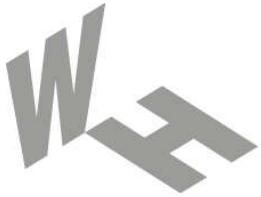


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Internet Sicherheit B
→ Einführung

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.

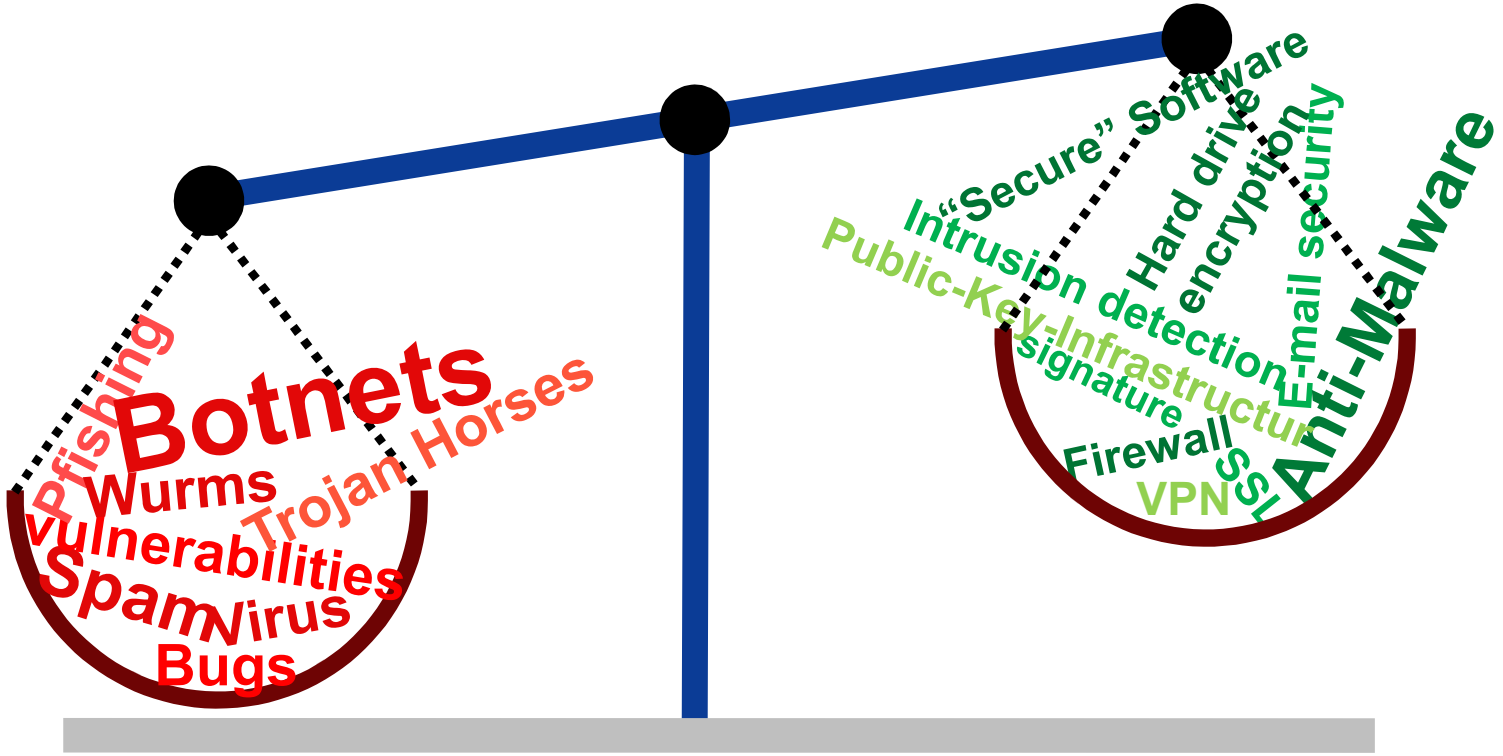
Inhalt

- Unser Problem
- Prinzipielle IT-Sicherheitsstrategien
- IT-Sicherheitsherausforderungen
- Basis und angemessene IT-Sicherheit
- Fazit und Ausblick

Inhalt

- **Unser Problem**
- Prinzipielle IT-Sicherheitsstrategien
- IT-Sicherheitsherausforderungen
- Basis und angemessene IT-Sicherheit
- Fazit und Ausblick

Internet Sicherheit
→ Situation



- Professionelle Hacker greifen alles erfolgreich an!
- NSA und Co. sammeln alle Daten und werten fleißig aus!
- Wir haben zurzeit zu viele ungelöste IT-Sicherheitsprobleme

Was sind die Problemfelder?
→ 1. Privatheit und Autonomie

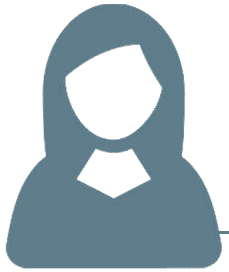
Verschiedenen Sichtweisen

Kulturelle Unterschiede
(Private Daten gehören den Firmen? US 76%, DE 22%)

Geschäftsmodelle „Bezahlen mit persönlichen Daten“

Privatheit / Autonomie

Staat *(NSA, BND, …)*: Identifizieren von terroristischen Aktivitäten



Nutzer: Autonomie im Sinne der Selbstbestimmung

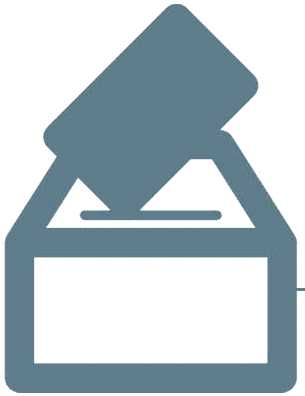
Was sind die Problemfelder?
→ 2. Wirtschaftsspionage

ca. 51 Milliarden € Schaden pro Jahr

Wirtschaftsspionage

Zum Vergleich:
Internet-Kriminalität: ca. 100 Millionen € pro Jahr
(Online Banking, DDoS, …)

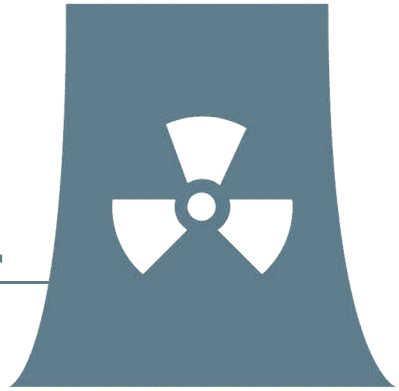
Was sind die Problemfelder?
→ 3. Cyberwar



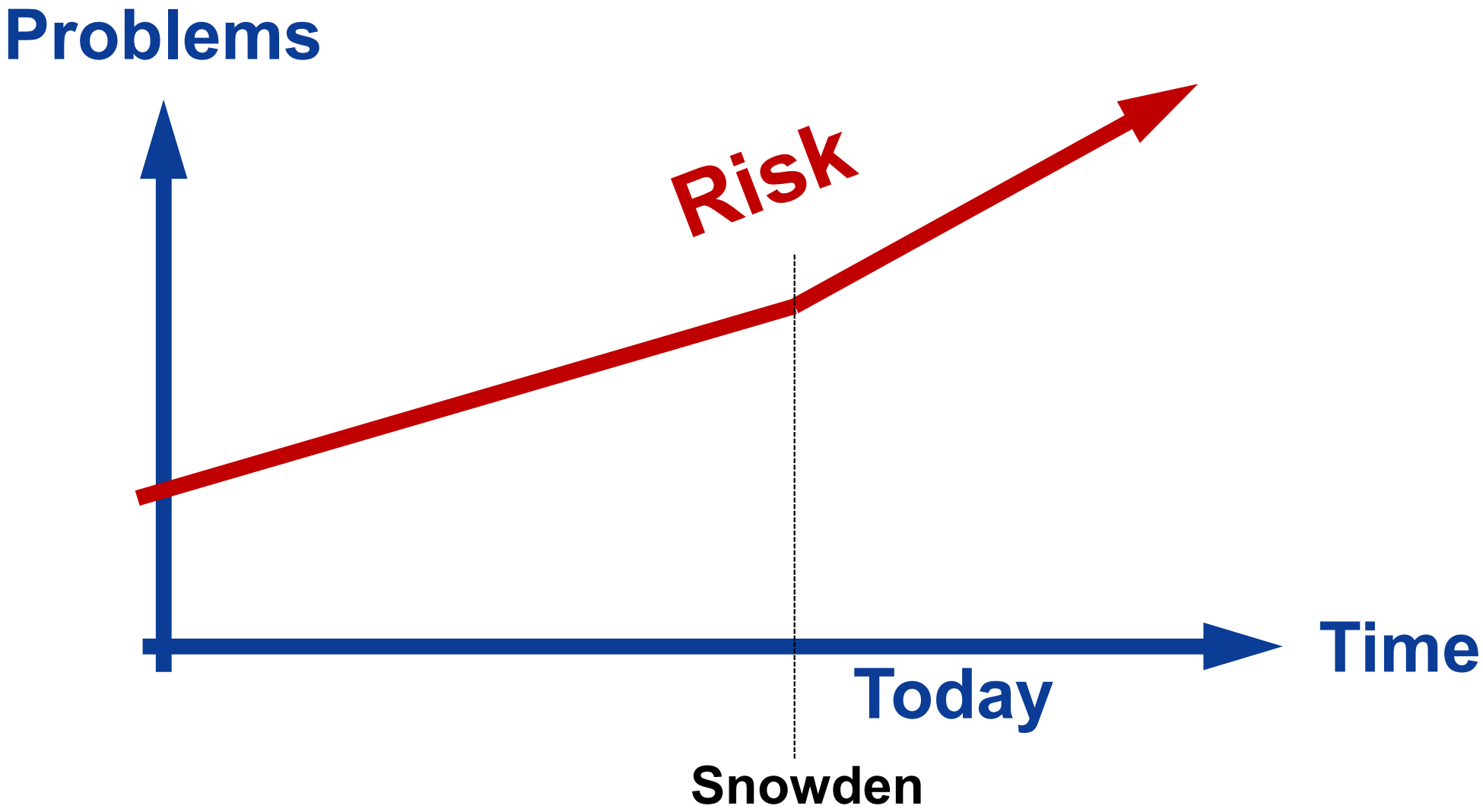
Umsetzung von politischen Zielen
→ „einfach“ und „preiswert“

Cyberwar

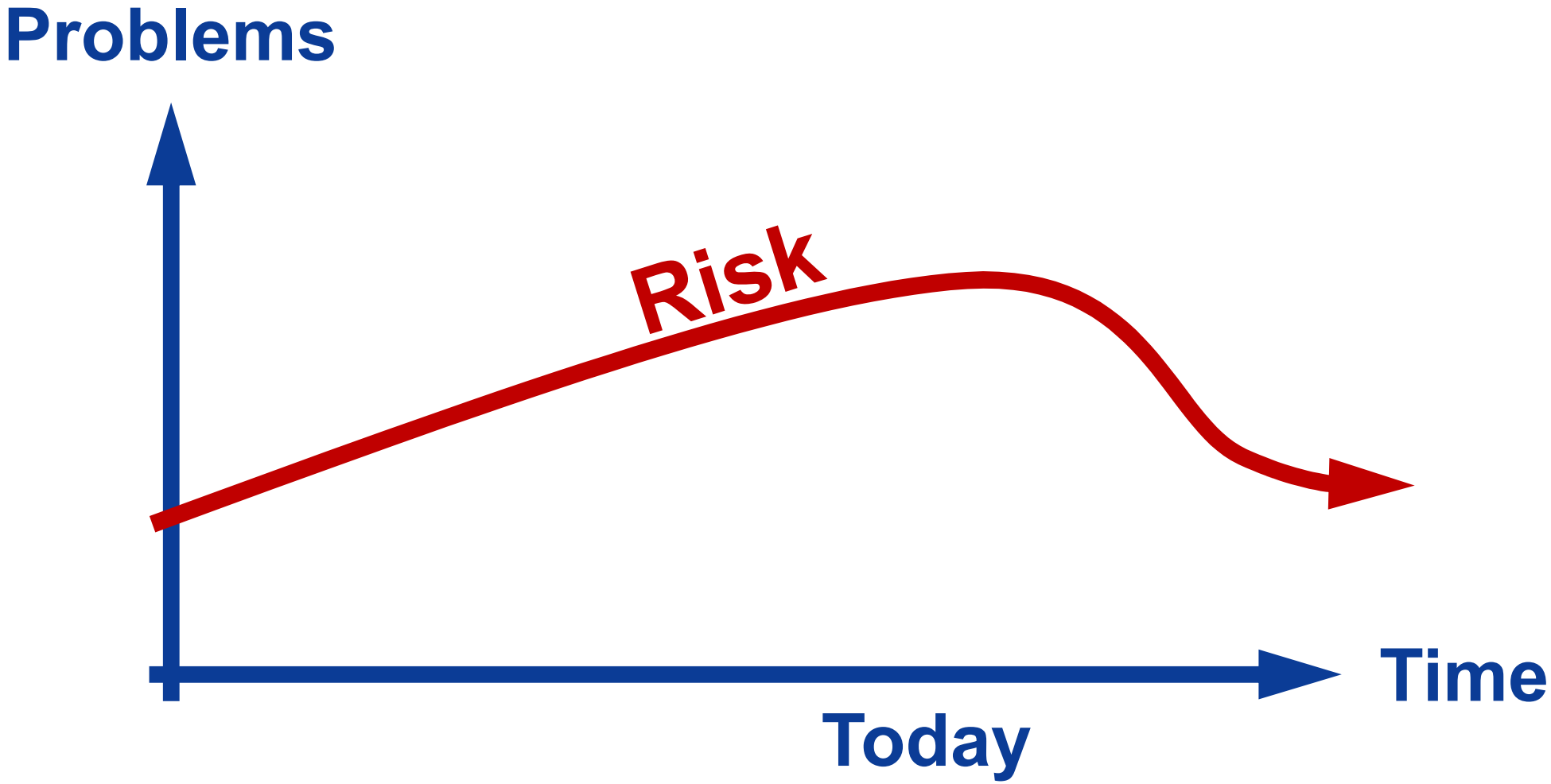
Angriffe auf Kritische Infrastrukturen
z.B. Stromversorgung, Wasserversorgung, …



IT-Sicherheit im Laufe der Zeit
→ Unser Problem



IT-Sicherheit im Laufe der Zeit
→ Unsere Herausforderung



Internet-Sicherheit
→ Evaluierung der Situation

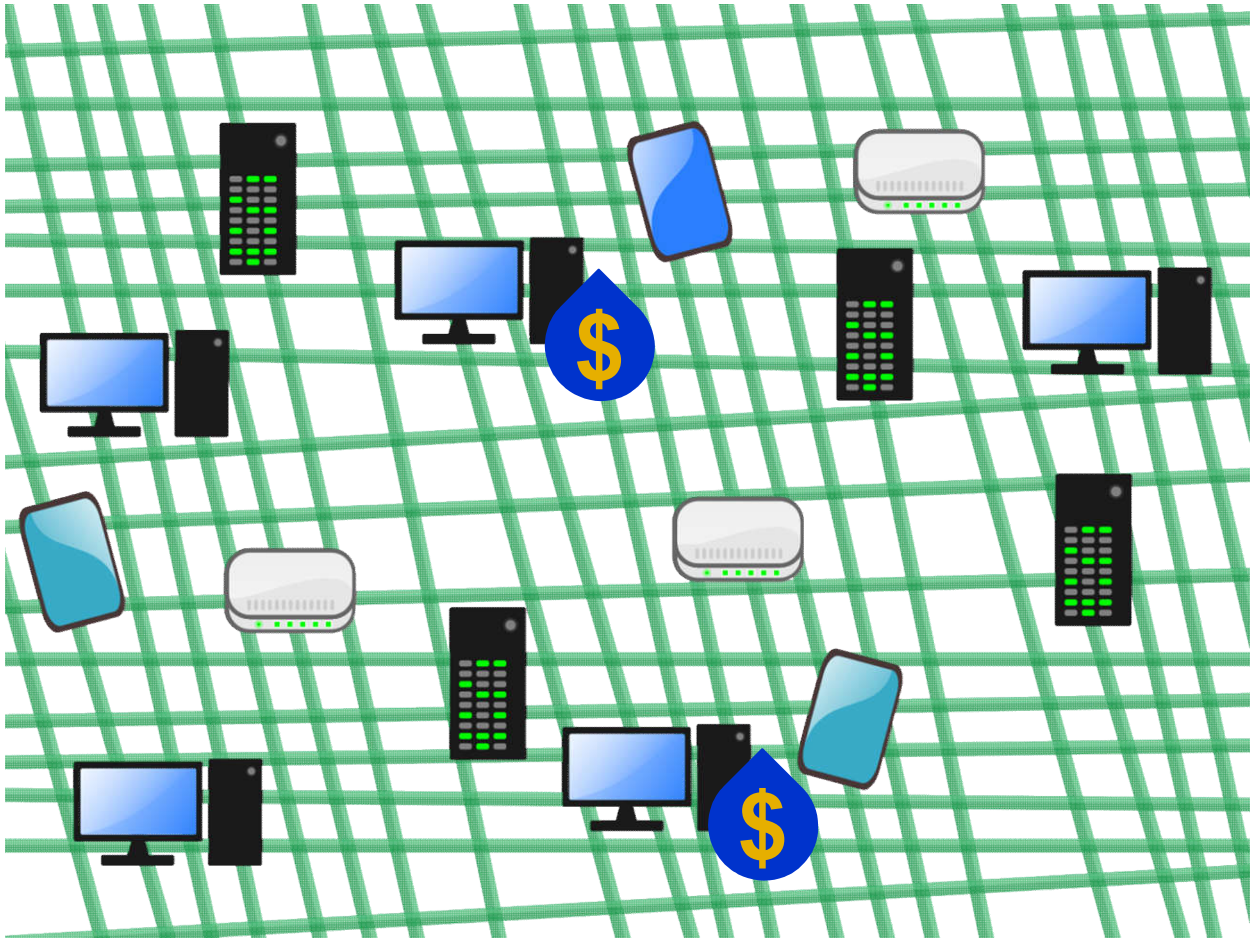
- **Wir kennen die IT-Sicherheitsprobleme**, doch die heute vorhandenen und genutzten IT-Sicherheitssysteme und IT-Sicherheitsmaßnahmen **reduzieren das IT-Sicherheitsrisiko nicht** ausreichend**!**
- Es handelt sich um ein globales Problem
- Die zukünftigen Angriffe werden die heutigen **Schäden** noch deutlich **überschreiten**
- **Wir brauchen innovative Ansätze** im Bereich der Internet-Sicherheit, um das Risiko für unsere Gesellschaft auf ein angemessenes Maß zu reduzieren

Inhalt

- Unser Problem
- **Prinzipielle IT-Sicherheitsstrategien**
- IT-Sicherheitsherausforderungen
- Basis und angemessene IT-Sicherheit
- Fazit und Ausblick

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?

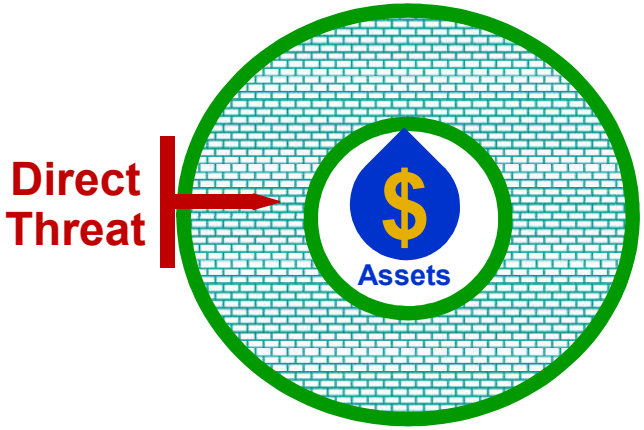
Prinzipielle IT Sicherheitsstrategien
→ Vermeiden von Angriffen – (1)

- **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)

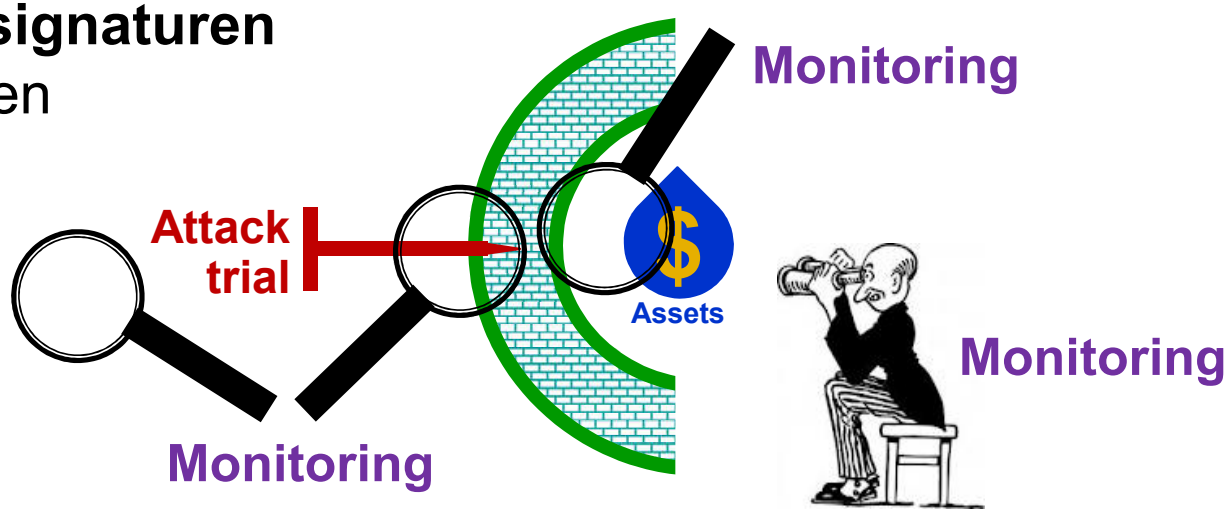
- Meist verwendete IT-Sicherheitsstrategie
- Beispiele, bei denen ein hoher Nachholbedarf besteht:
  - **Verschlüsselungssicherheitssysteme**
    (Datei-, Festplatten-, E-Mail-Verschlüsselung, VPN-Systeme, SSL, ...)
  - **Authentikationsverfahren**
    (Challenge-Response, globale Identität, Föderation,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

Inhalt

- Unser Problem
- Prinzipielle IT-Sicherheitsstrategien
- **IT-Sicherheits-herausforderungen**
- Basis und angemessene IT-Sicherheit
- Fazit und Ausblick

IT-Sicherheitsherausforderungen
→ Zu viele Schwachstellen in Software

- Die **Software-Qualität** der *Betriebssysteme* und *Anwendungen* ist **nicht gut genug!**

- **Fehlerdichte:**
  Anzahl an Fehlern pro 1.000 Zeilen Code (Lines of Code - LoC).

Fehlerdichte	Klassifizierung der Programme
< 0,5	stabile Programme
0,5 .. 3	reifende Programme
3 .. 6	labile Programme
6 .. 10	fehleranfällige Programme
> 10	unbrauchbare Programme

Betriebssysteme haben mehr als 10 Mio. LoC

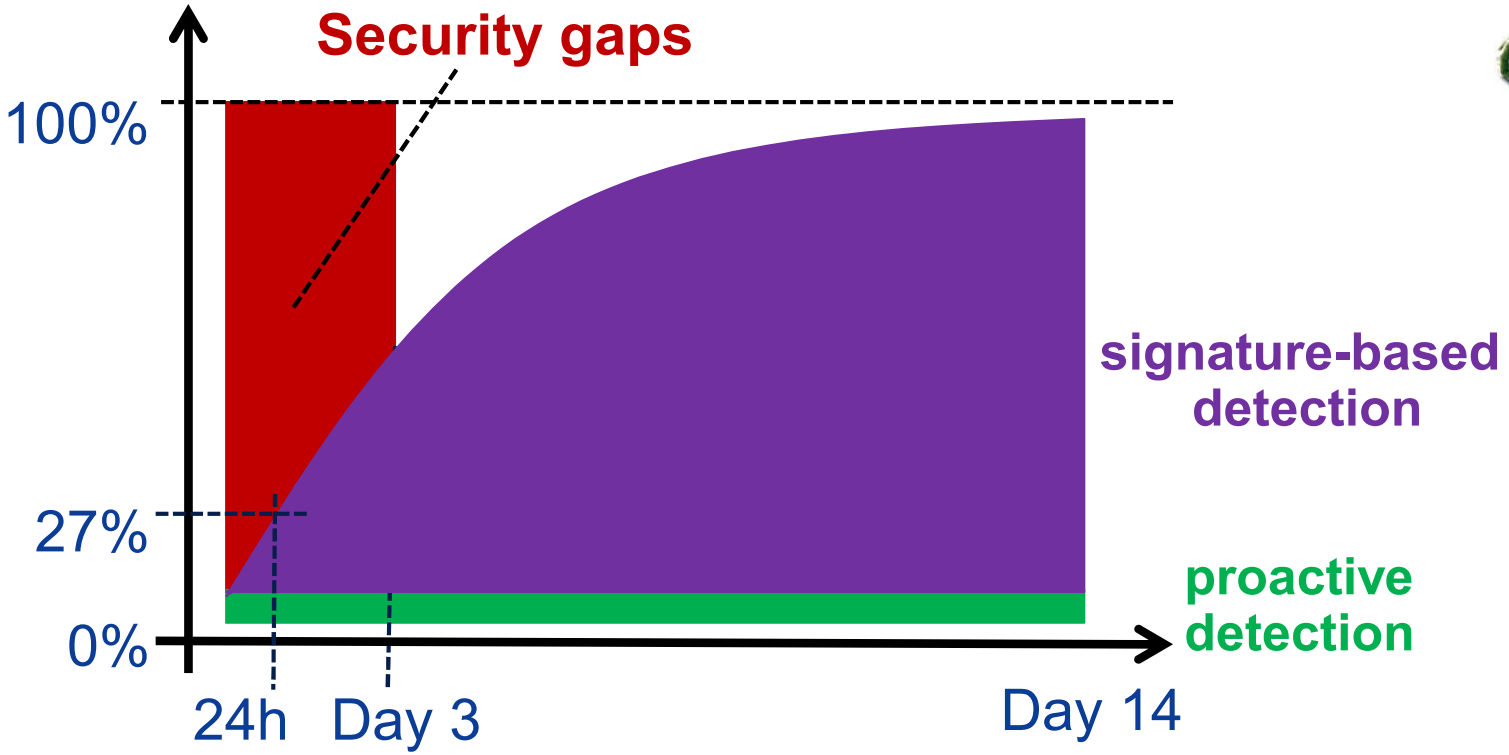
→ mehr als 3.000 Fehler
(Fehlerdichte 0,3)

→ und damit zu viele Schwachstellen

IT-Sicherheitsherausforderungen
→ Ungenügender Schutz vor Malware (1/2)

- **Schwache Erkennungsrate** bei Anti-Malware Produkten
  → nur 75 bis 95%!

- ***Bei direkten Angriffen weniger als 27%***



IT-Sicherheitsherausforderungen
→ Ungenügender Schutz vor Malware (2/2)

- **Jeder 10. Computer hat Malware!**
  - Datendiebstahl/-manipulation (Keylogger, Trojanische Pferde, …)
  - Spammen, Click Fraud, Nutzung von Rechenleistung, …
  - Datenverschlüsselung / **Lösegeld**, …

- **Cyber War (Advanced Persistent Threat - APT)**
  - Eine der größten Bedrohungen zurzeit!
  - Stuxnet, Flame, …

  → CyberWar

IT-Sicherheitsherausforderungen
→ Identity Management (2017)

- Passworte, **Passworte**, ***Passworte***, …
  sind das Mittel für die Authentikation im Internet!
- **Identifikationsbereiche liegen im Unternehmens- und Kundenumfeld, nicht international!**
- Föderationen sind noch nicht verbreitet genug!

Identitätsdiebstähle

Phishing Angriffe

Dienste-Übernahmen

…

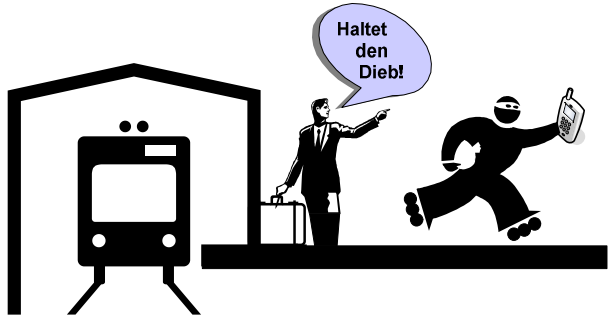
IT-Sicherheitsherausforderungen
→ Webserver Sicherheit

- Schlechte Sicherheit auf den Webservern / Webseiten
- **Heute wird Malware hauptsächlich über Webseiten verteilt**
  (ca. 2.5 % Malware auf den deutschen gemessen Webseiten)
- **Gründe für unsichere Webseiten**
  - Viele Webseiten sind nicht sicher implementiert!
  - Patches werden nicht oder sehr spät eingespielt,
  - Firmen geben **kein Geld für IT-Sicherheit** aus!
  - **Verantwortliche kennen das Problem nicht!**

© http://moneytipcentral.com/

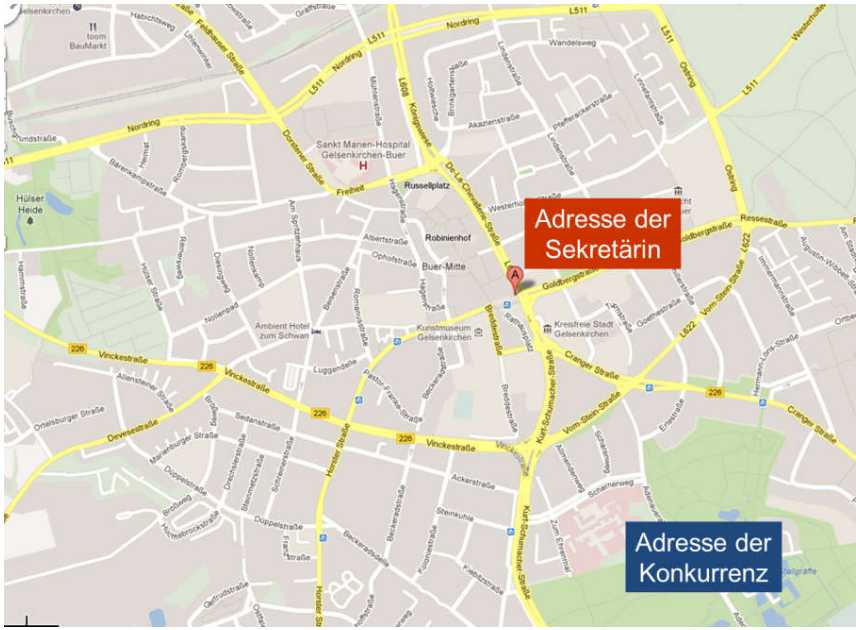
IT-Sicherheitsherausforderungen
→ Gefahren mobiler Geräte

- **Verlieren der mobilen Geräte**
  Ständig wechselnde **unsichere Umgebungen** (Flughäfen, Bahnhöfe, Cafés, …) …



… damit wird die Wahrscheinlichkeit des **Verlustes deutlich höher!**
(Handy-Statistik Taxis in London, Notebook-Statistik Flughäfen)

- **Apps als Spy-/Malware**
  (Masse statt Klasse)
- **Bewegungsprofilbildung**
- **Öffentliche Einsicht**



- **Falsche oder manipulierte Hotspots**
  (Vertrauenswürdigkeit)
- **Bring Your Own Devices / Consumerisation**

IT-Sicherheitsherausforderungen
→ Cloud Computing

- Dauerhafter und attraktiver zentraler Angriffspunkt
  - **Vernetzung bietet zusätzliche Angriffspunkte**

- Identitätsdiebstahl, Session-Hijacking, …
- **Schwachstellen** bei **Shared Services,** Abgrenzung der Unternehmensdaten
- Ich kenne die **Orte**, wo meine **Daten gespeichert sind** nicht!
- Wie kann ich sicher sein, dass die **Daten noch existieren?**
- Wie kann ich sicher sein, dass keiner meine Daten liest?
- **Datenverlust** (Platten-, Datenbank-, Anwendungsfehler, …)
- Datenlecks (Datenbank, Betriebssystem, …)
- **…**

IT-Sicherheitsherausforderungen
→ Internet-Nutzer

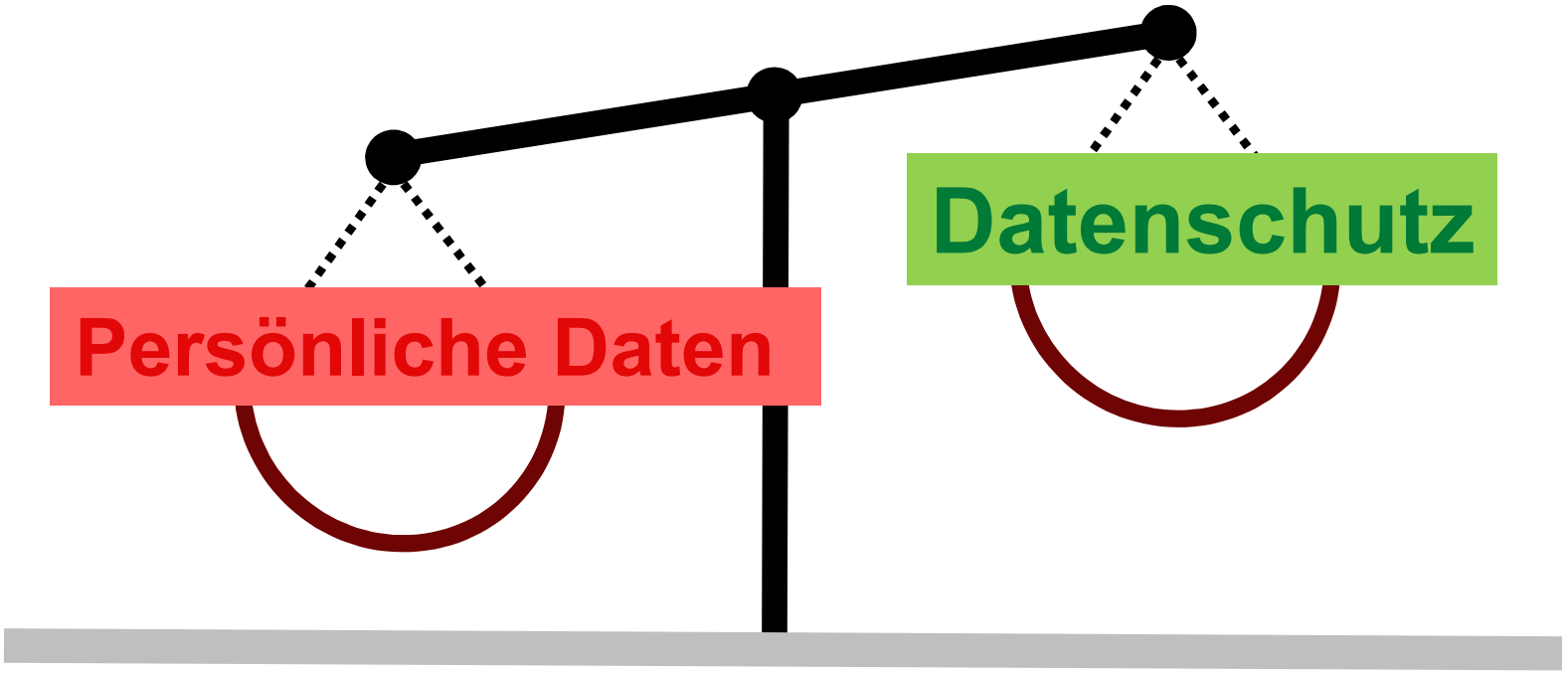
- Internet-Nutzer müssen die Gefahren des Internets kennen, sonst schaden sie sich und anderen!

- ***Umfrage BITKOM: (2012)***
  Fast jeder dritte **Internet-Nutzer** ***schützt sich nicht angemessen***!
  - ***keine*** Personal Firewall (30 %)
  - ***keine*** Anti-Malware (28 %)
  - gehen ***sorglos*** mit E-Mails und Links um
  - usw.

- ***Studie „Messaging Anti-Abuse Working Group“:***
  57 Prozent der Befragten haben schon einmal ***Spam-Mails geöffnet*** oder einen ***darin enthaltenen Link angeklickt***.

IT-Sicherheitsherausforderungen
→ Bezahlen mit persönlichen Daten

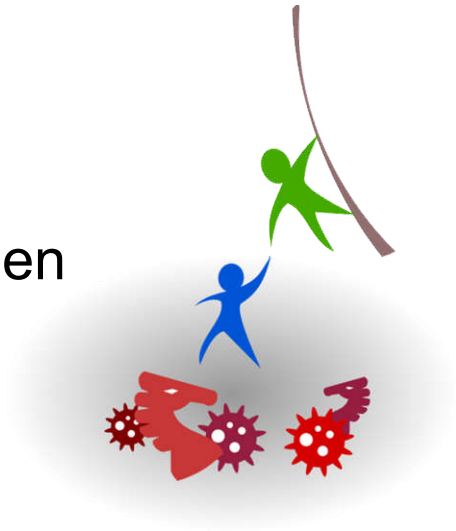
Persönliche Daten sind ein Rohstoff des Internetzeitalters



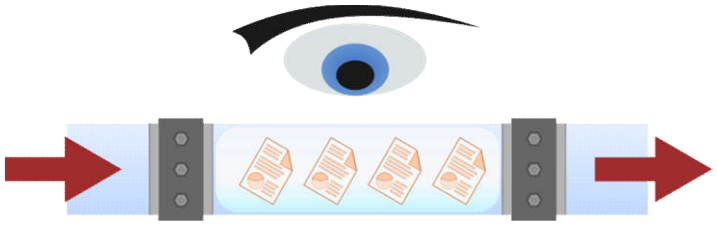
Geschäftsmodell: „Bezahlen mit persönlichen Daten“

IT-Sicherheitsherausforderungen
→ NSA - Herausforderungen

- **Grundsätzliche Probleme und fehlendes Vertrauen**
  - NSA kauft Zero-Day-Exploit für eigenen Angriffe, nicht für mehr Sicherheit
  - Die US IT Marktführer arbeiten mit der NSA zusammen
  - Gesetzliche Grundlagen (Patriot Act, …)
  - Die NSA macht Wirtschaftsspionage
  - …



- **Manipulierte IT und IT-Sicherheitstechnologie machen die Aktivitäten über das Internet unsicher!**
  - Fehler in IT-Sicherheitstechnologie (SSL, …)
  - Nutzung unsicherer Krypto-Algorithmen, z.B. Cipher Suite (RC4, DES, …)
  - **Schlechte Zufallszahlengeneratoren (Linux, RSA-Produkte, …)**
  - Hintertüren in Hardware und Software (BS, App, …)
  - Nutzen von NSA freundlichen E-Mail- und Cloud Angeboten
  - …



Notwendigkeit - Paradigmenwechsel
→ Änderungen der Rahmenbedingung (1/2)

Grundlegende Rahmenbedingungen haben sich geändert!

- **Das Internet geht über alle Grenzen und Kulturen hinaus!**
  - Problem bei der Strafverfolgung
  - Unterschiedliche **Auffassungen** darüber, was **richtig** und was **falsch** ist!
  - Herausforderungen bei verschiedenen Rechtssystemen

- **Radikale Entwicklung und Veränderung in der IT**
  - **Mobile Geräte**, *Soziale Netze*, **Cloud Computing**, …
    → *neue Player, neue Betriebssysteme, neue IT-Konzepte, neue Angriffe*
  - ***Internet der Dinge:*** SmartGrid, SmartCar, SmartTraffic, SmartHome, …
    → z.B. Atomausstieg sorgt für mehr Risiko im Internet

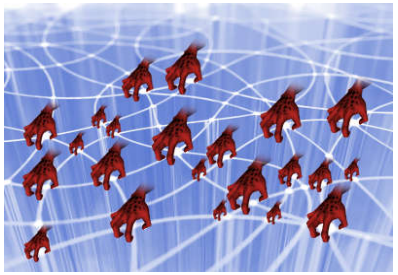
- **Die zu schützenden Werte steigen ständig und ändern sich mit der Zeit**
  - *Bits und Bytes repräsentieren:*
    - von Daten, Informationen, Wissen, ... zu **Intelligenzen (KI)**
    - Von überall zugreifbar (Mobile Geräte → Cloud Computing, …)

Notwendigkeit - Paradigmenwechsel
→ Änderungen der Rahmenbedingung (2/2)

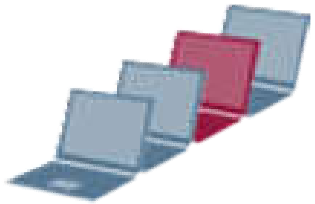
Ungleichgewicht bei Angreifern und Verteidigern im Internet

- **Hoch motivierte und sehr gut ausgebildete Angreifer**
- **Die Angriffsmodelle innovieren und Angreifer werden professioneller**

- **Angreifer arbeiten im Versteckten von überall in der Welt**



- **Nutzen sehr viele Computer (Malware, Botnetzte, …) mit unbegrenzter Leistung**



Inhalt

- Unser Problem
- Prinzipielle IT-Sicherheitsstrategien
- IT-Sicherheitsherausforderungen
- **Basis und angemessene IT-Sicherheit**
- Fazit und Ausblick

Basis u. angemessene IT-Sicherheit
→ Basis

- Sicherheit durch Einschränkung – Benutzerrechte
- Virenschutzprogramme / Anti-Malware Programme
- Personal Firewall
- Automatische Updates
- Regelmäßige Backups
- Passwortunterstützung
- …

- **Internet-Kompetenz**
  - Umgang mit Browser, E-Mail, …
  - Einschätzungen von Webseiten
  - Social Engineering
  - …

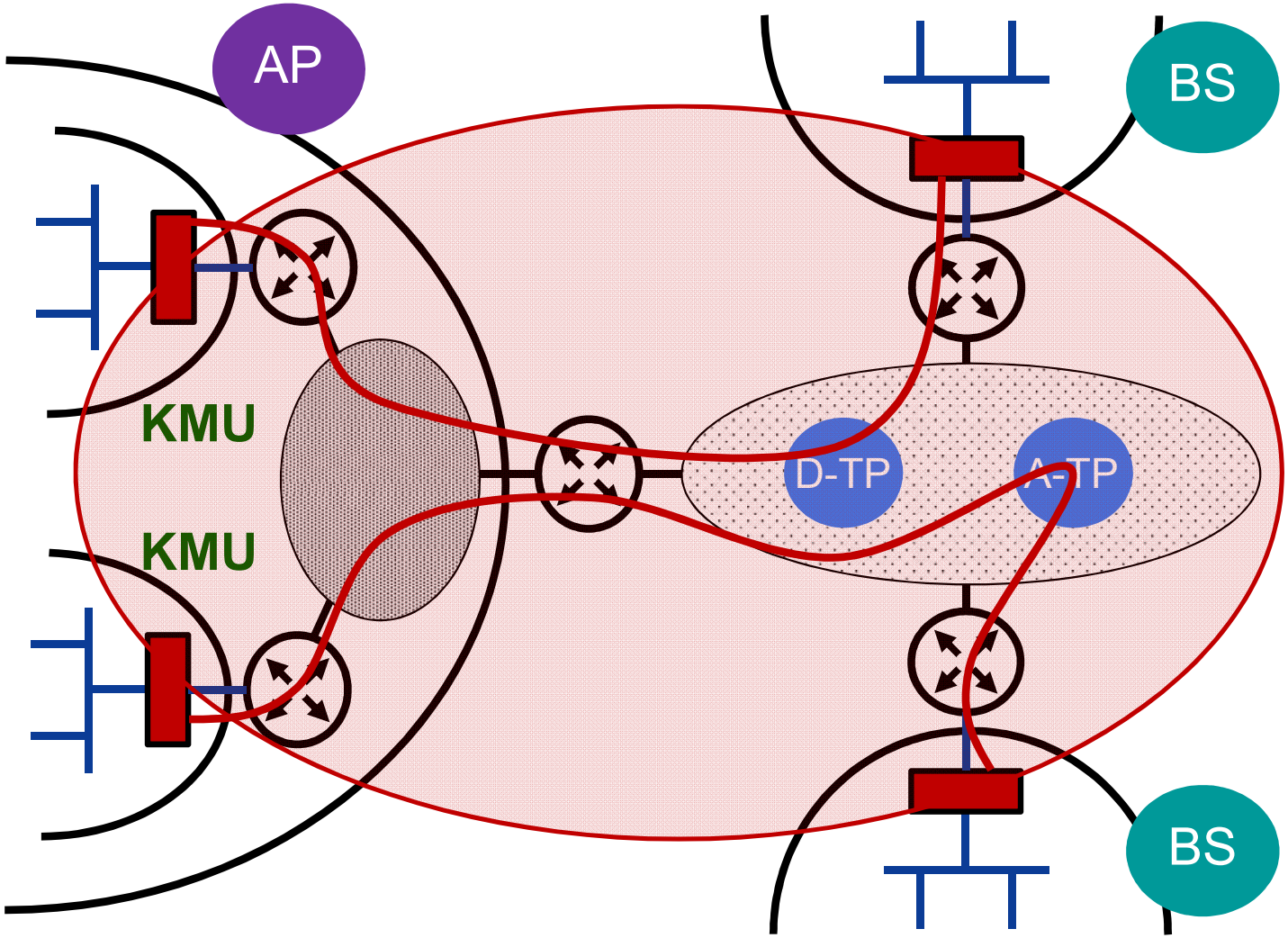
Siehe auch: www.sicher-im-internet.de

Aktive Verschlüsselung
→ Wichtige Aspekte

- Verschlüsselung für einen nachhaltigen Schutz der Daten (Kommunikation und Speicherung)
  - IPSec, SSL, …
  - E-Mail-Verschlüsselung, ...
  - Festplatten-, Datei-Verschlüsselung, …

- **Voraussetzungen:**
  - **Vertrauenswürdige Verschlüsselungstechnologie**
    (Keine Backdoors, starke Zufallszahlen, korrekte Implementierung, …)
    → *Sehr leistungsstarke IT-Sicherheitsindustrie in D*
    → *IT Security made in Germany*
  - **Vertrauenswürdige IT-Sicherheitsinfrastruktur**
    (PKI mit RA und CA; Root-Zertifikate, …)

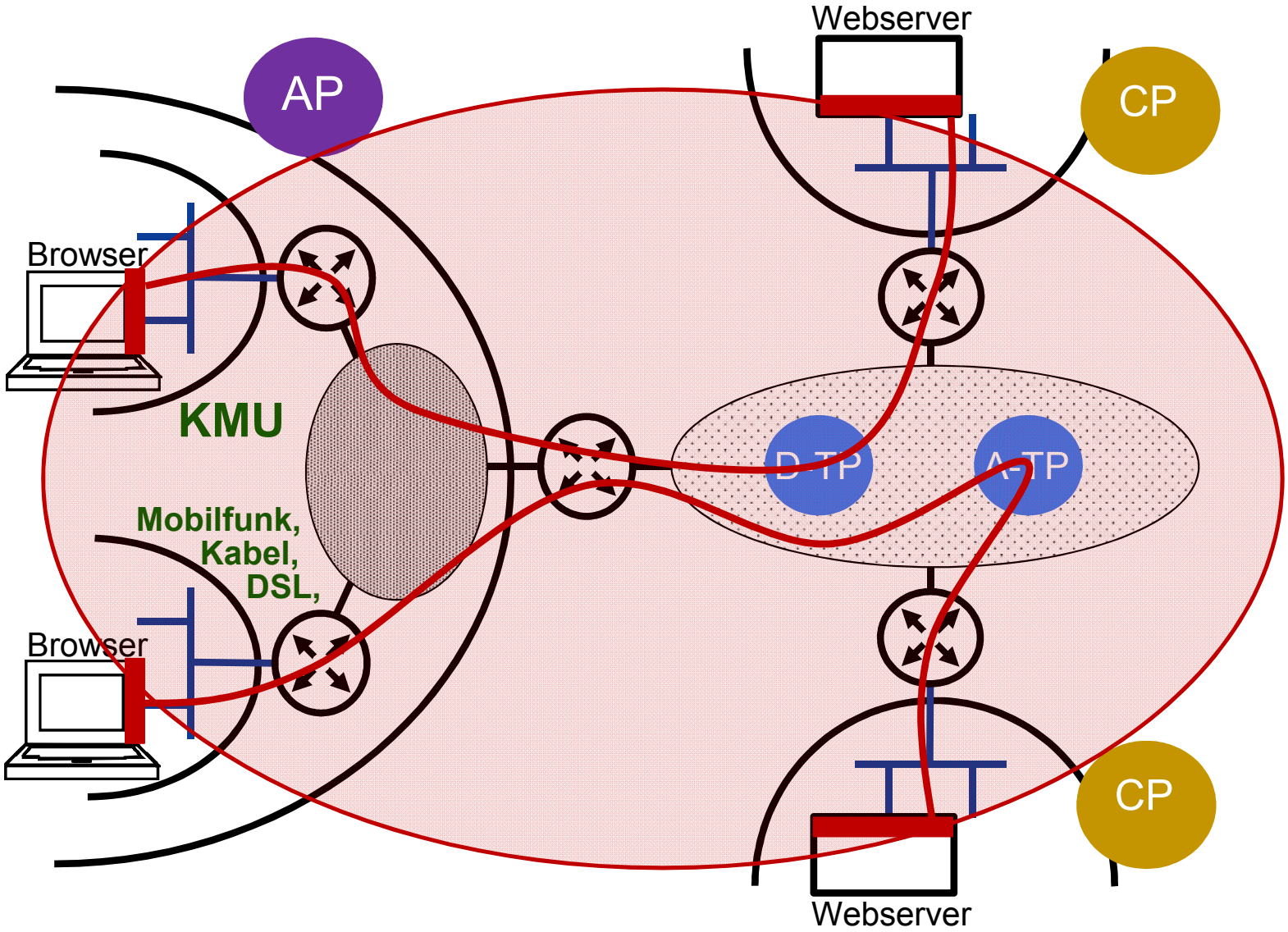
Verschlüsselung
→ IPSec



Jedes 125. Paket im Internet ist IPSec verschlüsselt

(Tendenz steigend)

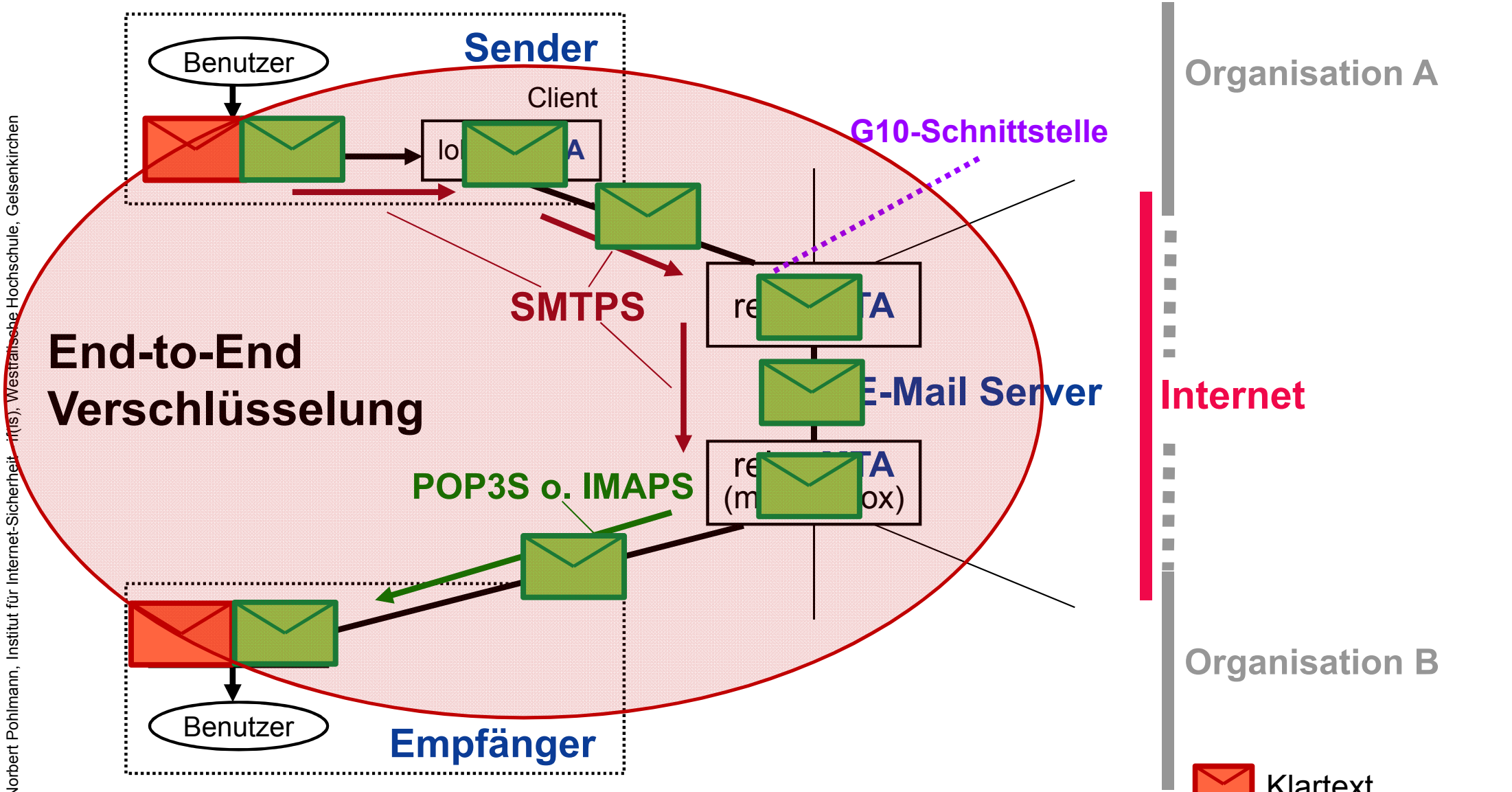
Verschlüsselung
→ SSL/TLS



Jedes 7. Paket im Internet ist SSL verschlüsselt

(SSL/TLS (Port 443) 23 % und HTTP (Port 80) 77 % - Tendenz steigend)

E-Mail-Verschlüsselung
→ PGP o. S/MIME



Vorteile: End-to-End-Verschlüsselung

Paradigmenwechsel

→ Mehr Vertrauenswürdigkeit statt Gleichgültigkeit

- **Produkthaftung**
  Software und Hardware arbeiten besser zusammen und Sicherheitsprobleme werden einfacher identifiziert und behoben.

- **Evaluierung / Zertifizierung**
  (BSI, ENISA, ISO 27001, eco, …)
  Unabhängige und qualifizierte Organisationen prüfen (verbessern) die Qualität und Vertrauenswürdigkeit von IT und IT Sicherheit in Produkten und Lösungen.

Paradigmenwechsel
→ Mehr proaktive statt reaktive IT-Sicherheit (1/2)

Reaktive IT-Sicherheitssysteme

- Bei reaktiven IT-Sicherheitssystemen rennen wir den **IT-Angriffen hinterher**!

- Das bedeutet, ***wenn*** wir einen **Angriff erkennen**, ***dann*** versuchen wir uns so schnell wie möglich zu **schützen**, um den Schaden zu reduzieren.

- **Beispiele für reaktive Sicherheitssysteme sind:**
  - *Firewall-Systeme*
  - *Intrusion Detection*
  - *Anti-Malwareprodukte*
  - *Anti-Spam /-Phishing, …*

„Airbag-Methode“
Wenn‘s passiert, soll es weniger „weh tun“

Paradigmenwechsel

→ Mehr proaktive statt reaktive IT-Sicherheit (2/2)

Proaktive Sicherheitssysteme

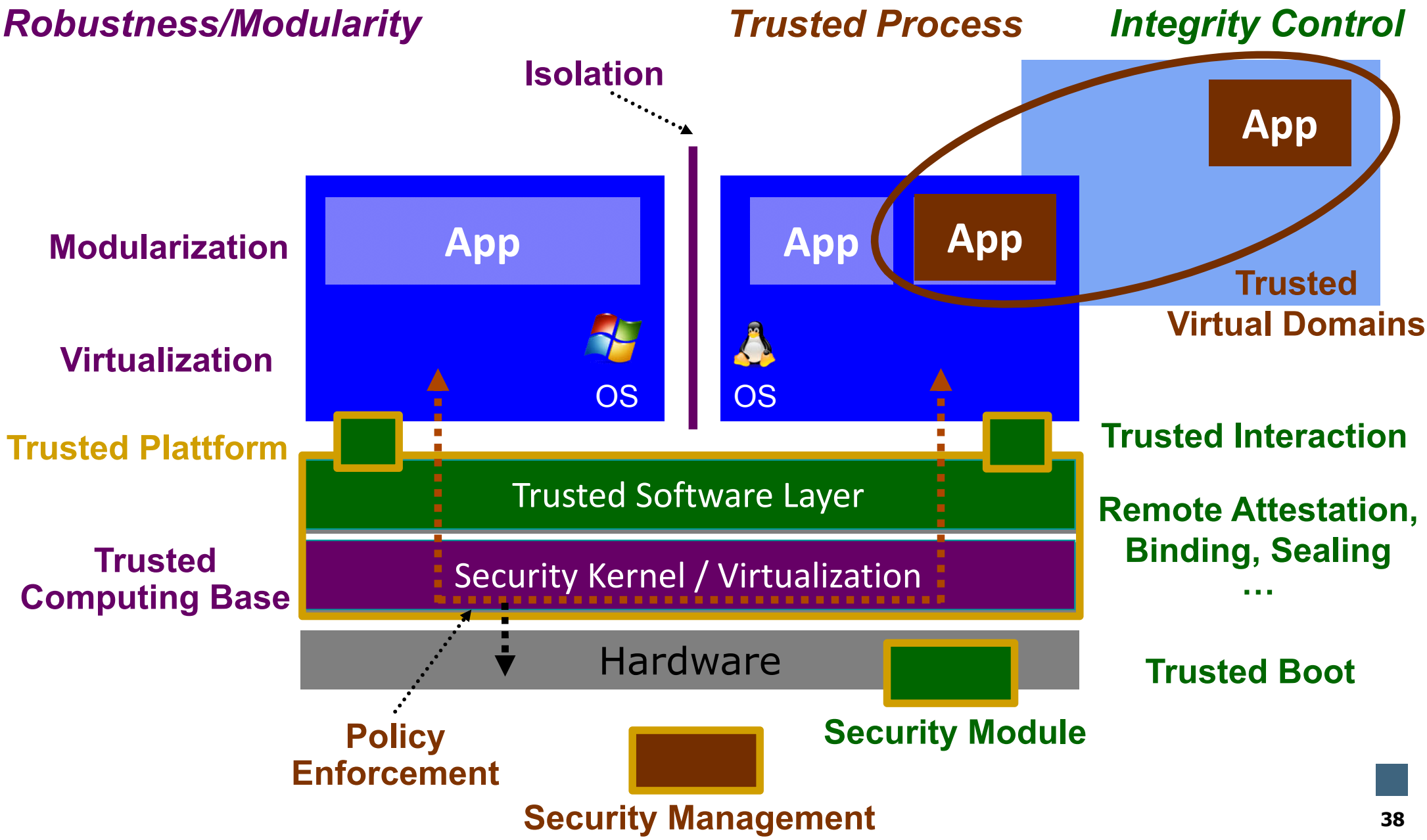
- Proaktive Sicherheitsmechanismen machen IT-Systeme robuster und vertrauenswürdiger.
- Hier spielen **Sicherheitsplattformen** auf der Basis von **intelligenten kryptographischen Verfahren** eine wichtige Rolle.

(Vertrauenswürdige Basis)

„ESP-Strategie“

Verhindern, dass man überhaupt ins Schleudern kommt

Paradigmenwechsel – (3)
→ Vertrauenswürdige Basis

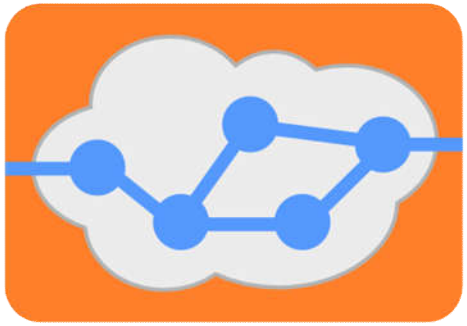


Paradigmenwechsel

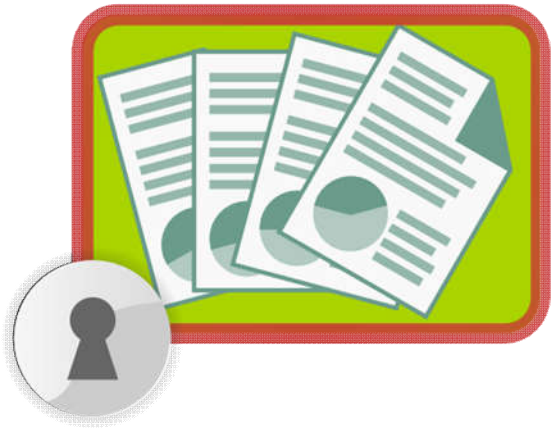
→ Vertrauenswürdige Basis (2/5)

Aufteilung in verschiedene virtuelle Maschinen (unterschiedliche Aufgaben und Sicherheitsbedarfe – 1)

Internet

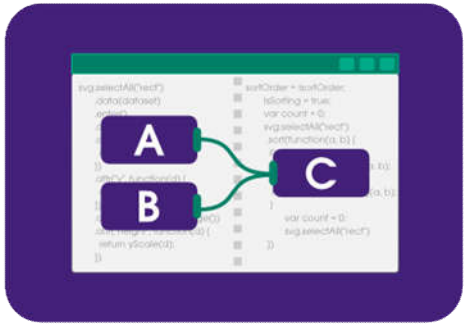


Office



Browser
E-Mail

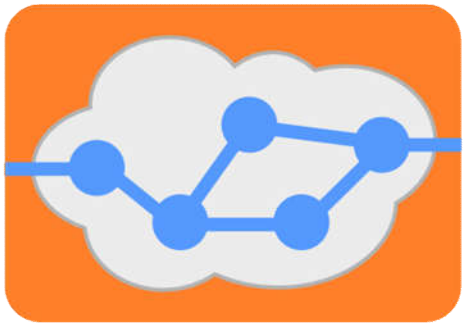
Development



Paradigmenwechsel
→ Vertrauenswürdige Basis (3/5)

Aufteilung in verschiedene virtuelle Maschinen
(unterschiedliche Aufgaben und Sicherheitsbedarfe – 2)

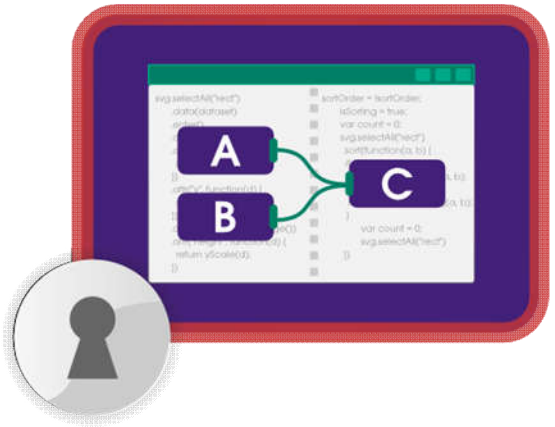
Internet



Office

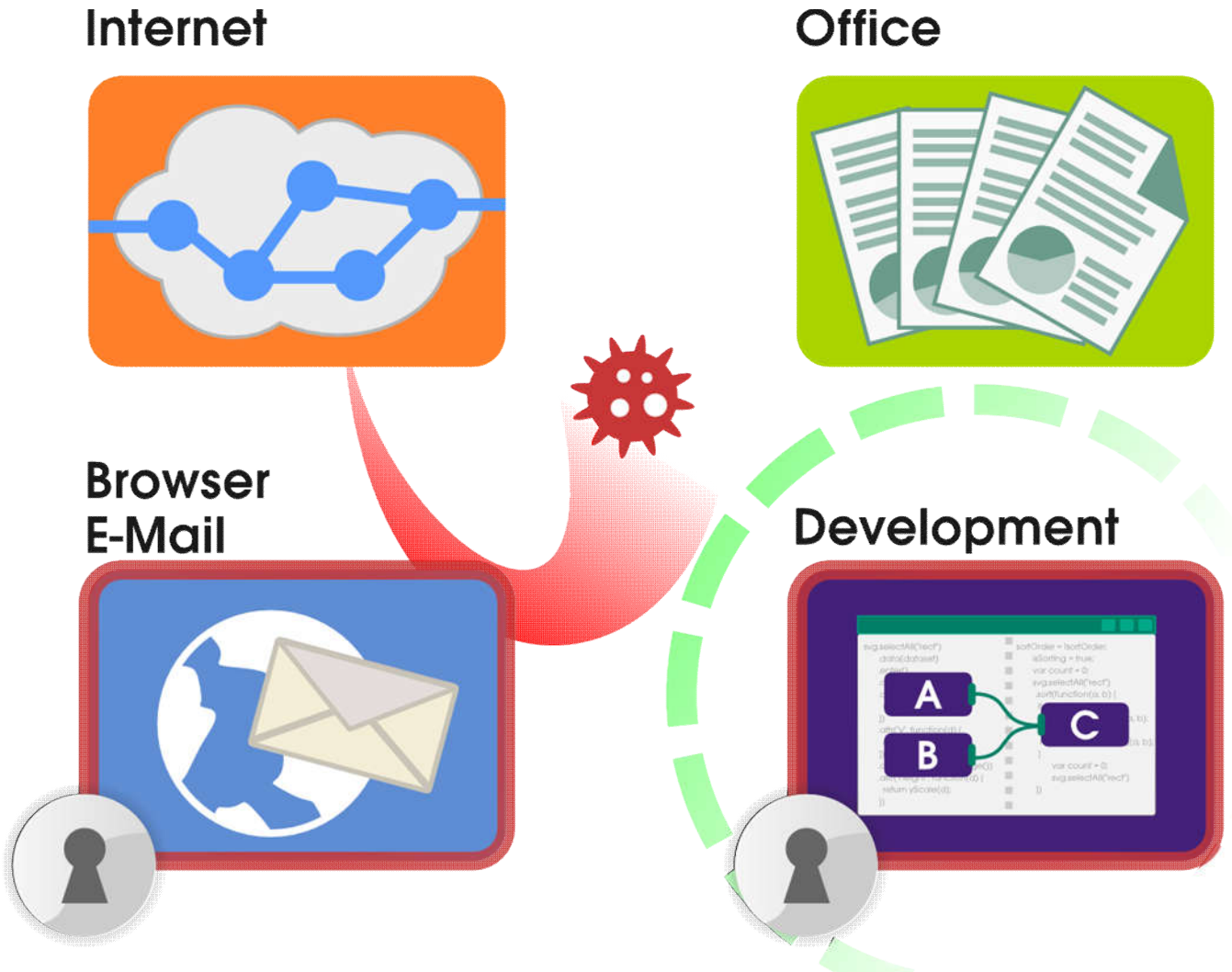
Browser
E-Mail

Development



Paradigmenwechsel
→ Vertrauenswürdige Basis (4/5)

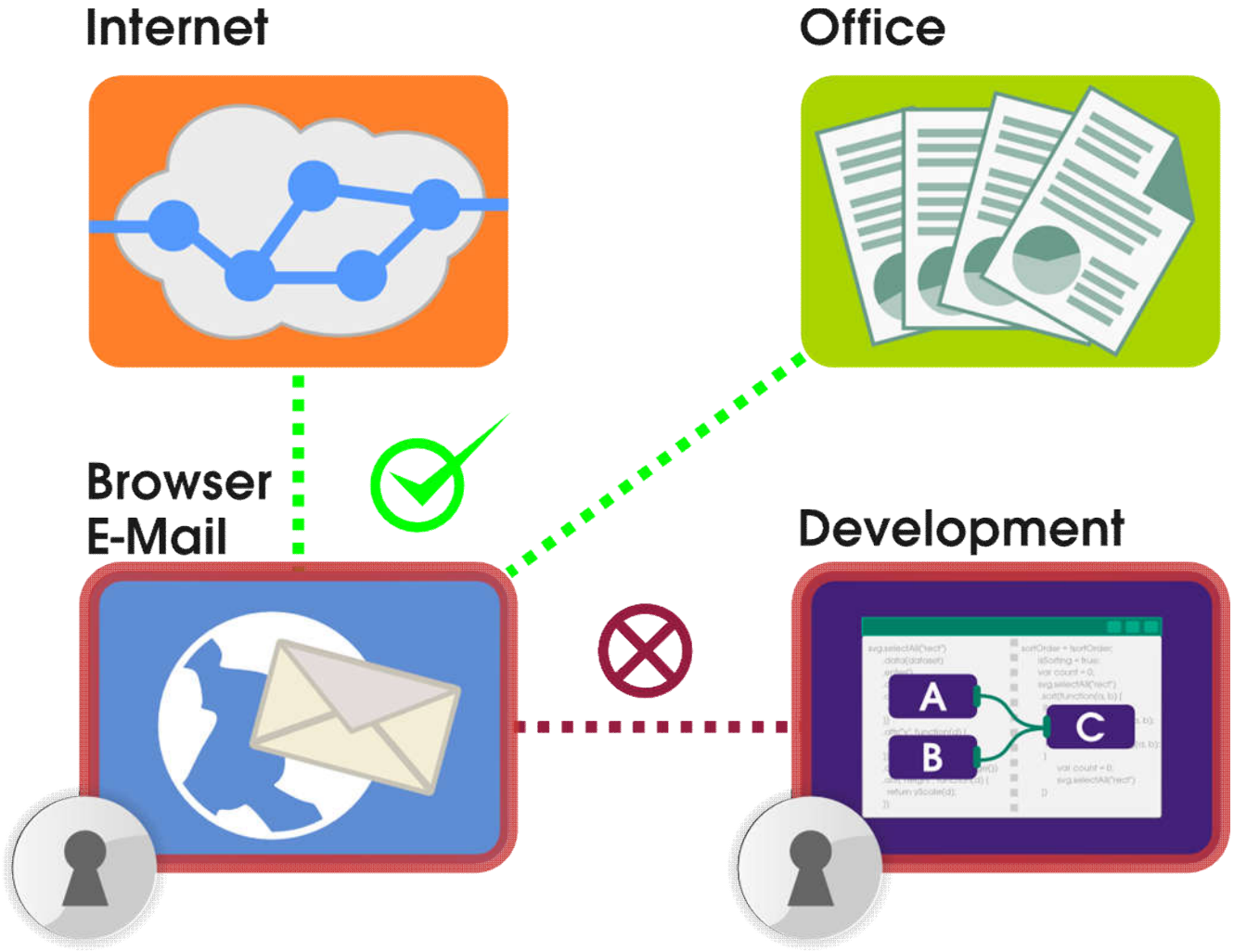
Wichtige Daten werden besonders in separaten, isolierten virtuellen Maschinen geschützt



Paradigmenwechsel

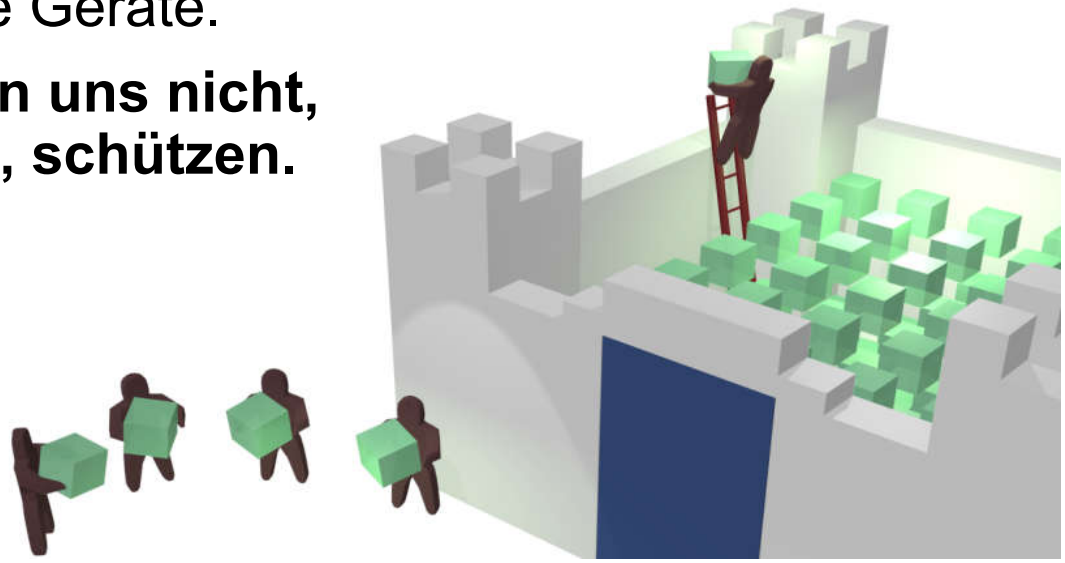
→ Vertrauenswürdige Basis (5/5)

Security Policies und ein Enforcement System sorgt für mehr Sicherheit und Vertrauenswürdigkeit



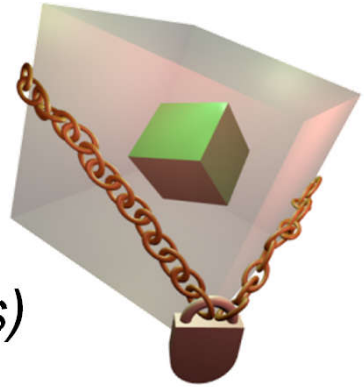
Paradigmenwechsel
→ Mehr Objekt- statt Perimeter-Sicherheit (1/2)

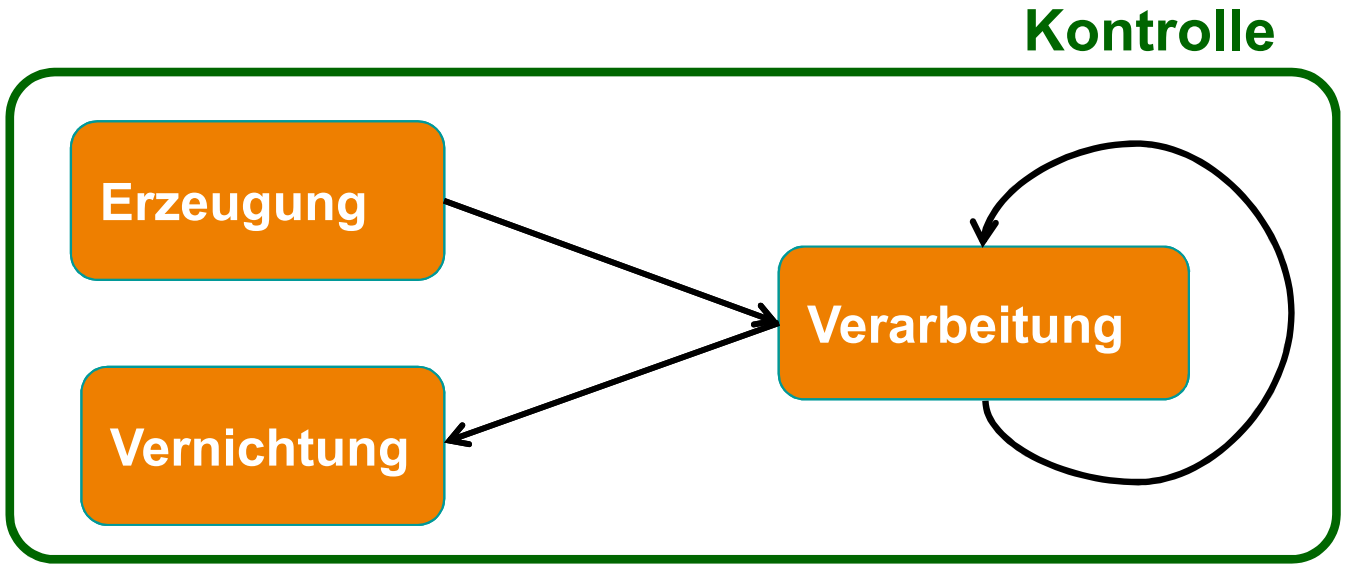
- **Perimeter-Sicherheit (Abschottung „Netz“)**
  - **Abwehrmodell:**
    - Schützt eine Anzahl von Computern und Netzwerken mit der Hilfe von Firewall-Systemen, VPNs, Intrusion Detection, usw.
    - Annahme: Die Computer und das Netz sind fest installiert.
  - **Bewertung:**
    - Die moderne Geschäftswelt nutzt flexible und verteilte mobile Geräte.
    - **Perimeter-Sicherheit kann uns nicht, wie in der Vergangenheit, schützen.**



Paradigmenwechsel
→ Mehr Objekt- statt Perimeter-Sicherheit (2/2)

- **Objekt-Sicherheit (Informationsflusskontrolle)**
  - **Idee:** Domänenorientierte Objektsicherheit, bei der die Objekte mit Rechten versehen werden, die definieren, wer sie in welcher IT-Umgebung wie nutzen darf.
    - *Object Lifecycle Protection*
    - *Distributed Policy Enforcement (even on foreigen systems)*





Paradigmenwechsel
→ Mehr Zusammenarbeit statt Separation

Ungleichgewicht bei Angreifern und Verteidigern im Internet

Kooperation hilft das Ungleichgewicht zu überwinden.

Inhalt

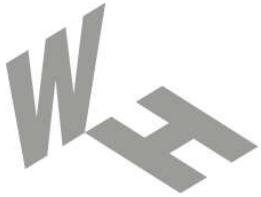
- Unser Problem
- Prinzipielle IT-Sicherheitsstrategien
- IT-Sicherheitsherausforderungen
- Basis und angemessene IT-Sicherheit
- **Fazit und Ausblick**

IT-Sicherheitsherausforderungen
→ Fazit und Ausblick

- **Grundlegende Rahmenbedingungen haben sich geändert!**
  - ***Radikale Veränderung in der IT*** (Mobile Geräte, Cloud, Soziale Netze, ...)
  - Die zu schützenden ***Werte steigen ständig*** und ändern sich mit der Zeit
    Die ***Angriffsmodelle innovieren*** und ***Angreifer werden professioneller***.

- **Mit der Zeit werden die IT-Sicherheits- und Datenschutzprobleme immer größer!**

- **Wir brauchen Paradigmenwechsel in der IT-Sicherheit, um in der Zukunft das Internet vertrauenswürdig nutzen zu können!**
  - **Mehr Vertrauenswürdigkeit statt Gleichgültigkeit**
  - **Mehr proaktive statt aktive IT-Sicherheit**
  - **Mehr Objekt- statt Perimeter-Sicherheit**
  - **Mehr Zusammenarbeit statt Separation**
  - **...**



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Internet Sicherheit B
→ Einführung

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.