



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Was sind die größten IT-Sicherheitsherausforderungen?

Prof. Dr. (TU NN)

Norbert Pohlmann

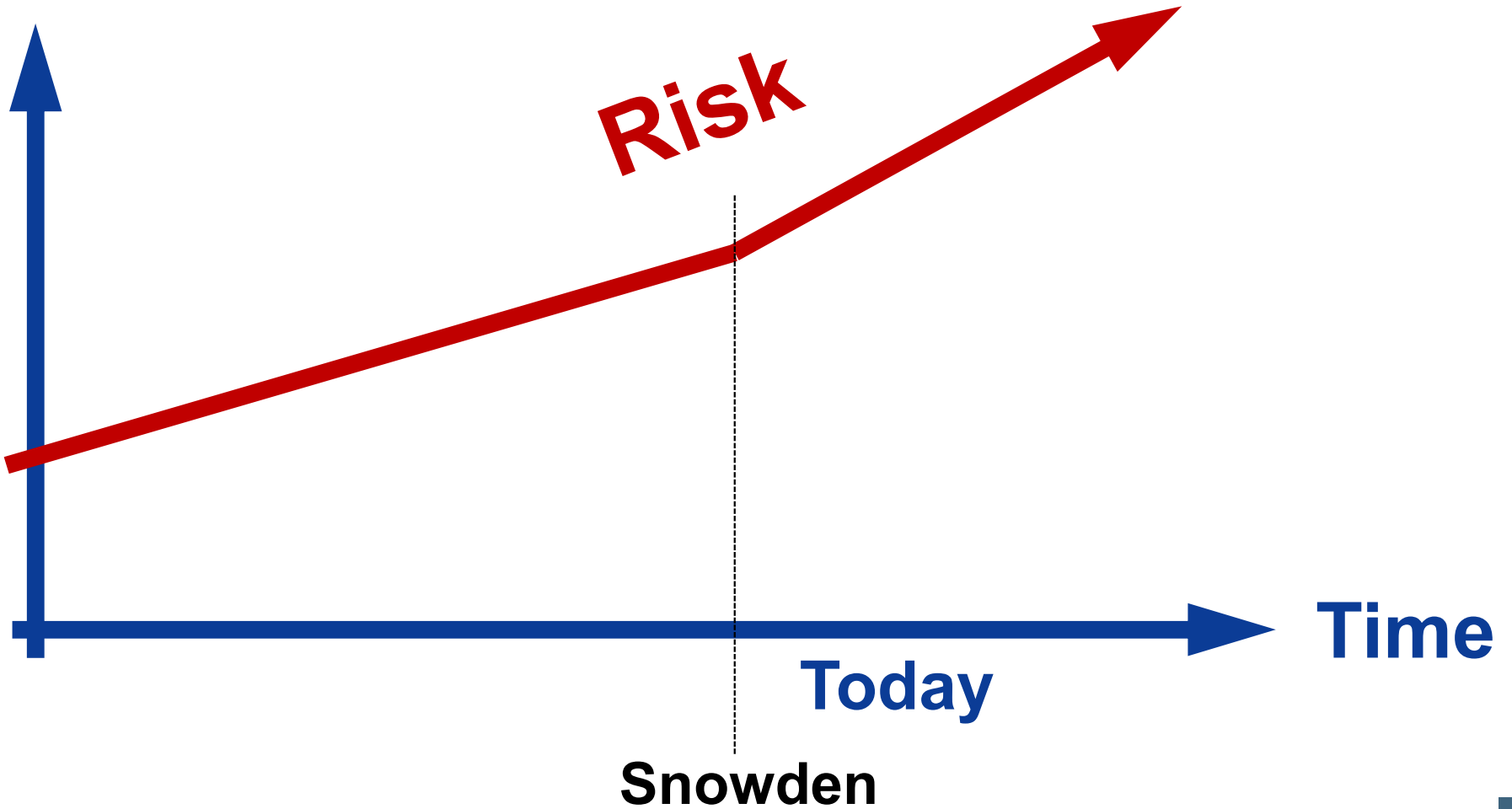
Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet-sicherheit.

IT-Sicherheit im Laufe der Zeit

→ Unser Problem

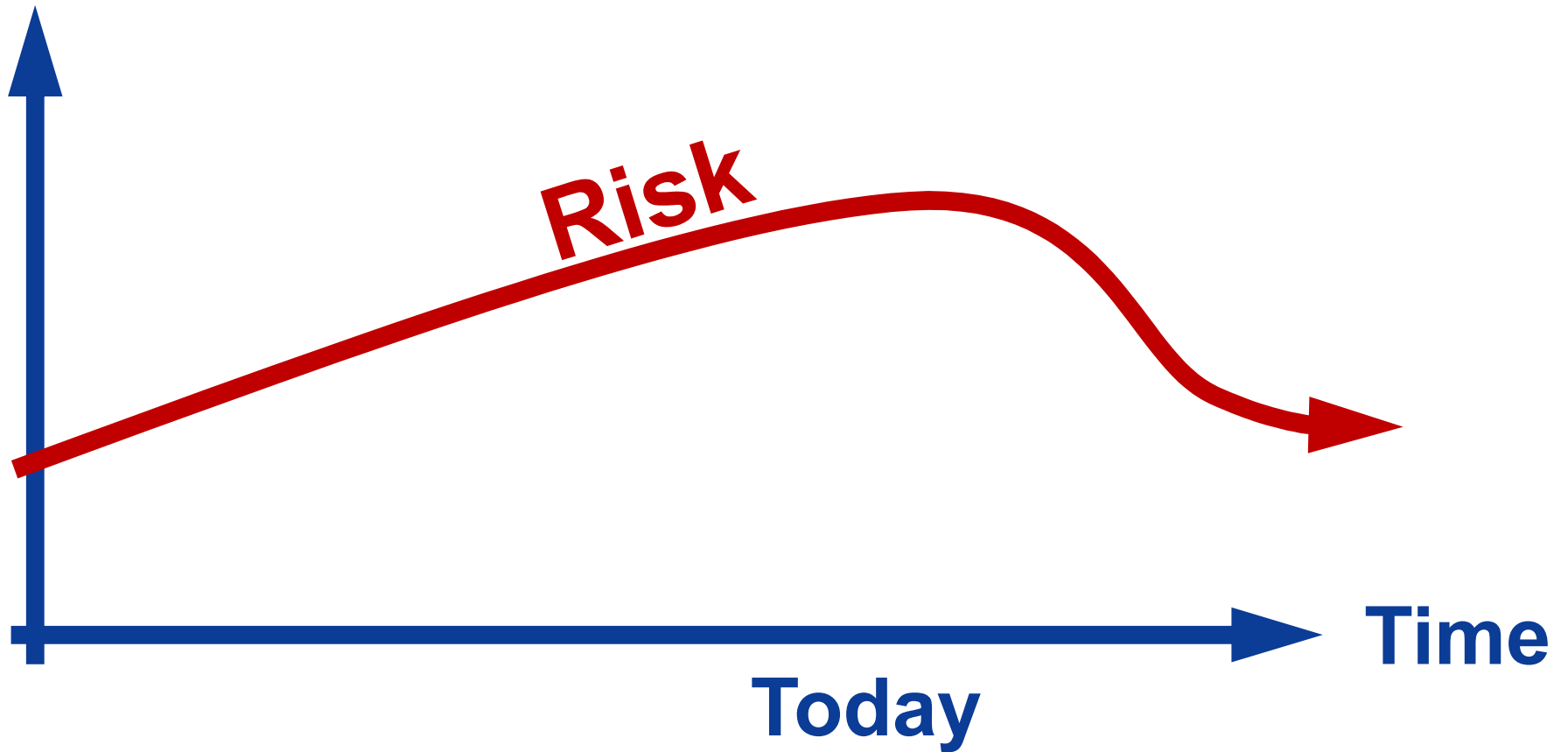
Problems



IT-Sicherheit im Laufe der Zeit

→ Unsere Herausforderung

Problems



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**

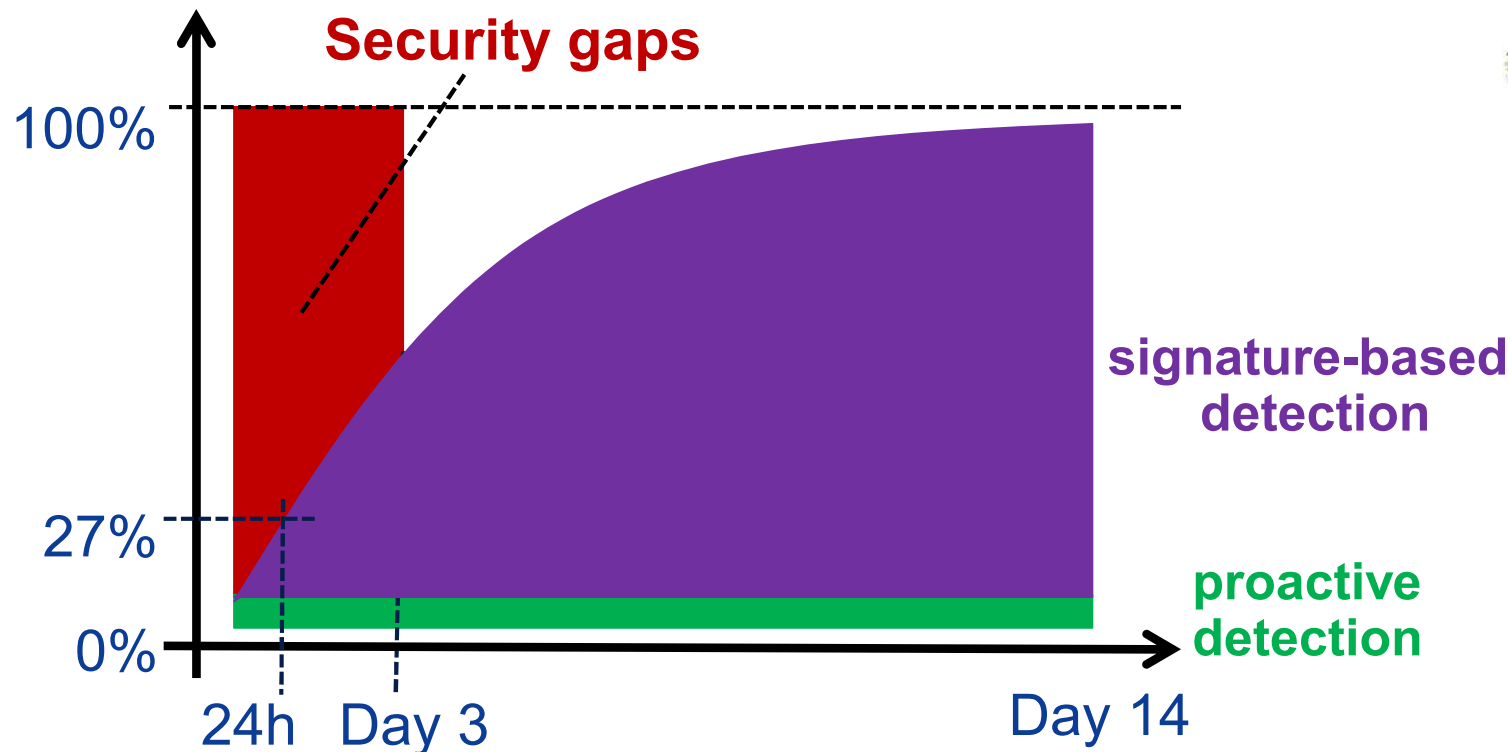
→ mehr als 3.000 Fehler
(Fehlerdichte 0,3)

**→ 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 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**

IT-Sicherheitsherausforderungen

→ Identity Management (2014)

- 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 gemessenen 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!**

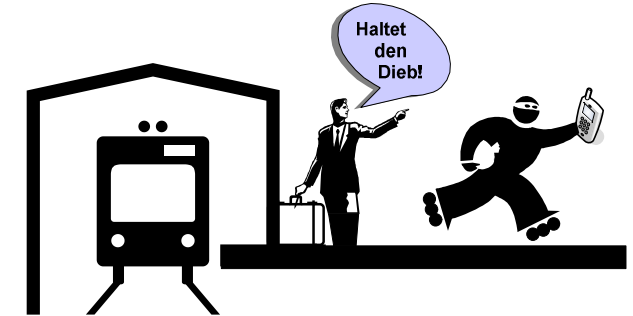


IT-Sicherheitsherausforderungen

→ 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

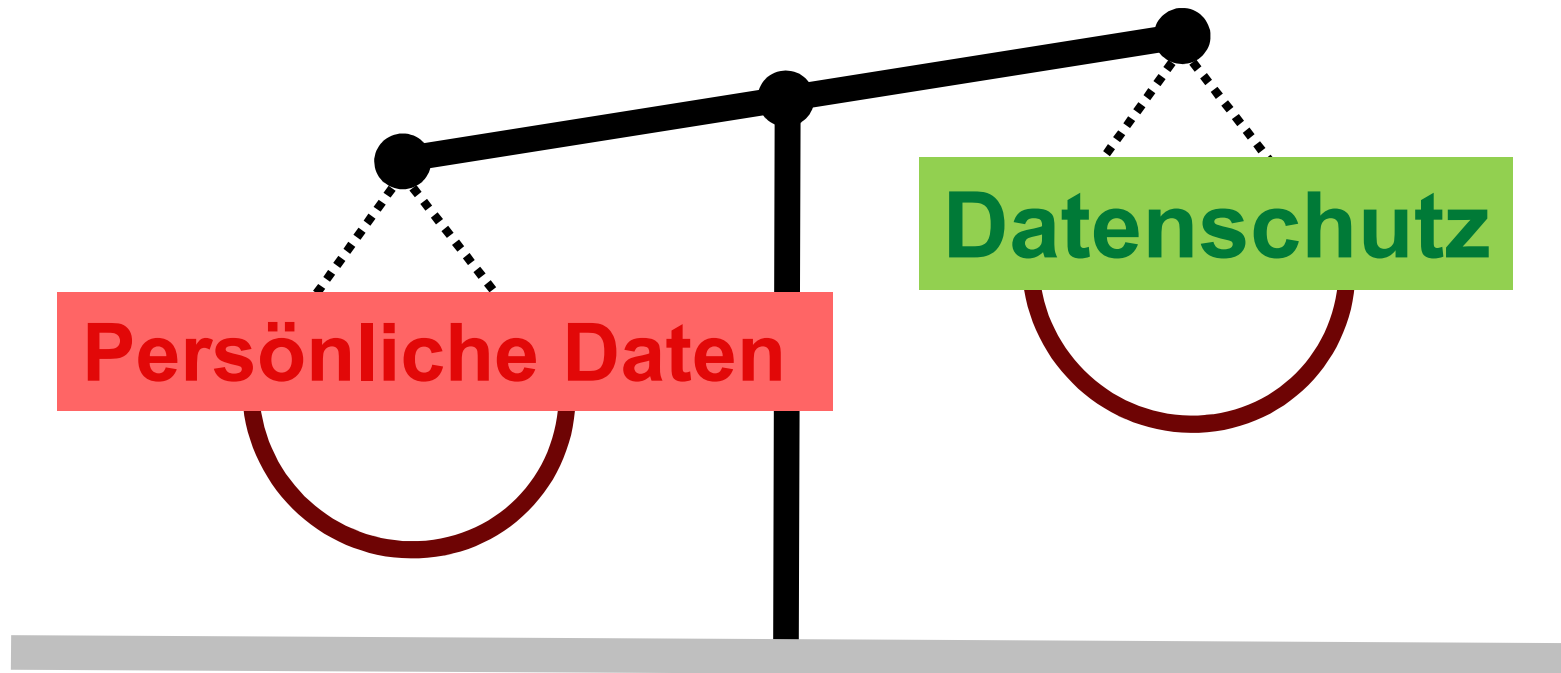
→ Internet-Nutzer

- 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“

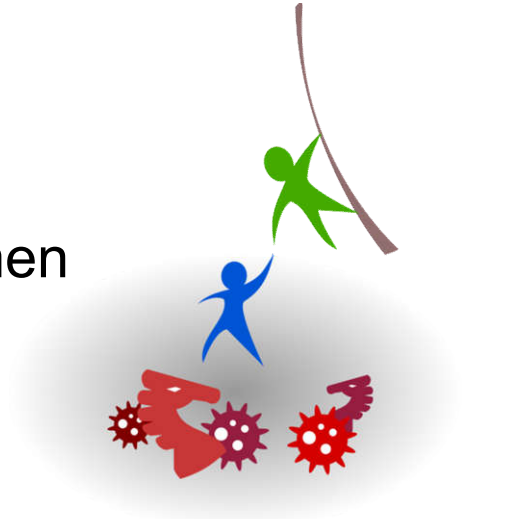


IT-Sicherheitsherausforderungen

→ NSA - Unsicherheiten

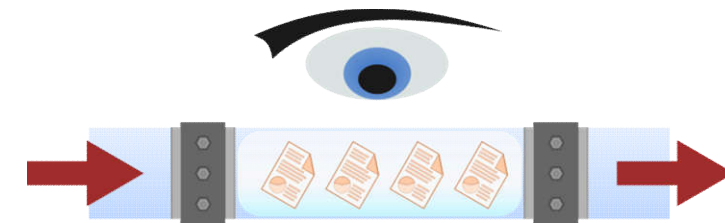
■ Grundsätzliche Probleme und fehlendes Vertrauen

- 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
- ...



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



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Was sind die größten IT-Sicherheitsherausforderungen?

**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.