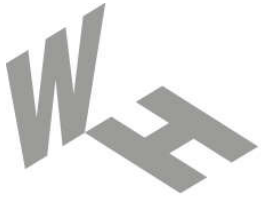


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

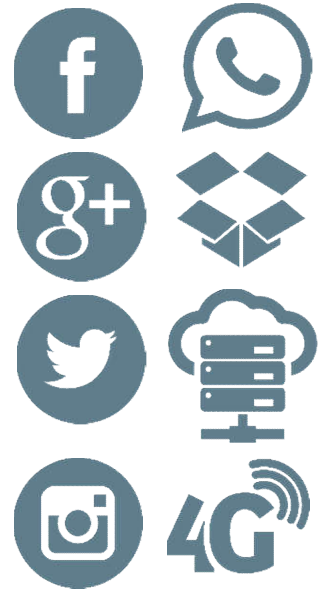
Die Lage der IT-Sicherheit

Prof. Dr. (TU NN)
Norbert Pohlmann

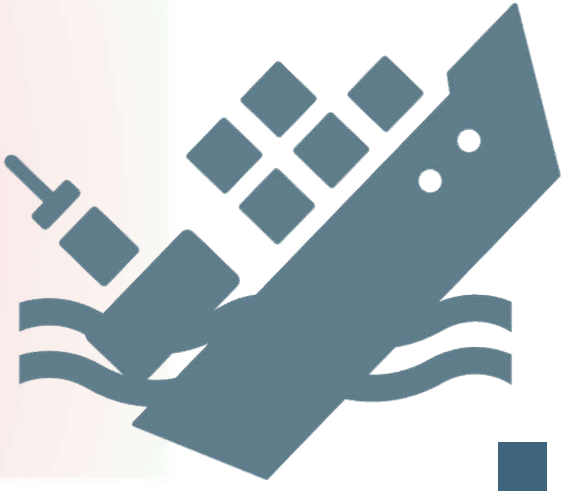
Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

IT und IT-Sicherheit
→ Situation

- IT ist **„der Motor“** und **die Basis** für das **Wohlergehen** unserer modernen und globalen **Gesellschaft.**
- Der **Digitalisierungsprozess** wird **immer schneller** und damit auch die **Veränderungen** in unseren **Lebensräumen.**
- Unsere Arbeit, unsere Firmen, unsere Hochschulen, unsere Freizeit, unser ganzes **Leben wird sich wandeln**.



- Die IT und IT-Sicherheitstechnologien sind nicht sicher und vertrauenswürdig genug *(**Widerstandsfähigkeit**)*!
- Professionelle **Hacker greifen** alles **erfolgreich an!**
- Das **Risiko wird immer größer**, die Schäden auch!



Was sind die Problemfelder?
→ 1. Privatheit und Autonomie

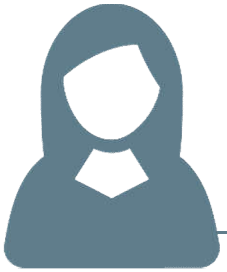
Verschiedenen Sichtweisen

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

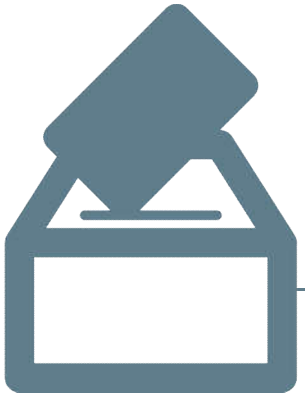
Was sind die Problemfelder?
→ 2. Wirtschaftsspionage

ca. 51 Milliarden € Schaden pro Jahr

Wirtschaftsspionage

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

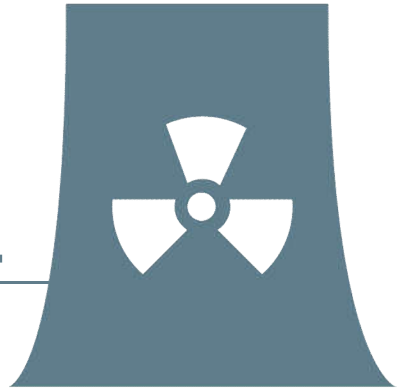
Was sind die Problemfelder?
→ 3. Cyberwar



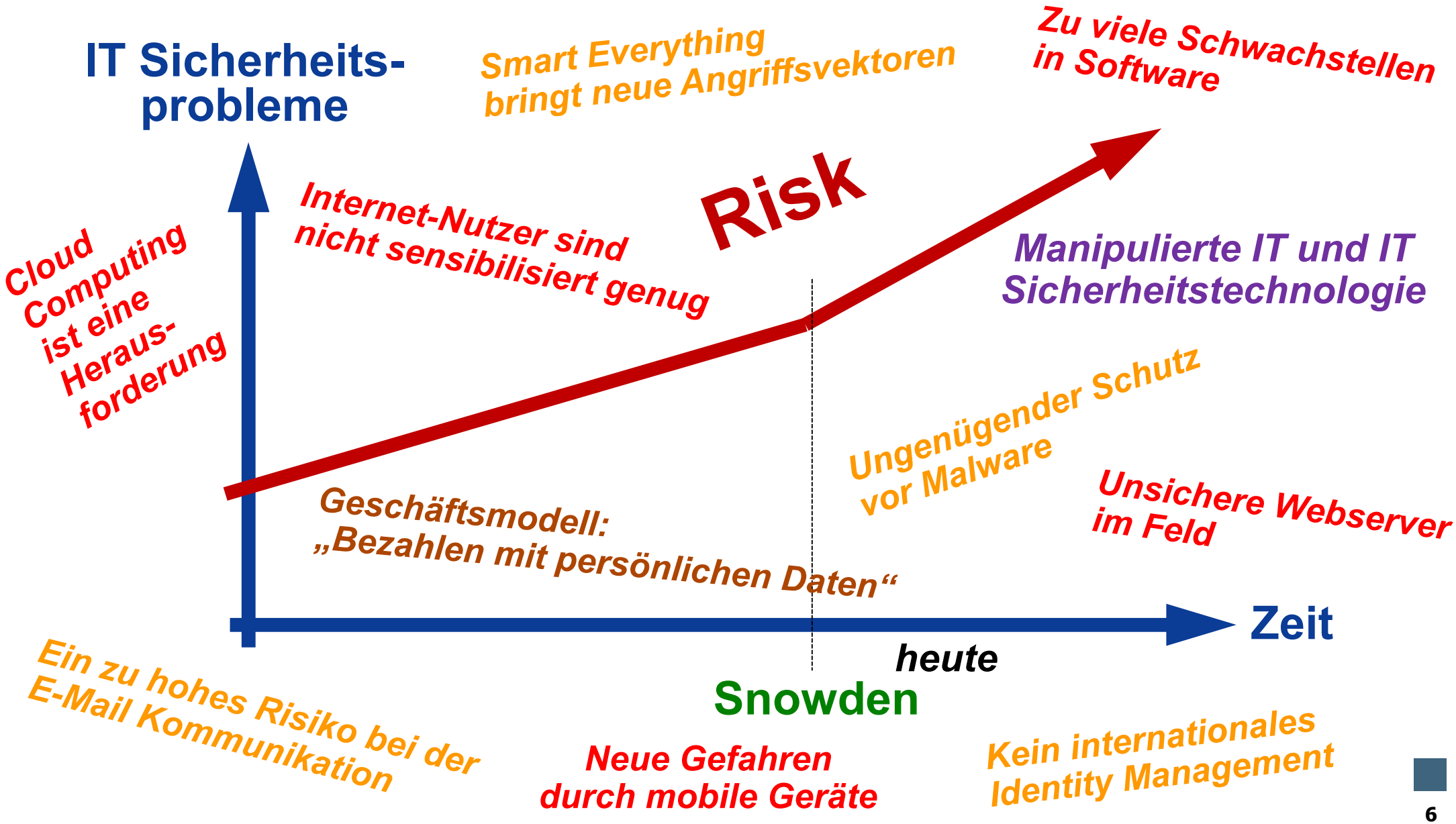
Umsetzung von politischen Zielen
→ „einfach“ und „preiswert“

Cyberwar

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



Internet-Sicherheit
→ Die größten Herausforderungen

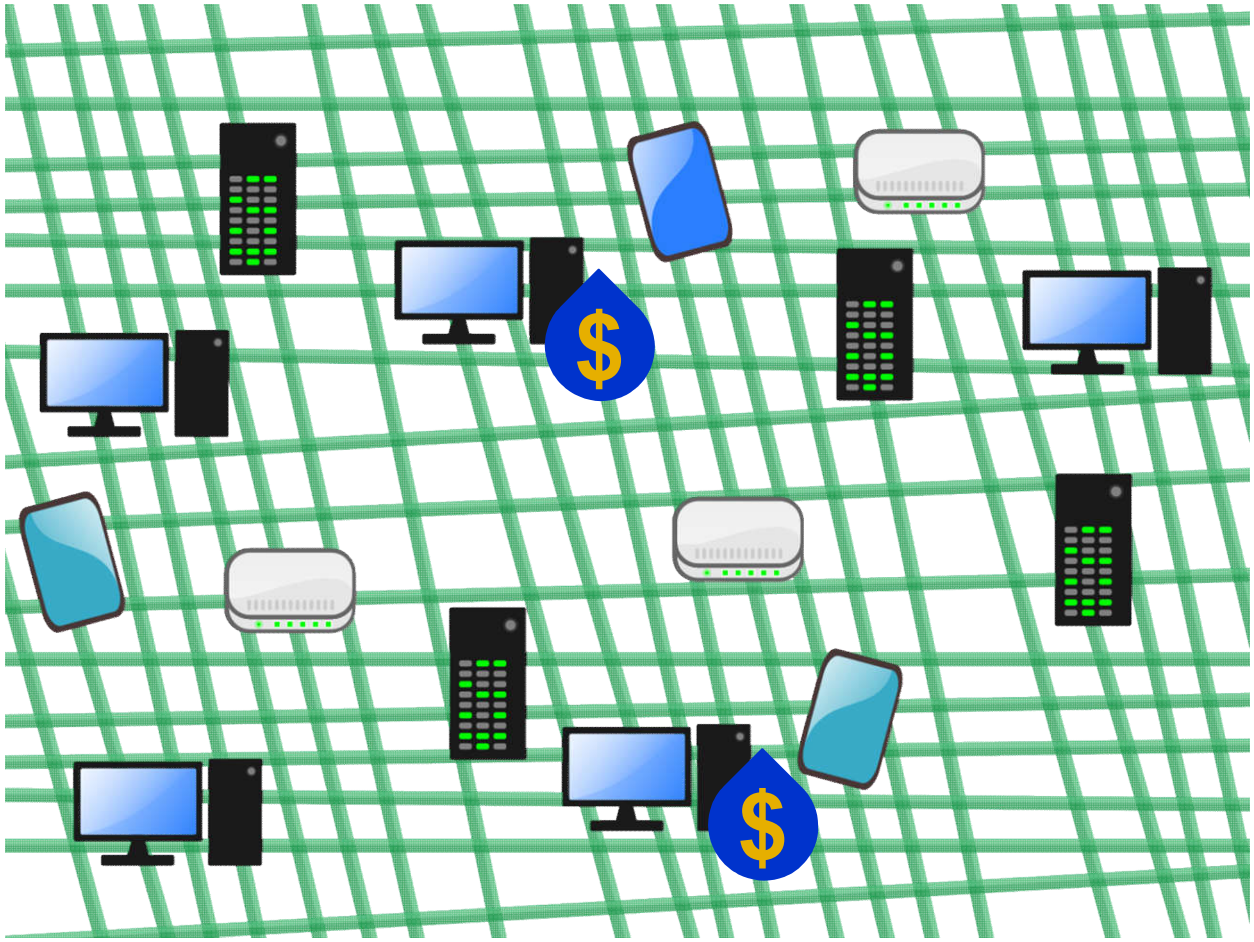


IT-Sicherheit
→ Evaluierung der Situation

- **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

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?

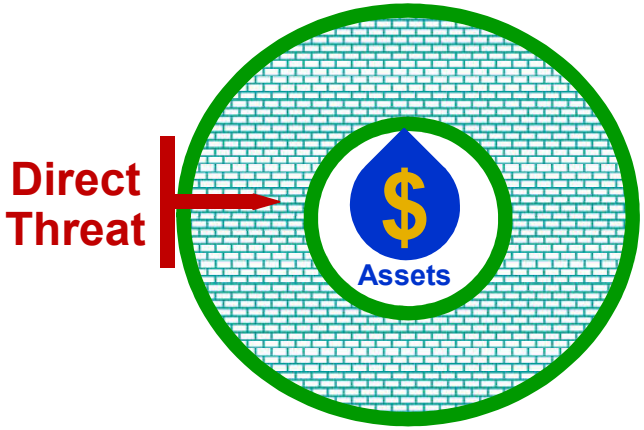
Prinzipielle IT Sicherheitsstrategien
→ Vermeiden von Angriffen – (1)

- **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)

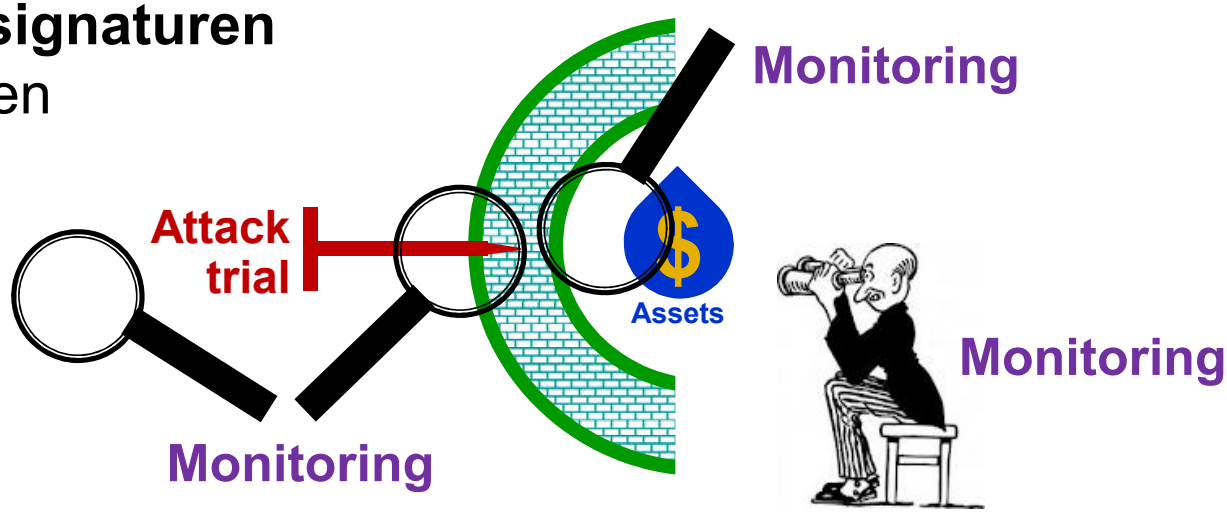
- Meist verwendete IT-Sicherheitsstrategie
- Beispiele, bei denen ein hoher Nachholbedarf besteht:
  - **Verschlüsselungssicherheitssysteme**
    (Datei-, Festplatten-, E-Mail-Verschlüsselung, VPN-Systeme, SSL, ...)
  - **Authentikationsverfahren**
    (Challenge-Response, globale Identität, Föderation,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

Neue Strategien und Lösungen

→ 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, CC, …)
  Unabhängige und qualifizierte Organisationen prüfen (verbessern) die Qualität und Vertrauenswürdigkeit von IT und IT Sicherheit in Produkten und Lösungen.

- **IT-Security Made in Germany**
  Qualitätssiegel für vertrauenswürdige IT-Sicherheitslösungen (Unternehmenshauptsitz in Deutschland, keine Backdoors, Datenschutz, …)

Neue Strategien und Lösungen
→ 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“

Neue Strategien und Lösungen

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

Proaktive Sicherheitssysteme

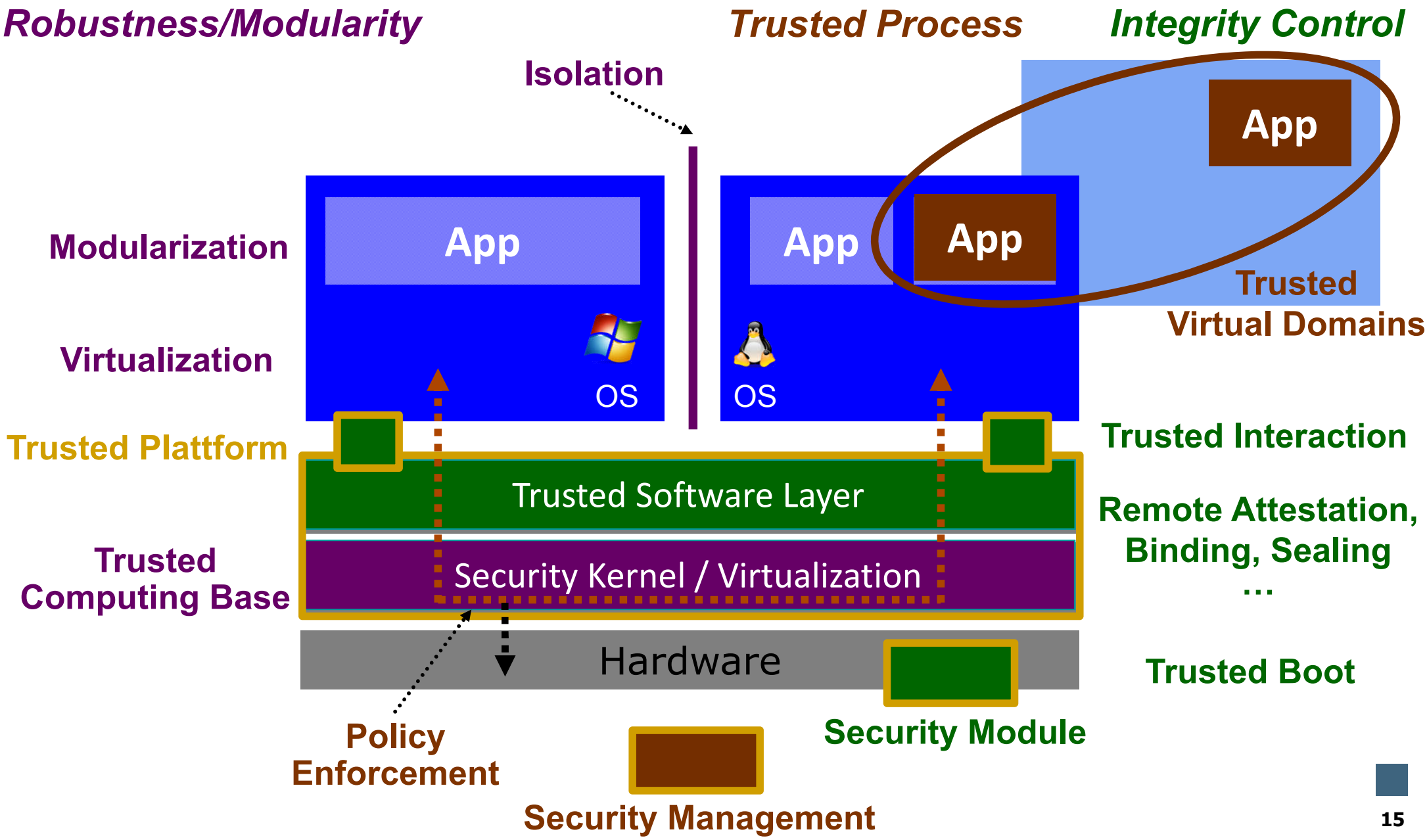
- Proaktive Sicherheitsmechanismen machen IT-Systeme robuster und vertrauenswürdiger.
- Hier spielen **Sicherheitsplattformen** auf der Basis von **intelligenten kryptographischen Verfahren** eine wichtige Rolle.

(Vertrauenswürdige Basis)

„ESP-Strategie“

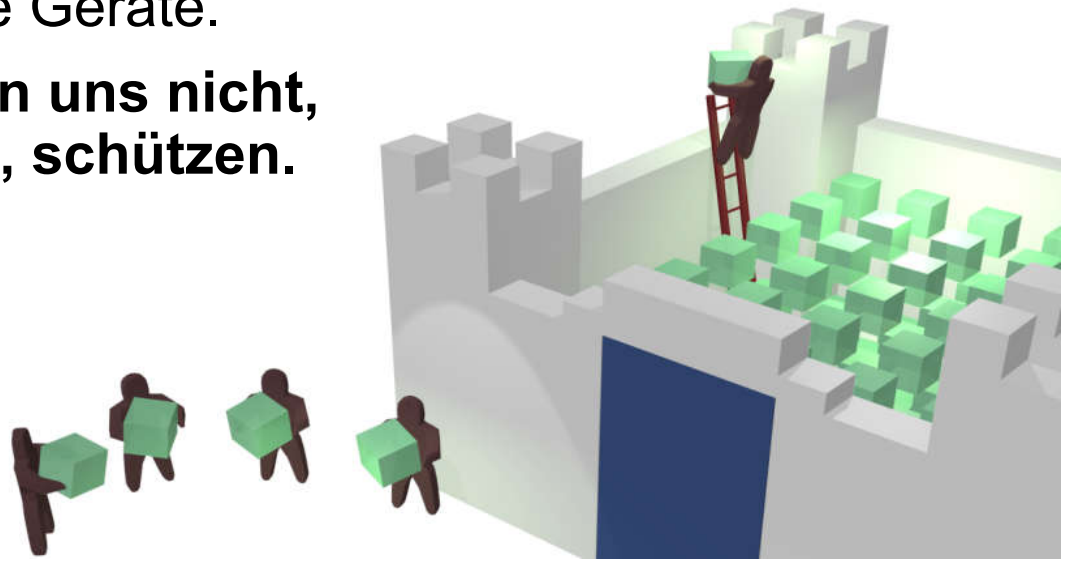
Verhindern, dass man überhaupt ins Schleudern kommt

Neue Strategien und Lösungen
→ Vertrauenswürdige Basis



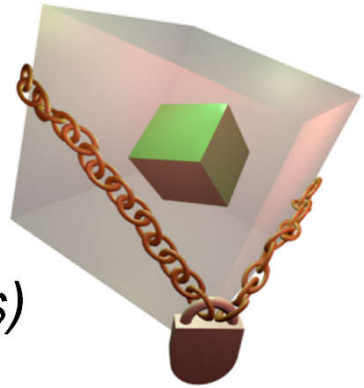
Neue Strategien und Lösungen
→ Mehr Objekt- statt Perimeter-Sicherheit (1/2)

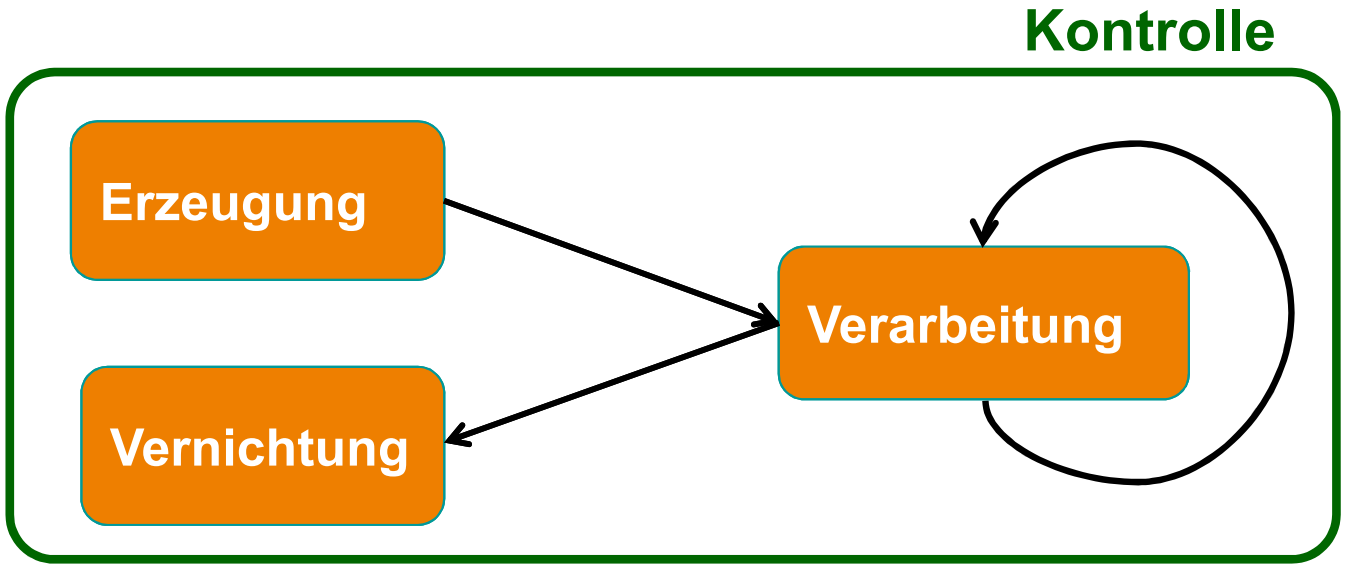
- **Perimeter-Sicherheit (Abschottung „Netz“)**
  - **Abwehrmodell:**
    - Schützt eine Anzahl von Computern und Netzwerken mit der Hilfe von Firewall-Systemen, VPNs, Intrusion Detection, usw.
    - Annahme: Die Computer und das Netz sind fest installiert.
  - **Bewertung:**
    - Die moderne Geschäftswelt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



Neue Strategien und Lösungen
→ 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)*





Neue Strategien und Lösungen
→ Mehr Zusammenarbeit statt Separation

Ungleichgewicht bei Angreifern und Verteidigern im Internet

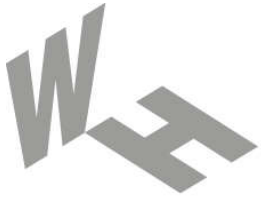
Zusammenarbeit hilft das Ungleichgewicht zu überwinden.

- Gemeinsame Kompetenzzentren
- Austausch von Lagebildern
- Gemeinsame Reaktionen auf Angriffe und Bedrohungen
- Definition von notwendigen IT-Sicherheitsmechanismen
- …

Die Lage der IT-Sicherheit
→ Fazit und Ausblick

- **Situation?**
  - Die **Angriffsmodelle innovieren** und **Angreifer** werden **professioneller**.
  - Wir kennen die IT-Sicherheitsprobleme, aber **heutige IT-Sicherheitsmaßnahmen** reduzieren das IT-Sicherheitsrisiko **nicht ausreichend!**

- Wir brauchen **neue Strategien und Lösungen** in der IT-Sicherheit, um in der Zukunft das Internet sicherer und vertrauenswürdiger nutzen zu können!
  - Mehr **Vertrauenswürdigkeit** *(statt Gleichgültigkeit)*
  - Mehr **proaktive IT-Sicherheit** *(statt aktive IT-Sicherheit)*
  - Mehr **Objekt-Sicherheit** *(statt Perimeter-Sicherheit)*
  - Mehr **Zusammenarbeit** *(statt Separation)*
  - **...**



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Die Lage der IT-Sicherheit

Mit Sicherheit in die Zukunft!

Prof. Dr. (TU NN)
Norbert Pohlmann

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