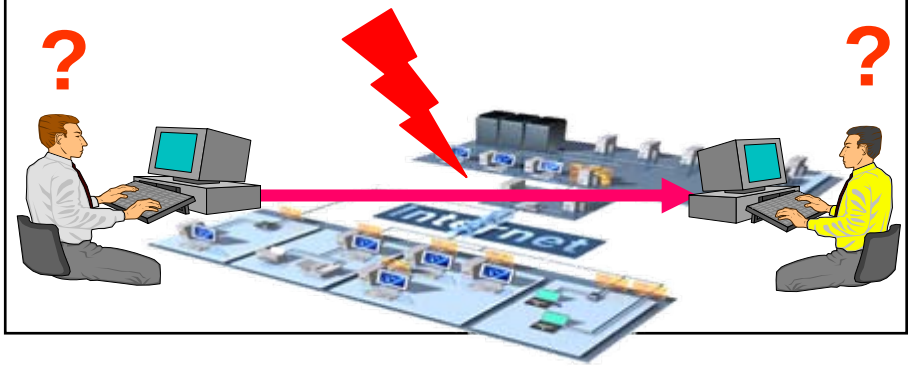
Reale Welt





Elektronische Welt benötigt

- Vertraulichkeit
- Authentisierung
- Datenintegrität
- Nachweisbarkeit



Wie kann sich die Informations- und Wissens-gesellschaft in der Zukunft angemessen schützen?

- elektronische Pförtner
  wie **Firewall- und PC-Sicherheitssysteme** schützen die internen IT-Systeme vor dem unerlaubten Zugriff von außen
- elektronische Sicherheitstransporter
  wie **Virtual Private Networks** schützen die Übertragung von elektronischen Informationen (Werte) vor unerlaubtem Auslesen und vor Manipulation
- elektronische Standesämter und Einwohnermeldeämter
  wie **Public Key Infrastructure (PKI) und deren Anwendungen** sorgen für eindeutige Identifikation von Kommunikationspartnern und die Verifikationsmöglichkeit im Internet
- elektronische Briefe/Signaturen
  wie **E-Mail-Sicherheit und elektronische Signaturen** stellen die Vertraulichkeit im „Briefverkehr“ über das Internet sicher, außerdem sorgen sie für Verbindlichkeit
- elektronische Safes
  wie **Datei- und Festplattenverschlüsselung** sorgen für eine sichere Aufbewahrung der elektronischen Informationen (Werte) auf den Rechnersystemen

Inhalt

- Reale Welt versus elektronische Welt
- **Die Begriffe Sicherheit und IT-Sicherheit**
- Bedeutungswandel der IT-Systeme
- IT-Sicherheit als Wirkungs- und Handlungszusammenhang
- Angriffsmöglichkeiten in Kommunikationssystemen
- Schäden
- Wer kümmert sich in Deutschland um die IT-Sicherheit?
- Zusammenfassung

Der Begriff „Sicherheit“

Sicherheit

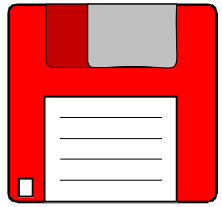
ein **zu schützendes Gut** so zu bewahren, dass für den Besitzer

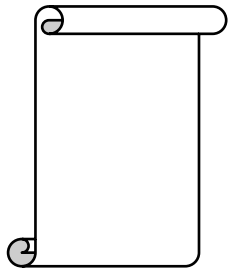
- kein **Schaden** entsteht,
- der **Wert** erhalten bleibt,
- keine **negativen Folgen** entstehen.

Der Begriff „IT-Sicherheit“

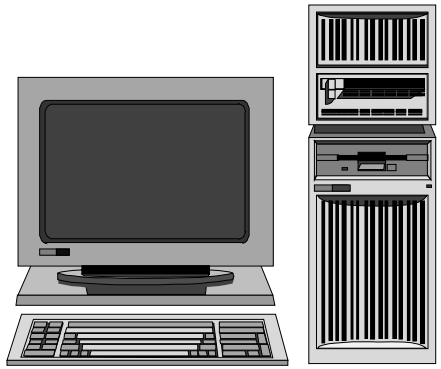
IT-Sicherheit

„zu schützendes Gut“ = **Informationen**,





die in einem Arbeitsprozess ver- bzw. erarbeitet werden,



und **Betriebsmittel**,

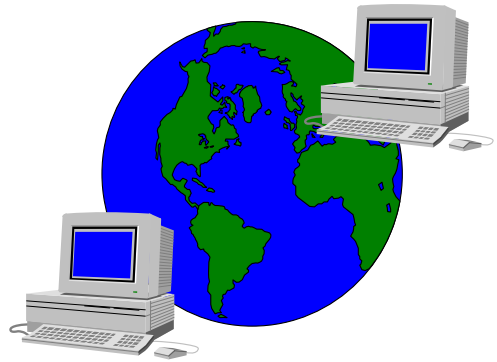
die für den Arbeits-prozess eingesetzt werden.

Inhalt

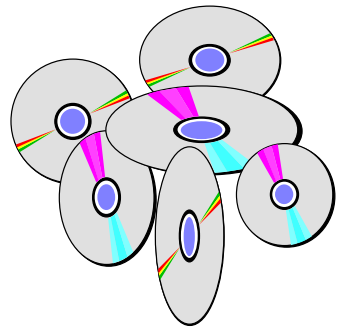
- Reale Welt versus elektronische Welt
- Die Begriffe Sicherheit und IT-Sicherheit
- **Bedeutungswandel der IT-Systeme**
- IT-Sicherheit als Wirkungs- und Handlungszusammenhang
- Angriffsmöglichkeiten in Kommunikationssystemen
- Schäden
- Wer kümmert sich in Deutschland um die IT-Sicherheit?
- Zusammenfassung

Bedeutungswandel der IT-Systeme (1/2)

- **zunehmende Verwendung von IT-Systemen**
  - effiziente Verarbeitung
  - rationelle Abwicklung
  - komplexer werdende Aufgaben
  - globale wirtschaftliche Ausdehnung

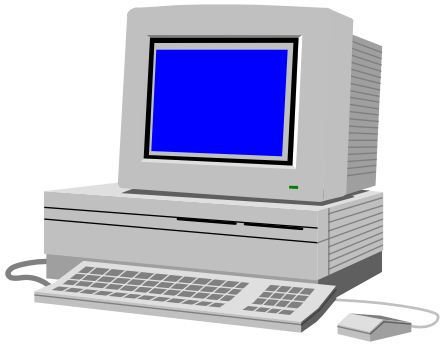


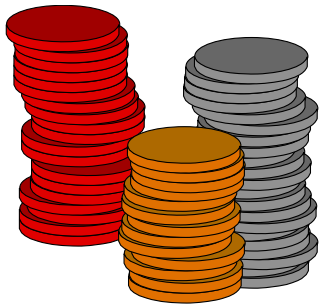
- **größer werdende Abhängigkeit von IT-Systemen**
  - Aufgaben sind nicht mehr ohne IT-Systeme zu erfüllen
  - Gefährdung der wirtschaftlichen Leistungsfähigkeit
  - Daten bleiben von der Eingabe bis zu ihrer Löschung in elektronischer Form



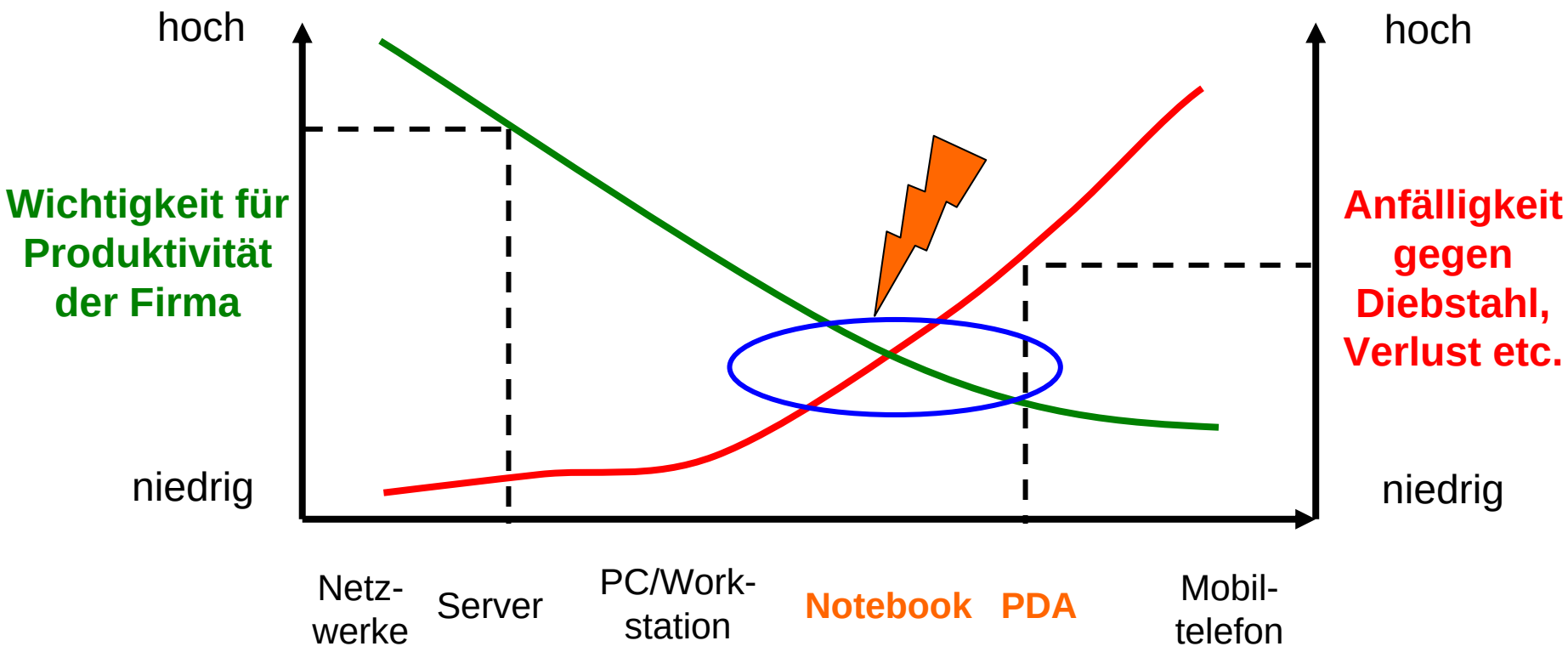
Bedeutungswandel der IT-Systeme (2/2)

- **Steigender Informationswert auf IT-Systemen**
  - vollständige Entwicklungs- und Fertigungsunterlagen
  - Geschäfts- und Betriebsergebnisse, Strategiepläne, usw.
  - Logistikinformationen
  - Kundendaten



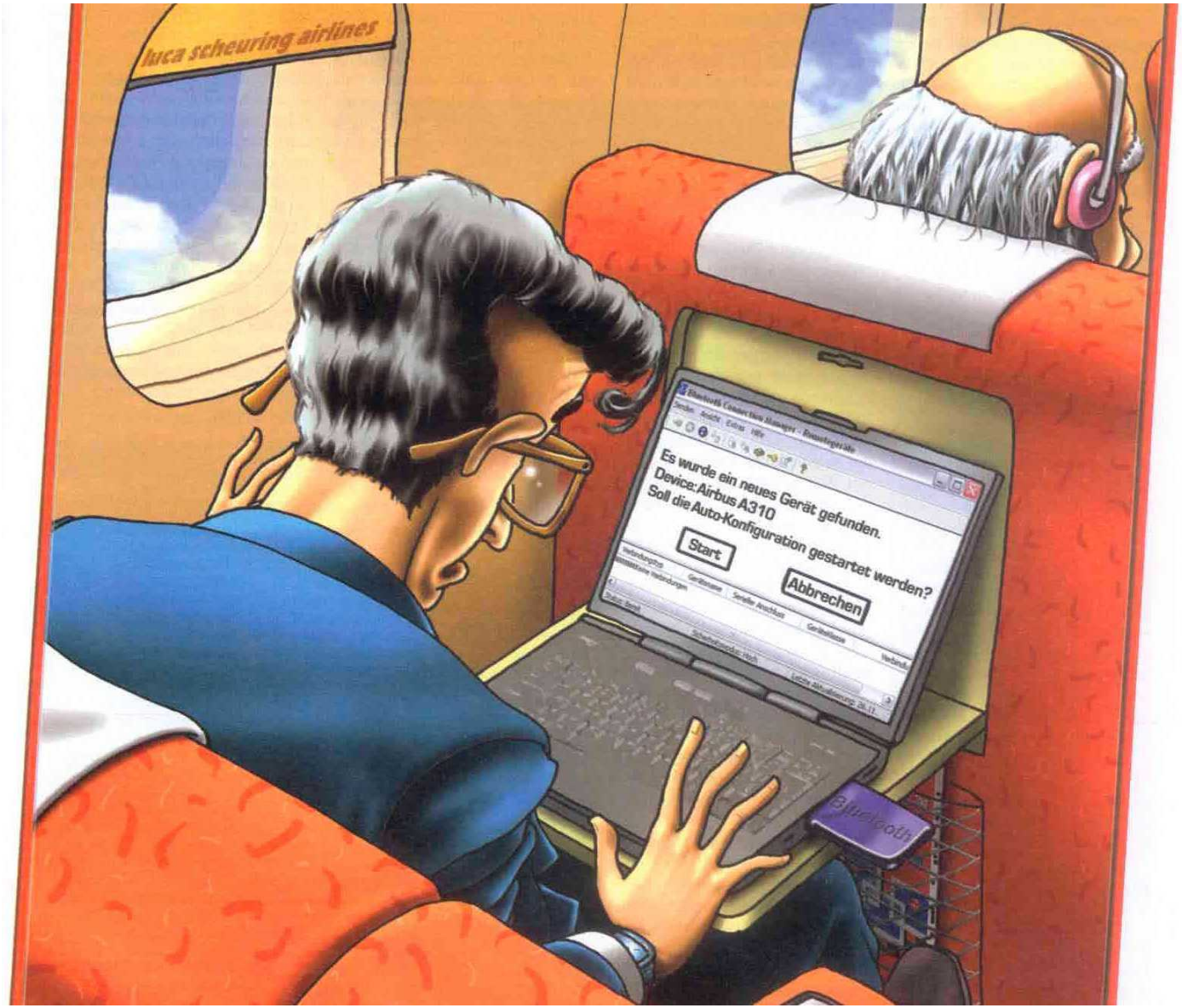


Neue Risiken durch gesteigerte Mobilität (1/2)



IT- und Kommunikationsinfrastruktur Komponenten
sortiert nach Mobilität

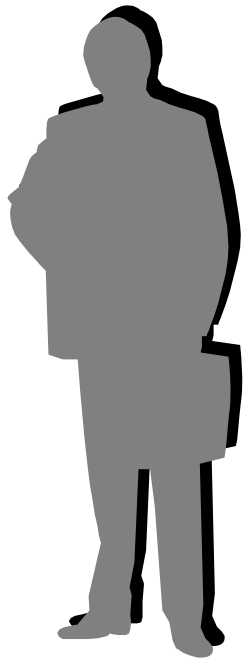
Neue Risiken durch gesteigerte Mobilität (2/2)



Sicherheitsanforderungen

- Einhaltung von Datenschutzgesetzen

- Unternehmen müssen sich selbst gegen Wirtschaftsspionage schützen



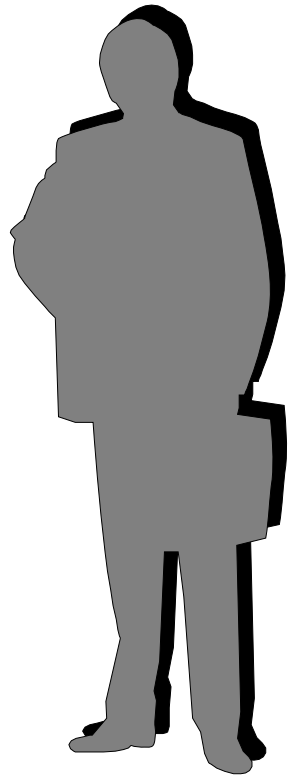
Mangelndes Unrechtsbewusstsein

Elektronische Welt:

- Erhöhter Aktionsradius
- Starke Abstraktion zwischen Handlung und Wirkung
- Dies verlangt einen wesentlich bewußteren Umgang in der elektronischen Welt

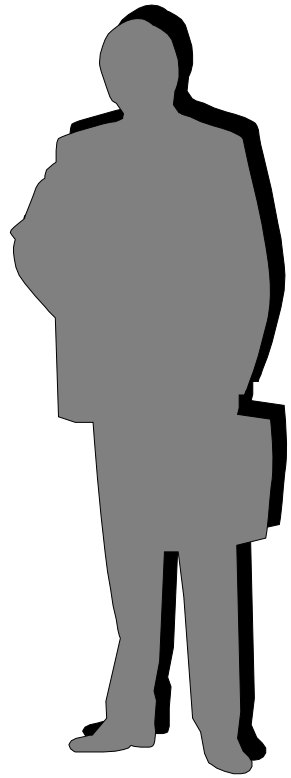
Spezielle Organisationen (1/2)

- **Geheimdienste**
  - Nach dem Ende des kalten Krieges wurden die Schwerpunkte innerhalb der Geheimdienste auf Wirtschaftsspionage gelegt.
  - Manipulierte Programme bedrohen vorhandene Datenbestände oder ermöglichen das Eindringen unbefugter Personen.
  - Schnell wachsende und unzureichend gesicherte Kommunikationsnetze ermöglichen die Manipulation übertragener Informationen.
  - Angebotene Sicherheitsprodukte sind nicht wirklich sicher (Hintertürchen, Fallen, Schlüssellänge, Trojanische Pferde, etc.).



Spezielle Organisationen (2/2)

- **Konkurrenzunternehmen**
  - Durch den verschärften Wettbewerb wird Wirtschaftsspionage für Unternehmen lukrativ.
  - Forschungs- und Entwicklungskosten können durch gezielte Spionage drastisch reduziert werden.
  - Es existiert kein Unrechtsbewußtsein, Konkurrenten werden mit allen verfügbaren Mitteln vom Markt verdrängt.
  - Einfachste Methoden erzielen technologische oder finanzielle Vorteile.



⇨ **Die Wettbewerbsfähigkeit der deutschen Industrie ist in Gefahr.**
⇨ **Der gesamtwirtschaftliche Schaden ist nicht zu unterschätzen.**

Inhalt

- Reale Welt versus elektronische Welt
- Die Begriffe Sicherheit und IT-Sicherheit
- Bedeutungswandel der IT-Systeme
- **IT-Sicherheit als Wirkungs- und Handlungszusammenhang**
- Angriffsmöglichkeiten in Kommunikationssystemen
- Schäden
- Wer kümmert sich in Deutschland um die IT-Sicherheit?
- Zusammenfassung

Wirkungs- und Handlungszusammenhang
→ Werte

- **Informationen und Daten**
  - Entwicklungsunterlagen, Fusionsabsichten, Strategiepapiere, Kundendatenbank, e-Filme, e-Musik, e-Bücher etc.
- **Ressourcen**
  - Rechnersysteme (HW u. SW), Drucker, etc.
  - CPU-Zeiten, spezielle Berechnungen (z.B. Steuern)
- **Dienstleistungen**
  - Datenbankabfragen
  - Application Service Provider (CAD, SAP, ...)
- **Prozesse und Abläufe (Finanzanwendungen, Materialwirtschaft, ...)**
- **Ansehen und Vertrauen**
- **Geschäftspotential**
- **…**

Wirkungs- und Handlungszusammenhang
→ Schutzbedarf

- **Gewährleistung der Vertraulichkeit**
  Damit keine unautorisierten Personen in der Lage sind, übertragene elektronische Informationen zu lesen.
- **Gewährleistung der Authentikation**
  Damit wir wissen, wer unser Partner bei der elektronischen Kommunikation oder Transaktion ist, beziehungsweise wer auf unsere Betriebsmittel und elektronischen Informationen zugreift.
- **Gewährleistung der Integrität**
  Damit wir überprüfen können, ob unsere elektronischen Informationen unverändert d.h. original sind.
- **Gewährleistung der Verbindlichkeit**
  Damit wir die Gewissheit haben, dass die elektronischen Prozesse und die damit verbundenen Aktionen auch verbindlich sind.
- **Gewährleistung der Verfügbarkeit**
  Damit wir die Gewissheit haben, dass die elektronischen Informationen und Dienste auch zur Verfügung stehen.

Wirkungs- und Handlungszusammenhang
→ Idee eines Angriffes

Der Angreifer versucht gezielt und absichtlich zu beeinflussen, um

- an bestimmte Informationen (Werte) zu gelangen, die nicht für ihn bestimmt sind,
- Reaktionen auszulösen, die er nicht auslösen darf, oder
- Ressourcen (Werte) zu nutzen, die er nicht nutzen darf.

Dies tut der Angreifer,

- um mit den Informationen Geld zu verdienen (zum Beispiel Entwicklungsdaten),
- oder ohne materielle Gewinnabsichten (Spielleidenschaft, Anerkennung, Zerstörungswut, ...)

Motivationen krimineller Handlungen: (Stand: 1997)

- mangelhaftes Berufsethos: 27 %
- Spielleidenschaft: 26 %
- persönlicher Gewinn: 25 %
- Rache: 22 %

Wirkungs- und Handlungszusammenhang
→ Angreifer (1/2)

- **Hacker**
  Hacker brechen in Rechnersysteme und Netzwerke ein, weil sie darin eine Herausforderung sehen und mit dem Erfolg ihren Status vergrößern wollen.
  Oft handelt es sich um Jugendliche, die aus »Spieltrieb«, also ohne böse Absicht handeln.
  Sie sind aber unberechenbar und können hohen Schaden verursachen.

- **IT-Spione**
  Bezahlte Spezialisten – teilweise mit einem sehr hohem Budget – versuchen, über gezielte Angriffe an Informationen zu kommen.
  Ihre Ziele sind politisch oder auch wirtschaftlich begründet (siehe »p«).

- **IT-Terroristen**
  Terroristen können Rechnersysteme und Netzwerke angreifen, um aus politischen Gründen Angst und Chaos zu verursachen.

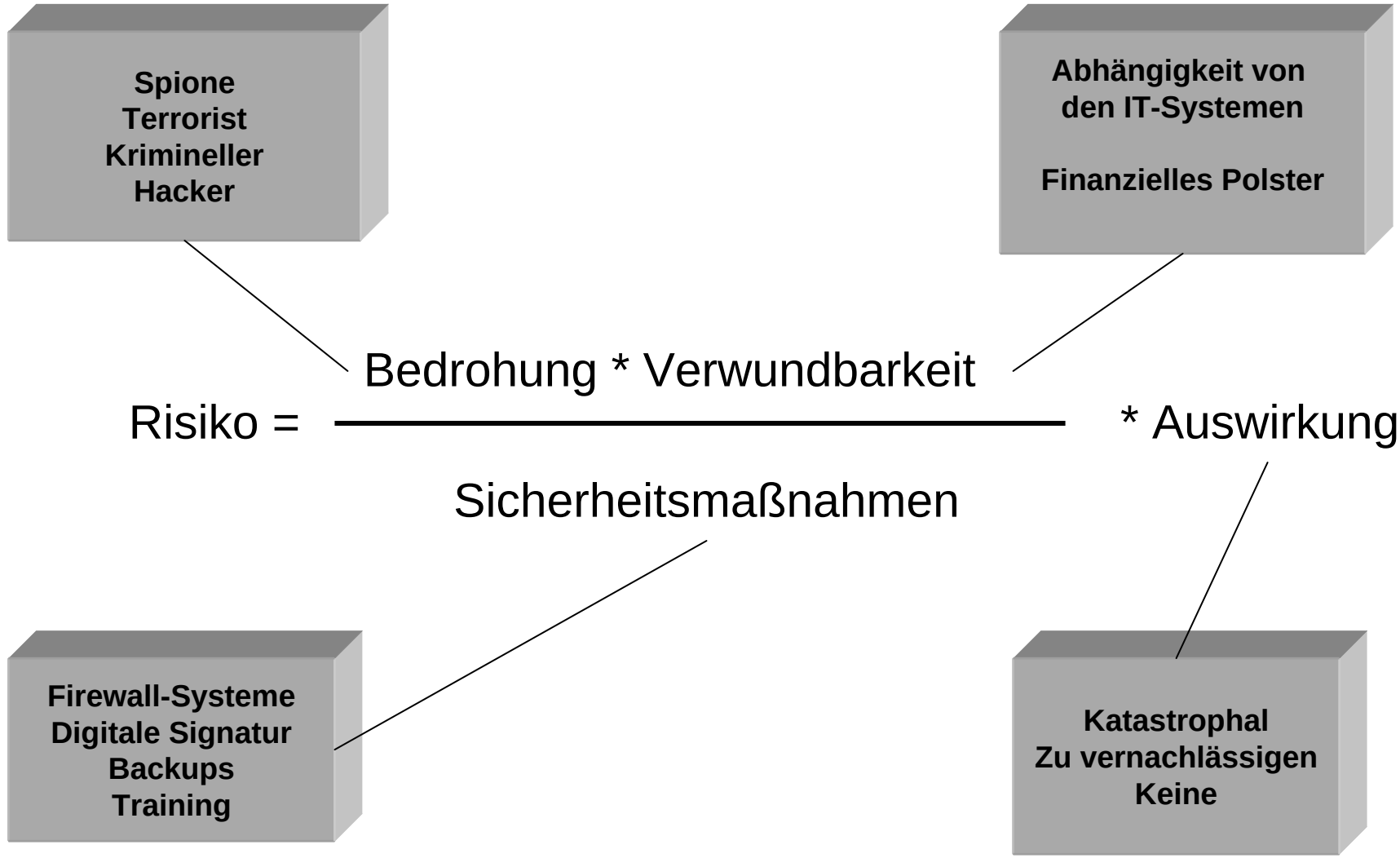
Wirkungs- und Handlungszusammenhang
→ Angreifer (2/2)

- **Unternehmens-Cracker**
  Dies sind Mitarbeiter, die auf Rechnersysteme und Netzwerke von Konkurrenzunternehmen zugreifen, um ihrem Unternehmen finanzielle Vorteile zu schaffen.
  Dazu spähen sie beispielsweise Entwicklungsunterlagen oder Strategiepläne aus.

- **Professionelle Kriminelle**
  Diese Personen wollen sich mit Angriffen persönlich bereichern, beispielsweise durch die nicht bezahlte Nutzung von Dienstleistungen oder durch das Abbuchen von fremden Konten.

- **Vandalen**
  Vandalen sind Personen, die Angriffe durchführen, um Organisationen oder Personen gezielt Schaden zuzufügen.

Wirkungs- und Handlungszusammenhang
→ Risiko eines Schadens



http://www.sans.org/infosecFAQ/securitybasics/risk.htm

Wirkungs- und Handlungszusammenhang
→ Bedrohung

- Potentielle Angriff auf Werte

- Höhe der Bedrohung hängt ab von:
  - Der Art der zu schützenden Werte
    (Attraktivität für Konkurrenz, Angreifer ...)
  - Bestehenden Sicherheitslücken
  - Umsetzungsmöglichkeiten

- Bedrohung besteht in Abhängigkeit von der eigenen Verwundbarkeit

Wirkungs- und Handlungszusammenhang
→ Sicherheitsmaßnahmen

- Sicherheitssoftware und/oder -hardware,
  mit der elektronische Werte geschützt werden können
  - Firewall-Systeme, Personal Firewalls
  - VPNs, SSL (TLS)
  - E-Mail-Security (Digitale Signatur, Objektverschlüsselung)
  - Anti-Virus/Anti-Malware
  - Festplattenverschlüsselung, Datei- oder Verzeichnisverschlüsselung
  - Intrusion Detection
  - Public-Key-Infrastruktur, digitale Signatur, SmartCards
  - Authentikation, Autorisierung
  - ...

➔ aber auch nicht-technische Sicherheitsmaßnahmen

Wirkungs- und Handlungszusammenhang
→ Eigentümer der Werte

- Die Angreifer wollen mit einem Angriff auf die Werte auch die Vorteile dieser ausnutzen und handeln somit gegen den Eigentümer der Werte.

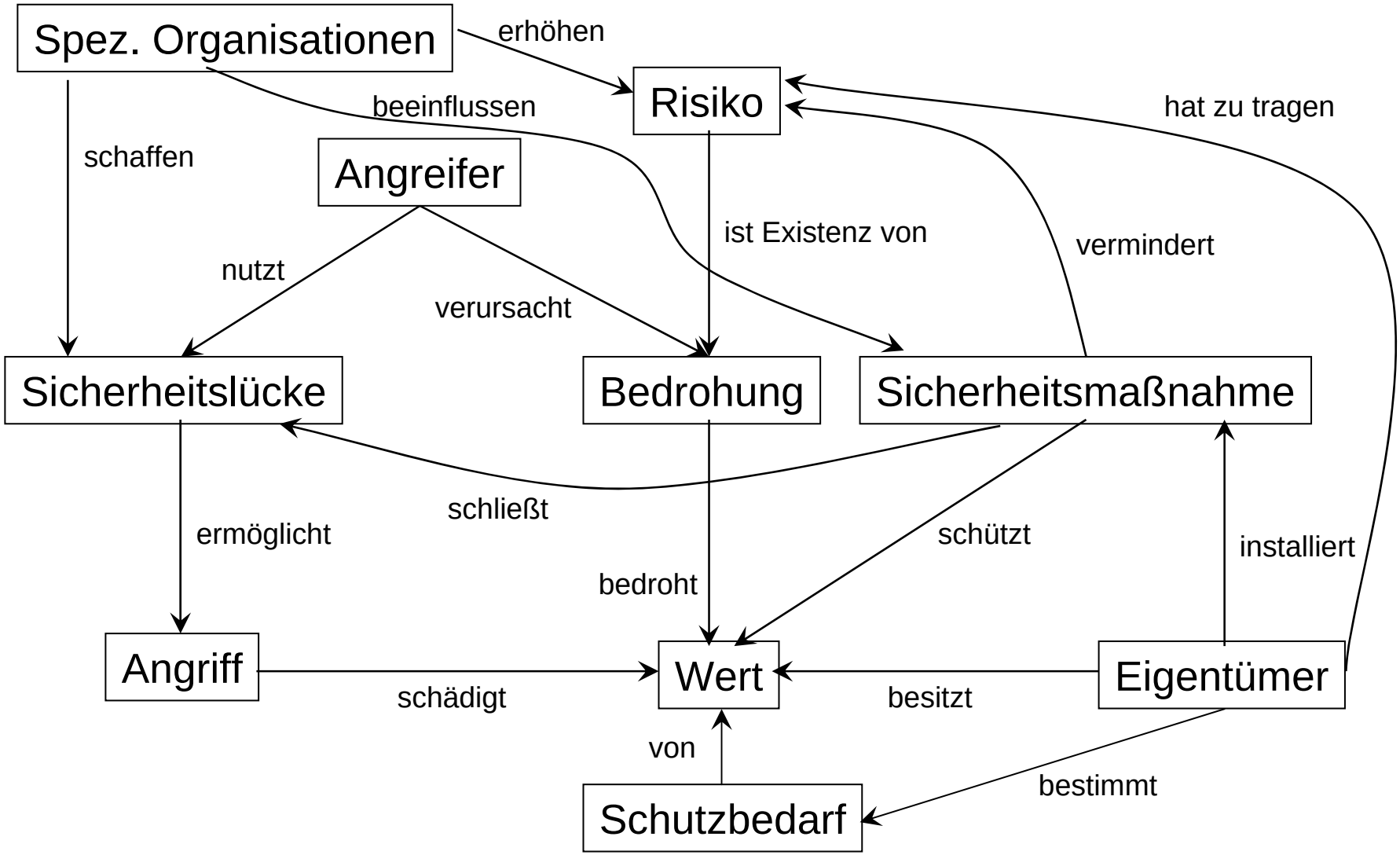
- Der Eigentümer nimmt den Angriff als Reduzierung seiner Werte wahr, **sofern er ihn bemerkt**.

- Die Sicherung der elektronischen Werte liegt in der Verantwortung des Eigentümers.

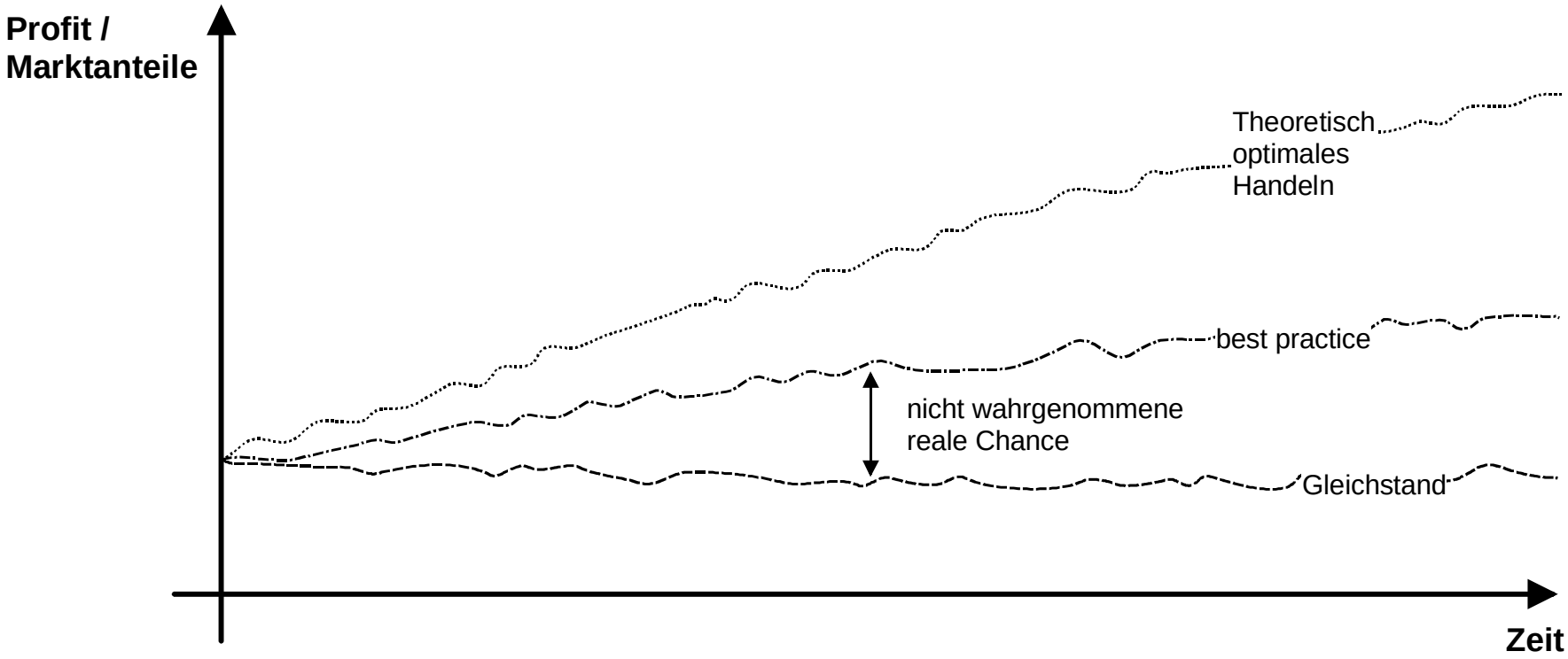
Wirkungs- und Handlungszusammenhang
→ Sicherheitslücken

- Fehler in den Betriebssystemen und Anwendungen
- Trap-Doors (vorsätzlich vom Hersteller eingebaute Sicherheitslücken)
- Falsche Konfiguration
- Konzeptionelle Schwachstellen
- Anwender wenden bestehende Sicherheitsapplikationen nicht oder nicht richtig an
- Anwender gehen nicht verantwortungsvoll mit den IT-Möglichkeiten und Angeboten um (z.B. SPAM)

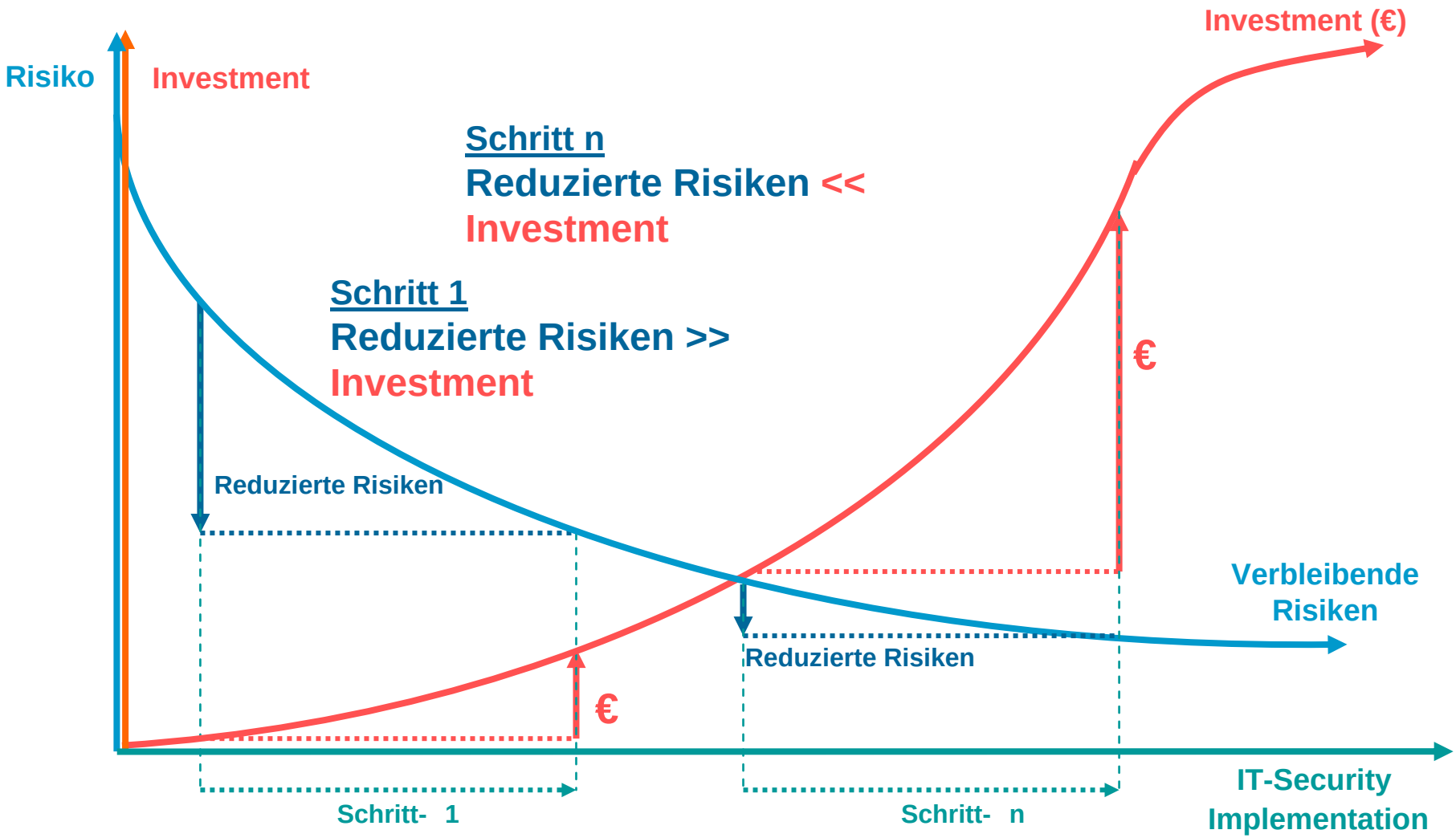
IT-Sicherheit als Wirkungs- und Handlungszusammenhang



Chancenoptimiertes geschäftliches Handeln
→ Best Practice



IT-Security Risiken & Investment



Investment zur Risikominderung

Investment ?????

Grundschutz

Pareto-Prinzip (80:20 Regel)

20% der möglichen IT-Sicherheitsmechanismen richtig eingesetzt liefern

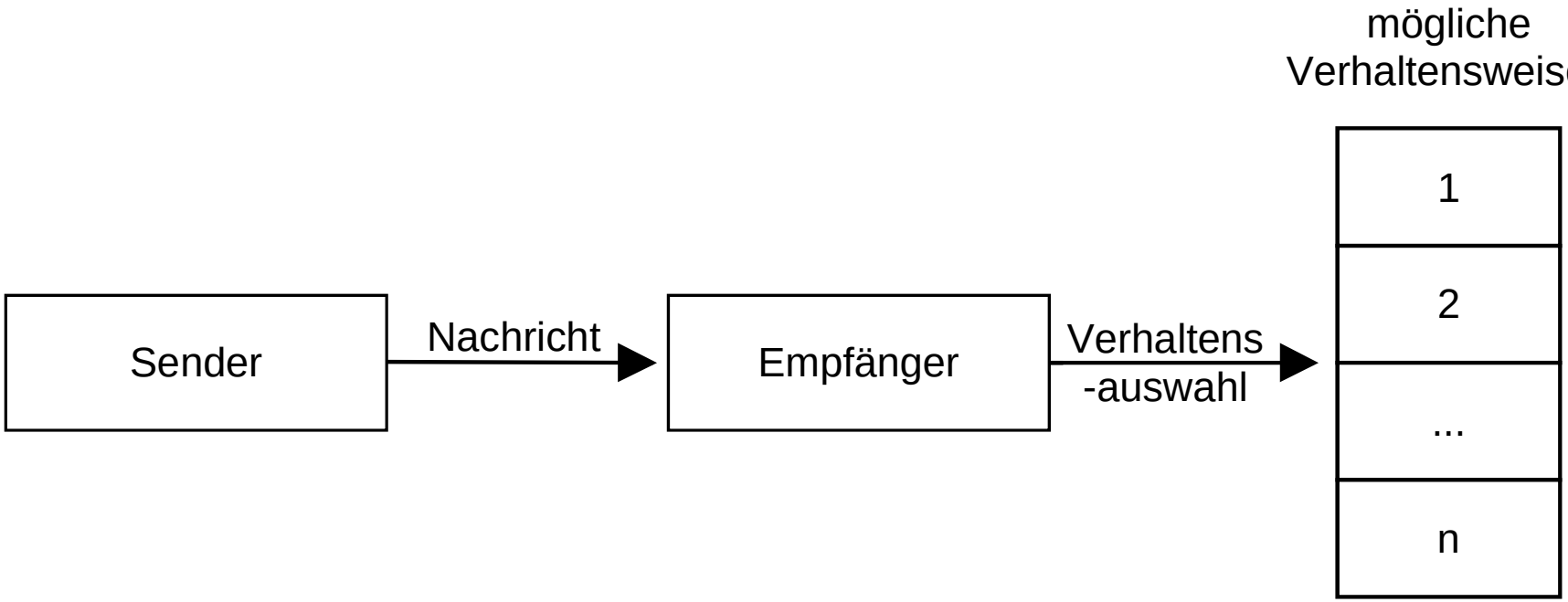
80% Schutz vor potentiellen Bedrohungen

- Das bedeutet, dass mit dem Einsatz der richtigen IT-Sicherheitsmaßnahmen durch ein relativ geringen Aufwand, einen vernünftiger Grundschutz für IT-Systeme hergestellt werden kann.

Inhalt

- Reale Welt versus elektronische Welt
- Die Begriffe Sicherheit und IT-Sicherheit
- Bedeutungswandel der IT-Systeme
- IT-Sicherheit als Wirkungs- und Handlungszusammenhang
- **Angriffsmöglichkeiten in Kommunikationssystemen**
- Schäden
- Wer kümmert sich in Deutschland um die IT-Sicherheit?
- Zusammenfassung

Angriffsmöglichkeiten in Kommunikationssystemen

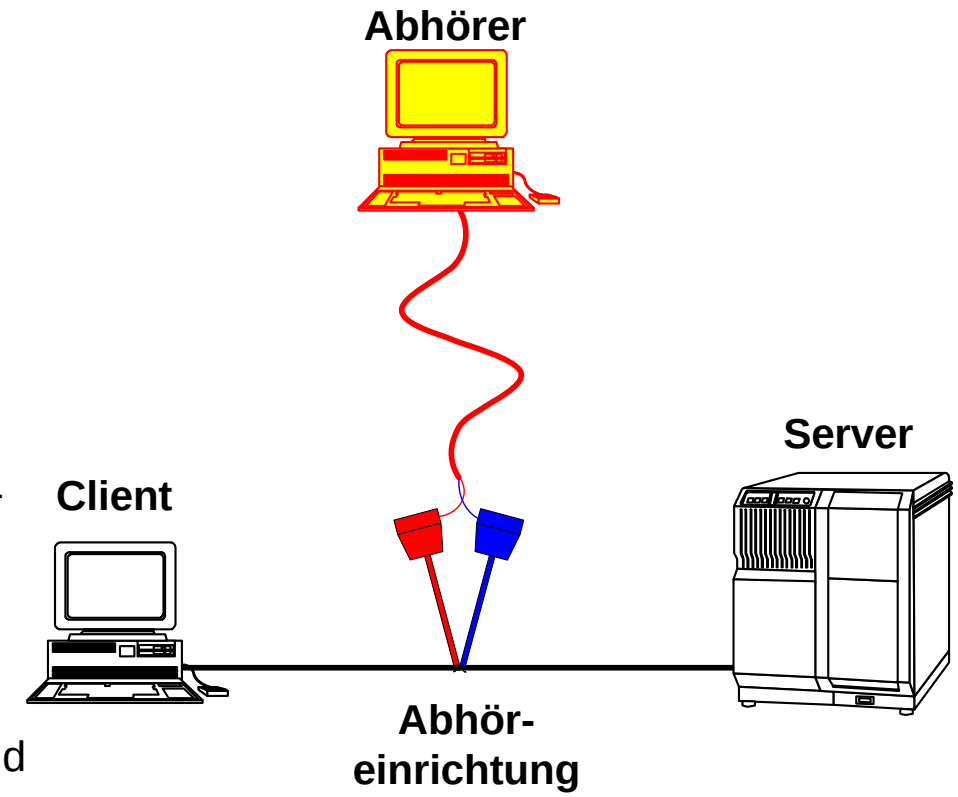


Reaktionsmöglichkeiten des Empfängers einer Nachricht

- Ein Angreifer kann das Verhalten des Empfängers und Senders interpretieren (durch abhören)
- der Angreifer kann die Reaktion des Empfängers zielgerichtet beeinflussen (durch verändern)

Angriffsmöglichkeiten in Kommunikationssystemen
→ Passive Angriffe

- **Abhören von Daten**
  Ein Abhörer gelangt unmittelbar in den Besitz der Nachricht und kann sie zu seinem Zweck verwerten.
- **Abhören von Paßwörtern**
- **Abhören von Teilnehmer-Identitäten**
  Der Lauscher erfährt, welche Teilnehmer untereinander eine Datenverbindung aufbauen und Daten austauschen.
- **Verkehrsflußanalyse**
  Größenordnung, Zeitpunkt, Häufigkeit und Richtung des Datentranfers



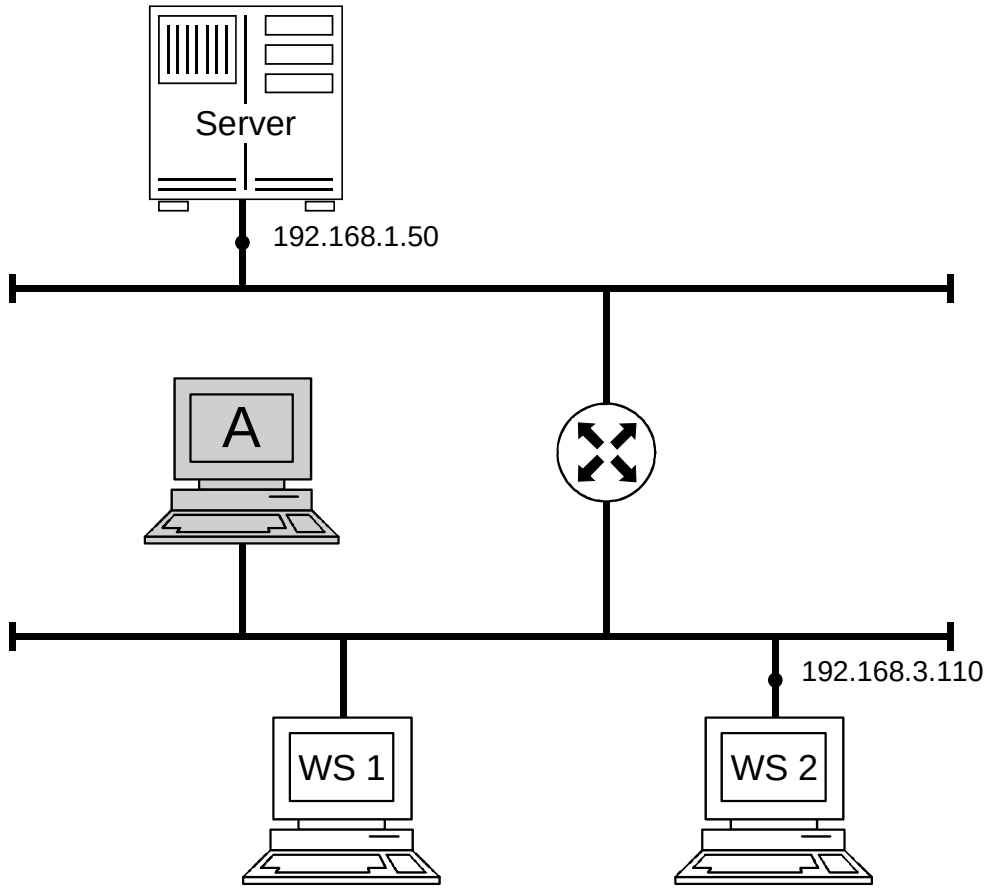
Angriffsmöglichkeiten in Kommunikationssystemen
→ Abhören der Daten im lokalen Netz

Hilfsmittel:

- Protokollanalysatoren (z.B. Ethereal)

Ziele:

- Paßwörter
- vertrauliche Informationen



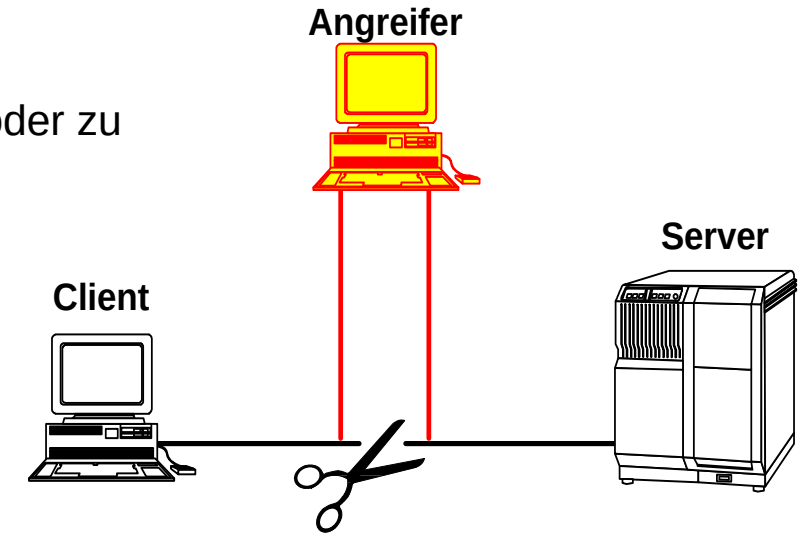
Angriffsmöglichkeiten in Kommunikationssystemen
→ Abhören der e-Kommunikation - ECHELON

z.B.
Bad Aibling

Abhören jeglicher Art
e-Kommunikation weltweit
Computergestützt
> 2 Mio. Verbindungen/h
nach Abstammung, Sprache, Schlüsselworten

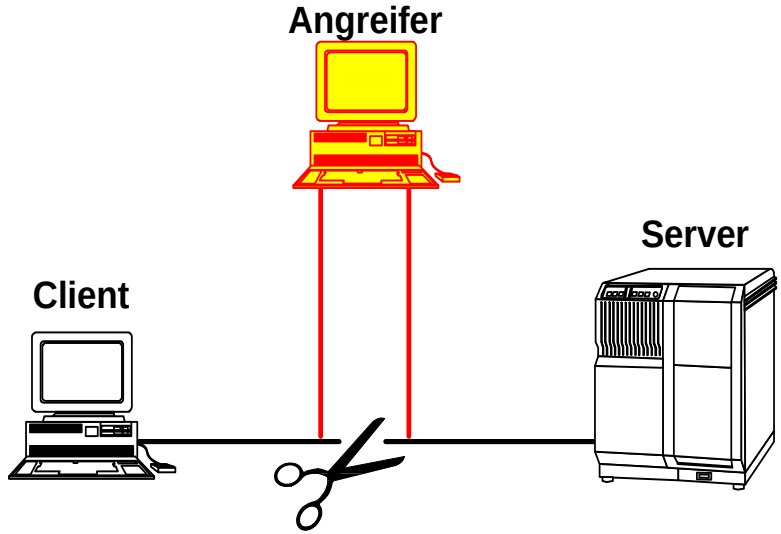
Angriffsmöglichkeiten in Kommunikationssystemen
→ Aktive Angriffe (1/2)

- **Bedrohung durch Dritte**
  - **Wiederholung oder Verzögerung**
    Hierdurch kann der Empfänger irritiert oder zu einer falschen Aktion veranlaßt werden. (Mehrfachüberweisungen)
  - **Einfügen und Löschen**
    Beispiel E-Mail:
    - Kaufen Sie *keine* neuen Aktien
    - Kaufen Sie neue Aktien
  - **Modifikation**
    Beispiel: Veränderung der Kontonummer
  - **Boykott**
    Beispiel: Realzeitanwendungen
  - **Malware**
    Viren, Würmen, Trojaner, SPAMs, ...



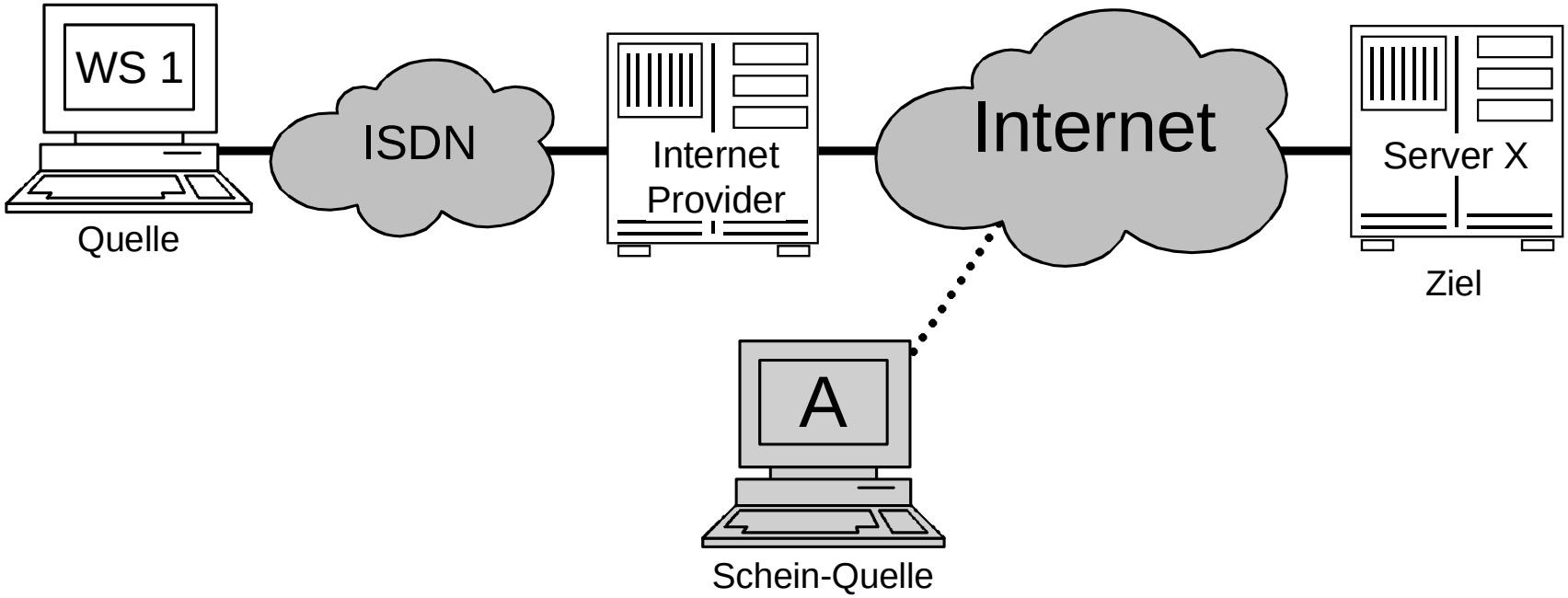
Angriffsmöglichkeiten in Kommunikationssystemen
→ Aktive Angriffe (2/2)

- **Bedrohung durch den Kommunikationspartner**
  - **Vortäuschen** einer falschen Identität
  - **Nutzung** fremder Betriebsmittel
  - **Leugnen** einer Kommunikationsbeziehung



Angriffsmöglichkeiten in Kommunikationssystemen

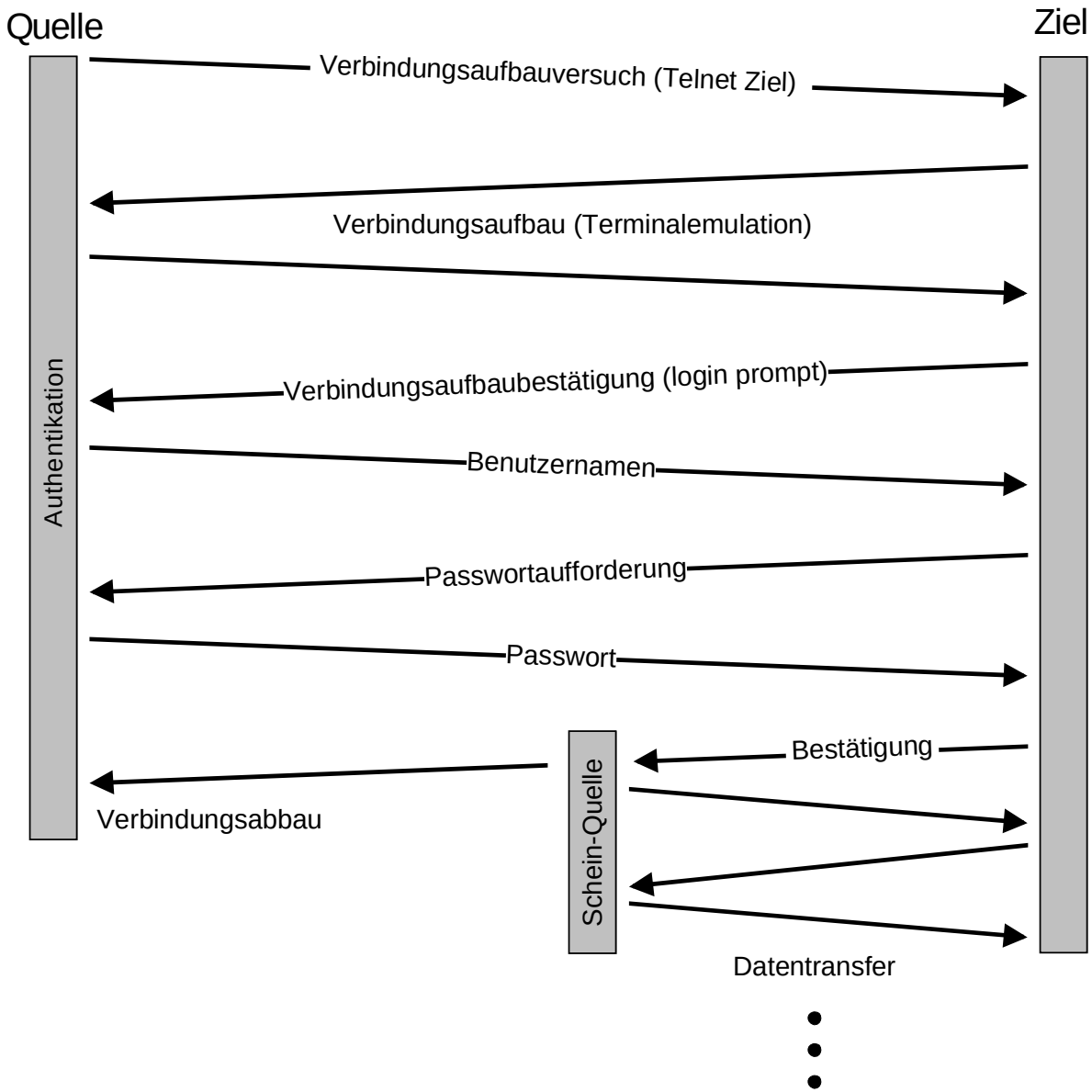
→ Beispiel eines aktive Angriffes: Trittbrettfahrer (1/2)



- Trittbrettfahrer hängen sich z.B. an einen Knoten (Router, Rechnersystem) und verfolgen einen Verbindungsaufbau

Angriffsmöglichkeiten in Kommunikationssystemen

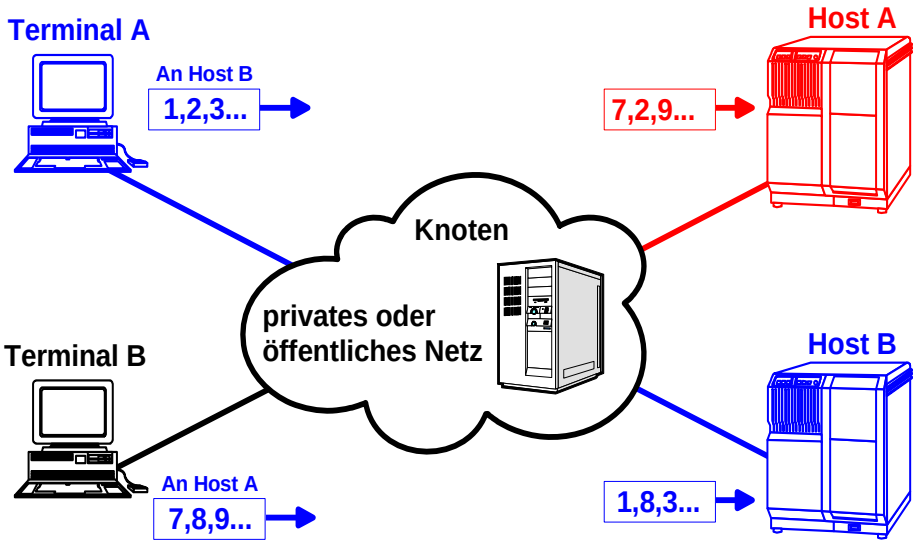
→ Beispiel eines aktive Angriffes: Trittbrettfahrer (2/2)



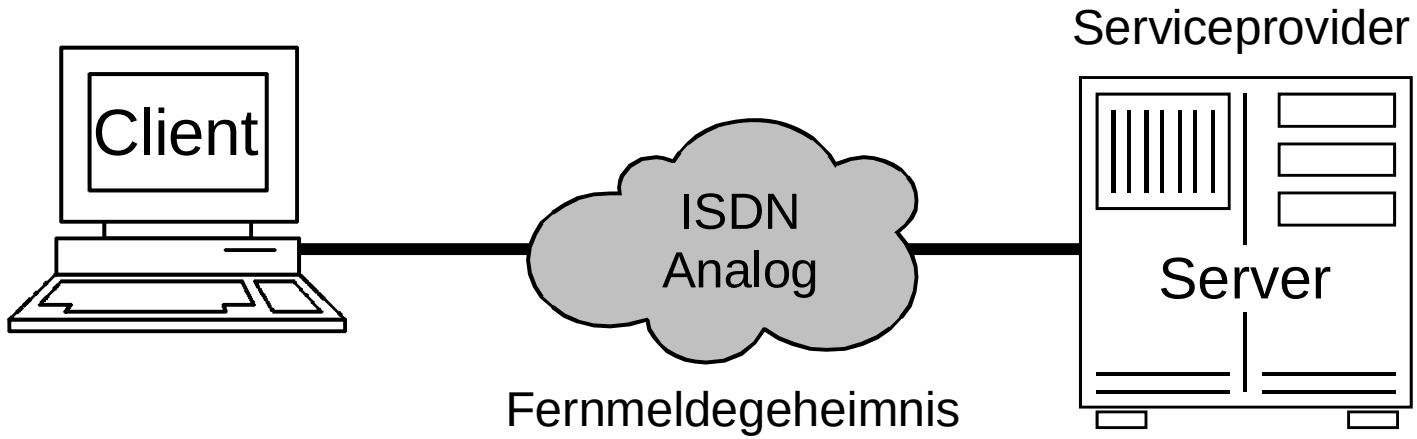
- **Hinweis:**
  Auch kryptographische Methoden können unterlaufen werden!

Angriffsmöglichkeiten in Kommunikationssystemen
→ Zufällige Verfälschungsmöglichkeiten

- Fehlrouting von Informationen
- Übertragungsfehler
- Softwarefehler
- Hardwarefehler durch Umwelteinflüsse
- Fehlbedienung

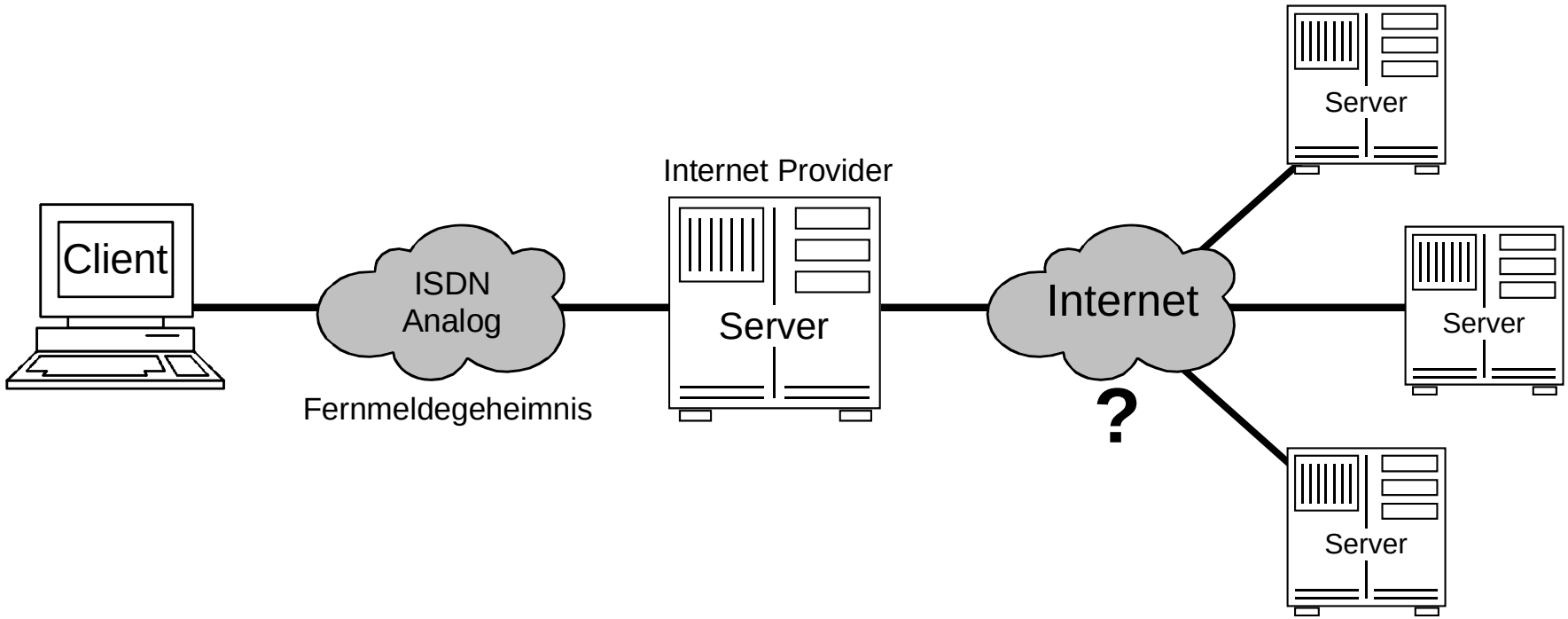


Weitere Aspekte (1/3)
→ Fernmeldegeheimis



- In Deutschland gibt es für alle Anbieter von Telekommunikationsdienstleistungen das Fernmeldegeheimnis.
- Schafft ein hohes Maß an Vertrauenswürdigkeit

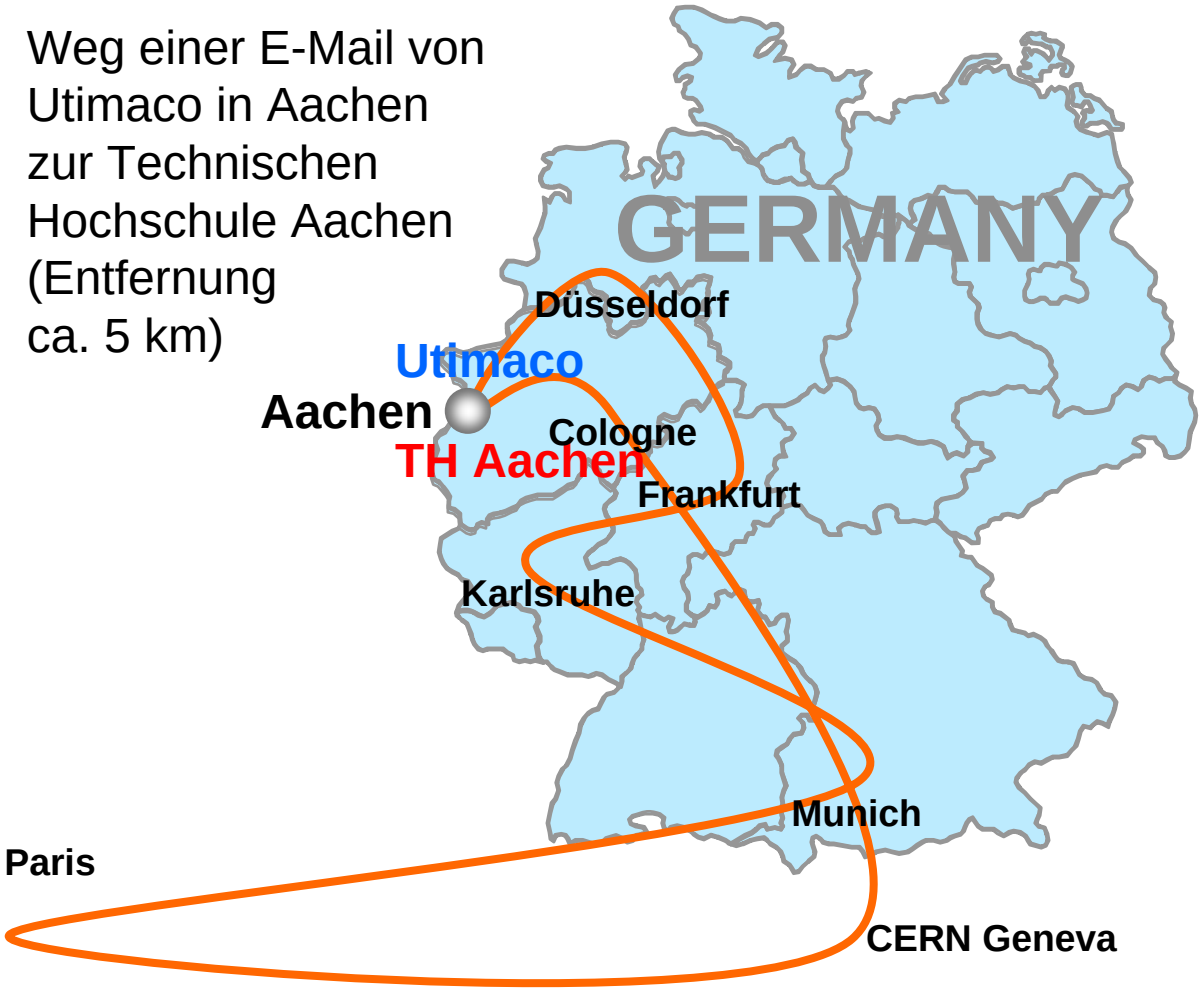
Weitere Aspekte (2/3)
→ Internet und das Fernmeldegeheimnis



- Da das Internet international ist, verlassen wir den geregelten, geschützten Bereich.

Weitere Aspekte (3/3)
→ Kommunikationsweg einer E-Mail

Weg einer E-Mail von Utimaco in Aachen zur Technischen Hochschule Aachen (Entfernung ca. 5 km)



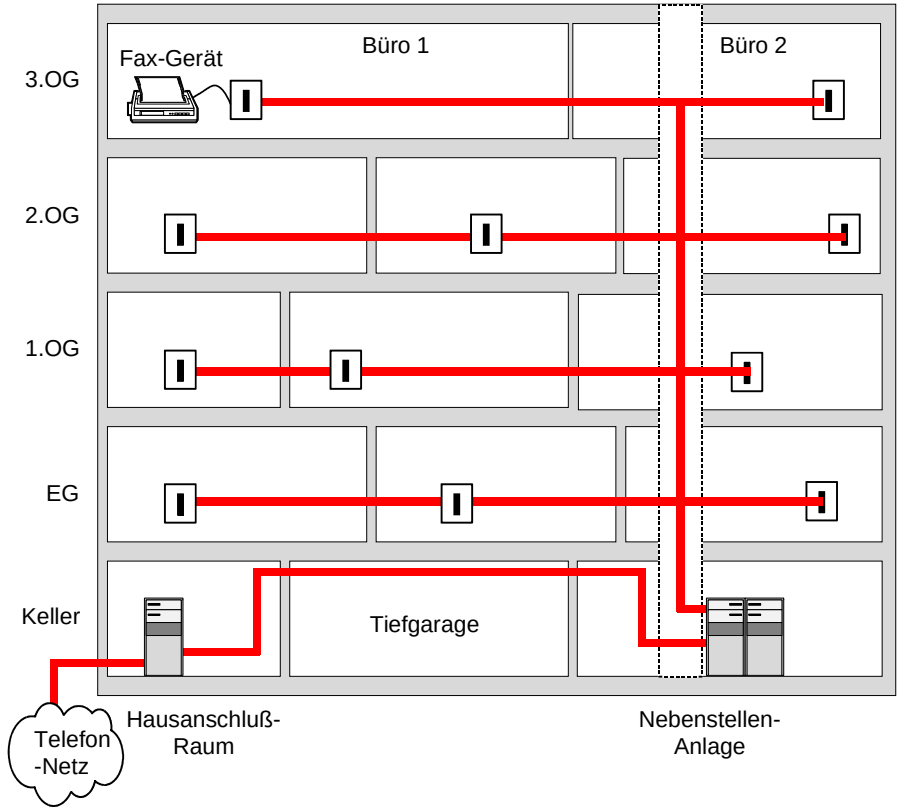
23 (!) Routers:

1. **Router.utimaco.aachen.de**
2. **local.aachen.core.csl-gmbh.net**
3. **local2.erkrath.core.csl-gmbh.net**
4. **xip2.erkrath.core.csl-gmbh.net**
5. **cisco.csl-gmbh.net**
6. **frankfurt.core.xlink.net**
7. **langen.core.xlink.net**
8. **karlsruhe.core.xlink.net**
9. **muenchen.core.xlink.net**
10. **Munich-EBS.EBONE.NET**
11. **Paris-EBS2.EBONE.NET**
12. **Cern-EBS1.Ebone.NET**
13. **CH-s2.dante.bt.net**
14. **Ch-f0-0.eurocore.bt.net**
15. **DE-s1-0.eurocore.bt.net**
16. **De-f0-dante.bt.net**
17. **ipgate2.win-ip.dfn.de**
18. **ipgate21.win-ip.dfn.de**
19. **ZR-Koeln1.WiN-IP.DFN.DE**
20. **RWTH-Achen1.WiN-IP.DFN.DE**
21. **cisco-bwin.rz.rwth-aachen.de**
22. **informat-05.rz.RWTH-Aachen.DE**
23. **terpi.Informatik.RWTH-Achen.DE**

Viele Möglichkeiten zum Abhören / Manipulieren

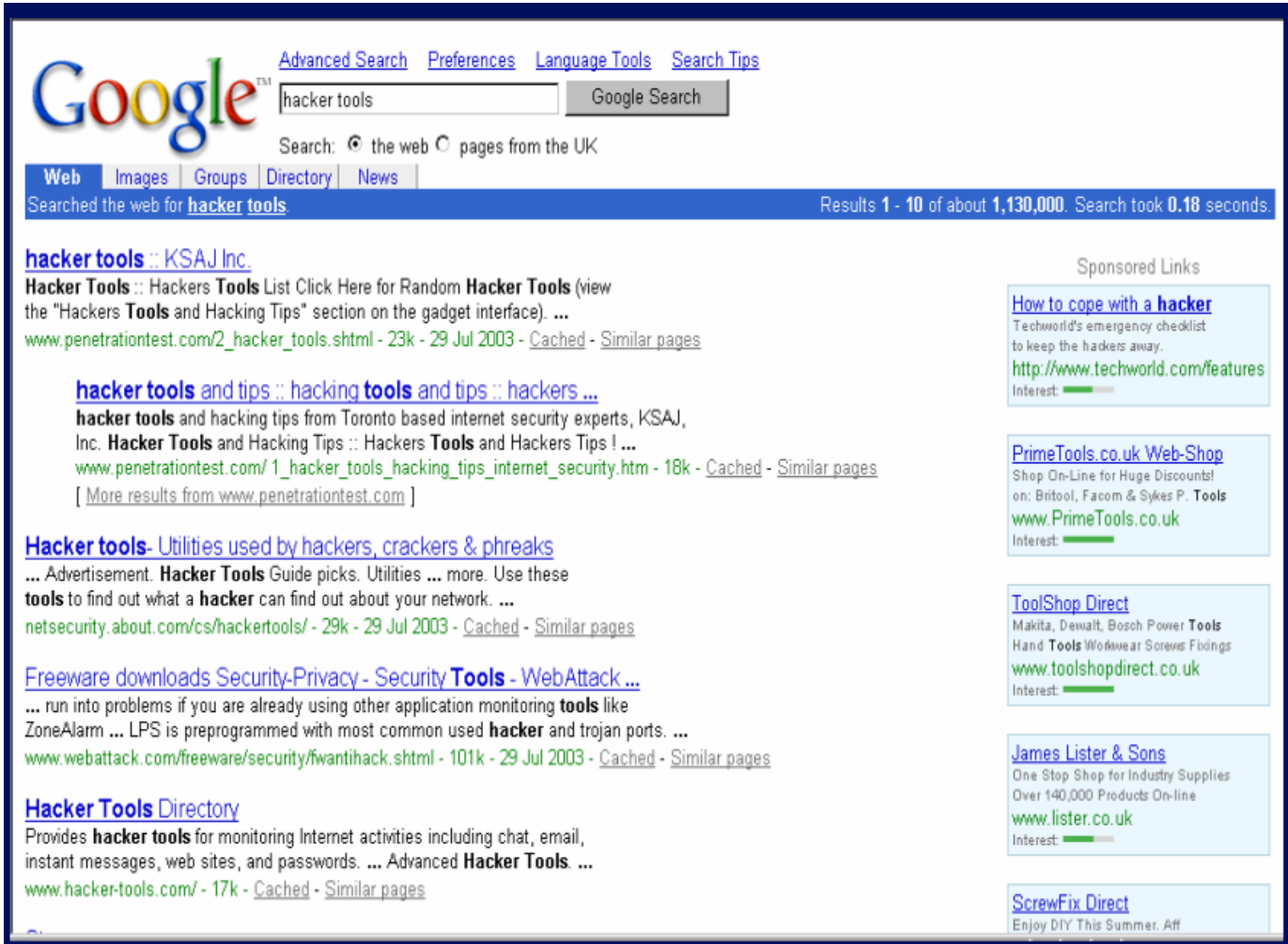
Eintrittswahrscheinlichkeit für einen Angriff

- Die Motivation für einen Angriff steigt mit dem **Wert** der übertragenen Daten.
- Es werden nur **einfache** und **kostengünstige Hilfsmittel** benötigt.
- Angriffspunkte:
  - angrenzende Büros
  - Kabelschächte
  - Hausanschlussräume
  - Nebenstellenanlagen
  - Tiefgaragen



sehr hoch

Eintrittswahrscheinlichkeit für einen Angriff



A basic search for 'hacker tools' produces 1,130,000 results

QinetiQ

Inhalt

- Reale Welt versus elektronische Welt
- Die Begriffe Sicherheit und IT-Sicherheit
- Bedeutungswandel der IT-Systeme
- IT-Sicherheit als Wirkungs- und Handlungszusammenhang
- Angriffsmöglichkeiten in Kommunikationssystemen
- **Schäden**
- Wer kümmert sich in Deutschland um die IT-Sicherheit?
- Zusammenfassung

Schadenskategorien

- **Verstoß gegen Gesetze/Vorschriften/Verträge**
  Grundgesetz, Datenschutzgesetze, ...
- **Beeinträchtigung der persönlichen Unversehrtheit**
  Verletzung oder sogar den Tod von Personen
- **Beeinträchtigung der Aufgabenerfüllung**
  verzögerte Bearbeitung
- **Negative Außenwirkung (Imageverlust)**
  Renommeeverlust, Vertrauensverlust
- **Finanzielle Auswirkungen (25.000,- bis 5 Mio.)**
  Unmittelbare und mittelbare finanzielle Schäden

Bekannte Schadensfälle

- **1. Fall: Abhören von 2 MBit-Strecken**
  Auftrag im Umfang von mehreren Milliarden **verloren**

- **2. Fall: Videokonferenz über Satellit**
  Vertrauliche Strategiegespräche wurden nachweislich **abgehört**

- **3. Fall: Abhören von Modemverbindungen**
  Entwicklungsdaten wurden abgehört, mit denen die Konkurrenz ein gleichwertiges Produkt **kostengünstiger** anbieten konnte

- **4. Fall: Internet-Fall**

  “Kavaliersdelikte" wie das massenhafte Kopieren von urheberrechtlich geschützter Musik (mp3s) aus dem Internet (Schadenshöhe im Milliardenbereich)

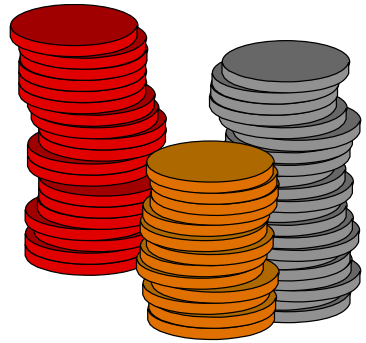
sehr hohe Dunkelziffer

Kosten/Nutzen-Betrachtung

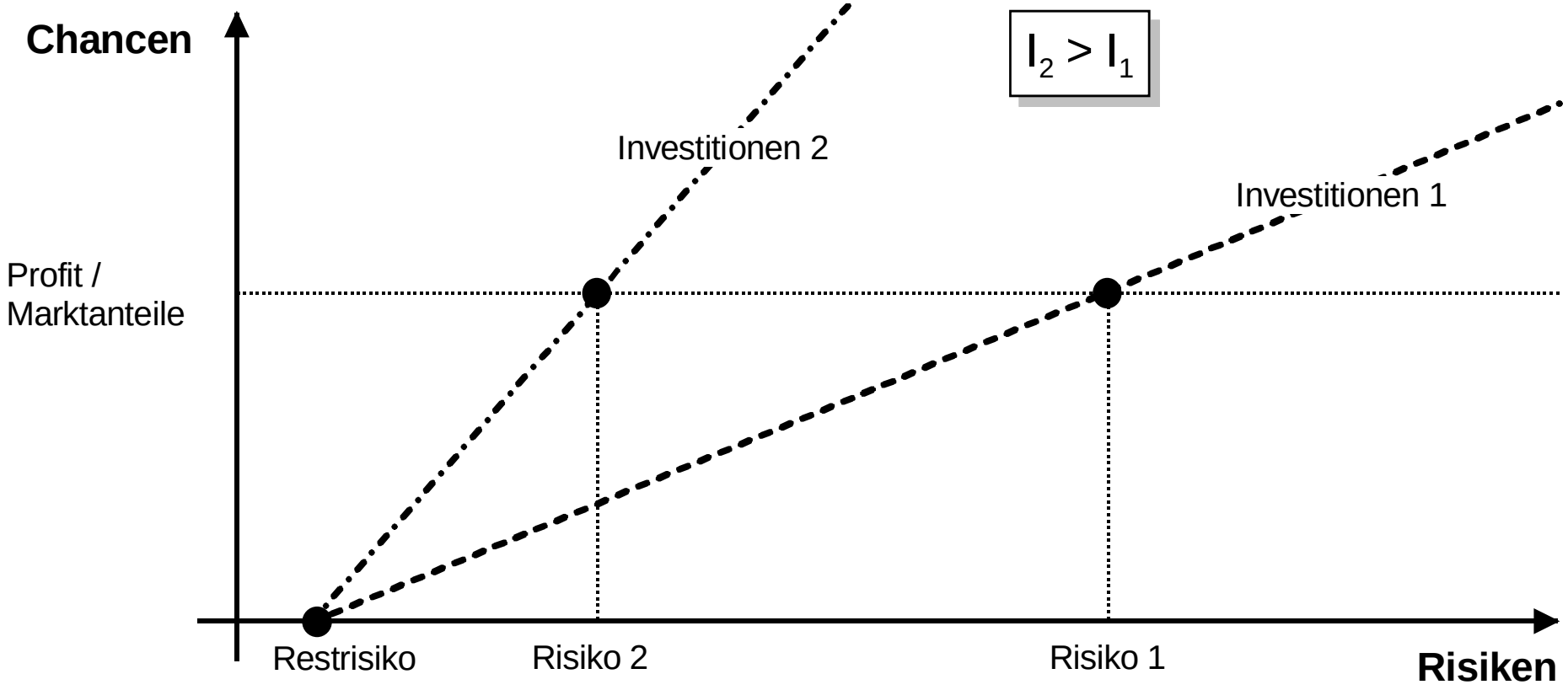
- **Gewinn**
  - 500 Mio €/Jahr

- **Schaden**
  Die 500 wichtigsten Kunden werden mit Namen und Kontostand in der Zeitung veröffentlicht
  - sofort: 10-100 Mio €
  - mittelfristig: 1-10 Mio €/Jahr

- **Kosten Sicherheitssystem**
  - sofort: 2 Mio € (< 1% vom Gewinn)
  - mittelfristig: 25 000 €/Jahr



IT-Sicherheit ist kein Selbstzweck

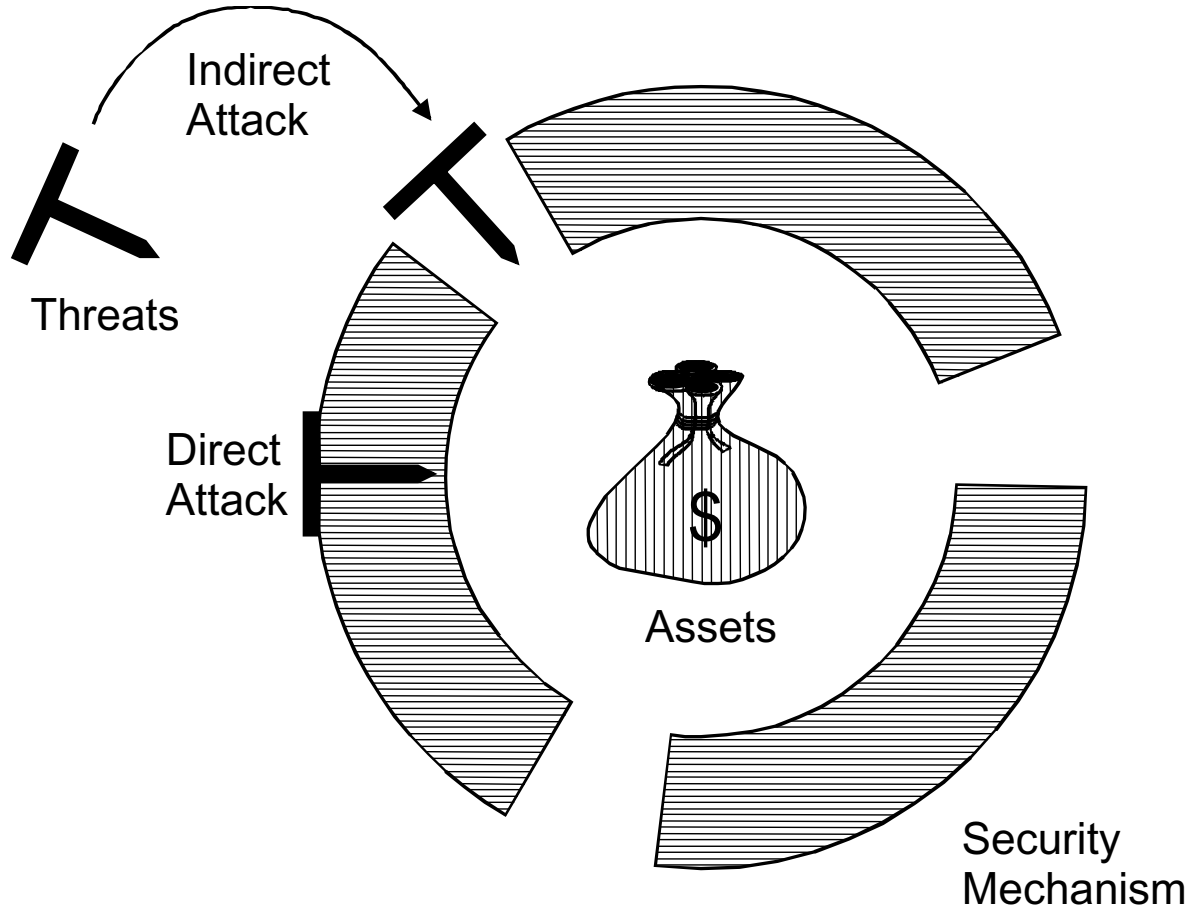


- IT-Sicherheit bedeutet

  ⇨Chancen nutzen + ⇨Risiken minimieren

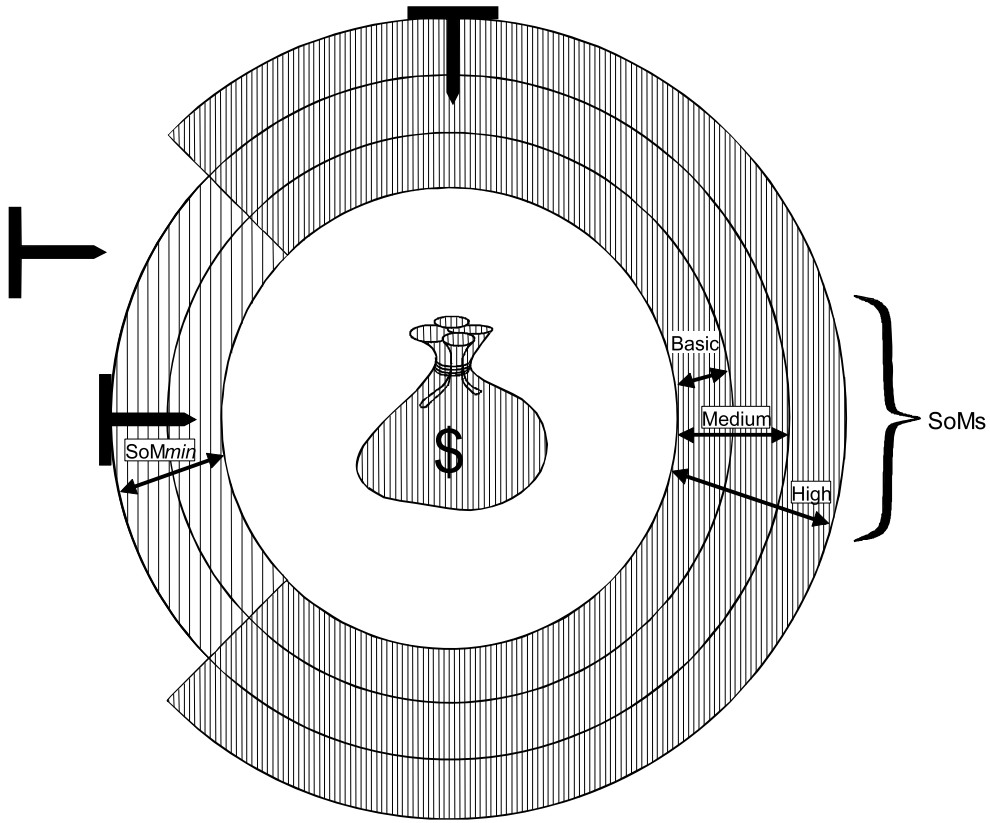
Sicherheit und Vertrauenswürdigkeit
→ Wirksamkeit von Sicherheitssystemen

- Für die Beurteilung von Sicherheitssystemen ist ein wichtiges Kriterium, ob die Sicherheitssysteme auch tatsächlich geeignet sind, den realen Angriffen entgegen zu wirken.



Sicherheit und Vertrauenswürdigkeit
→ Stärke von Sicherheitsmechanismen

- Ein wichtige Größe für die Bewertung von Sicherheitsmechanismen ist die Stärke des Sicherheitsmechanismus, die notwendig ist, um allen Angriffen erfolgreich entgegenzuwirken.



- Kriterien für die Bewertung der Stärke sind:
  - Fachkenntnisse (Laie, kenntnisreiche Person, Experte)
  - Ressourcen (Zeit, Ausstattung)
  - Gelegenheit (allein, mit Anwender, mit Systemverwalter)

Sicherheit und Vertrauenswürdigkeit
→ Korrektheit der Sicherheitsmechanismen

- Korrektheit der Sicherheitsmechanismen
  - Korrekt implementiert
  - Vertrauen in die Korrektheit

- IT-Systeme sind nur sicher, wenn
  - die Wirksamkeit
  - die Stärke und
  - die Korrektheit

  angemessen vorhanden sind.

Sicherheit und Vertrauenswürdigkeit
→ Was heißt Vertrauenswürdigkeit?

- **Sicherheit** in dem Sinne, dass wir IT-Produkte und Lösungen risikoärmer nutzen können.
- **Zutrauen**, dass die Hersteller, die Netz- und Serviceprovider eine verlässliche und sichere IT-Technologie zur Verfügung stellen, was in der jungen Vergangenheit in der IT-Branche nicht optimal geschehen ist.
- Mit **Zuverlässigkeit** ist gemeint, dass die IT-Produkte und Lösungen nur die Dinge tun, die gewünscht sind, und das möglichst 100% zuverlässig.
- **Gewissheit**, dass sich jemand um die Sicherheitsfragen und die anderen Aspekte der Vertrauenswürdigkeit kümmert.
- **Glaubwürdigkeit** in die Aussagen, die gemacht werden, und in die Aktivitäten, die im Bereich der IT getan werden, um mehr Sicherheit, mehr Vertrauenswürdigkeit zu erlangen.
- Weitere Aspekte der Vertrauenswürdigkeit sind z.B.: Aufrichtigkeit, Pflichtbewusstsein, Gewissenhaftigkeit und vor allem Verantwortlichkeit.

Inhalt

- Reale Welt versus elektronische Welt
- Die Begriffe Sicherheit und IT-Sicherheit
- Bedeutungswandel der IT-Systeme
- IT-Sicherheit als Wirkungs- und Handlungszusammenhang
- Angriffsmöglichkeiten in Kommunikationssystemen
- Schäden
- **Wer kümmert sich in Deutschland um die IT-Sicherheit?**
- Zusammenfassung

Wer kümmert sich in Deutschland um die IT-Sicherheit?

- **Bundesamt für Sicherheit in der Informationstechnologie (BSI)**
  - Schutz der Bundesregierung
  - mehr Sicherheit für die IT-Sicherheit in D
- **CERT**
  - Aufdecken von Sicherheitslücken
  - Bereitstellung von Informationen über Schwachstellen und Empfehlungen für deren Behebung
  - CERT: Hochschulen, BSI, Unternehmen, BITKOM, ...
- **Bundeswirtschaftsministerium (BMWI)**
  - Aufklärung über die Notwendigkeit der IT-Sicherheit (insbesondere KMUs)
- **Forschungsministerium**
  - Förderung neuer IT-Sicherheitstechnologie
- **TeleTrusT**
  - Mehr Vertrauenswürdigkeit in der IT-Gesellschaft
- und viele mehr ....

Inhalt

- Reale Welt versus elektronische Welt
- Die Begriffe Sicherheit und IT-Sicherheit
- Bedeutungswandel der IT-Systeme
- IT-Sicherheit als Wirkungs- und Handlungszusammenhang
- Angriffsmöglichkeiten in Kommunikationssystemen
- Schäden
- Wer kümmert sich in Deutschland um die IT-Sicherheit?
- **Zusammenfassung**

Zusammenfassung

- Wir leben in einer Informations- und Wissensgesellschaft, in der die IT eine immer wichtigere Rolle spielt.
- Die IT-Geräte, die IT-Prozesse und die elektronischen Werte sind Wirtschaftsgüter, welche angemessen geschützt und abgesichert werden müssen.
- Die Sicherheit der IT (mit den Prozessen und den elektronischen Werten) liegt in der Verantwortung des Eigentümers.
- Wirkungs- und Handlungszusammenhang der IT-Sicherheit ist sehr komplex und braucht eine genaue Analyse und Bewertung.
- Die Angriffsmöglichkeiten, die Eintrittswahrscheinlichkeit und die Schäden sind sehr vielfältig und zeigen den notwendigen Handlungsbedarf auf.
- In dieser Vorlesung geht es hauptsächlich um den Aufbau, die Prinzipien, die Architektur sowie die Funktionsweise von technischen IT-Sicherheitsmaßnahmen im Bereich der elektronischen Kommunikation.

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen