



**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.

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

- **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?

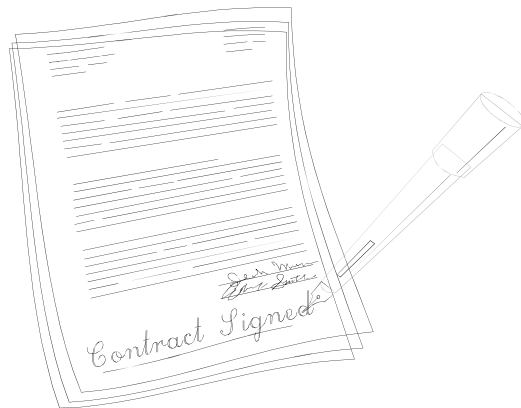
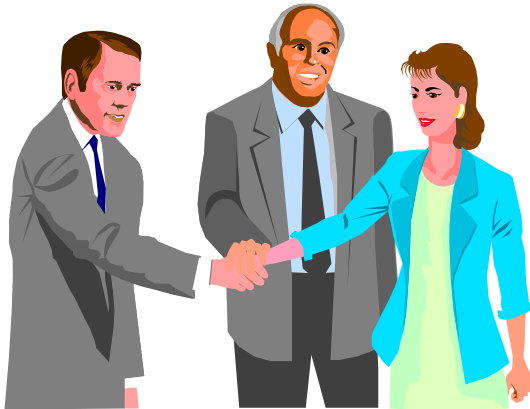
- Informationen und Wissen (also Macht) sind ungleich verteilt
- Einbruch und Diebstahl gefährden Eigentum
- Betrug und Verrat beeinflussen das Geschäftsleben
- Anschläge und Terror zählen zum Alltag

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.)

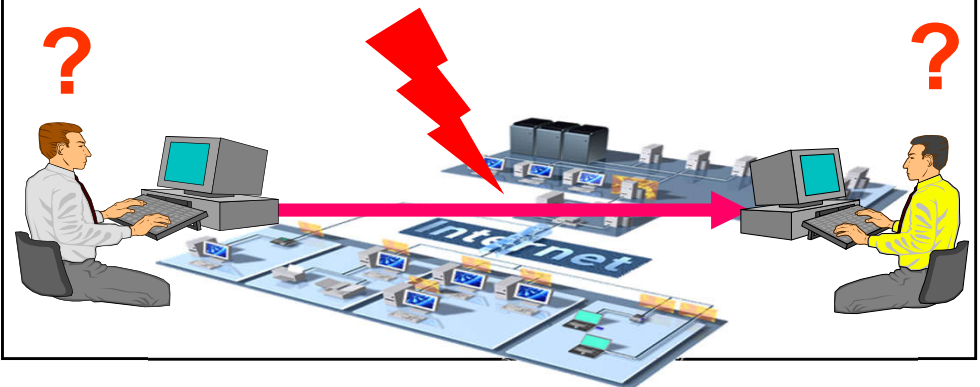
„Vertrauenswürdigkeit in der elektronischen Welt“

Reale Welt



Elektronische Welt benötigt

- Vertraulichkeit
- Authentisierung
- Datenintegrität
- Nachweisbarkeit



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

- elektronische Pfortner
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

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

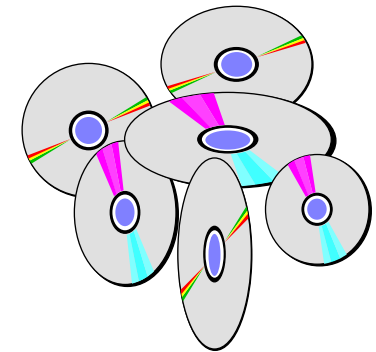
■ zunehmende Verwendung von IT-Systemen

- effiziente Verarbeitung
- rationelle Abwicklung
- komplexer werdende Aufgaben
- globale wirtschaftliche Ausdehnung

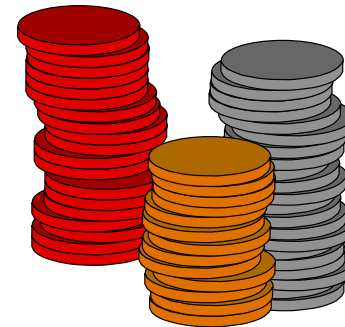
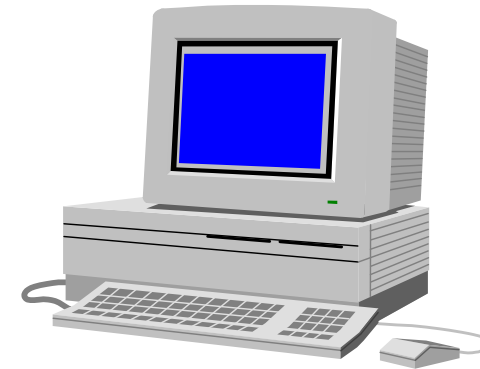


■ größer werdende Abhängigkeit von IT-Systemen

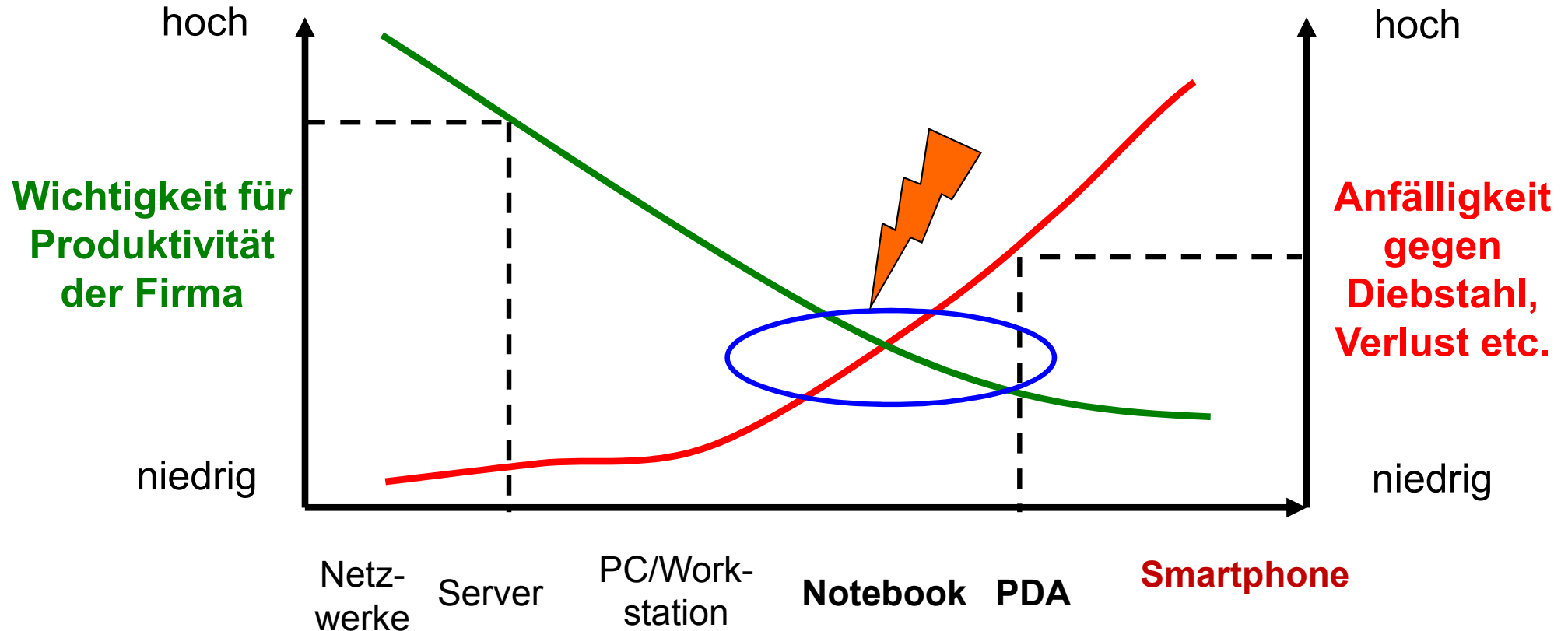
- Aufgaben sind nicht mehr ohne IT-Systeme zu erfüllen
- Gefährdung der wirtschaftlichen Leistungsfähigkeit
- Daten bleiben von der Eingabe bis zu ihrer Löschung in elektronischer Form



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

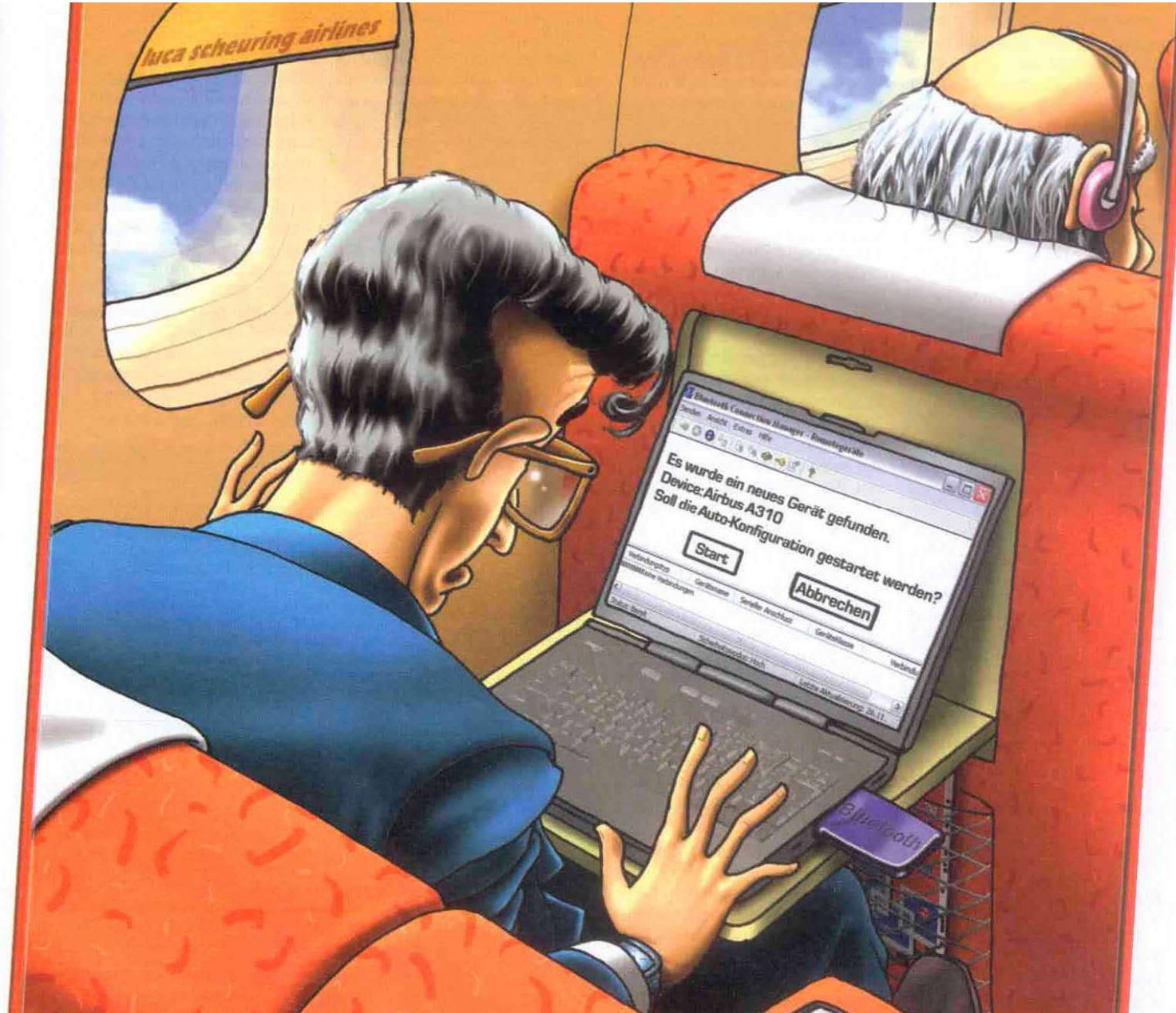


Neue Risiken durch gesteigerte Mobilität (1/2)

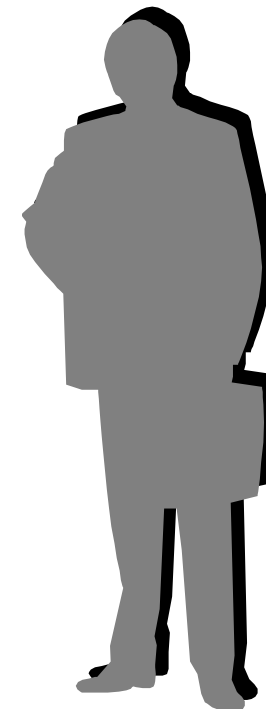


IT- und Kommunikationsinfrastruktur Komponenten
sortiert nach Mobilität

Neue Risiken durch gesteigerte Mobilität (2/2)



- Einhaltung von Datenschutzgesetzen
- Unternehmen müssen sich selbst gegen Wirtschaftsspionage schützen



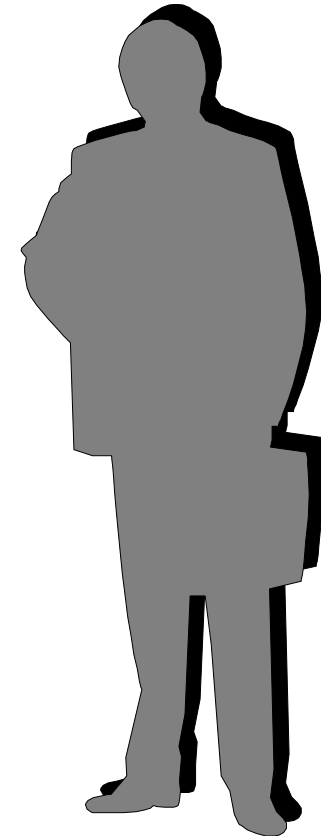
Elektronische Welt:

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



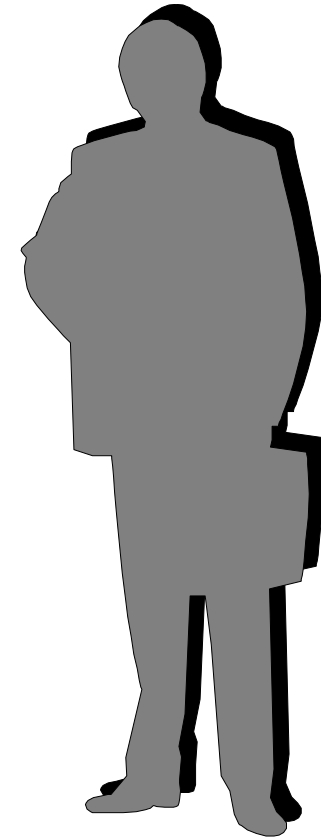
■ Geheimdienste

- 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.).



■ 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.**



- 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?

Schutzbedürfnisse:

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

Wirkungs- und Handlungszusammenhang

→ Authentifikation

- Gewährleistung der **Echtheit** und **Glaubwürdigkeit der Identität** eines Objektes.
- Verfahren:
 - Passwort
 - PIN
 - Biometrie
 - Smartcards, Security-Tokens, ... (mit Challenge-Response)
 - Neuer Personalausweis
 - XignQR
- **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:**
 - Klassifizierung
 - Zugriffsrechte (Wer darf was sehen?)
 - Verschlüsselung
- **Beispiele:**
 - SSL / IPSec
 - Klassifizierung von Militärunterlagen
 - Pool Account in der FH
 - Schengen Routing ???

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
 - Anti-DDoS-Systeme

Wirkungs- und Handlungszusammenhang

→ Verbindlichkeit

- Gewährleistung einer unzweifelhaften **Zuordnung** einer Aktion zu einem Subjekt.
- **Verfahren:**
 - Protokollierung
 - Signaturen (Digitale Unterschrift, ...) – Vertrauensdienste → eIDAS
- **Beispiele:**
 - Prüfungssystem

Wirkungs- und Handlungszusammenhang

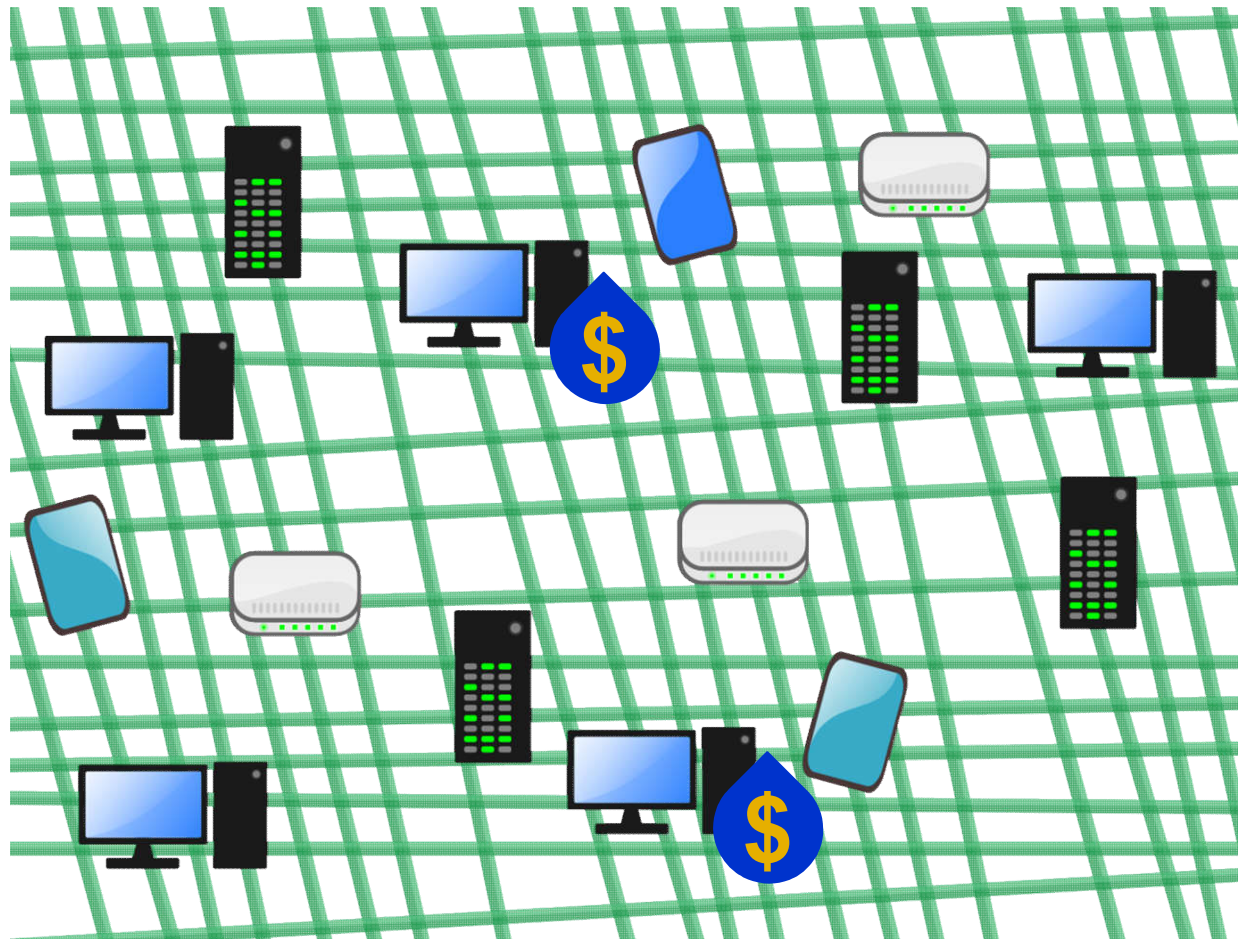
→ Anonymisierung oder Pseudonomisierung

- 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.

Prinzipielle IT Sicherheitsstrategien

→ Fokussierung

- Im Schnitt sind nur ca. **5 %** aller vorhandenen Daten in Unternehmen **besonders schützenswert**.



- Aber **welche Daten** sind besonders schützenswert und wie können diese **angemessen geschützt** werden?

Prinzipielle IT Sicherheitsstrategien

→ Vermeiden von Angriffen – (1)

- **Generell gilt: Das Prinzip der digitalen Sparsamkeit.**
→ So wenig Daten generieren wie möglich, so viele wie nötig.
- **Keine Technologie und Produkte mit Schwachstellen verwenden**
(z.B. Browser, Betriebssysteme, Internet-Dienste, ...)

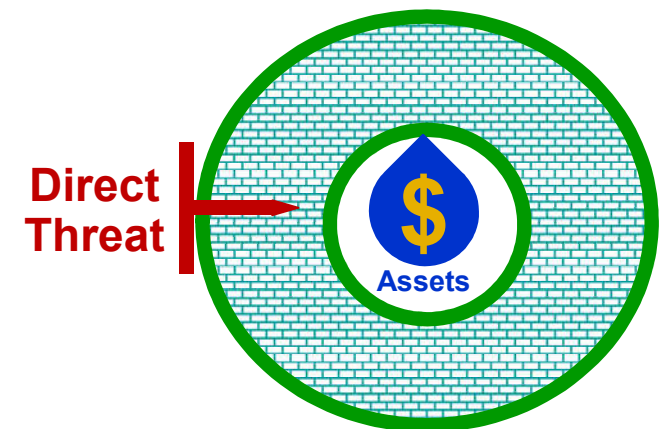


- **Bewertung der Vermeidung**
 - **Vermeidung von Angriffen ist die beste IT-Sicherheitsstrategie!**
 - **Ist nur begrenzt umsetzbar, wenn wir IT mit allen Vorteilen nutzen wollen!**

Prinzipielle IT Sicherheitsstrategien

→ Entgegenwirken von Angriffen – (2)

- Meist verwendete IT-Sicherheitsstrategie
- Beispiele, bei denen ein hoher Nachholbedarf besteht:
 - **Verschlüsselungssicherheitssysteme**
(Datei-, Festplatten-, E-Mail-Verschlüsselung, VPN-Systeme, SSL, ...)
 - **Authentikationsverfahren**
(Challenge-Response, globale Identität, Föderation, ...)
 - **Vertrauenswürdige IT-Systeme**
(Security Kernel, Isolierung u. Separierung, ..)
 - ...

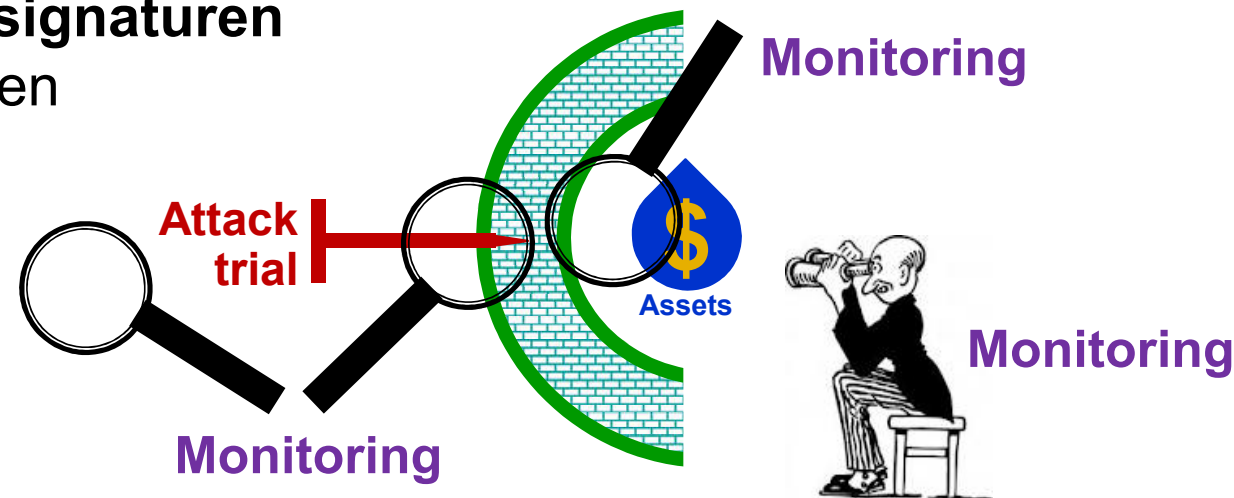


- **Bewertung des Entgegenwirkens**
 - Eine naheliegende IT-Sicherheitsstrategie
 - **Leider stehen zurzeit nicht genug *wirkungsvolle* und *vertrauenswürdige* IT-Sicherheitstechnologien, -lösungen und -produkte zur Verfügung oder sind im Einsatz**

Prinzipielle Sicherheitsstrategien

→ Erkennen von Angriffen – (3)

- **Erkennen** von Angriffen, denen nicht entgegengewirkt werden kann
- Angriffe erkennen und versuchen, den Schaden so schnell wie möglich zu minimieren (APT)
- Generell IT-Sicherheitssysteme, die Warnungen erzeugen, wenn Angriffe mit Hilfe von **Angriffssignaturen** oder **Anomalien** erkannt werden



- **Bewertung des Erkennens**
 - Die IT-Sicherheitsstrategie, Erkennen von Angriffen, ist sehr hilfreich, hat aber definierte Grenzen

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

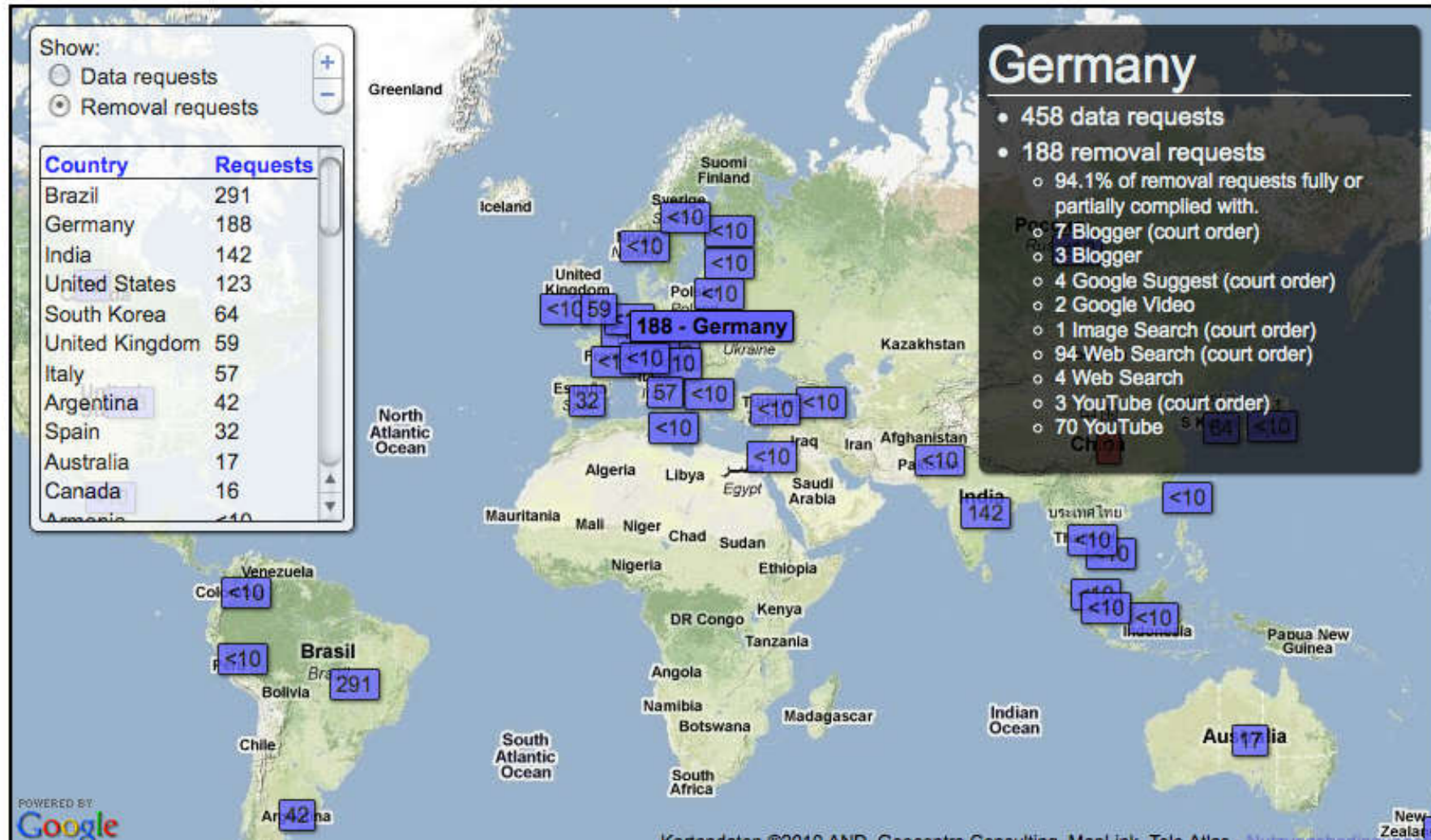
Wirkungs- und Handlungszusammenhang

→ 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

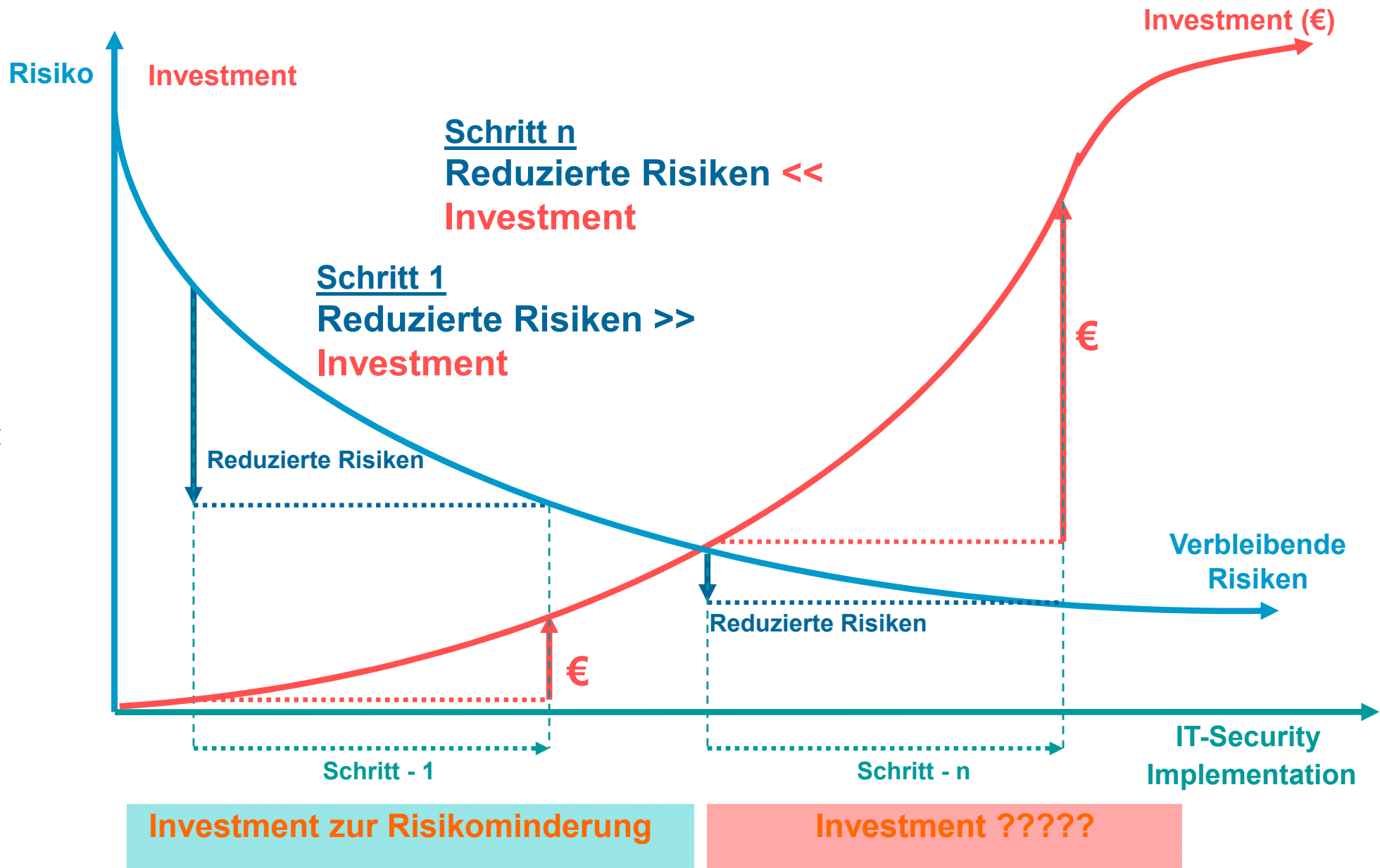
Wirkungs- und Handlungszusammenhang

→ 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!



The image shows a screenshot of a blog post from F-Secure Labs. The page header includes the F-Secure logo and the title "News from the Lab". The main content area features a world map with several yellow location markers. The article title is "Hacking into GSM for only \$1500 Demonstrated and documented" by Bill Ray, dated Wednesday, August 4, 2010. The article text discusses vulnerabilities in Apple's iOS and the demonstration of a kit for spoofing GSM base stations.

Hacking into GSM for only \$1500 Demonstrated and documented
By [Bill Ray](#) • [Get more from this author](#)
Posted in [Mobile](#), 2nd August 2010 12:38 GMT

A researcher at the DefCon hackers' meet has demonstrated kit for spoofing GSM base stations, allowing even those on a limited budget to intercept phone calls and text messages.

The audience attending the talk by Chris Paget were able to see their own handsets transferring to his spoofed base station, with calls receiving a recorded message explaining that the security had been compromised, [Associated Press reports](#). The demonstration would presumably have been a lot less impressive if Las Vegas had better 3G coverage.

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



The screenshot shows a news article from The Register. The header is red with the logo 'The Register' in white. Below the header is a navigation bar with categories: Hardware, Software, Music & Media, Networks, Security, Public Sector, Business, Science, and O. Below that is another navigation bar with categories: Crime, Malware, Enterprise Security, Spam, and ID. The main content area features a Dell advertisement for a Vostro 3700 laptop. The ad includes the Dell logo, a laptop image, and text: 'BUSINESS', 'VOSTRO™ 3700', 'Mit Intel® Core™ i5 Prozessor', 'Statt 730 €', 'JETZT 659 €', and 'Zzgl. MwSt. und 25 € Versand'. There is a 'JETZT' button. Below the ad are social media sharing options: Print, Retweet, Facebook, and Alert. The article title is 'Armed with exploits, ATM hacker hits the jackpot' with a subtitle '‘Game over’ vulns spew cash on demand'. The author is 'By Dan Goodin in Las Vegas' and the article was posted on '28th July 2010 23:56 GMT'. The article text starts with 'Black Hat A startling percentage of the world’s automated teller machines are vulnerable to physical and remote attacks that can steal administrative passwords and personal identification numbers to say nothing of huge amounts of cash, a security researcher said Wednesday.'

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

Hackers Wirelessly Crash Car's Computer At Highway Speeds



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



The screenshot shows a blog post from McAfee Labs. The header includes the McAfee logo and the text 'McAfee Labs Blog Cutting-edge security as it happens'. The main article title is 'Remote iPhone Jailbreak Using PDF Exploit Should Serve as Wake-Up Call', dated Tuesday August 3, 2010 at 8:54 am CST, posted by David Marcus. The article text discusses the author's experience with jailbreaking an iPhone and mentions the Electronic Frontier Foundation (EFF) and the Digital Millennium Copyright Act. It also mentions the Dev-Team and VUPEN.

McAfee

McAfee Labs Blog
Cutting-edge security as it happens

Archives

- ▶ [August 2010](#)
- ▶ [July 2010](#)
- ▶ [June 2010](#)
- ▶ [May 2010](#)
- ▶ [April 2010](#)
- ▶ [March 2010](#)
- ▶ [February 2010](#)
- ▶ [January 2010](#)
- ▶ [December 2009](#)
- ▶ [November 2009](#)
- ▶ [October 2009](#)
- ▶ [September 2009](#)
- ▶ [August 2009](#)
- ▶ [July 2009](#)

Remote iPhone Jailbreak Using PDF Exploit Should Serve as Wake-Up Call
Tuesday August 3, 2010 at 8:54 am CST
Posted by **David Marcus** 24 Comments; Trackback

Like many iPhone users, I "[jailbreak](#)" my iPhone. I do this for many reasons, but mainly for console-level access and the darn cool infosec tools that are available through [Cydia](#). Like many iPhone users, I was quite happy when the [Electronic Frontier Foundation \(EFF\)](#) was able to get jailbreaking included under "fair use" within the [Digital Millennium Copyright Act](#). Like many iPhone users, I was also **very** happy to learn that [Dev-Team](#) would soon make remote jailbreaking possible by simply visiting their jailbreakme website. Alas my happiness was not to last.

While still at Defcon, I saw through Twitter that one exploit or another was being used to remotely jailbreak the iPhone. (I believe the first tweets I saw were from Brian Krebs.) I then saw posts from [VUPEN](#) that several flaws were being exploited. From their advisory:

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.

SQL Injection

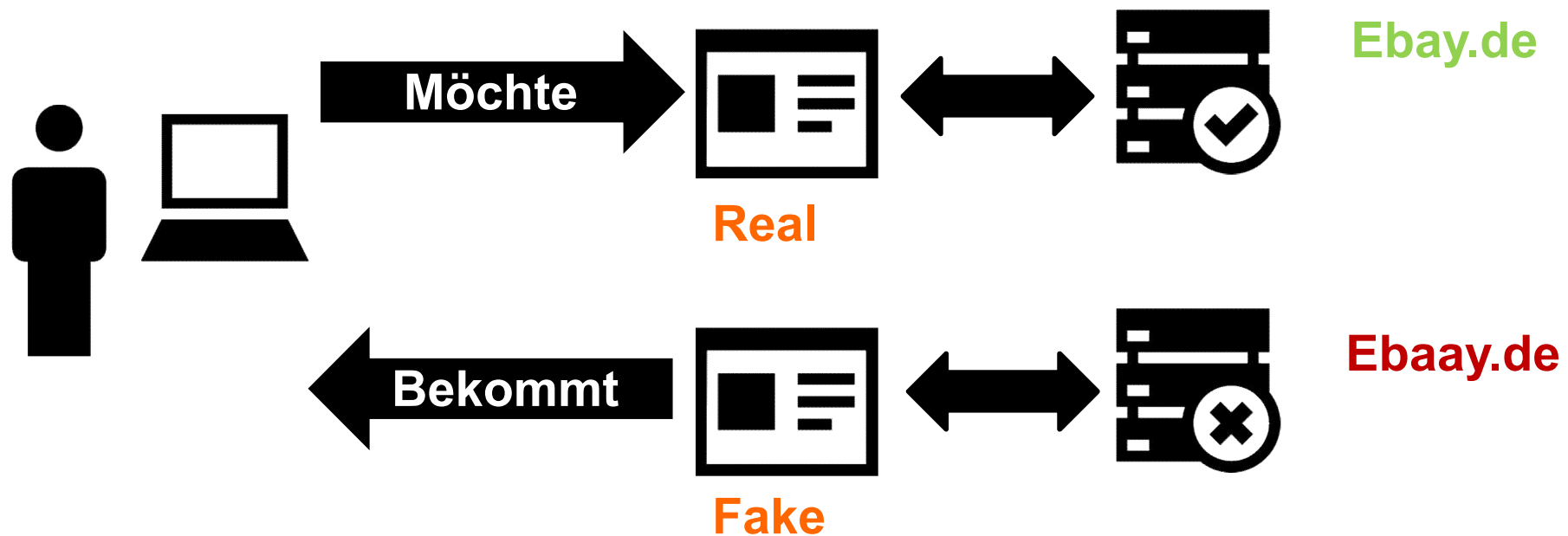
- Praktisch alle Web Anwendungen nutzen Datenbanksysteme im Hintergrund
- Eingaben in Inputs werden meist direkt weitergeleitet als SQL Query an die Datenbank
- Bei unzureichender Validierung des Inputs kann direkt einfluss auf das Query genommen werden
- Beispielsweise:
 - `select * from user where 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

- 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 personenbezogener 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:
 - ⇒ Unmittelbaren 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.