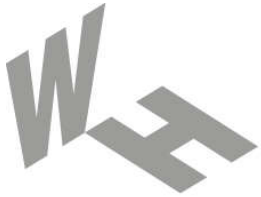


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Houston, we have a Problem!

→ Paradigmenwechsel in der IT-Sicherheit

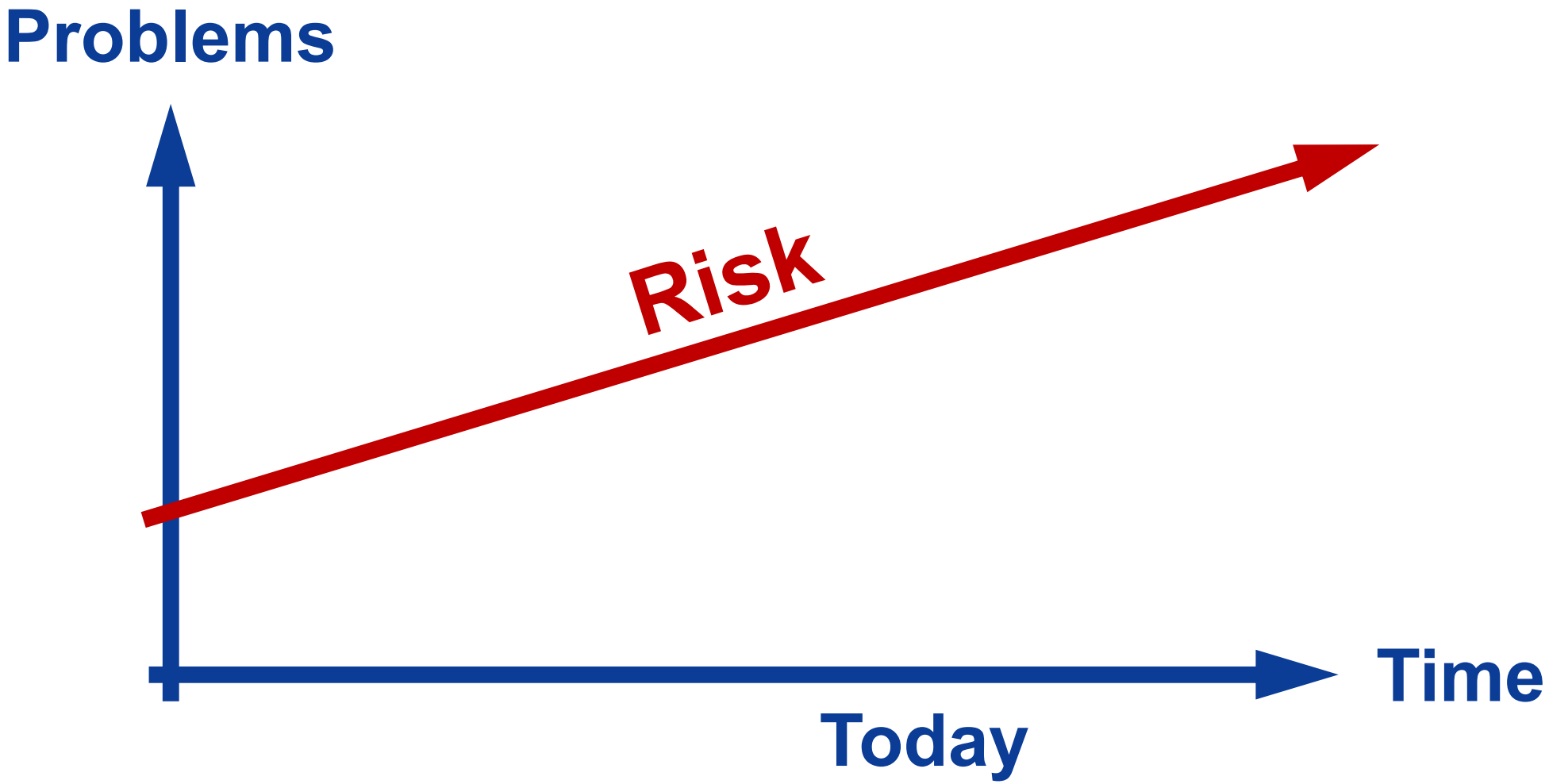
Prof. Dr. (TU NN)
Norbert Pohlmann

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

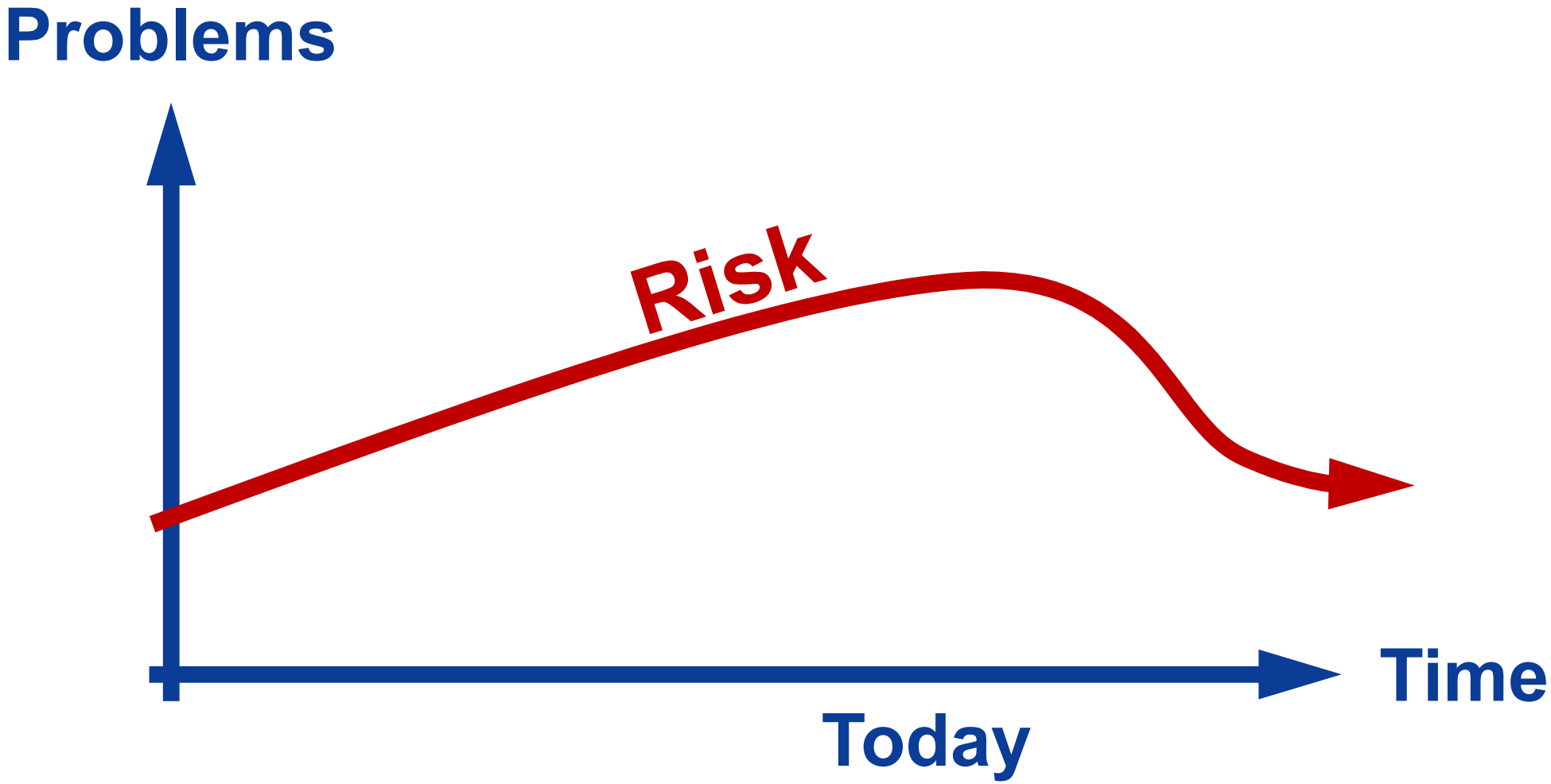
Inhalt

- **IT-Sicherheit im Laufe der Zeit**
- **We have a Problem!**
  → IT-Sicherheitsherausforderungen
- **Veränderungen der Rahmenbedingungen**
- **Paradigmenwechsel in der IT-Sicherheit**
- **Fazit und Ausblick**

IT-Sicherheit im Laufe der Zeit
→ Unser Problem



IT-Sicherheit im Laufe der Zeit
→ Unsere Herausforderung



IT-Sicherheit im Laufe der Zeit
→ 1985 - 1995: Kommunikationssicherheit

- **IT-Trend:**
  - Mit dem PC kam eine Individualisierung und Dezentralisierung der IT.
  - Der Wunsch, diese dezentralen IT-Systeme über Leitungen oder Daten-Netze, wie X.25-Netz zu verbinden.

- **IT-Sicherheitstrend:**
  - Mit ***Leitungsverschlüsselung*** (Modem, 2 MBit/s, …) und ***X.25-Verschlüsselungsgeräten*** die neuen Sicherheitsprobleme lösen.

- **Unsere Einstellung:**
  - Wir müssen uns beeilen, sonst sind alle IT-Sicherheitsprobleme gelöst.

IT-Sicherheit im Laufe der Zeit
→ 1995 - 2005: Perimeter Sicherheit

- **IT-Trend:**
  - Unternehmen haben sich ans Internet angeschlossen, um am **E-Mail-** und **Web-System** teilhaben zu können.
  - Zusätzlich wurden Niederlassungen über das Verbundnetz **Internet** einfach angebunden.

- **IT-Sicherheitstrend: „*Perimeter Sicherheit*“**
  - Abwehrmodell: Firewall- und VPN-Systeme
  - Digitale Signatur, E-Mail-Sicherheit, PKI

- **Unsere Einstellung:**
  - Wir haben die IT-Sicherheitsprobleme im Griff!

IT-Sicherheit im Laufe der Zeit
→ 2005 - 2012: Malware/Software-Updates

- **IT-Trend:**
  - Immer mehr PCs, Notebooks, Smartphones zunehmend über GSM, UMTS, LTE, Hotspots, … (**gehen an der zentralen Firewall vorbei**) ins Internet
  - Die Anzahl der Schwachstellen durch **Softwarefehler** wird immer größer (die Marktführer im SW-Bereich erkennen, dass es einen SW-Entwicklungsprozess gibt :-))

- **IT-Sicherheitstrend:**
  - **Verteilte Softwareangriffe** mit Hilfe von Malware
  - Anti-Malware, Software-Upgrades und Personal Firewalls
  - ***Generierung der Sicherheitslage***

- **Unsere Einstellung:**
  - Die IT-Sicherheitsprobleme wachsen uns über den Kopf!

We have a Problem!
→ IT-Sicherheitsherausforderungen (1/9)

- **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

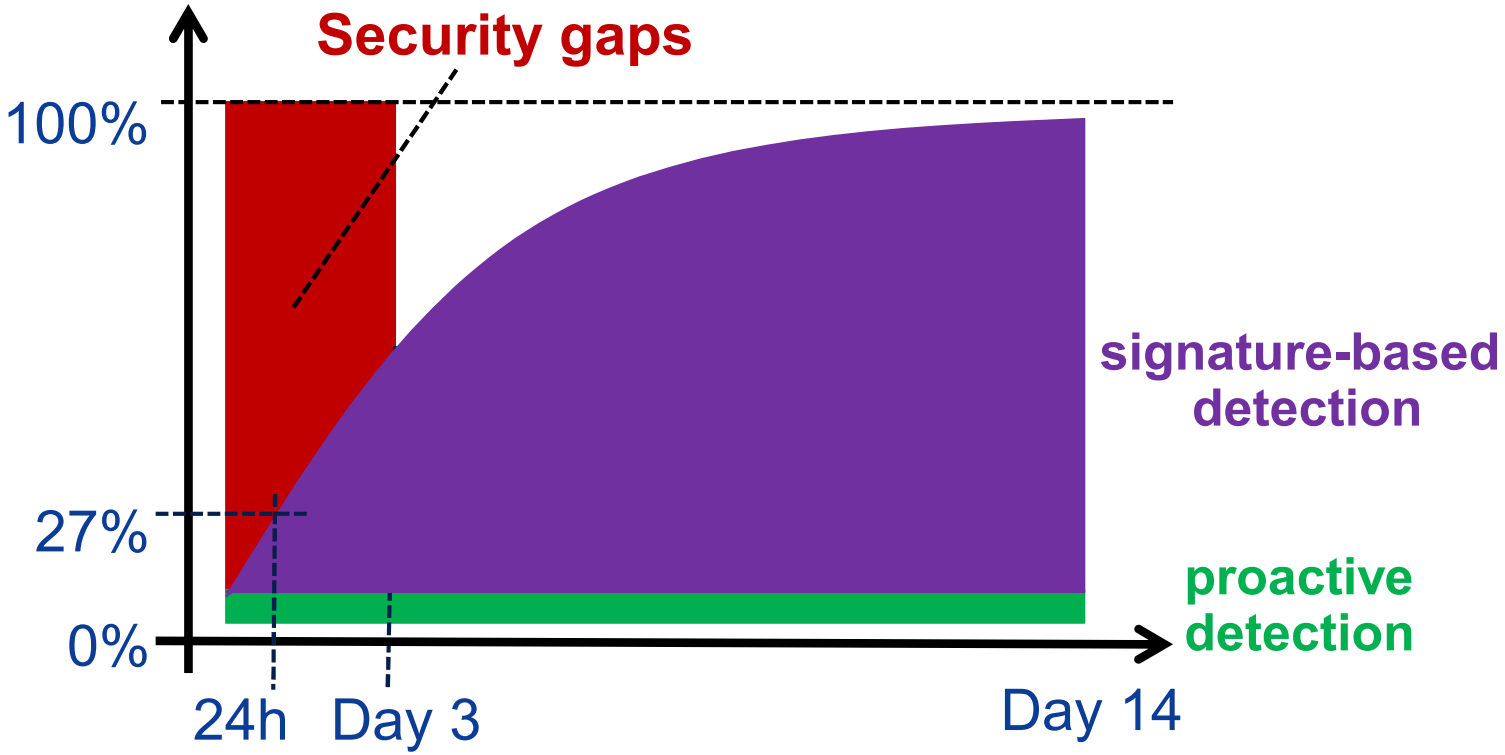
Betriebssysteme haben mehr als 10 Mio. LoC

→ mehr als 3.000 Fehler
(Fehlerdichte 0,3)

→ und damit zu viele Schwachstellen

We have a Problem!
→ IT-Sicherheitsherausforderungen (2/9)

- **Ungenügender Schutz vor Malware (1/2)**
  - **Schwache Erkennungsrate** bei Anti-Malware Produkten
    → nur 75 bis 95%!
  - ***Bei direkten Angriffen weniger als 27%***



We have a Problem!
→ IT-Sicherheitsherausforderungen (3/9)

- **Ungenügender Schutz vor Malware (2/2)**
  - **Jeder 25. 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

We have a Problem!
→ IT-Sicherheitsherausforderungen (4/9)

- **Identity Management (2013)**
  - Passworte, **Passworte**, ***Passworte***, …
    sind das Mittel im Internet!
  - **Identifikationsbereiche liegen im Unternehmens- und Kundenumfeld, nicht international!**
  - Föderationen sind noch nicht verbreitet genug!

Identitätsdiebstähle

Phishing Angriffe

Dienste-Übernahmen

…

We have a Problem!
→ IT-Sicherheitsherausforderungen (5/9)

- **Webserver Sicherheit**
  - Schlechte Sicherheit auf den Webservern / Webseiten
  - **Heute wird Malware hauptsächlich über Webseiten verteilt**
    (ca. 2.5 % Malware auf den deutschen gemessen Webseiten)

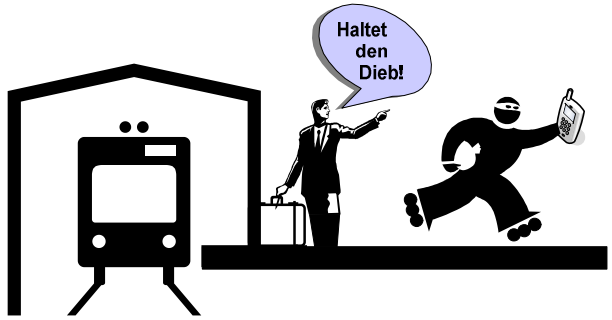
- **Gründe für unsichere Webseiten**
  - Viele Webseiten sind nicht sicher implementiert!
  - Patches werden nicht oder sehr spät eingespielt,
  - Firmen geben **kein Geld für IT-Sicherheit** aus!
  - **Verantwortliche kennen das Problem nicht!**

© http://moneytipcentral.com/

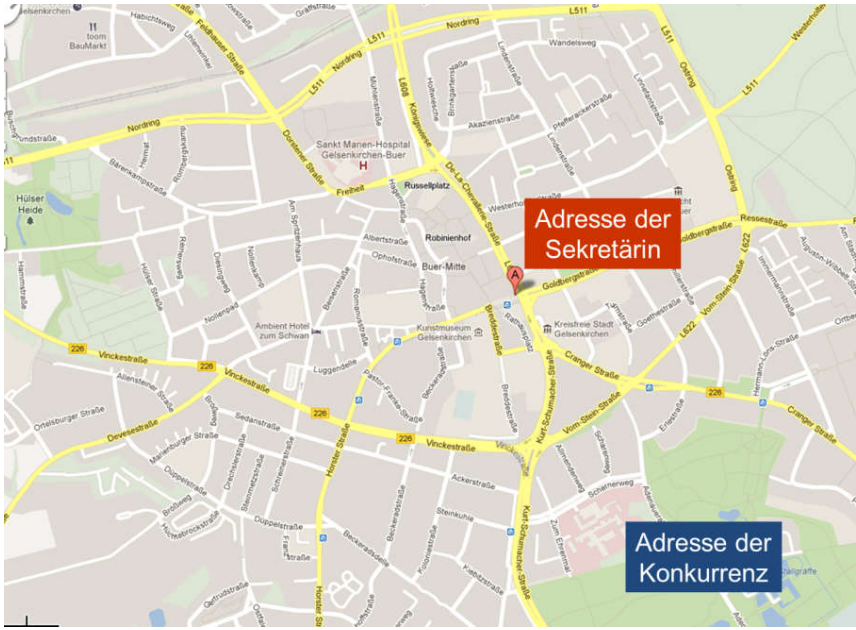
We have a Problem!
→ IT-Sicherheitsherausforderungen (6/9)

- **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**

We have a Problem!
→ IT-Sicherheitsherausforderungen (7/9)

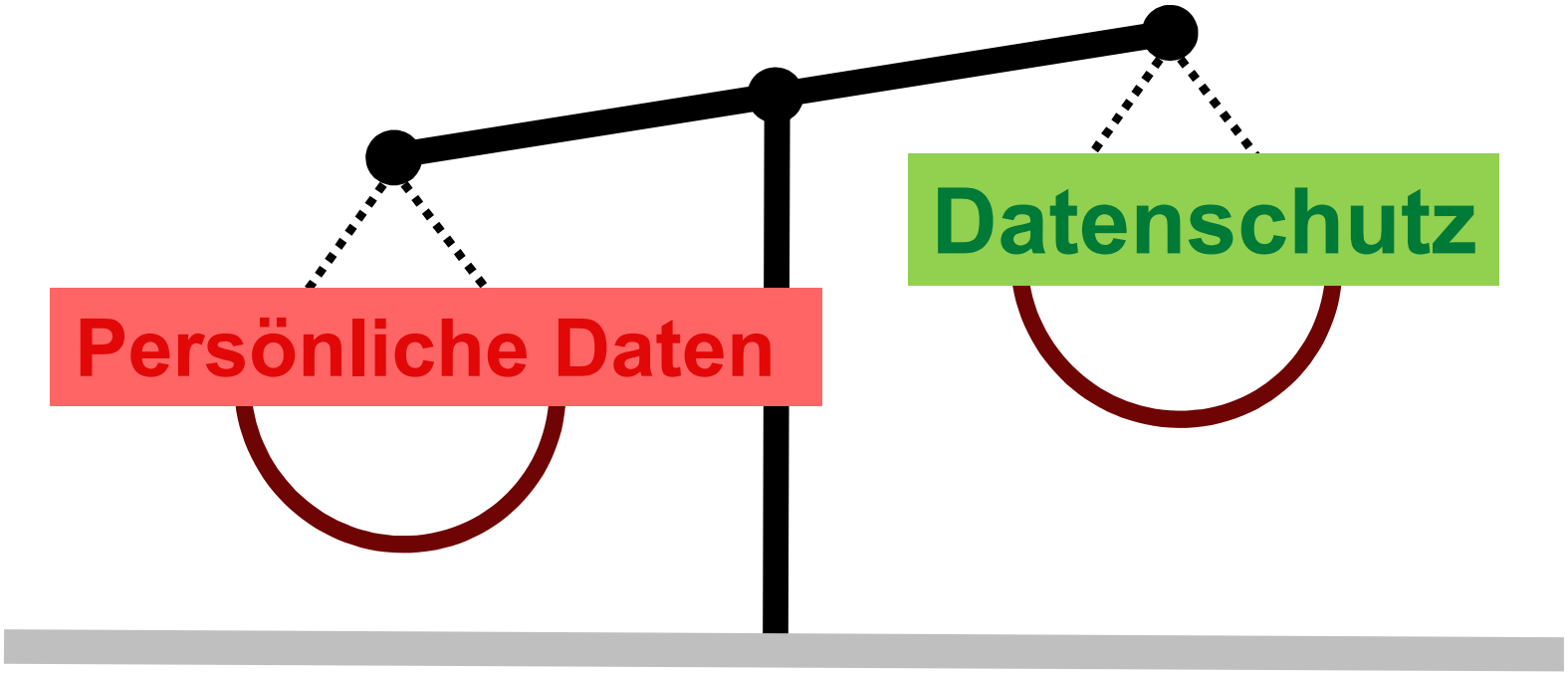
- **Cloud Computing ist eine Herausforderung**
  - Dauerhafter und attraktiver zentraler Angriffspunkt
    - **Vernetzung bietet zusätzliche Angriffspunkte**
  - Identitätsdiebstahl, Session-Hijacking, …
  - **Schwachstellen bei Shared Services, Abgrenzung der Unternehmensdaten**
  - Ich kenne die Orte, 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, …) – Hacker!
  - …

We have a Problem!
→ IT-Sicherheitsherausforderungen (8/9)

- **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***.

We have a Problem!
→ IT-Sicherheitsherausforderungen (9/9)

Persönliche Daten sind ein Rohstoff des Internetzeitalters



Geschäftsmodell: „Bezahlen mit persönlichen Daten“

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**
    - Von überall zugreifbar (Mobile Geräte → Cloud Computing, …)

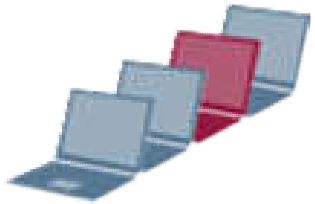
Notwendigkeit - Paradigmenwechsel
→ Änderungen der Rahmenbedingung (2/2)

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**



Paradigmenwechsel – (1)

→ Mehr Vertrauenswürdigkeit statt Gleichgültigkeit

- Welchen Firmen können wir vertrauen?

Security und Cloud Storage

Freier Zugang für alle: Peinliche Sicherheitspanne bei Dropbox

von Lars Bube

Share

21.06.2011

Beim beliebten Cloud Storage Dienst Dropbox gab es gestern (Montag) peinliche Datenpanne. Für mehrere Stunden konnten sich die User mit

30.06.2011 13:05

US-Behörden dürfen auf europäische Cloud-Daten zugreifen

Cloud-Anbieter wie Microsoft müssen US-Strafverfolgungsbehörden Zugriff auf von K gewähren, be
europäischen
Markteinführu
zusichern kön

Transparente Gesetze!

6 Ausgaben mit ...

as Unternehmen seinen Firmensitz in den USA habe, müsse es die dortigen Ges
Das gilt insbesondere für den Patriot Act, der US-Strafverfolgern weitreichende Zug
Frazer zufolge würden Kunden über die Herausgabe von Daten "informiert, wann imm
Garantie dafür könne er jedoch nicht geben. Denn in den USA kann das FBI mit einer
(NSL) ein Redeverbot (Gag order) für den Betreffenden aussprechen. In diesem Fa

Geschäftsmodell vs. IT Sicherheit

- **Evaluierung / Zertifizierung**
  (BSI, ENISA, ISO 27001, eco, …)
- **Produkthaftung**

- **Versicherungen**

Paradigmenwechsel – (2)

→ Mehr proaktive statt aktive 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 – (2)

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

Proaktive Sicherheitssysteme

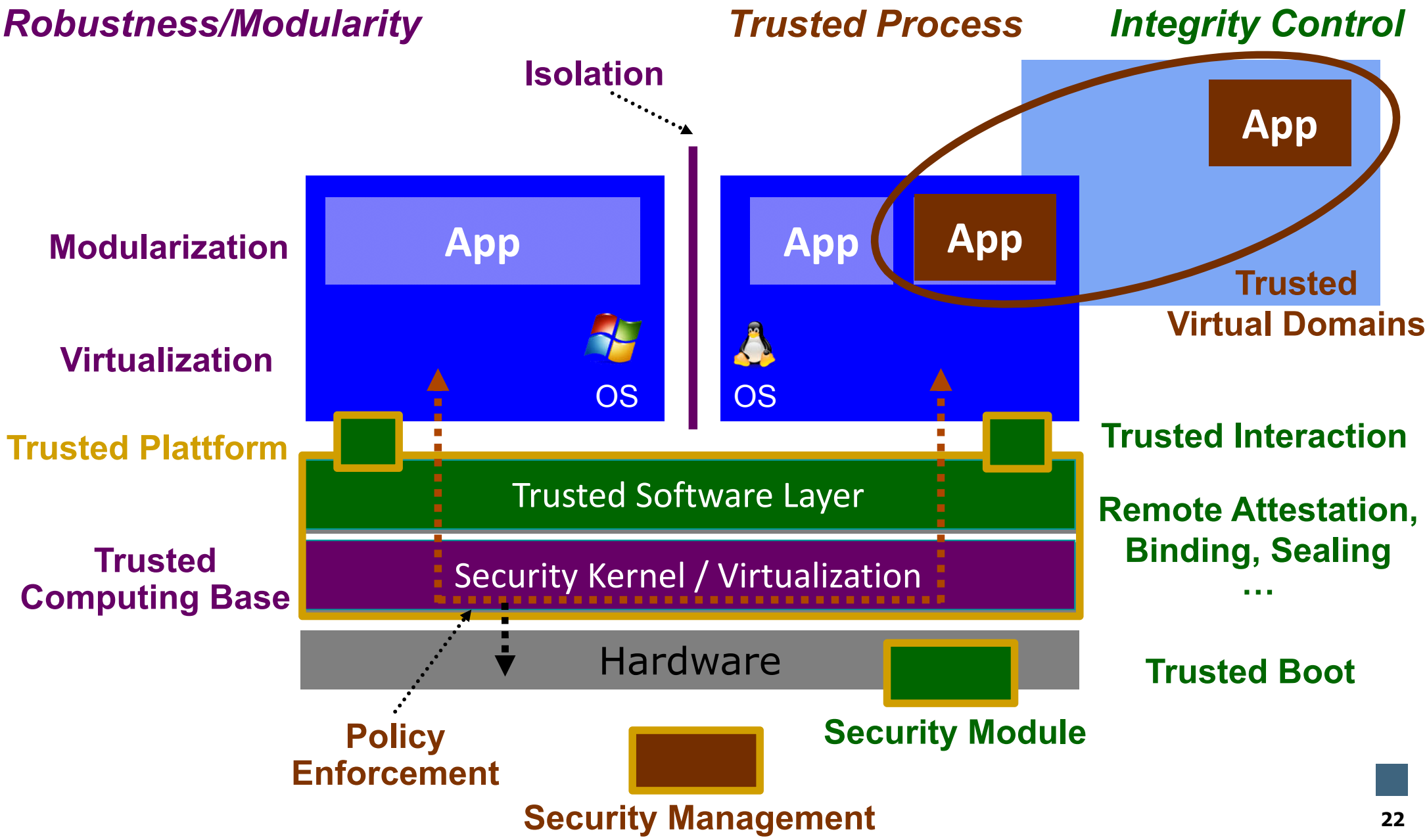
- Es ist viel besser, wenn wir proaktive Sicherheitsmechanismen etablieren und nutzen, damit unsere IT-Systeme **robuster** und **vertrauenswürdiger** werden.
- Hier spielen **Sicherheitsplattformen** auf der Basis von **intelligenten kryptographischen Verfahren** eine wichtige Rolle.

(Vertrauenswürdige Basis)

„ESP-Strategie“

Verhindern, dass man überhaupt ins Schleudern kommt

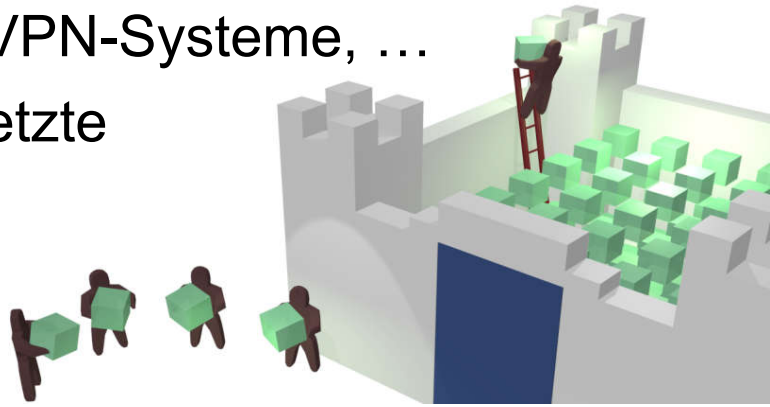
Paradigmenwechsel – (2)
→ Vertrauenswürdige Basis



Paradigmenwechsel – (3)
→ Mehr Objekt- statt Perimeter-Sicherheit (1/2)

Heute unzureichende Sicherheitsmodelle *(inhärente Schwachstellen)*

- **Perimeter-Sicherheit (Abschottung „Netz“)**
  - **Abwehrmodell:** Verhindern, dass
    - Fremde aus dem Internet ins eigene Unternehmensnetz zugreifen können (Abschottung) und
    - dass die ausgetauschten Daten nicht von anderen gelesen und manipuliert werden können.
  - **IT-Sicherheitsmechanismen:** Firewall- und VPN-Systeme, …
  - **Bewertung:** Immer offenere Unternehmensnetzte (Mobilfunk - UMTS, LTE, … , WLAN, ….)

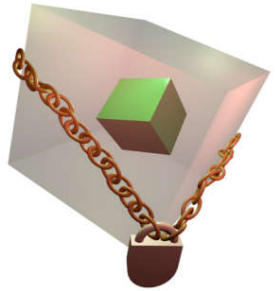


- **Zugriffskontrolle (Abschottung „Rechner“)**
  - **Idee:** Nur Autorisierte haben Zugriff auf ein Rechnersystem
  - **Bewertung:** fehlende IDM-Lösungen; Sicherheitslösungen laufen „auf“ den komplexen Betriebssystemen (Malware)

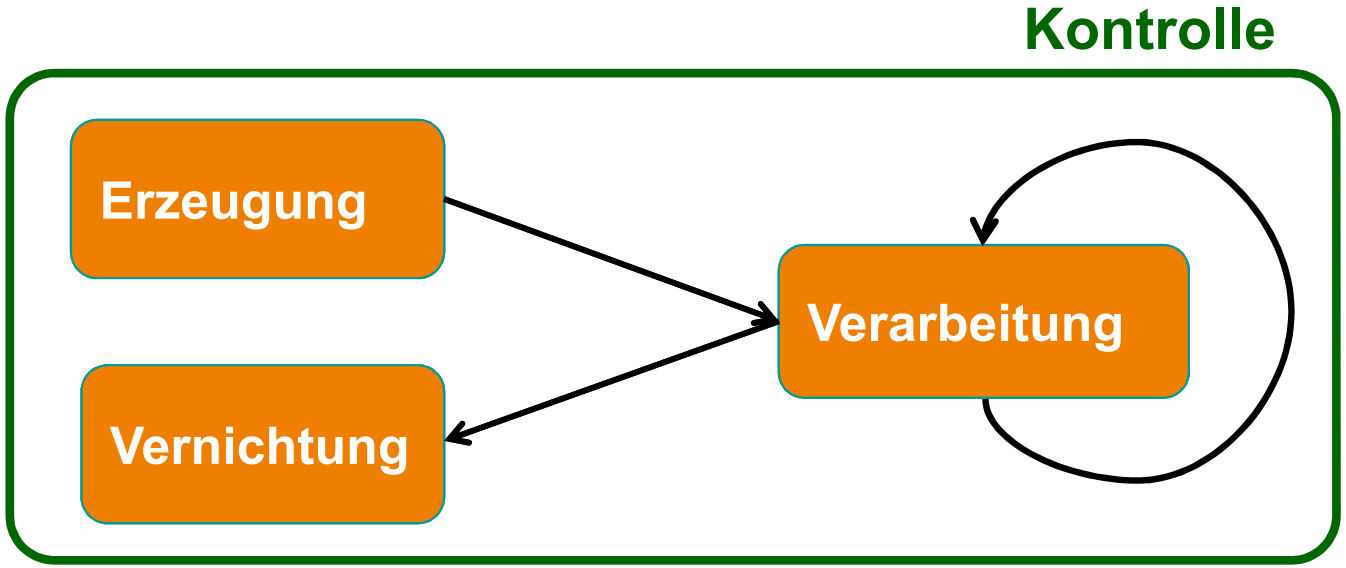
Paradigmenwechsel – (3)

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

- **Objekt-Sicherheit (Informationsflusskontrolle)**
  - **Idee:** Domänenorientierten 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 – (4)
→ Mehr Zusammenarbeit statt Separation

We have a Problem!
→ 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

Houston, we have a Problem!

→ Paradigmenwechsel in 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.