

Mehr **IT-Souveränität** durch **Zusammenarbeit** → **Vertrauen** ist eine **Herausforderung** für die **Zukunft**

Prof. Dr. (TU NN)

Norbert Pohlmann

Vorstandsvorsitzender TeleTrust - Bundesverband IT-Sicherheit e.V.

Professor für Informationssicherheit und

Leiter des Instituts für Internet-Sicherheit – if(is)

- Es gibt in Deutschland eine **massive Abhängigkeit** von der **IT/dem Internet**
 - **Marktführende IT-Technologien** kommen in vielen Bereichen aus dem **Ausland**
 - Wunsch nach **IT-Souveränität** (IT-Sicherheit/Vertrauenswürdigkeit)

- Zwiespalt: **Zurzeit keine angemessene Vertrauenswürdigkeit**
 - ▶ Steigende Zahl von IT-Sicherheitsvorfällen zeigt, dass das allgemeine **Sicherheitsniveau** zurzeit nicht angemessen ist
 - ▶ Die **Wirkung** von IT-Sicherheitslösungen ist an vielen Stellen heute nicht mehr ausreichend (*unterschiedliche Gründe: Softwarequalität, IT-Sicherheitsansätze, Zusammenarbeit, NSA&Co., ...*)
 - ▶ Die **Vertrauenswürdigkeit** von IT-Systemen ist eine **wichtige** und **notwendige Eigenschaft** für eine erfolgreiche Zukunft

IT-Sicherheit Deutschland

→ Besondere Stärken und Möglichkeiten

- **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

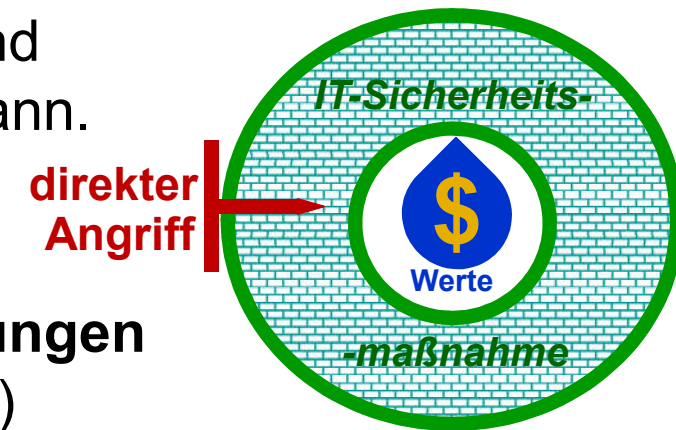
- **vertrauenswürdige**

- globales Internet für die Zukunft entscheidend mitgestalten

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"

IT Security made in Germany

→ Die Kriterien des Qualitätssiegels

- Der Unternehmenshauptsitz muss in Deutschland sein.
- Das Unternehmen muss vertrauenswürdige IT-Sicherheitslösungen anbieten.
- Die angebotenen Produkte dürfen keine versteckten Zugänge enthalten (no "Backdoors").
- Die IT-Sicherheitsforschung und -entwicklung des Unternehmens muss in Deutschland stattfinden.
- Das Unternehmen muss sich verpflichten, den Anforderungen des deutschen Datenschutzrechtes zu genügen.

SecurITy
made
in
Germany

Zurzeit ca. 95 IT-Sicherheitsunternehmen

IT-Sicherheitssituation, DE-Stärken, Wirkung von IT-Sec, Qualitätssiegel, ...

Was brauchen wir?

IT Security Replaceability

schafft durch eine **stärkere Kooperation** mehr **Vertrauen**

- 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
- 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**

Deutsche Stärken der IT-Sicherheit

→ Besondere Kompetenzen in Deutschland



Zahlreiche IT-Sicherheitstechnologien aus Deutschland:

- **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, ...*)



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**.

Einordnung von Wirkungsklassen

→ TTT-Modell

Wirkungsklasse 0	Bürger mit privater Nutzung	Prozentualer Anteil:
	<ul style="list-style-type: none">• Gefahren: Privatsphäre, Cybercrime• Kosten: Grundbetrag +5% (<i>vertrauenswürdige IT-Sicherheitstechnologien</i>)	100%
Wirkungsklasse 1	Unternehmen, Organisationen, Behörden	70%
	<ul style="list-style-type: none">• Gefahren: Privatsphäre, Cybercrime mit höherem Gefährdungsgrad, gesetzlicher Datenschutz• Schutzbedarf: mittel• Kosten: Grundbetrag +10% (<i>Punktuell vertrauenswürdige IT-Sicherheitstechnologien aus Deutschland</i>)	
Wirkungsklasse 2	Unternehmen, Organisationen, Behörden, Infrastruktur	27%
	<ul style="list-style-type: none">• Gefahren: Cybercrime, gezielte Angriffe auf Werte des Unternehmens, Industriespionage• Schutzbedarf: hoch• Kosten: Grundbetrag +20% (<i>Einige vertrauenswürdige IT-Sicherheitstechnologien aus Deutschland</i>)	
Wirkungsklasse 3	Unternehmen, Organisationen, Behörden, Infrastruktur	3%
	<ul style="list-style-type: none">• Gefahren: Wirtschaftsspionage (Nachrichtendienste) und Cyberattacken, Cyberwar (Sabotagen)• Schutzbedarf: sehr hoch, inkl. VS-NfD• Kosten: Grundbetrag +50% (<i>Möglichst viel vertrauenswürdige IT-Sicherheitstechnologien aus Deutschland</i>)	+ Infrastrukturkosten
Wirkungsklasse 4	Verschlusssachen	0,01%
	<ul style="list-style-type: none">• Nationale Sicherheit• Schutzbedarf: gemäß Geheimschutzordnung GSO, ab VS/V• Kosten: Grundbetrag +400%	

Kernklassen



Wir sind heute hier, um die **Kooperation**
zwischen
Microsoft und der **deutschen IT-Sicherheitsindustrie**
weiter voranzutreiben!

Mehr IT-Souveränität durch Zusammenarbeit
→ **Vertrauen ist Herausforderung für die Zukunft**

*Mit Hilfe von IT Security Replaceability
eine stärkere Kooperation für mehr Vertrauen!*

Prof. Dr. (TU NN)

Norbert Pohlmann

Vorstandsvorsitzender TeleTrust - Bundesverband IT-Sicherheit e.V.

Professor für Informationssicherheit und

Leiter des Instituts für Internet-Sicherheit – if(is)