

# Wie viel IT-Sicherheit und Vertrauenswürdigkeit brauchen wir für unsere komplexe digitale Zukunft?

*Prof. Dr. (TU NN)*

**Norbert Pohlmann**

*Professor für Cyber-Sicherheit und Leiter des Instituts für Internet-Sicherheit – if(is), Westfälische Hochschule, Gelsenkirchen*

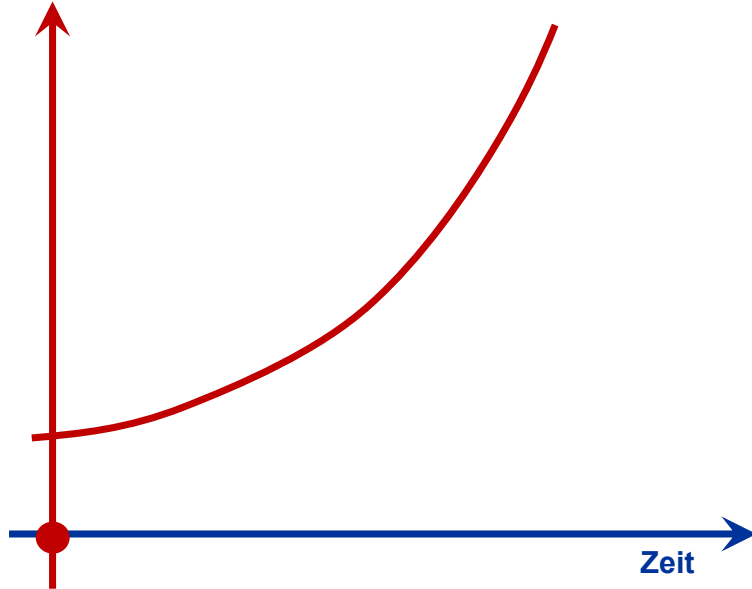
*Vorstandsvorsitzender Bundesverband IT-Sicherheit - TeleTrust*

*Vorstand im Verband der Internetwirtschaft - eco*

# Cyber-Sicherheitslage

## → Eine Einschätzung

Risiko durch  
die Digitalisierung



- *IT-Systeme und -Infrastrukturen sind nicht sicher genug konzipiert, aufgebaut, konfiguriert und upgedatet (... gegen zunehmend intelligente Angriffe)*
- *IT-Systeme und -Infrastrukturen werden immer komplexer (... Angriffsfläche wird größer)*
- *Methoden der Angreifer werden ausgefeilter (... erfolgreiche kriminelle Ökosysteme)*
- *Angriffsziele werden kontinuierlich lukrativer (... immer mehr digitale Werte auf IT-Systeme)*
- *Es fällt uns immer schwerer festzustellen, was echt und falsch ist (... KI verändert das Internet)*

# IT-Sicherheitszahlen

## → Übersicht und ein Gedankenspiel

- Zwei wichtige Zahlen zur IT-Sicherheit

### Cybercrimeschaden in 2024

**179 Mrd. €**

Verursacht durch Cyber-Attacken in Deutschland, rund 20% mehr als im Vorjahr.

Studie Wirtschaftsschutz (Bitkom, 2024)



### Investition in IT-Sicherheit

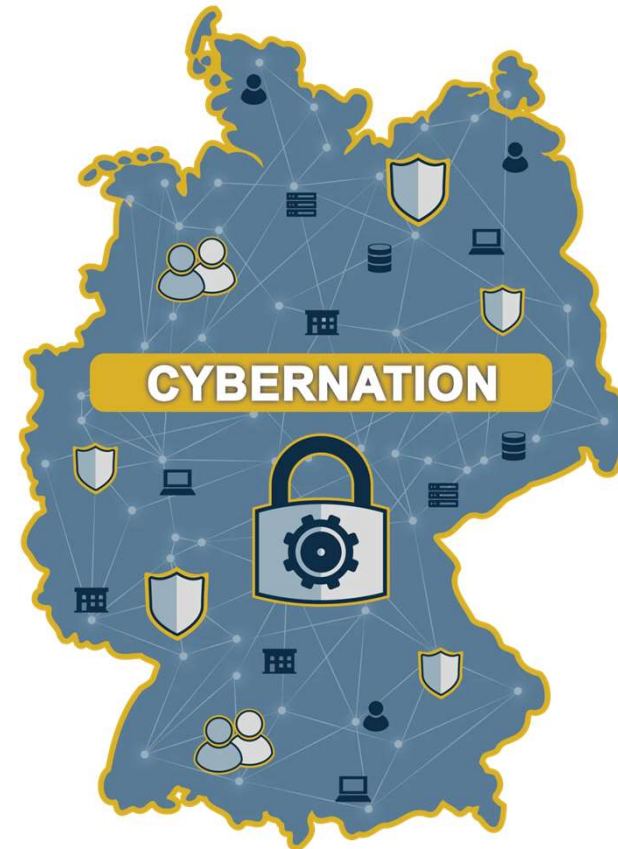
**11,2 Mrd. €**

Im Jahr 2024 in Deutschland, rund 14% mehr als im Vorjahr.

Presseinformationen (Bitkom, 2024)



- **Gedankenexperiment:**
  - Wir verdoppeln die Investitionen:  
*von 11,2 Milliarden auf 22,4 Milliarden*
- **Vermutung:**
  - Dadurch wird der Schaden um die Hälfte reduziert:  
*von 179 Milliarden auf 89,5 Milliarden*
- **Ergebnis:**
  - Diese Investition zahlt sich aus:  
*78,3 Milliarden Gewinn*



# E-Mail-Sicherheitsjahr 2025

## → Übersicht

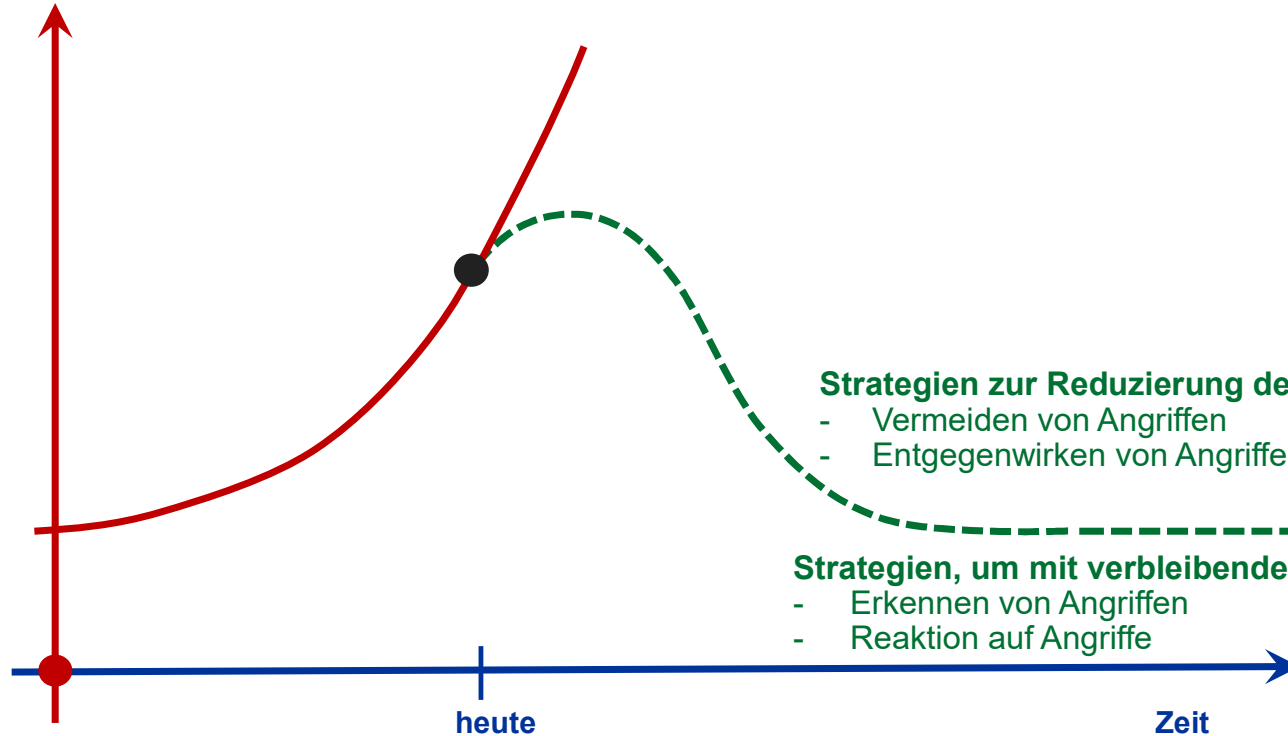
- BSI, Bitkom und eco haben zusammen das E-Mail-Sicherheitsjahr 2025 ausgerufen.
- Wir (eco / BSI) haben **Workshops beim BSI** durchgeführt.
  - **E-Mail-Provider**  
(Henne-Ei, Business ...)
  - **Hoster**  
(vertreten die Masse – KMU, Handwerk ...)
  - **Große Unternehmen**  
(DNSSEC ...)
- Am 22.08. eine Pressekonferenz beim eco in Berlin:
  - Hall of Fame
- Im September+ werden sehr viele Veranstaltungen sein.



# Cyber-Sicherheitsstrategien

## → Übersicht

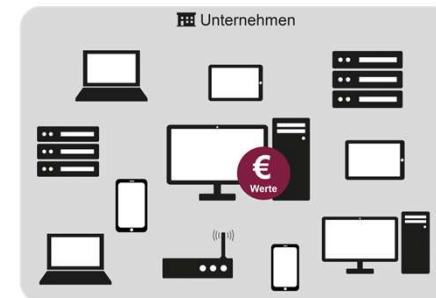
Risiko durch  
die Digitalisierung



# Cyber-Sicherheitsstrategie

## → Vermeiden von Angriffen

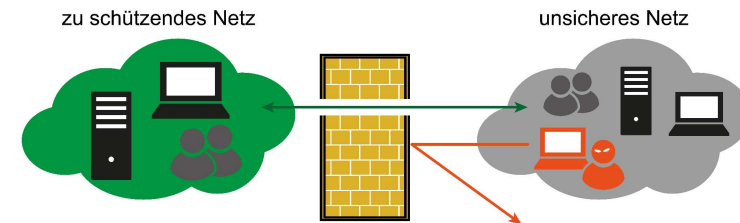
- Mit Hilfe der Vermeidungsstrategie wird eine **Reduzierung der Angriffsfläche** und damit die **Reduzierung der Risiken** erreicht.
- Die Herausforderung besteht darin, **die IT so einzurichten**, dass **alles wirklich *Notwendige* umgesetzt**, aber **alles andere *aktiv* vermieden** wird.



### Cyber-Sicherheitsmechanismen

- **Digitale Datensparsamkeit**
- **Fokussierung** (ca. 5 % sind besonders schützenswert)
- **Nur sichere IT-Technologien, -Produkte und -Dienste verwenden**
- **Reduzierung von IT-Möglichkeiten** (SW, Rechte, Kommunikation ...)

- **Sicherheitsbewusste Mitarbeiter**



# Cyber-Sicherheitsstrategie

## → Entgegenwirken von Angriffen

- Das Entgegenwirken von Angriffen ist die meistverwendete Cyber-Sicherheitsstrategie, um das vorhandene Risiko zu minimieren und damit Schäden zu vermeiden.
- Dazu werden Cyber-Sicherheitsmechanismen verwendet, die eine **hohe Wirkung** gegen **bekannte Angriffe** zur Verfügung stellen und damit die Werte angemessen schützen.

### Cyber-Sicherheitsmechanismen

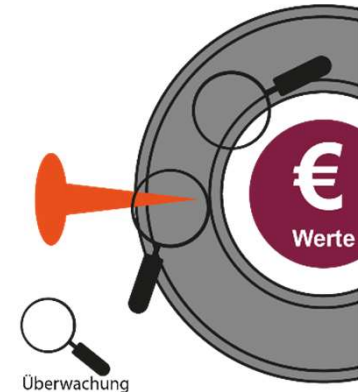
- **Verschlüsselung** (*in Motion, at Rest, in Use*)
- **Multifaktor-Authentifikationsverfahren**
- **Anti-Malware-Lösungen** (*neue Konzepte ... End-Point Security*)
- **Anti-DDoS-Verfahren** (*gemeinsame Strukturen*)
- **Zero Trust-Prinzipien** (*TCB, Virtualisierung, Authentifikation aller Entitys ...*)
- **Confidential Computing** (*Basis CPU, Daten/Code verschlüsselt/überprüft*)
- **Digitale Signaturverfahren / Zertifikate** (*E-Mail, SSI ...*) – PKI, BC
- **Hardware-Sicherheitsmodule** (*Smartcard, TPM, HSM, Smartphone-SM*)
- **EU-Wallet** (*jeder Bürger in der EU bis Ende 2026*)



# Cyber-Sicherheitsstrategie

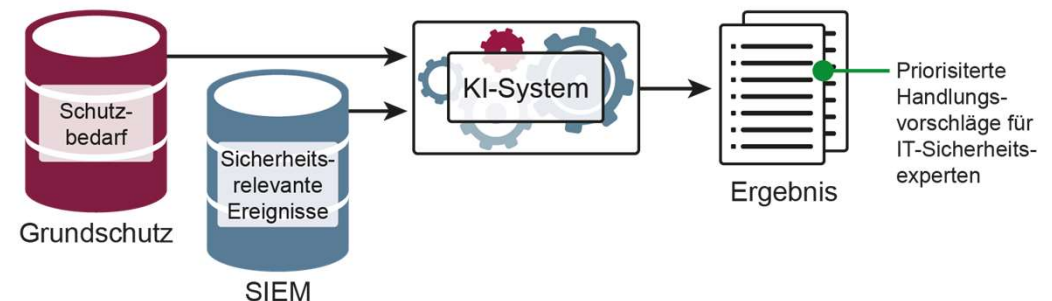
## → Erkennen von Angriffen

- Wenn Angriffen nicht vollständig entgegengewirkt werden oder eine Vermeidung nicht ausreichend die Angriffsfläche reduzieren kann, dann bleibt noch die Strategie, **Angriffe zu erkennen** und zu versuchen, den Schaden so schnell wie möglich zu minimieren.
- Hier ist die Idee, in einem definierten Bereich (IT- und Kommunikationsinfrastruktur, IT-Endgeräte, ...) nach **Angriffssignaturen** oder **Anomalien** zu suchen.



## Cyber-Sicherheitsmechanismen

- **Frühwarn- und Lagebildsysteme**
- **Bewertung von sicherheitsrelevanten Ereignissen (Priorisierung)**



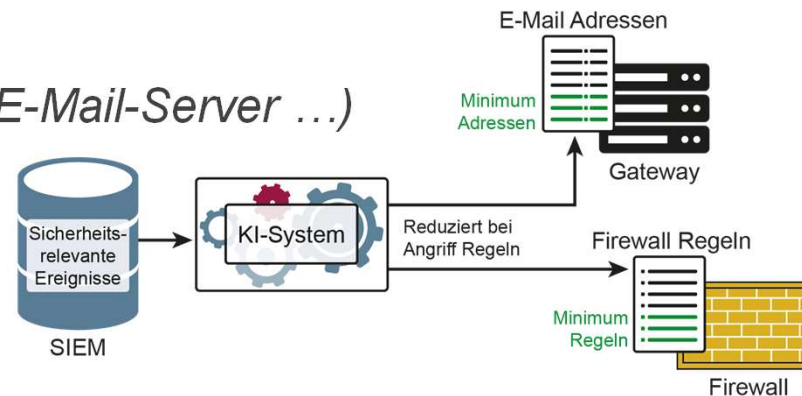
# Cyber-Sicherheitsstrategie

## → Reaktion auf Angriffe

- Wenn Angriffe erkannt werden, sollte so schnell wie möglich mit passenden Aktionen reagiert werden, die den **Schaden** im optimalen Fall noch **verhindern** oder zumindest die Höhe **reduzieren**.

## Cyber-Sicherheitsmechanismen

- **Automatisierte Reaktion** (Firewall, E-Mail-Server ...)



- **Digitale Forensik** (Maßnahmen optimieren, Schwachstellen schließen)
- **Definition von Befugnissen, Informationsflüsse, Entscheidungsprozess und Kommunikationsstrategien**
- **Notfallplanung definieren und trainieren**

# Der Einsatz von IT basiert auf Vertrauen

## → Vertrauenswürdigkeit schafft Vertrauen

**Status Quo:** Aufgrund der Digitalisierung erhöht sich der Grad an Komplexität, wodurch es für den Anwender zunehmend schwieriger wird, einzelne **IT-Lösungen** und deren Hintergründe **verstehen** und **bewerten** zu können.

**Folge:** Die **Unsicherheit** macht den Menschen Angst und **schränkt** sie in ihrer **Handlungsfähigkeit ein**.

**Fazit:** Vertrauen ist unerlässlich, um handlungsfähig sein zu können.

**Wichtig:** Anwender wollen Vertrauen können.

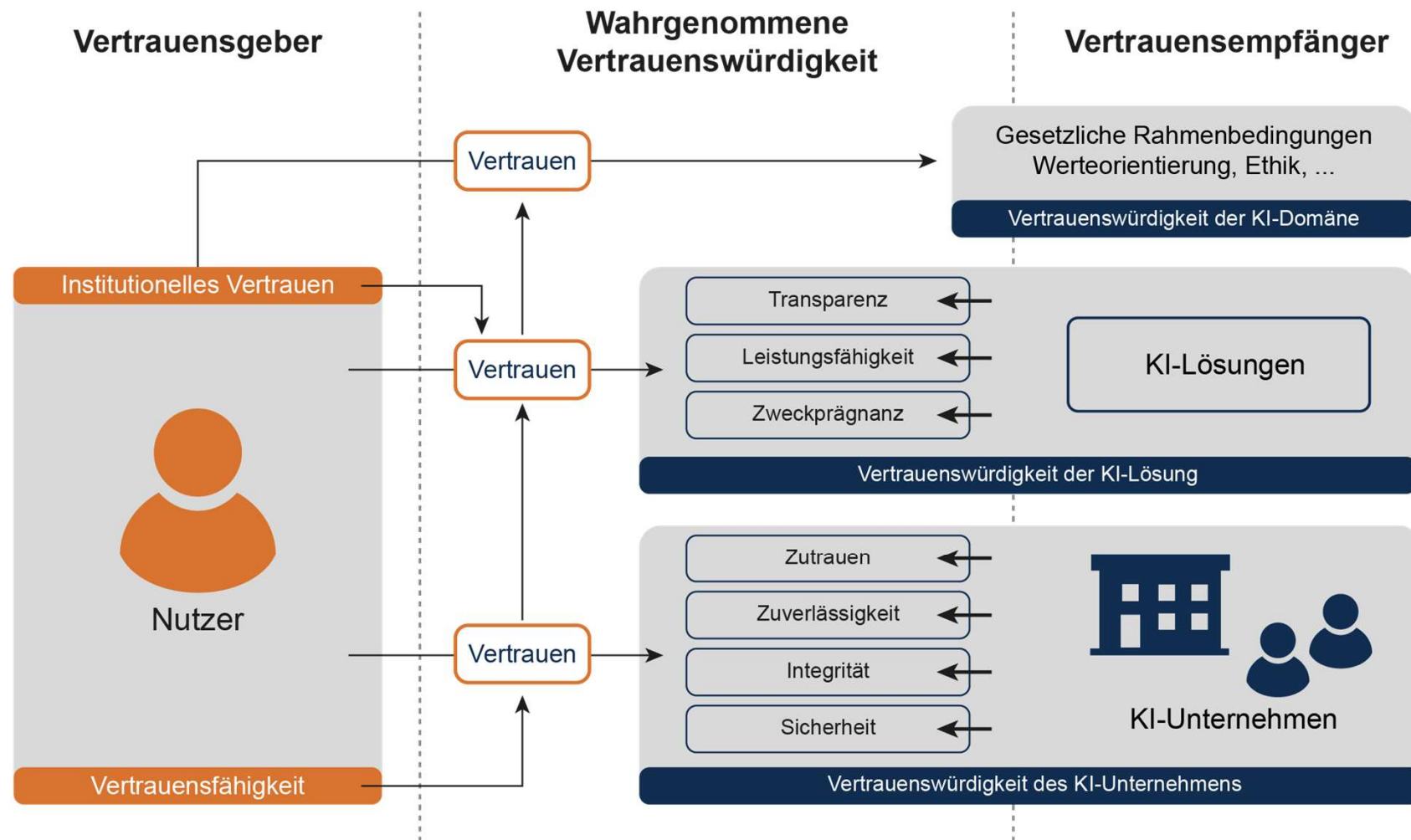
**Das bedeutet:** IT-Hersteller müssen vertrauenswürdig agieren.

**Fazit:** Damit der Anwender ein gerechtfertigtes Vertrauen in **IT-Hersteller** sowie deren **IT-Lösung** aufbauen kann, müssen diese alles tun, um ihre **Zuverlässigkeit, Ehrlichkeit** und ihre **Qualifikation unter Beweis zu stellen**.



# Der Einsatz von IT basiert auf Vertrauen

## → Vertrauenswürdigkeitsmodell



# IT-Sicherheit für Anwender/Anbieter → Marktplatz IT-Sicherheit

## Gemeinsam für mehr IT-Sicherheit

Der zentrale Marktplatz für IT-Sicherheit bündelt alles, was Sie brauchen:  
Aktuelles IT-Sicherheitswissen, bewährte IT-Sicherheitstools und praxisnahe IT-  
Sicherheitslösungen – kompakt, verständlich und einsatzbereit.  
Schützen Sie sich jetzt effektiv vor Cyberangriffen – mit Wissen, Werkzeugen und Strategien  
an einem Ort.

Mehr erfahren ▼



- Ziel: *die über 4 Mio. Unternehmen im deutschsprachigen Raum* zu unterstützen und ihre **IT-Sicherheit kontinuierlich zu gewährleisten**.
- Es werden **substanzielle Informationen, umfangreiches IT-Sicherheitswissen** und **hilfreiche IT-Sicherheits-Tools** *kostenlos* zur Verfügung gestellt.
- Darüber hinaus bringt der Marktplatz IT-Sicherheit, **Anwenderunternehmen** und **IT-Sicherheitslösungsanbieter** zusammen und *fördern einen regen Austausch*.

# Wie viel IT-Sicherheit und Vertrauenswürdigkeit brauchen wir für unsere komplexe digitale Zukunft?

*„Deutlich mehr als heute“*

*Prof. Dr. (TU NN)*

**Norbert Pohlmann**

***Professor für Cyber-Sicherheit und Leiter des Instituts für Internet-Sicherheit – if(is), Westfälische Hochschule, Gelsenkirchen***

***Vorstandsvorsitzender Bundesverband IT-Sicherheit - TeleTrust***

***Vorstand im Verband der Internetwirtschaft - eco***

# Anhang / Credits

## Wir empfehlen

### Cyber-Sicherheit

Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2022  
<https://norbert-pohlmann.com/cyber-sicherheit/>



### 7. Sinn im Internet (Cyberschutzraum)

<https://www.youtube.com/cyberschutzraum>



### Master Internet-Sicherheit

<https://it-sicherheit.de/master-studieren/>



### Glossar Cyber-Sicherheit

<https://norbert-pohlmann.com/category/glossar-cyber-sicherheit/>



### It's all about Trust!

<https://vertrauenswürdigkeit.com/>



## Quellen Bildmaterial

Eingebettete Piktogramme: Institut für Internet-Sicherheit – if(is)

## Besuchen und abonnieren Sie uns :-)

### WWW

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

### Facebook

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

### Twitter

[https://twitter.com/\\_ifis](https://twitter.com/_ifis)

<https://twitter.com/ProfPohlmann>

### YouTube

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

### Prof. Norbert Pohlmann

<https://norbert-pohlmann.com/>



Der Marktplatz IT-Sicherheit

## Der Marktplatz IT-Sicherheit

Alles rund um IT-Sicherheit: Wissensaustausch, Unterstützung, IT-Sicherheitsanbieter & -Lösungen, News/Artikel/Blogs, Veranstaltungen.  
<https://www.it-sicherheit.de/>