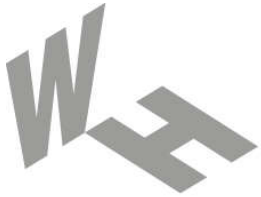


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Status Quo zur Sicherheit
→ Eine Sichtweise

Prof. Dr. (TU NN)
Norbert Pohlmann

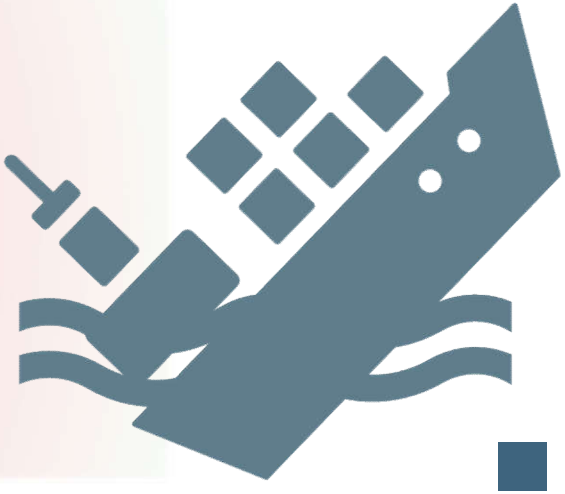
Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Status Quo zur Sicherheit
→ Situation

- Wir entwickeln uns zur einer **Internet-Gesellschaft** *(Informationsquelle, eCommerce, eGovernment, …, eAssistenten, …, Industrie 4.0, Internet der Dinge, …)*
- Viele lokale Dienste werden **an das Internet gebunden** *(intelligente Analysen → Internetkonnektivität)*
- **Private-** und **Unternehmensdaten** „lagern“ immer häufiger **im Internet** *(zentrale Speicherung → Internetkonnektivität)*

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



Was sind die Problemfelder?
→ 1. Privatheit und Autonomie

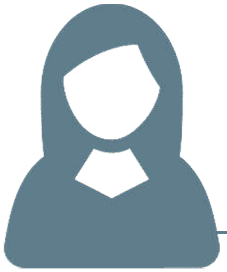
Verschiedenen Sichtweisen

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

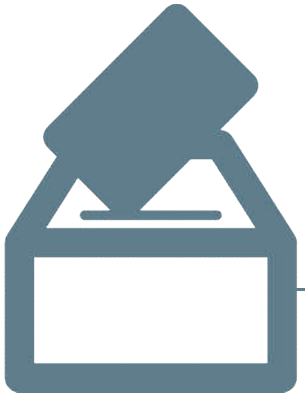
Was sind die Problemfelder?
→ 2. Wirtschaftsspionage

ca. 51 Milliarden € Schaden pro Jahr

Wirtschaftsspionage

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

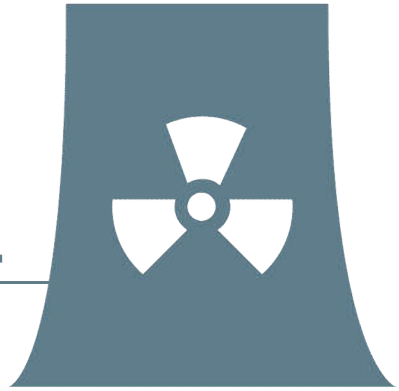
Was sind die Problemfelder?
→ 3. Cyberwar



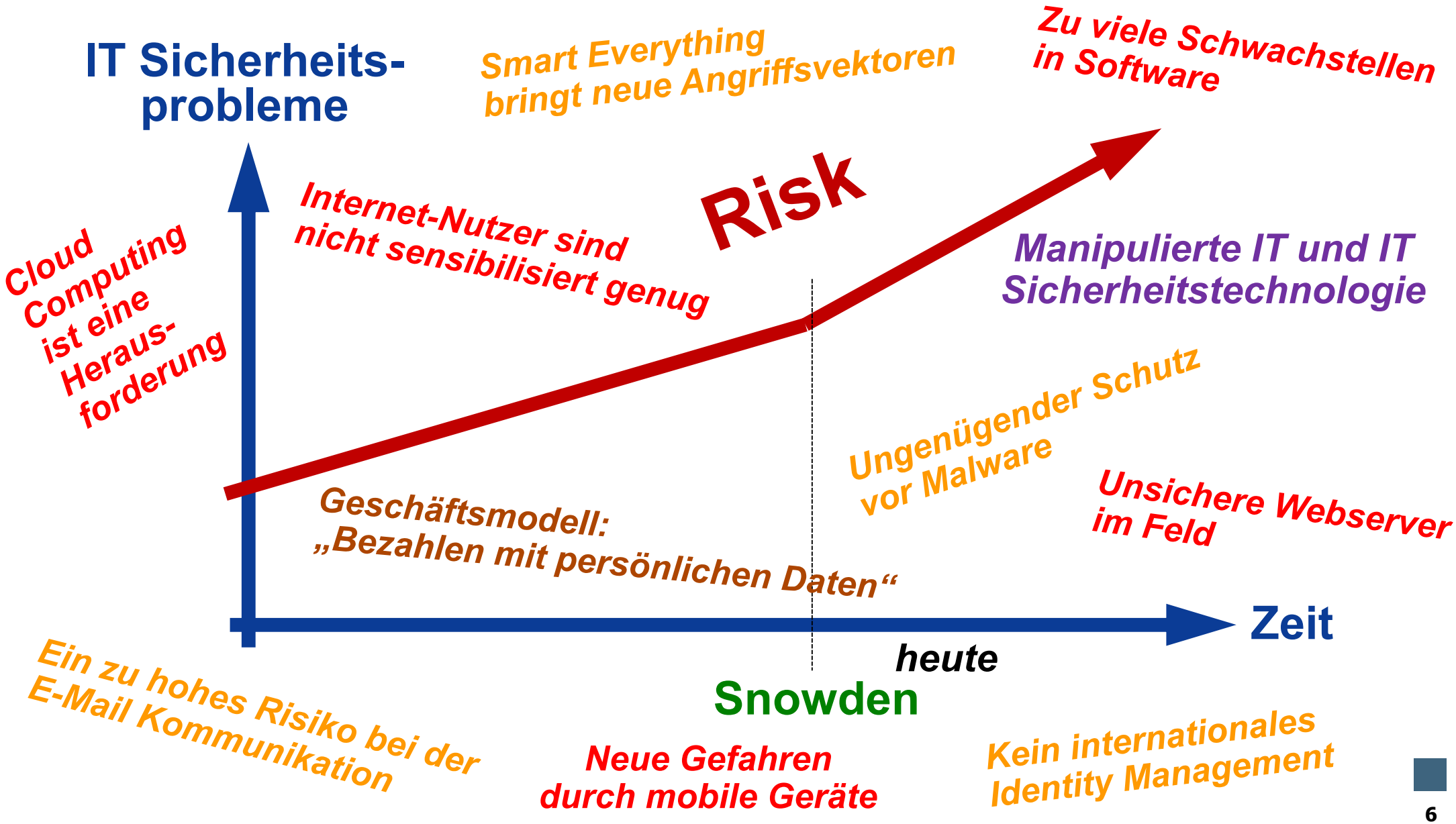
Umsetzung von politischen Zielen
→ „einfach“ und „preiswert“

Cyberwar

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



Status Quo zur Sicherheit
→ Die größten Herausforderungen



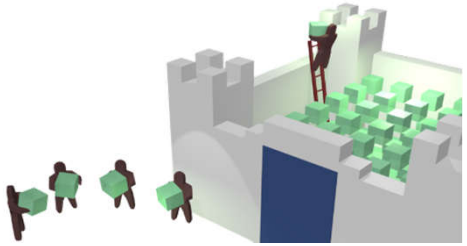
Status Quo zur Sicherheit
→ Evaluierung der Situation

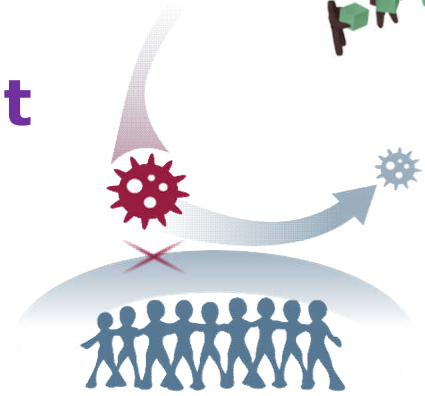
- **Wir kennen die IT-Sicherheitsprobleme**, doch die heute vorhandenen und genutzten IT-Sicherheitssysteme und IT-Sicherheitsmaßnahmen **reduzieren das IT-Sicherheitsrisiko nicht** ausreichend**!**
- Es handelt sich um ein globales Problem
- Die zukünftigen Angriffe werden die heutigen **Schäden** noch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

Neue Strategien und Lösungen!
→ Ideen

- Mehr **Verschlüsselung**
  (statt offen)
- Mehr **Vertrauenswürdigkeit**
  (statt Gleichgültigkeit)
- Mehr **proaktive IT-Sicherheit**
  (statt aktive IT-Sicherheit)
- Mehr **Objekt-Sicherheit**
  (statt Perimeter-Sicherheit)
- Mehr **Zusammenarbeit**
  (statt Separation)

...





Was ist wichtig für die Zukunft?
→ Thesen (1)

- **Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung!**
  - Die Gesellschaft muss **intolerant** gegenüber **unsichere IT-Lösungen** sein!
  - **Risikobasierte Ansätze** und **adaptive IT-Sicherheits-Architekturen**. (für primären Applikationen und industriellen Steuerungskomponenten)
  - **Alle Stakeholder** (Politik, Verwaltung, Forschung, Anwender und Hersteller) müssen für eine erfolgreiche und nachhaltige Umsetzung einer **gemeinsamen** sicheren und vertrauenswürdigen IT bessere und wirkungsvolle IT-Lösungen entwickeln und einsetzen.
  - **IT-Sicherheit** ist kein Business-Enabler mehr, sondern eine wichtige **Grundanforderung** im End-to-End Prozess.

- **Gemeinsam mehr wirkungsvollere IT-Sicherheitslösungen nutzen**
  - Enge **Zusammenarbeit** zwischen den Herstellern und Anwendern ist nötig.
  - Zusammenarbeit mit IT-Marktführern ist notwendig.
  - Vom angebotsgetriebenen zum **anforderungsgetriebenen IT-Sicherheitsmarkt.**
  - Anwenderunternehmen sollten ihre **Einkaufsmacht fair nutzen**.

Was ist wichtig für die Zukunft?
→ Thesen (2)

- **Verschlüsselung, Transparenz und Vertrauen sind die digitalen Werkzeuge für die informationelle Selbstbestimmung!**
  - **Keine staatlich motivierten Schwachstellen und Hintertüren** in IT-Lösungen.
  - Gemeinsam werden wir **vorhandene Hemmnisse abbauen**, damit deutlich mehr Verschlüsselungslösungen zum Einsatz kommen.
  - Zukünftige **Verschlüsselungsprodukte** müssen sicher und vertrauenswürdig, aber für den Nutzer möglichst **transparent sein** (wie z.B. der Airbag im Auto).

- **Security-by-Design und nachvollziehbare Qualitätssicherung sind unabdingbar!**
  - **Security-by-Design** ist ein wichtiges **Entwicklungsparadigmen** bei der Herstellung, Bewertung und Auswahl von IT-Lösungen.
  - Eine **(Mit)Verantwortung** aller Nutzer, für wichtige **OpenSource-Komponenten**, muss übernommen werden.
  - Die **Benutzbarkeit** und Nutzererfahrung von IT ist das **allerentscheidende** und muss vom Nutzer aus betrachtet werden.

Was ist wichtig für die Zukunft?
→ Thesen (3)

- **Cyber-War wird immer bedrohlicher**
  - Die immer wichtiger werdende Bedrohung **Cyber-War** muss in die **Risikobewertung der Unternehmen** eingebunden.
  - Alle wichtigen IT-Anwendungen werden unter dem Aspekt Cyber-War beleuchtet und bewertet, damit IT-Sicherheitsmaßnahmen für einen **angemessenen sicheren und robusteren Betrieb** umgesetzt werden können.

- **Wir brauchen eigene Souveränität von IT-Sicherheitsinfrastrukturen**
  - Der technologische Stand in Europa muss ausgebaut, gesichert und gefördert werden, um die **eigene Souveränität** behalten zu können.

Status Quo zur Sicherheit
→ Zusammenfassung

- **Wir kennen die IT-Sicherheitsprobleme**, doch die heute vorhandenen und genutzten IT-Sicherheitssysteme und IT-Sicherheitsmaßnahmen **reduzieren das IT-Sicherheitsrisiko nicht** ausreichend**!**

- Durch den **immer schneller werdenden Digitalisierungsprozess**, werden wir in der Lage sein **moderne sichere und vertrauenswürdige IT-Technologien** schnell in die Fläche von wichtigen und zukunftsorientierten Anwendungsbereichen zu bekommen.

- Nur **gemeinsam** sind wir in der Lage, mehr **wirkungsvolle IT-Sicherheit** in unseren IT-Lösungen zu bekommen.

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Status Quo zur Sicherheit
→ Eine Sichtweise

Gemeinsame Verantwortung wahrnehmen für mehr Sicherheit und Vertrauenswürdigkeit

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.