



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# **Das Manifest zur IT-Sicherheit**

**→ Situation, Stärken, Vorgehensweisen, ...**

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 und IT-Sicherheit

## → Situation

- Das Internet ist „**der Motor**“ und **die Basis** für das **Wohlergehen** unserer modernen und globalen **Gesellschaft**.
- Der **Digitalisierungsprozess** wird **immer schneller** und damit auch die **Veränderungen** in unseren **Lebensräumen**.
- Unsere Arbeit, unsere Firmen, unsere Hochschulen, unsere Freizeit, unser ganzes **Leben wird sich wandeln**.



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



# Das Manifest zur IT-Sicherheit

## → Der Weg ist das Ziel

Zielsetzung



# Das Manifest zur IT-Sicherheit

## → 1: IT-Sicherheit wird immer wichtiger

- IT und das Internet sind „der Motor“ und die Basis für das Wohlergehen unserer modernen und globalen Gesellschaft
- ... heutigen IT-Architekturen sind nicht sicher genug!
- Die Herausforderungen gemeinsam zu bewältigen, ist für die erfolgreiche Zukunft entscheidend

### Gemeinsame Aufgaben:

- Mitglieder der Verbände widmen dem Thema IT-Sicherheit **besondere Aufmerksamkeit**, um mit gemeinsamen Maßnahmen eine angemessene Risikolage für eine erfolgreiche Zukunft sicherzustellen
- Insbesondere der immer schneller werdende **Digitalisierungsprozess wird uns helfen**, notwendige IT-Sicherheits- und Vertrauensaspekte berücksichtigen zu können

# Was sind die Problemfelder?

## → 1. Privatheit und Autonomie

### Verschiedenen Sichtweisen

**Kulturelle Unterschiede**  
(Private Daten gehören den Firmen? US 76%, DE 22%)



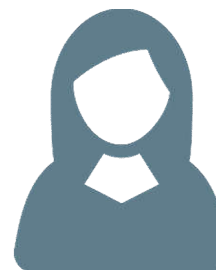
**Geschäftsmodelle**  
„Bezahlen mit persönlichen Daten“



# 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



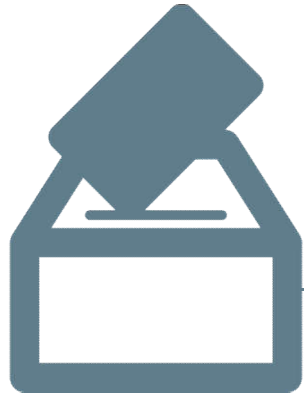
Zum Vergleich:

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



# Was sind die Problemfelder?

## → 3. Cyberwar



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

Cyberwar



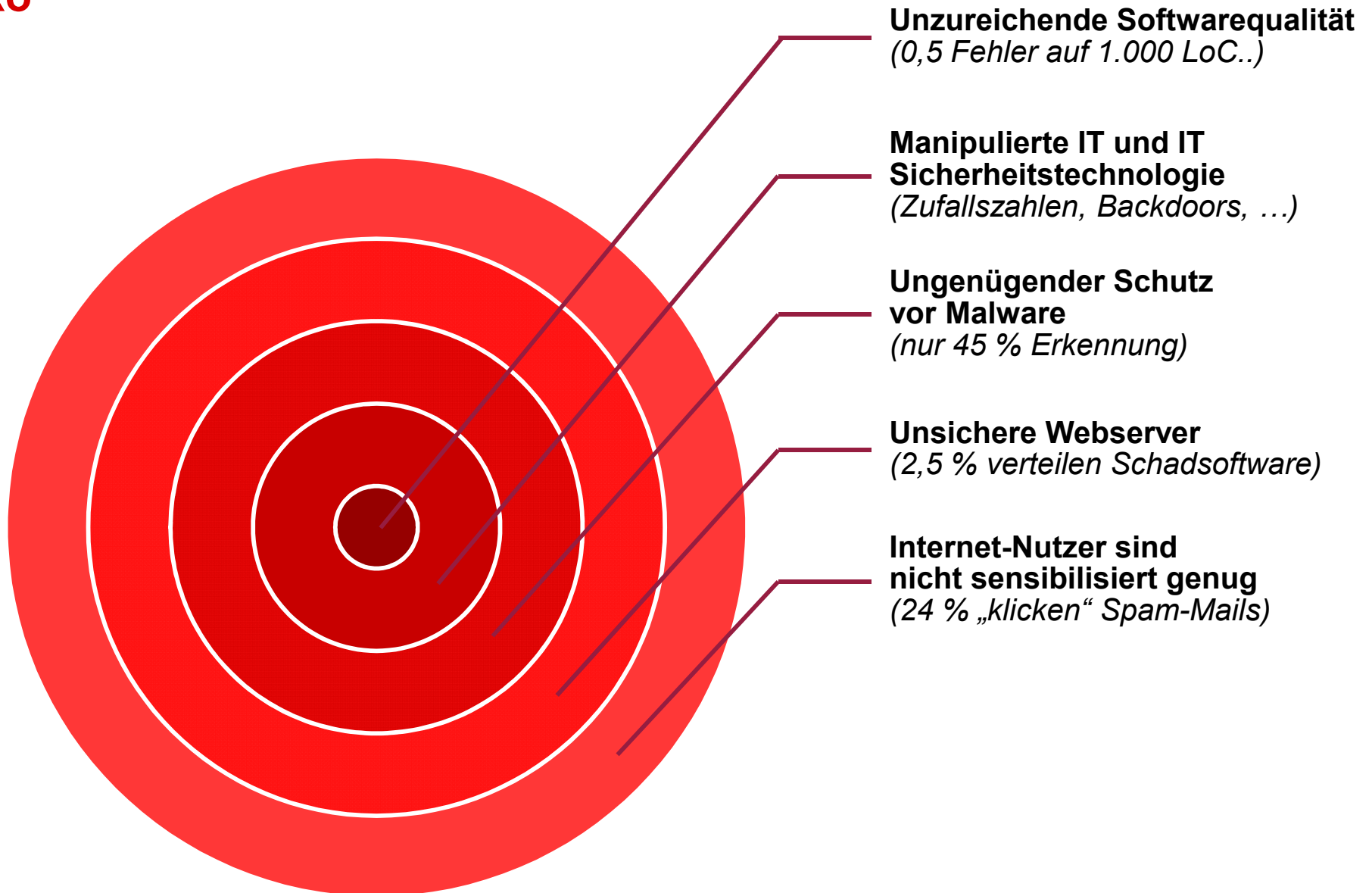
Angriffe auf Kritische Infrastrukturen  
z.B. Stromversorgung, Wasserversorgung, ...



# IT-Sicherheit

## → Die größten Herausforderungen

### Risiko



# IT-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



# Motivation

## → Eine Bestandsaufnahme

- **IT-Sicherheitsmarkt ist Hersteller dominiert & stark fragmentiert**
  - Für jedes der „20 Probleme“ muss jeweils eine Lösung erworben werden
  - Nicht alles harmoniert miteinander
- **Kann ein Markt gemeinsam geschaffen werden?**  
(durch Anwender und Hersteller)
  - Hürden:  
Know-How, Verbreitung, Kosten, Supportverfügbarkeit, Rolloutfähigkeit
- **Herausforderungen: Digitalisierung, Fintechs und i4.0**
  - Angriffsfläche vergrößert sich, Angriffe werden komplexer

**Was bereitet Ihnen als Anwender im Hinblick auf IT-Sicherheit Ihres Unternehmens die größte Sorge?**

# IT-Sicherheit

## → Situation DE/EU

IT-Sicherheitsindustrie USA

groß mit gewaltiger Schlagkraft

IT-Sicherheitsindustrie DE / EU

klein - mittelständisch

Know-how in DE/EU vorhanden

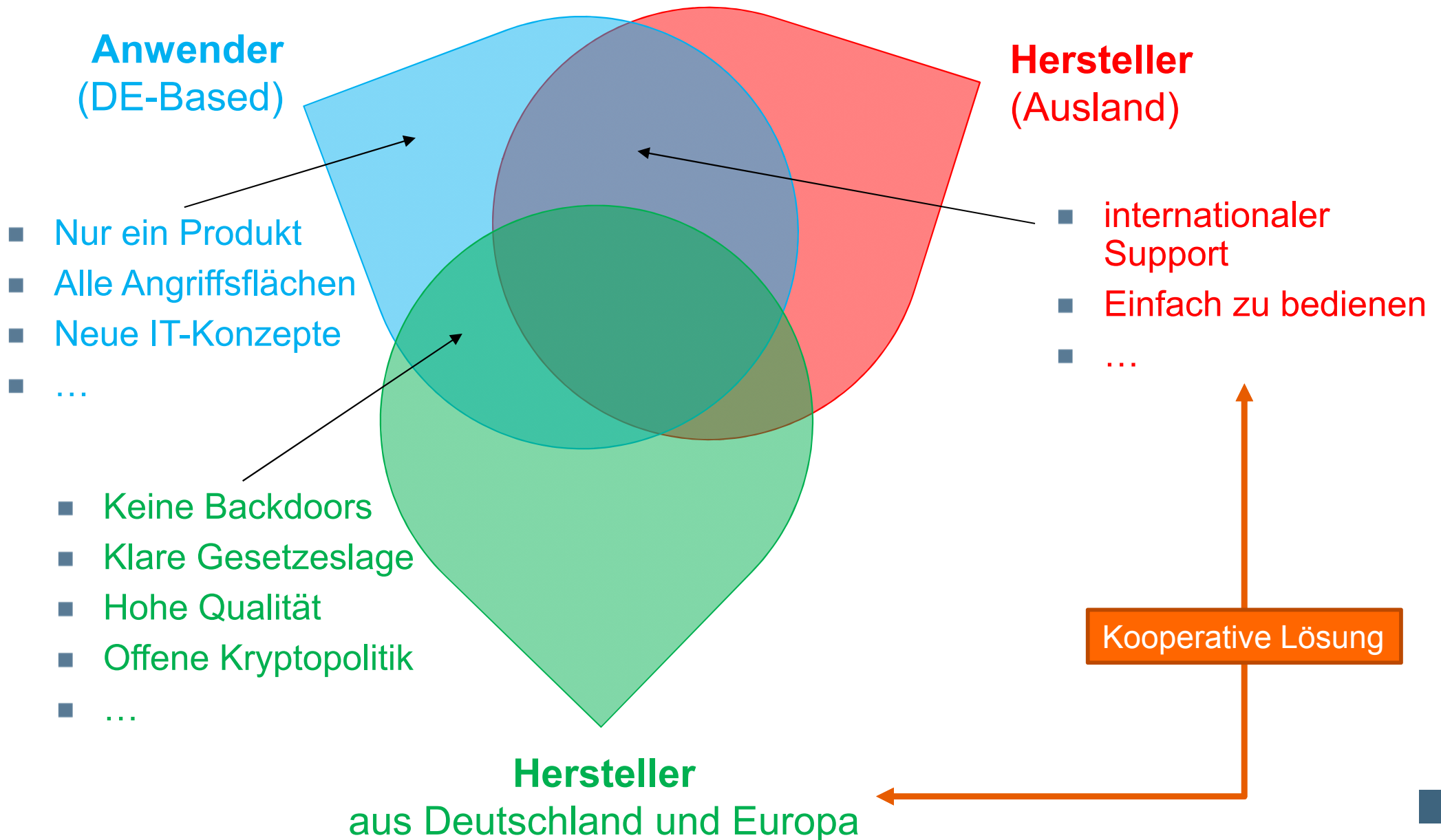
Kompetenz in DE/EU vorhanden

▶ Bündelung der Kräfte fehlt

▶ Beschaffungen der Großanwender richten sich bei **Kernprodukten** primär an USA/Israel

▶ Nischenprodukten an DE/EU

# Der Weg zum anforderungsgetriebenen → IT-Sicherheitsmarkt

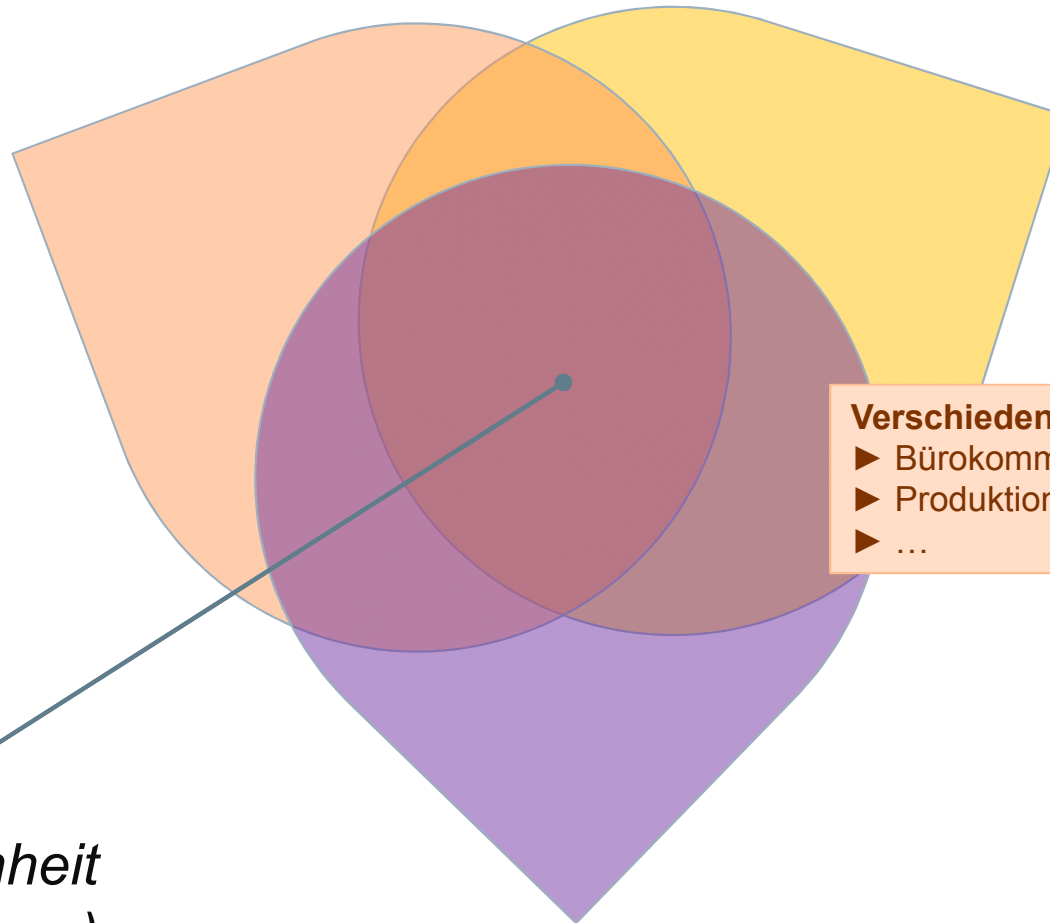


# Der Weg zum anforderungsgetriebenen

## → Bedürfnisse der Anwender unterschiedlich

Anforderungen  
& Bedürfnisse  
**Anwender A**

Anforderungen  
& Bedürfnisse  
**Anwender B**



**Verschiedene Perspektiven:**

- ▶ Bürokommunikation
- ▶ Produktion
- ▶ ...

*Deckungsgleichheit  
(der Bedürfnisse)*

**Synergien  
müssen  
geschaffen  
werden**

Anforderungen & Bedürfnisse  
**Anwender C**

# Das Manifest zur IT-Sicherheit

## → 2: Mehr wirkungsvolle Lösungen

- Gründe, die dafür sorgen, dass nicht mehr eingesetzt werden:
  - Probleme bei der Integration in Massenlösungen der US-Marktführer
  - Kein Vertrauen in die Wirkung bei bestimmten Herstellern
  - Zu viele unterschiedliche Produkte, die verwaltet werden müssen
  - Schlechte Bedienbarkeit der IT-Sicherheitslösungen
  - Fehlender internationaler Support

### Gemeinsame Aufgaben:

- **Enge Zusammenarbeit zwischen den Herstellern und Anwendern** von IT-Sicherheitslösungen, um **mehr angemessene und wirkungsvolle IT-Sicherheitslösungen** in den operativen Einsatz zu bringen
- **Artikulation von Anforderungen** und Wünschen durch die Anwender an die IT-Sicherheitshersteller, um funktionales Angebot von Lösungen mit den Anforderungen der Anwender in Einklang zu bringen
- **Zusammenarbeit mit den internationalen IT-Marktführern**, um eine optimale Integration in die Hardware und Software umsetzen zu können

- **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
  - ▶ hoher Grad der Vertrauenswürdigkeit
  
- **Kulturell gute Voraussetzungen**
  - ▶ traditionell verlässliche IT-Sicherheit
  - ▶ hohes Verständnis für IT-Sicherheit und Datenschutz
  - ▶ sehr viel Erfahrung bei der Umsetzung von IT-Sicherheitslösungen

# Das Manifest zur IT-Sicherheit

## → 3: Verschlüsselung hilft

- Verschlüsselung hilft, potenzielle Angriffsflächen zu reduzieren ...
- Wir brauchen flächendeckende Verschlüsselung für die Übertragung und Speicherung digitaler Werte
- Dazu brauchen wir Produkte, die einfach zu integrieren und zu nutzen sind

### Gemeinsame Aufgaben:

- Die Hersteller + Anwender von Verschlüsselungslösungen werden eng zusammenarbeiten, damit mehr Verschlüsselung zum Einsatz kommt
- Die IT-Sicherheitshersteller werden bei der Entwicklung zukünftiger Produkte die Anwender stärker einbeziehen, um für eine bessere Bedienbarkeit und einfache Integration zu sorgen
- Zukünftige Produkte müssen sicher, aber für den Nutzer möglichst transparent sein (wie z.B. der Airbag im Auto)

Technologieanalyse IT-Sicherheit in DE	Bedeutung für die Zukunft	Technologischer Vorsprung in DE	Marktstärke der dt. Unternehmen	Abstand zwischen Soll- und Ist-Zustand ( $\Delta$ )
SICHERE ANBINDUNG MOBILER USER / TELEARBEITER	Green	Light Green	Yellow	Light Green
LAYER3-VPN	Green	Light Green	Yellow	Light Green
LAYER2-ENCRYPTION	Green	Light Green	Yellow	Yellow
DATENDIODE	Light Green	Light Green	Light Green	Light Green
FIREWALL	Green	Yellow	Yellow	Yellow
IPS/IDS	Green	Yellow	Red	Red
SICHERER BROWSER/RECOBS	Green	Light Green	Light Green	Yellow
VIRTUELLE SCHLEUSE	Light Green	Yellow	Yellow	Red
AUTHENTIFIKATION	Green	Light Green	Yellow	Red
SICHERE ANBINDUNG ZWISCHEN ANBIETER UND ANWENDER	Green	Yellow	Yellow	Yellow
HARDWARE-SICHERHEITSMODUL (HSM)	Green	Light Green	Light Green	Yellow
PUBLIC-KEY-INFRASTRUKTUR (PKI)	Green	Light Green	Light Green	Red
AV UND PERSONAL FIREWALL	Yellow	Yellow	Yellow	Yellow
EXPLOIT PROTECTION / SICHERER BROWSER	Green	Green	Red	Red
DEVICE UND PORTKONTROLLE	Green	Yellow	Red	Yellow
FULL DISK ENCRYPTION	Green	Yellow	Yellow	Red
FILE & FOLDER ENCRYPTION	Green	Yellow	Yellow	Yellow
VOLL-VIRTUALISIERUNG / TRUSTEDCOMPUTING, SEPERATION	Green	Yellow	Yellow	Yellow
DATA LEAKAGE PREVENTION	Green	Yellow	Yellow	Red
E-MAIL-VERSCHLÜSSELUNG	Green	Yellow	Yellow	Red
SICHERES LOGON (SMARTCARD ETC.)	Green	Yellow	Light Green	Red
REMOTE ACCESS / SECURED VPN	Green	Light Green	Yellow	Yellow
APP SECURITY / SECURE MARKETPLACE	Green	Yellow	Yellow	Red
SICHERE PLATTFORM	Green	Light Green	Yellow	Red
CLOUD ENCRYPTION	Green	Light Green	Light Green	Red
VOICE ENCRYPTION	Green	Light Green	Yellow	Yellow
SECURE INSTANT MESSAGING	Green	Yellow	Yellow	Red
MOBILE DEVICE MANAGEMENT	Green	Green	Yellow	Red
BASISTECHNOLOGIE (SECURE EXECUTION ENVIRONMENT)	Green	Yellow	Yellow	Green

- **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-Sicherheitsinfrastrukturen für VPNs, E-Mail-Verschlüsselung, Domänenzertifikate, usw. sollten in europäischer Verantwortung liegen
- Über die IT-Sicherheitsinfrastrukturen können flächendeckende Angriffe umgesetzt werden, da sie den Vertrauensanker in der heutigen Internetwelt bilden

### Gemeinsame Aufgaben:

- Bei den eingesetzten IT-Sicherheitslösungen wird das **Attribut IT-Sicherheitsinfrastruktur** in Europa in der Zukunft ein besonderer Wert zugemessen
- Deutschland und Europa müssen in gewissen Teilen **technologisch souverän werden und dauerhaft bleiben**
- Die EU muss kurz bis mittelfristig Maßnahmen ergreifen, um **die Souveränität im Bereich IT-Sicherheit aufzubauen und zu sichern**



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# **Das Manifest zur IT-Sicherheit**

**→ Situation, Stärken, Vorgehensweisen, ...**

**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>

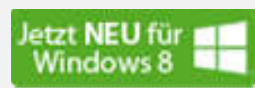
**if(is)**  
internet-sicherheit.

## Wir empfehlen unsere kostenlose App securityNews

- Kostenlose App vom Institut für Internet-Sicherheit
- Aktuelle Sicherheitshinweise für Smartphone, Tablet, PC und Mac
- Warnung vor Sicherheitslücken in Standardsoftware, dank Schwachstellenampel
- Konkrete Anweisungen für Privatanwender und Unternehmen



securityNews



## Besuchen und abonnieren Sie uns :-)

### WWW

<https://www.internet-sicherheit.de>

### Facebook

<https://www.facebook.com/Internet.Sicherheit.ifis>

### Twitter

<https://twitter.com/ifis>

### Google+

<https://plus.google.com/107690471983651262369/posts>

### YouTube

<https://www.youtube.com/user/InternetSicherheitDE/>

## Quellen Bildmaterial

Eingebettete Piktogramme:

- Institut für Internet-Sicherheit – if(is)
- Icon made by Freepik from [www.flaticon.com](http://www.flaticon.com)

## IT-Sicherheitsstrategie für Deutschland

Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe

Ein Aspekt der IT-Sicherheitsstrategie für DE

<https://www.internet-sicherheit.de/downloads/publikationen-vortraege/dokumente-2015.html>