Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Grundlagen der IT-Sicherheit

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Inhalt

- **Reale Welt versus elektronische Welt**
- **Bedeutungswandel der IT-Systeme**
- **Wirkungs- und Handlungszusammenhang**
- **Schadenskategorien**

Inhalt

- **Reale Welt versus elektronische Welt**
  - Bedeutungswandel der IT-Systeme
  - Wirkungs- und Handlungszusammenhang
  - Schadenskategorien

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

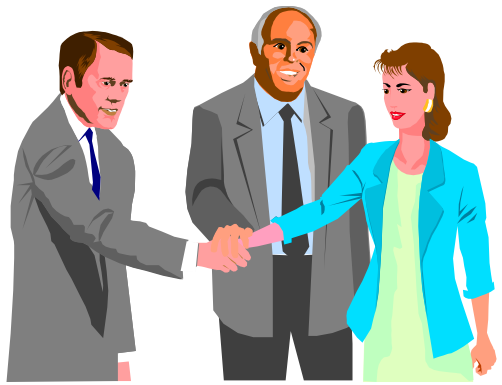
- **Briefe/Handgeschriebene Unterschrift**
  sorgt für den vertraulichen Austausch von Informationen und die Verbindlichkeit der damit verbundenen Aktionen

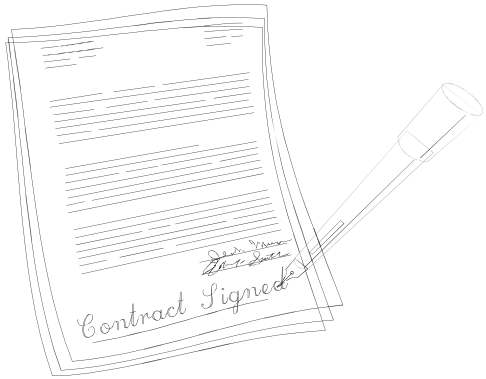
- **Safe/abschließbare Schränke**
  sorgt für eine sichere Aufbewahrung der Werte (Informationen, Strategiepapiere, Bürgerdaten etc.)

Reale versus elektronische Welt

„Vertrauenswürdigkeit in der elektronischen Welt”

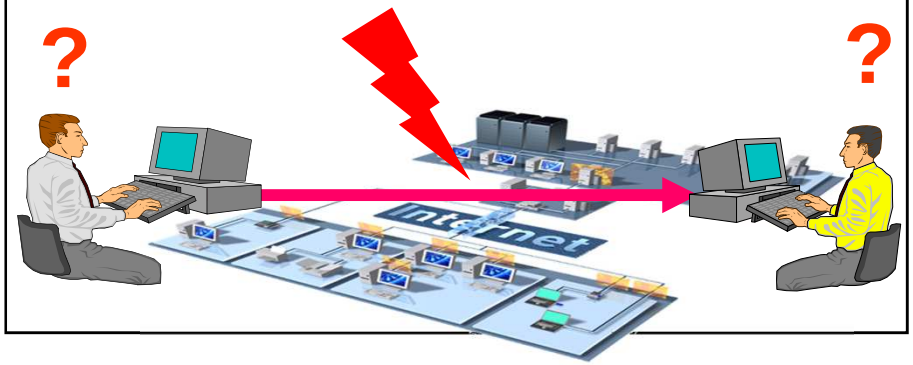
Reale Welt





Elektronische Welt benötigt

- Vertraulichkeit
- Authentisierung
- Datenintegrität
- Nachweisbarkeit



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

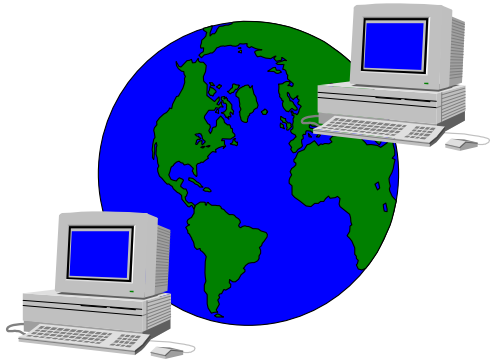
- elektronische Pförtner
  wie **Firewall- und PC-Sicherheitssysteme** schützen die internen IT-Systeme vor dem unerlaubten Zugriff von außen
- elektronische Sicherheitstransporter
  wie **Virtual Private Networks** schützen die Übertragung von elektronischen Informationen (Werte) vor unerlaubtem Auslesen 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

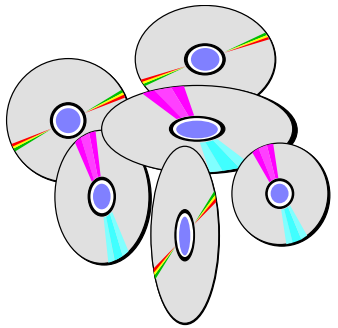
- Reale Welt versus elektronische Welt
- **Bedeutungswandel der IT-Systeme**
- Wirkungs- und Handlungszusammenhang
- Schadenskategorien

Bedeutungswandel der IT-Systeme (1/2)

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

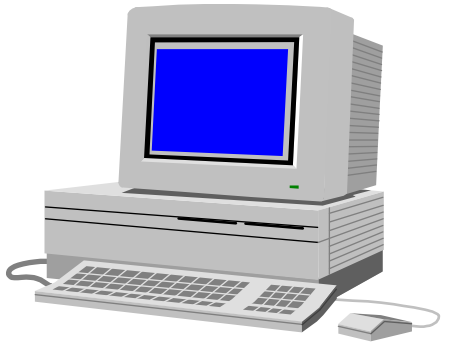


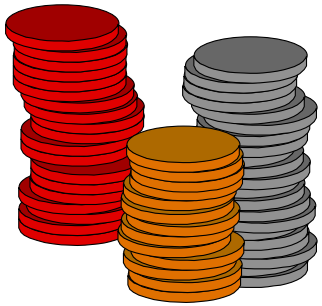
- **größer werdende Abhängigkeit von IT-Systemen**
  - Aufgaben sind nicht mehr ohne IT-Systeme zu erfüllen
  - Gefährdung der wirtschaftlichen Leistungsfähigkeit
  - Daten bleiben von der Eingabe bis zu ihrer Löschung in elektronischer Form



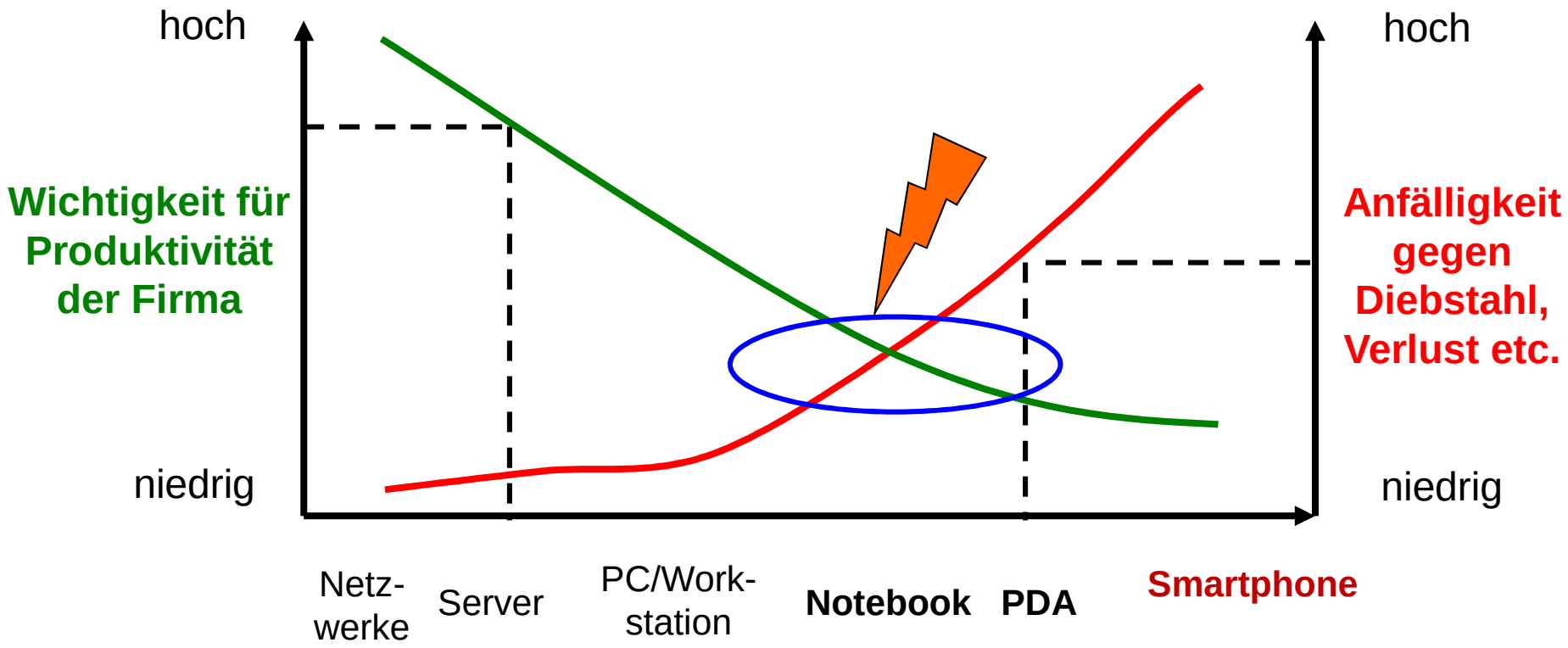
Bedeutungswandel der IT-Systeme (2/2)

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



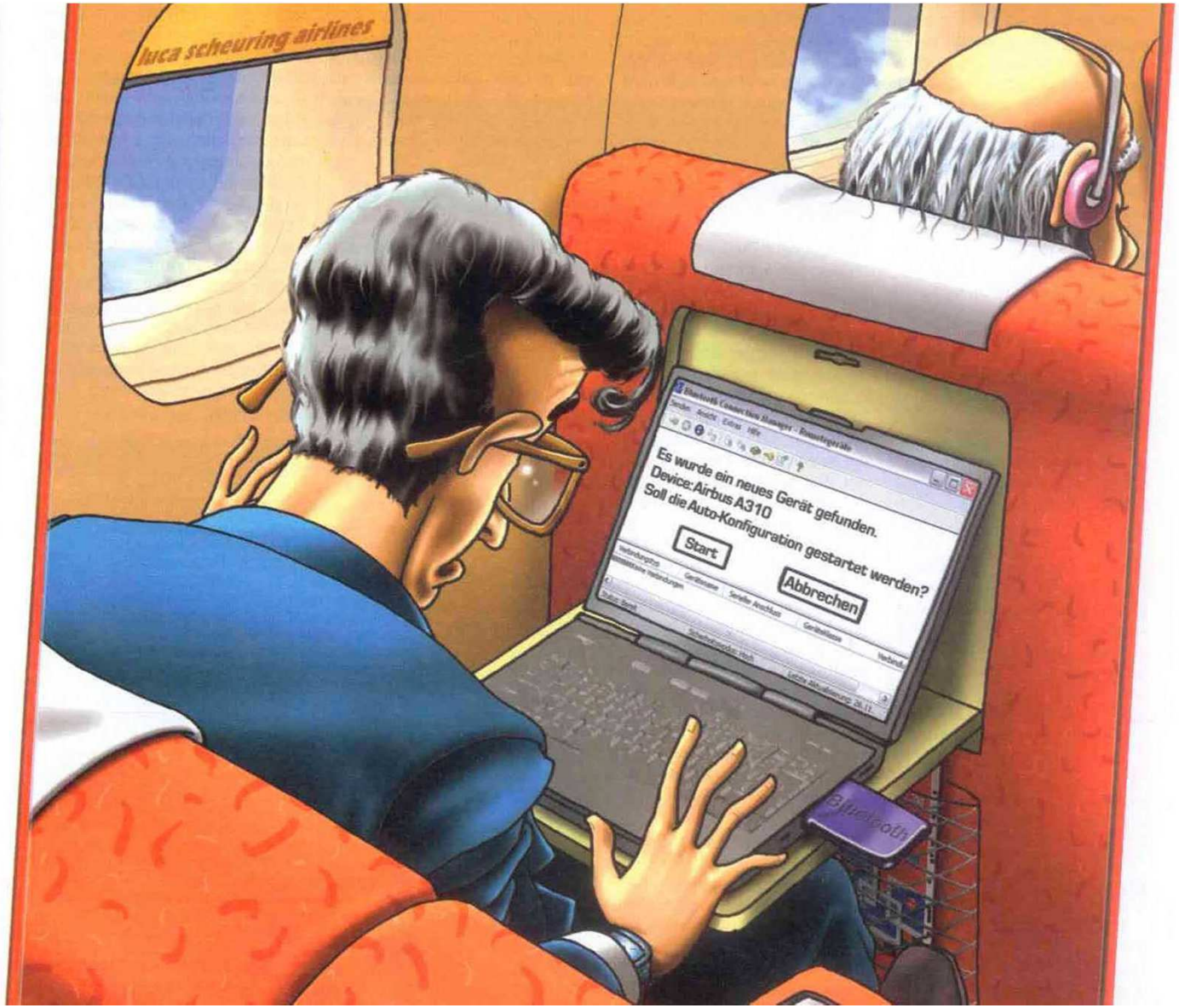


Neue Risiken durch gesteigerte Mobilität (1/2)



IT- und Kommunikationsinfrastruktur Komponenten
sortiert nach Mobilität

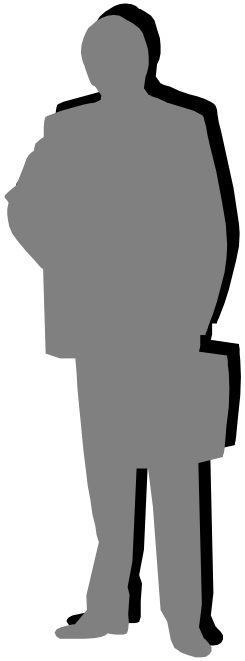
Neue Risiken durch gesteigerte Mobilität (2/2)



Sicherheitsanforderungen

- Einhaltung von Datenschutzgesetzen

- Unternehmen müssen sich selbst gegen Wirtschaftsspionage schützen



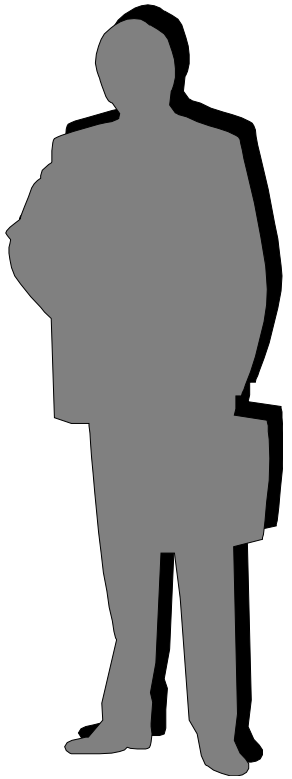
MangelIndes Unrechtsbewusstsein

Elektronische Welt:

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

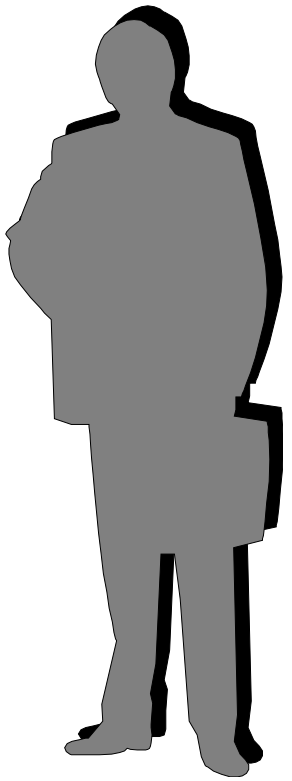
Spezielle Organisationen (1/2)

- **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
- Bedeutungswandel der IT-Systeme
- **Wirkungs- und Handlungszusammenhang**
- Schadenskategorien

Wirkungs- und Handlungszusammenhang
→ Welche Objekte müssen geschützt werden? (1/2)

- **Informationen und Daten**
  - Firmengeheimnisse (Strategiepapiere, Fusionsabsichten, Entwicklungsunterlagen)
  - Kundendatenbank
  - Filme, Musik, Bücher
  - Private Informationen (E-Mails, Bilder etc)

- **Ressourcen**
  - Rechnersysteme (Hardware und Software)
  - CPU - Zeiten

Wirkungs- und Handlungszusammenhang
→ Welche Objekte müssen geschützt werden? (2/2)

- **Dienstleistungen**
  - Datenbanken
  - Application Service Provider (ASP)
- **Prozesse und Abläufe**
- **Ansehen und Vertrauen**
- **Geschäftspotential**
- **IT unterstützte Systeme (Autos, Kühlschränke, Zugangssysteme, etc)**

Wirkungs- und Handlungszusammenhang
→ Wie wird der Schutz gewährleistet?

- **Durch Gewährleistung der:**
  - Authentikation
  - Integrität
  - Vertraulichkeit
  - Verfügbarkeit
  - Verbindlichkeit
  - Anonymisierung oder Pseudomisierung

Wirkungs- und Handlungszusammenhang
→ Authentikation

- **Gewährleistung der Echtheit und Glaubwürdigkeit der Identität eines Objektes.**
- Verfahren:
  - Passwort
  - PIN
  - Biometrie
  - Smartcards
  - Security-Tokens
  - Neuer Personalausweis
- **Beispiele:**
  - Login Systeme
  - Zugangskontrollen

Wirkungs- und Handlungszusammenhang
→ Integrität

- **Gewährleistung der Unveränderlichkeit des Objektes durch unbeteiligte.**
- **Verfahren:**
  - Prüfsummen
  - Digitale Signaturen
- **Beispiele:**
  - S/MIME oder OpenPGP (E-Mail Signierung)
  - CRC bei Archiven

Wirkungs- und Handlungszusammenhang
→ Vertraulichkeit

- **Gewährleistung der Geheimhaltung des Objektes vor unbeteiligte.**
- **Verfahren:**
  - Verschlüsselung
  - Klassifizierung
  - Zugriffsrechte (Wer darf was sehen?)
- **Beispiele:**
  - SSL / IPSec
  - Klassifizierung von Militärunterlagen
  - Pool Account in der FH

Wirkungs- und Handlungszusammenhang
→ Verfügbarkeit

- **Gewährleistung des Schutzes vor unbefugter Beeinträchtigung der Funktionalität / Dienste etc.**

- **Verfahren:**
  - Überwachen / Regulieren von Zugriffen auf Objekte
    - Was?
    - Wann?
    - Welche?

- **Beispiele:**
  - Prüfungssystem

Wirkungs- und Handlungszusammenhang
→ Verbindlichkeit

- **Gewährleistung einer unzweifelhaften Zuordnung einer Aktion zu einem Subjekt.**

- **Verfahren:**
  - Protokollierung
  - Signaturen (Digitale Unterschrift)

- **Beispiele:**
  - Prüfungssystem

Wirkungs- und Handlungszusammenhang
→ Anonymisierung oder Pseudonomisierung

- **Gewährleistung des Rechtes auf Informationelle Selbstbestimmung, den Schutz der Privatsphäre und der damit verbundenen personenbezogenen Daten.**

- **Verfahren:**
  - Datensparsamkeit
  - Zweckbindung
  - Notwendigkeit
  - Pseudo und oder Anonymisierung

- **Beispiele:**
  - Matrikelnummer anstatt Klarnamen etc.

Wirkungs- und Handlungszusammenhang
→ Wie wird das Schutzziel Gewährleistet? (1/2)

- **Vermeidung / Verhinderung**
  - VPN, SSL (TLS)
  - Festplattenverschlüsselung
  - PKI, Digitale Signatur
  - Smart Cards
  - Authentikation / Autorisierung
  - …
- **Erkennung**
  - Intrusion Detection System (IDS)
  - Honey Pots
  - Protokolle / Logging Systeme
  - …

Wirkungs- und Handlungszusammenhang
→ Wie wird das Schutzziel Gewährleistet? (2/2)

- **Schadensbegrenzung**
  - Datensicherungen
  - Isolation
  - Abschaltung

- Nicht alle Lösungen fallen nur unter eine Kategorie
  - Intrusion Prevention System (Erkennung, Verhinderung)
  - Firewall (Verhinderung, Schadensbegrenzung)
  - Deep Packet Inspection (Verhinderung, Erkennung)
  - Etc

⇒ **Nicht nur Software / Hardware**

Wirkungs- und Handlungszusammenhang
→ Was passiert bei einem Angriff?

- **Bei einem Angriff wird durch einen aktiven oder passiven Eingriff, eine ungewünschte Aktion mit Objekten gewährt.**

- **Ziel:**
  - Informationsgewinn
  - Reaktionen auslösen
  - Ressourcen nutzen

Wirkungs- und Handlungszusammenhang
→ Welche Motivation hat ein Angreifer?

- Neugierde
- Zerstörungswut
- Geld
- Anerkennung
- Herausforderung
- Spaß an der Technik
- Strafverfolgung

Wirkungs- und Handlungszusammenhang
→ Wer greift IT Systeme an? (1/3)

- **Berufskriminelle**
  - Geld als Motivation
- **Hacker**
  - Spaß an der Technik, Anerkennung, Herausforderung
- **Spione (Wirtschaft, Regierung)**
  - Geld (Wirtschaft), Informationsgewinn
- **Terroristen**
  - Politische Interessen
- **Vandalen**
  - Zerstörungswut
- **Behörden!**
  - Strafverfolgung

Wirkungs- und Handlungszusammenhang
→ Wer greift IT Systeme an? (2/3)

- Behörden – Anfragen an Google über Löschung / Daten

Wirkungs- und Handlungszusammenhang
→ Wer greift IT Systeme an? (3/3)

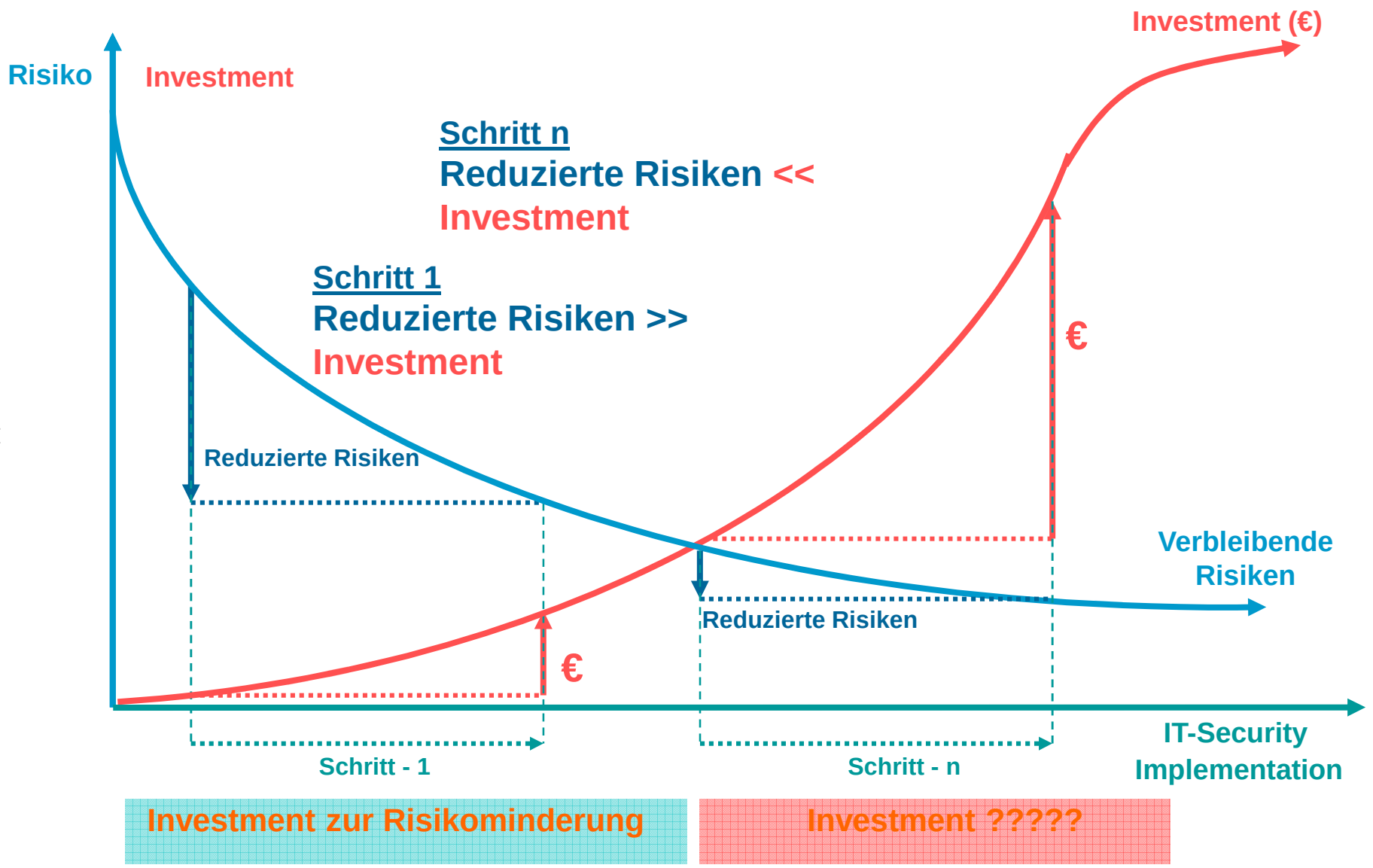
Der Wert von alltäglichen Objekten im Internet

Objekt	Kosten
Twitter	100-200$ / Account
MSN	1.40$ / Account
Gmail	82$ / Account
RapidShare	5$
Facebook	1000 Accounts 25$ (<10 Freunde) 1000 Accounts 45$ (>10 Freunde)
Steam	5-7$
Bank Account	1-1500$ / Account
Kompletter Satz Persönliche Daten	US: 5-8$ EU: 10-24$ World: 7$
Email	20-100$ / 1 Million Accounts
Botnet	67$ / 24h 9$ / 1h

Wirkungs- und Handlungszusammenhang
→ Kosten für IT-Sicherheit und Schäden?

- **80/20 Regel**
- Sensibilität für Sicherheit noch nicht überall gegeben
  - Verhältnis zwischen Umsatz und Ausgaben für Sicherheit nicht gerechtfertigt

Wirkungs- und Handlungszusammenhang
→ Kosten für IT-Sicherheit und Schäden?



Wirkungs- und Handlungszusammenhang
→ Wie wird ein Angriff durchgeführt? (1/2)

Durch Ausnutzung von:

- **Sicherheitslücken des (Software-) Systems**
  - Design Fehler (XSS, CSRF, Zertifikate...)
  - Fehlerhafte Implementierung (vorallem im Krypto Bereich)
  - Mangelhafte Konfiguration (Default Passwörter, falsch konfigurierte Firewalls/Router etc)
  - Validierung von Eingaben (Buffer- over/under flows, SQL Injection)
  - Hintertüren der Hersteller (Lawefull Interception etc)
- **Physikalischen** Eigenschaften (Side Channel Attacks)
  - SPA (Simple Power Analysis) / DPA (Differential Power Analysis)
  - Elektromagnetische Abstrahlung

Wirkungs- und Handlungszusammenhang
→ Wie wird ein Angriff durchgeführt? (2/2)

- **Beeinflussung des Benutzers**
  - Social Engineering
    - Phishing
    - Spamming

Wirkungs- und Handlungszusammenhang
→ Was ist Bedrohung in der IT-Sicherheit?

- Bedrohungen entstehen wenn Angriffe, Schwachstellen eines Systems ausnutzen. Dabei werden Schutzziele beeinträchtigt
- Eine Bedrohung ist demzufolge das Produkt von:
  - **Bedrohung = Angriff * Schwachstelle**
- Bei einem Starken Angriff (viele Angriffe, Komplexe, Effektive) ist auch bei einer geringen Schwachstelle eine hohe Bedrohung gegeben.
- Große Schwachstellen (Viele, Potential etc) können schon bei einfachsten Angriffen hohe Bedrohungen ergeben
- **Beispiele:**
  - DDOS ist ein „Starker“ Angriff auf eine geringe Schwachstelle
  - Admin Passwort auf default Wert ist ein schwacher Angriff aber eine große Schwachstelle.

Wirkungs- und Handlungszusammenhang → Beispiele für Angriffe (1/4)

GSM

- „Hacking into GSM for only $1500“
- GSM ist schon seit einer Weile „gebrochen“ allerdings war bisher die Geräte dafür ziemlich teuer. Das ist nun anders!

Wirkungs- und Handlungszusammenhang → Beispiele für Angriffe (2/4)

ATM (Bankautomaten)

- Bei einer Präsentation wurde gezeigt wie einfach es ist diese Automaten zu „hacken“
- Spucken Geld aus oder verwendete PINs von benutzern

Wirkungs- und Handlungszusammenhang
→ Beispiele für Angriffe (3/4)

Autos

- Eins der IT Systeme die vor Jahren schon als Ziel für Angriffe erkannt wurde
- Ist nun auch im Zielfeld von Hackern und wurde erfolgreich angegriffen

Wirkungs- und Handlungszusammenhang → Beispiele für Angriffe (4/4)

iPhone Jailbreak

- Jailbreak nutzt Sicherheitslücken
- Letzter Jailbreak kann remote komplette Kontrolle über Gerät erlangen, Besuch einer Webseite ist ausreichend

Wirkungs- und Handlungszusammenhang → Die Klassiker (1/3)

Buffer Overflow

- In ein Datenfeld werden mehr Daten geschrieben als dort reserviert wurden
- Dadurch werden weitere Speicherstellen überschrieben die dann im Laufe der Programmausführung selbst als Code ausgeführt werden könnten und dadurch eine ungewollte Operation ausführen.

Wirkungs- und Handlungszusammenhang → Die Klassiker (2/3)

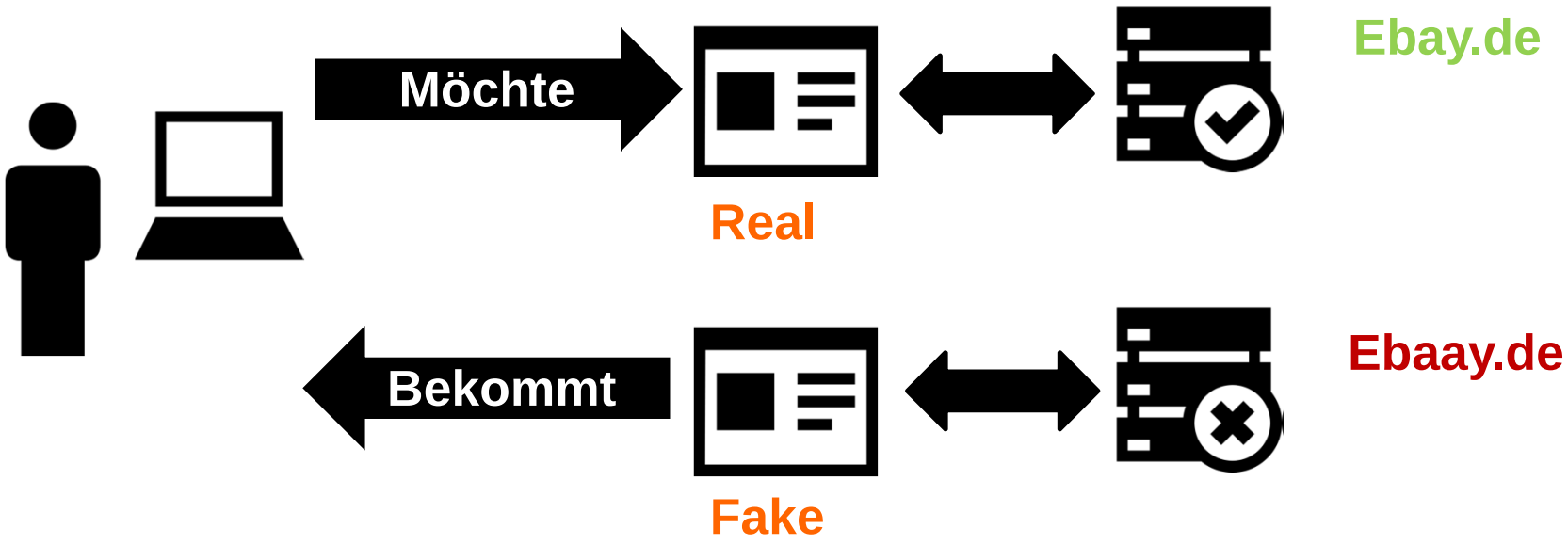
SQL Injection

- Praktisch alle Web Anwendungen nutzen Datenbanksysteme im Hintergrund
- Eingaben in Inputs werden meist direkt weitergeleitet als SQL Query an die Datenbank
- Bei unzureichender Validierung des Inputs kann direkt einfluss auf das Query genommen werden
- Beispielsweise:
  - select * from user where username=%user% and pass=%pass%
  - Wenn nun %user% direkt durch ein Formular gefüllt wird:
  - Select * from user where username=admin—
  - %user% = admin--

Wirkungs- und Handlungszusammenhang → Die Klassiker (3/3)

Phishing

- Das täuschen des Benutzers eine von ihm gewünschte Webseite zu besuchen, die allerdings durch eine Kopie ersetzt wurde.
- Diese Kopie dient dazu Login Details zu klauen



Wirkungs- und Handlungszusammenhang

→ Wie groß ist die Eintrittswahrscheinlichkeit eines Angriffes?

- Hängt direkt zusammen mit dem Wert des Objektes und der Kosten für den Angriff
- Wert muss nicht Geld sein!
- Hoher Wert sorgt für stärkeres Interessen
  - Forschungsergebnisse etc (Millionen Beträge)
- Gelegenheit als Zusatz zu der Motivation (wenn es einfacher ist, ist auch die Motivation größer)
- Masse nicht unterschätzen:
  - Sicherheitslücke kaufen/finden und ausnutzen
  - Ziel Millionen von Systemen
    - ⇒ Auch kleiner Wert interessant genug
- Eintrittswahrscheinlichkeit (E) setzt sich demnach zusammen aus:

Eintrittswahrscheinlichkeit = Bedrohung * (Motivation + Gelegenheit)

Wirkungs- und Handlungszusammenhang
→ Wie groß ist das Risiko einer Bedrohung?

- Das Risiko setzt sich zusammen aus:

Risiko = Eintrittswahrscheinlichkeit * Schaden

Eintrittswahrscheinlichkeit = Bedrohung * (Motivation + Gelegenheit)

Bedrohung = Angriffe * Schwachstelle

Inhalt

- Reale Welt versus elektronische Welt
- Bedeutungswandel der IT-Systeme
- Wirkungs- und Handlungszusammenhang
- **Schadenskategorien**

Schadenskategorien
→ Schadenskategorien (1/7)

Verstoß gegen Gesetze/Vorschriften/Verträge

- Schwere des Schadens abhängig von Konsequenzen die daraus entstehen
  - ⇒ Vertragsstrafen
  - ⇒ Strafrechtliche Strafen
  - ⇒ etc.

- Entstehen durch Verlust der:
  - ⇒ Vertraulichkeit
  - ⇒ Integrität
  - ⇒ Verfügbarkeit

Schadenskategorien
→ Schadenskategorien (2/7)

Beeinträchtigung des informationellen Selbstbestimmungsrechts

- Verletzung der informationellen Selbstbestimmung
- Missbrauch personenbezogner Daten
- Entsteht bei der Implementierung und dem Betrieb von IT-Systemen und/oder Anwendungen

Schadenskategorien
→ Schadenskategorien (3/7)

Beeinträchtigung der persönlichen Unversehrtheit

- Fehlfunktion eines IT-Systems oder Anwendung kann:
  - ⇒ Unmittelbar die Verletzung
  - ⇒ Die Invalidität
  - ⇒ Den Tod

- Höhe des schadens ist direkt an dem persönlichen Schaden zu messen

Schadenskategorien
→ Schadenskategorien (4/7)

Beeinträchtigung der Aufgabenerfüllung

- Verlust der Verfügbarkeit eines IT-Systems
- Verlust der Integrität der Daten
- Schwere des Schadens richtet sich nach:
  - ⇒ Zeitlicher Dauer der Beeinträchtigung
  - ⇒ Umfang der Einschränkungen der angebotenen Dienstleistungen

Schadenskategorien
→ Schadenskategorien (5/7)

Negative Außenwirkung

- Verlust der:
  - ⇒ Integrität
  - ⇒ Vertraulichkeit
  - ⇒ Verfügbarkeit
- Führt zu:
  - ⇒ Ansehensverlust
  - ⇒ Vertrauensverlust
  - ⇒ Vertrauen in die Arbeitsqualität

Schadenskategorien
→ Schadenskategorien (6/7)

Finanzielle Auswirkungen

- Verlust der:
  - ⇒ Integrität
  - ⇒ Vertraulichkeit
  - ⇒ Verfügbarkeit
- Führt zu:
  - ⇒ Unittelbaren oder mittelbaren finanziellen Schäden
- Höhe des Schadens grob in 3 Kategorien:
  - ⇒ Bis 25 000 Euro
  - ⇒ 25 000 – 5 Millionen Euro
  - ⇒ Über 5 Millionen Euro

Schadenskategorien
→ Schadenskategorien (7/7)

Fachanwendungsspezifische Schadensszenarien

- Kategorie für „alles andere“
- Hierbei wird betrachtet inwieweit die Vertraulichkeit, Integrität und Verfügbarkeit der Daten unter dem Szenario leiden

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Grundlagen der IT-Sicherheit

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.