



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Wirkung von IT-Sicherheitsmaßnahmen

→ Die neue Herausforderung

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-Sicherheitslage**
(Situation, Bewertung, Herausforderungen)
- **IT-Sicherheit Deutschland**
(Stärken, Möglichkeiten, Kompetenzen / Technologien)
- **Wirkung von IT-Sicherheitsmaßnahmen**
(Aspekte, IT Security Replaceability, Kooperation)
- **Einordnung von Wirkungsklassen**
(Gefahren, Schutzbedarf, Vertrauenswürdigkeit)
- **Fazit**

- **IT-Sicherheitslage**
(Situation, Bewertung, Herausforderungen)
- **IT-Sicherheit Deutschland**
(Stärken, Möglichkeiten, Kompetenzen / Technologien)
- **Wirkung von IT-Sicherheitsmaßnahmen**
(Aspekte, IT Security Replaceability, Kooperation)
- **Einordnung von Wirkungsklassen**
(Gefahren, Schutzbedarf, Vertrauenswürdigkeit)
- **Fazit**

IT-Sicherheitslage

→ Die größten Herausforderungen

IT Sicherheitsprobleme



- **IT-Sicherheitslage**
(Situation, Bewertung, Herausforderungen)
- **IT-Sicherheit Deutschland**
(Stärken, Möglichkeiten, Kompetenzen / Technologien)
- **Wirkung von IT-Sicherheitsmaßnahmen**
(Aspekte, IT Security Replaceability, Kooperation)
- **Einordnung von Wirkungsklassen**
(Gefahren, Schutzbedarf, Vertrauenswürdigkeit)
- **Fazit**

- **Sehr hohe Kompetenz im Bereich des Datenschutzes**

- Erfahrungen mit dem Schutz der Privatsphäre



- **Sehr hohes Vertrauen im Bereich der IT-Sicherheit**

- mittelstandsgeprägte IT-Sicherheitsindustrie

- umfangreiche und kompetente IT-Sicherheitsforschung

- hohe Kompetenz bei IT-Sicherheitsevaluierungen (BSI, „TÜVs“, ...)

- offene Kryptopolitik

- **Kulturell gute Voraussetzungen**

- traditionell verlässliche IT-Sicherheit

- hohes Verständnis für IT-Sicherheit und Datenschutz

- sehr viel Erfahrung bei der Umsetzung von IT-Sicherheitslösungen

- Deutschland sollte **Verantwortung übernehmen** und ein

- **sicheres** und

- **vertrauenswürdige**

- globales Internet für die Zukunft entscheidend mitgestalten

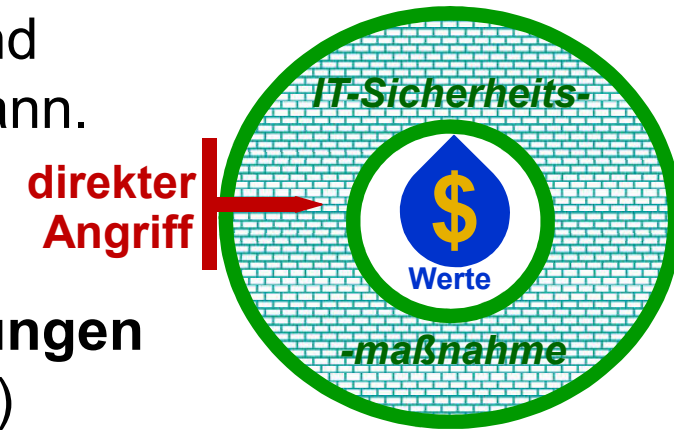
- **Sicherheitskern** (*Sicheres Booten, Separierungstechnologien, ...*)
- **Security Token** (*Smartcards, Hardware-Sicherheitsmodule, ...*)
- **Verschlüsselungstechnologien** (*Kommunikations- und Objektverschlüsselung, Kryptohardware*)
- **Proaktive IT-Sicherheitstechnologien** zur Exploitbekämpfung
- Technologie zur **Abwehr von Schadsoftware**
- Höherwertige **Firewall-Technologien**
- Technologien für **sichere Identitäten** (*PKI, TrustCenter*)
- **Frühwarnsysteme** (*Angriffserkennung, Lagebildgenerierung, ...*)

- **IT-Sicherheitslage**
(Situation, Bewertung, Herausforderungen)
- **IT-Sicherheit Deutschland**
(Stärken, Möglichkeiten, Kompetenzen / Technologien)
- **Wirkung von IT-Sicherheitsmaßnahmen**
(Aspekte, IT Security Replaceability, Kooperation)
- **Einordnung von Wirkungsklassen**
(Gefahren, Schutzbedarf, Vertrauenswürdigkeit)
- **Fazit**

Wirkung von IT-Sicherheitsmaßnahmen

→ Unterschiedliche Wirkungsaspekte

Es gibt unterschiedliche **IT-Sicherheitsmaßnahmen** und Aspekte, wie eine **maximale Wirkung** erzielt werden kann.



- Die **prinzipielle** Wirkung gegen konkrete Bedrohungen (z.B. Verschlüsselung gegen das Lesen von Klartext)

- Maßnahme: Darstellung der Wirkung von Kryptoverfahren

z.B. RSA 4096

- Die **konkrete** Wirkung gegen konkrete Bedrohungen (z.B. richtige Implementierung von Verschlüsselungstechnologien; Zufallszahlen, Algorithmus, Einbindung, ...)

- Maßnahme: Evaluierung /Zertifizierung von IT-Sicherheitslösungen

z.B. CC EAL4

- Die **gewollte** Wirkung gegen konkrete Bedrohungen (z.B. Hintertüren oder gewollte Schwächen eingebaut)

- Maßnahme: Qualitätssiegel: "IT Security made in Germany"

- Die IT-Marktführer stellen **offene Schnittstellen** zur Verfügung, die eine Austauschbarkeit von IT-Sicherheitstechnologien
 - **einfach** und
 - **nachhaltig**in den IT-Produkten und -Lösungen möglich macht.
- *Beispiele:*
 - **Krypto-Technologien**
 - Algorithmen (Private/Public-Key-Verfahren, Hashfunktionen, ...)
 - Zufallszahlengeneratoren
 - ...
 - **Weitere IT-Sicherheitslösungen**
 - Verschlüsselung (Festplatte, Dateien, Objekte, ...)
 - Abschottungstechnologien (Ports, Virtuelle Maschinen, ...)
 - IT-Sicherheitstoken (Smartcards, HSMs, ...)
 - ...

- Die **IT-Markführer** schaffen deutlich mehr **Vertrauenswürdigkeit** für ihre IT-Lösungen
 - Kunden müssen entscheiden!**
- Die ~~Kunden können entscheiden~~, welche IT-Sicherheitstechnologien sie einsetzen wollen (abhängig vom Schutzbedarf – TTT-Modell)
- Die **deutsche IT-Sicherheitsindustrie** hat einen einfachen **Zugang zum globalen Markt**

eine echte **WIN-WIN-Situation**

Kooperation für mehr Vertrauen

→ Beispiel

- **Wirksamkeit** von Verschlüsselung und **Vertrauen** in IT-Sicherheitslösungen in Anhängigkeit des eigenen Schutzbedarfs

▶ z.B. Microsoft Windows Bitlocker Verschlüsselungssoftware (USA), Voll integriert ins Betriebssystem und weitgehend vorkonfiguriert
Herausforderung: IT Security Replaceability

Vertrauenswürdigkeit

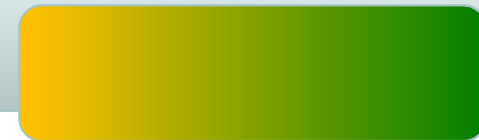


Prinzipielle Wirkung ist gegeben; **konkrete Wirkung** muss nachgewiesen werden
Gewollte Wirkung muss beurteilt werden, in Abhängigkeit des eigenen Schutzbedarfes

Beispiel einer möglichen Kooperation

▶ Deutsche Verschlüsselungssoftware (z.B.: Sirrix Trusted-Disk), Softwarelösung als eigenständiges IT-Sicherheitsprodukt zusätzlich zu bestehenden Softwarekomponenten auf dem Rechner

Vertrauenswürdigkeit



Gewollte Wirkung per Definition gegeben („Made in Germany“)
(zugelassene Software, d.h. die Vertrauenswürdigkeit durch eine nationale Behörde bestätigt; auch prinzipielle und konkrete Wirkung)

- Möglichkeit einer **Schnittstelle zum Ersetzen** bestehender eingebauter IT-Sicherheitstechnologien durch **deutsche IT-Sicherheitslösungen** für eine **höhere Wirkung der IT-Sicherheit**.

- **IT-Sicherheitslage**
(Situation, Bewertung, Herausforderungen)
- **IT-Sicherheit Deutschland**
(Stärken, Möglichkeiten, Kompetenzen / Technologien)
- **Wirkung von IT-Sicherheitsmaßnahmen**
(Aspekte, IT Security Replaceability, Kooperation)
- **Einordnung von Wirkungsklassen**
(Gefahren, Schutzbedarf, Vertrauenswürdigkeit)
- **Fazit**

Einordnung von Wirkungsklassen

→ TTT-Modell

Wirkungsklasse 0 **Bürger mit privater Nutzung**

Prozentualer Anteil:

- Gefahren: Privatsphäre, Cybercrime
- Kosten: Grundbetrag +5% (*vertrauenswürdige IT-Sicherheitstechnologien*)

100%

Wirkungsklasse 1 **Unternehmen, Organisationen, Behörden**

- Gefahren: Privatsphäre, Cybercrime mit höherem Gefährdungsgrad, **gesetzlicher Datenschutz**
- Schutzbedarf: mittel
- Kosten: Grundbetrag +10% (*Punktuell vertrauenswürdige IT-Sicherheitstechnologien aus Deutschland*)

70%

Wirkungsklasse 2 **Unternehmen, Organisationen, Behörden, Infrastruktur**

- Gefahren: Cybercrime, gezielte Angriffe auf Werte des Unternehmens, **Industriespionage**
- Schutzbedarf: hoch
- Kosten: Grundbetrag +20% (*Einige vertrauenswürdige IT-Sicherheitstechnologien aus Deutschland*)

27%

Wirkungsklasse 3 **Unternehmen, Organisationen, Behörden, Infrastruktur**

- Gefahren: Wirtschaftsspionage (Nachrichtendienste) und Cyberattacken, **Cyberwar (Sabotagen)**
- Schutzbedarf: sehr hoch, inkl. VS-NfD
- Kosten: Grundbetrag +50% (*Möglichst viel vertrauenswürdige IT-Sicherheitstechnologien aus Deutschland*)

3%

+ Infrastrukturkosten

Wirkungsklasse 4 **Verschlusssachen**

- Nationale Sicherheit
- Schutzbedarf: gemäß Geheimschutzordnung GSO, ab VS/V
- Kosten: Grundbetrag +400%

0,01%

Kernklassen

- **IT-Sicherheitslage**
(Situation, Bewertung, Herausforderungen)
- **IT-Sicherheit Deutschland**
(Stärken, Möglichkeiten, Kompetenzen / Technologien)
- **Wirkung von IT-Sicherheitsmaßnahmen**
(Aspekte, IT Security Replaceability, Kooperation)
- **Einordnung von Wirkungsklassen**
(Gefahren, Schutzbedarf, Vertrauenswürdigkeit)
- **Fazit**



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Wirkung von IT-Sicherheitsmaßnahmen

→ Die neue Herausforderung

**Wir brauchen eine IT-Sicherheitsstrategie,
die das Risiko für unsere Gesellschaft auf ein
angemessenes Maß reduziert!**

Prof. Dr. (TU NN)

Norbert Pohlmann

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

if(is)
internet-sicherheit.