

Aktuelle Cybersicherheitslage und Cyber-Sicherheitsstrategien zur Reduzierung der Risiken

Prof. Dr. (TU NN)

Norbert Pohlmann

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

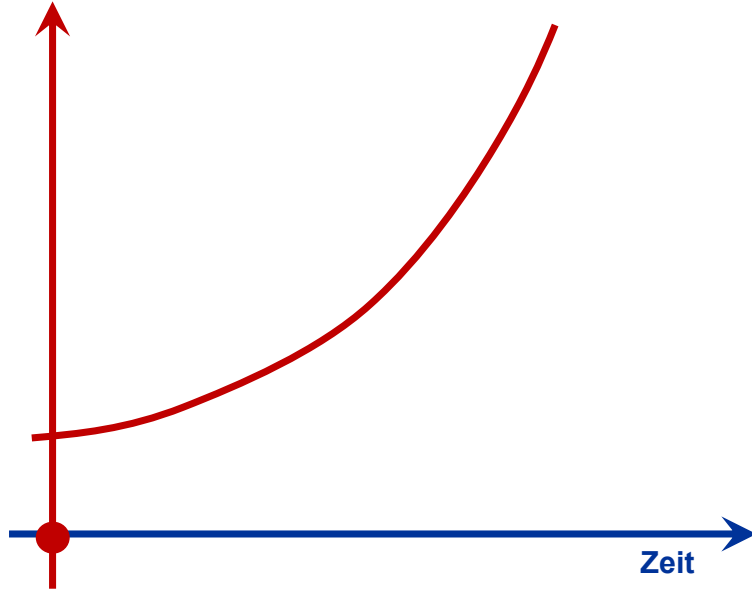
Vorstandsvorsitzender Bundesverband IT-Sicherheit - TeleTrust

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)*

Softwarefehler - Update - CrowdStrike

→ Ein Beispiel für die schlechte Cyber-Sicherheitslage

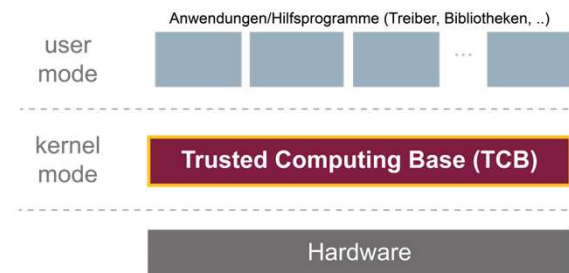
- Ein **Softwarefehler** in einem Update der IT-Sicherheitsfirma CrowdStrike hat im letzten Jahr dafür gesorgt, dass nicht nur deren End Point-Sicherheit, sondern auch **8,5 Millionen Microsoft-Systeme** und daraus resultierend flächendeckend kritische Anwendungen **nicht mehr funktioniert haben** (1,5 Milliarden Euro Schaden).

Verschiedene Sichtweisen auf diesen Vorfall

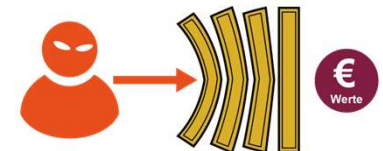
CrowdStrike ... *nicht gut genug getestet, flache Update-Strategie*



Microsoft ... *alte monolithische Betriebssysteme, fallen bei einen SW-Fehler aus*



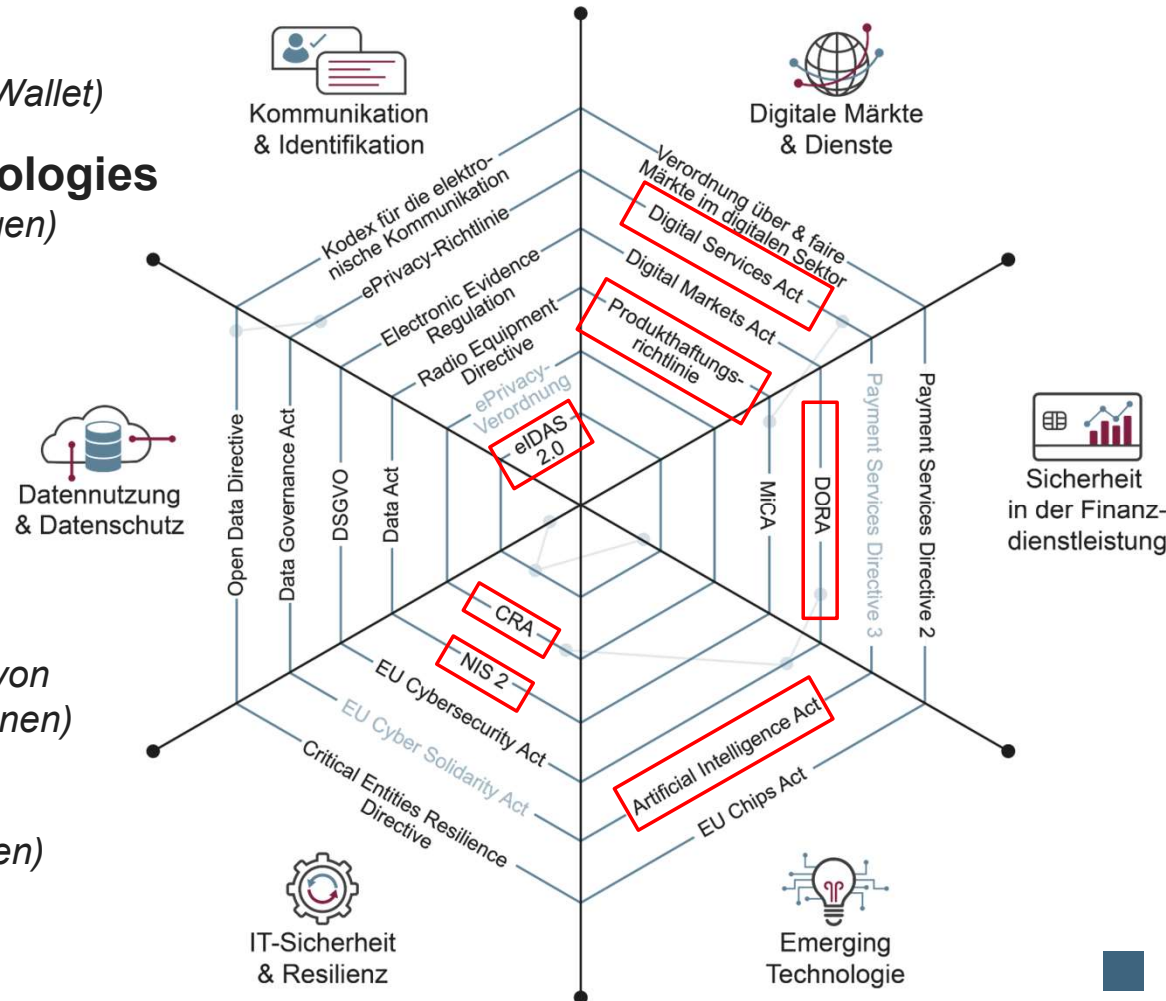
Anwender ... *keine Redundanz für kritische Anwendungen*



Die Lösung des Gesetzgebers

→ Das IT-Sicherheitsnetz wird von der EU vorgegeben

- **Wirtschaft fördern**
(z.B. Aufbau des Ökosystems rund um die Digitale Wallet)
- **Rahmen festlegen für Emerging Technologies**
(z.B. IT-Sicherheit, Vertrauen u. ethische Bedingungen)
- **Funktionalität sicherstellen**
(z.B. Leistungsfähigkeit des Finanzsektors)
- **Recht an IT-Rechtsentwicklung anpassen**
(z.B. Definition von Software als Produkt)
- **Fake News und Kriminalität reduzieren**
(z.B. Verbreitung illegaler Inhalte und Manipulation von Informationen durch Plattformen sowie Suchmaschinen)
- **IT-Sicherheit und Vertrauen schaffen**
(z.B. SBOMs und Berichts- bzw. Transparenzpflichten)
- **Alternative Systeme fördern**
(z.B. Open-Source)



IT-Sicherheitszahlen

→ Übersicht *und* ein Gedankenexperiment

Schadenssumme in 2024

179 Mrd. €

Verursacht durch Cyber-Attacks
in Deutschland.

Studie Wirtschaftsschutz (Bitkom, 2024)

Investition in IT-Sicherheit

11,2 Mrd. €

Im Jahr 2024 in Deutschland.

Presseinformationen (Bitkom, 2024)

Gedankenexperiment:

Wir verdoppeln das Investment: von 11 Mrd. *auf 22. Mrd.*

Annahme:

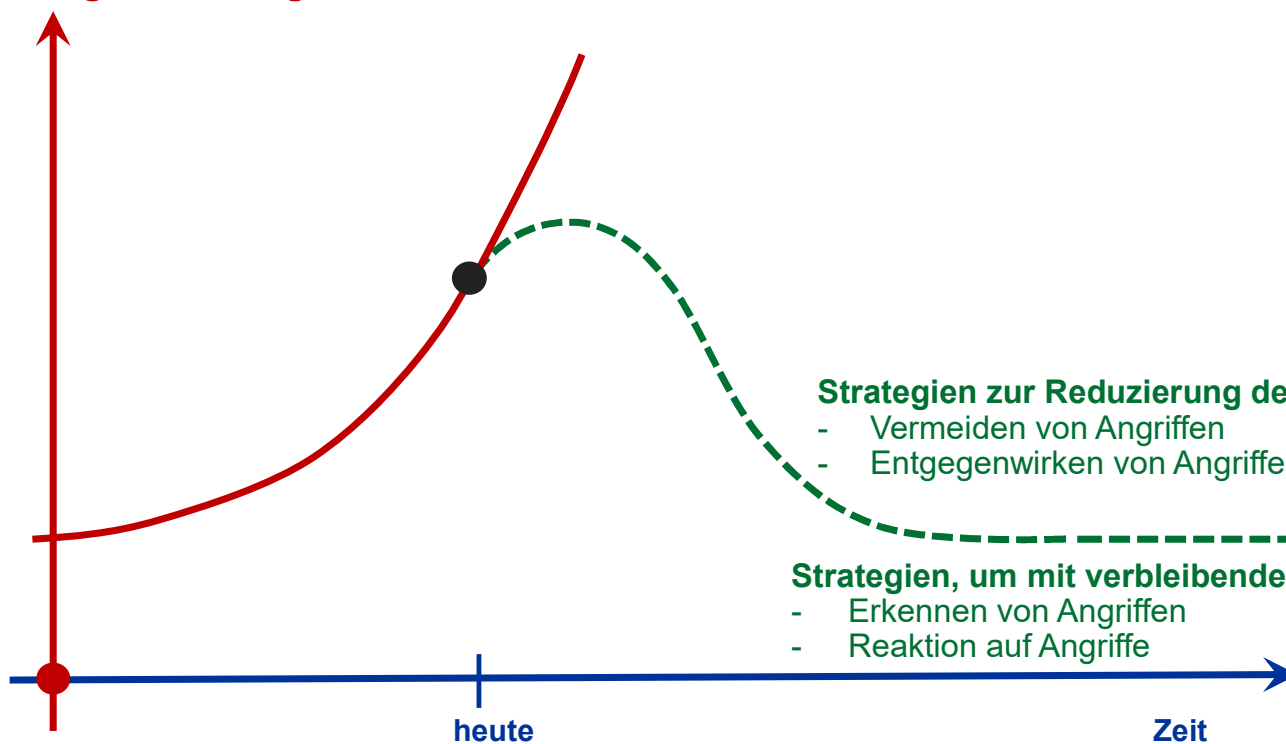
Damit werden die Schäden auf die Hälfte reduziert: von 179 Mrd. *auf 90 Mrd.*

Ein Investment, das sich sehr lohnt: 78 Mrd. Gewinn

Cyber-Sicherheitsstrategien

→ Übersicht

Risiko durch
die Digitalisierung



Strategien zur Reduzierung der Risiken

- Vermeiden von Angriffen
- Entgegenwirken von Angriffen

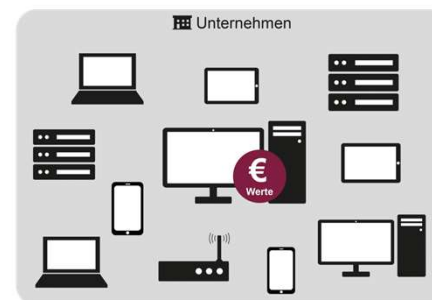
Strategien, um mit verbleibenden Risiken umzugehen

- Erkennen von Angriffen
- Reaktion auf Angriffe

Cyber-Sicherheitsstrategie

→ Vermeiden von Angriffen

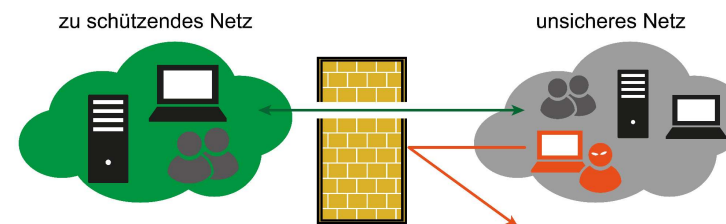
- Mit Hilfe der Vermeidungsstrategie wird eine **Reduzierung der Angriffsfläche** und damit die **Reduzierung der Risiken** erreicht.
- Die Herausforderung besteht darin, **die IT so einzurichten**, dass **alles wirklich *Notwendige* umgesetzt**, aber **alles andere *aktiv* vermieden** wird.



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

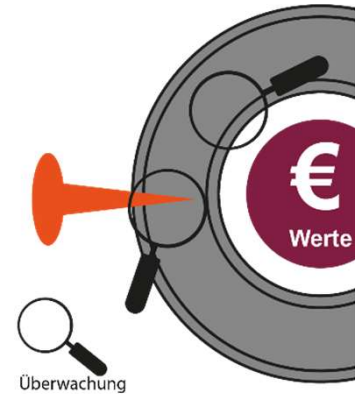
- **Verschlüsselung** (*in Motion, at Rest, in Use*)
- **Multifaktor-Authentifikationsverfahren**
- **Anti-Malware-Lösungen** (*neue Konzepte ... End-Point Security*)
- **Anti-DDoS-Verfahren** (*gemeinsame Strukturen*)
- **Zero Trust-Prinzipien** (*TCB, Virtualisierung, Authentifikation aller Entitys ...*)
- **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

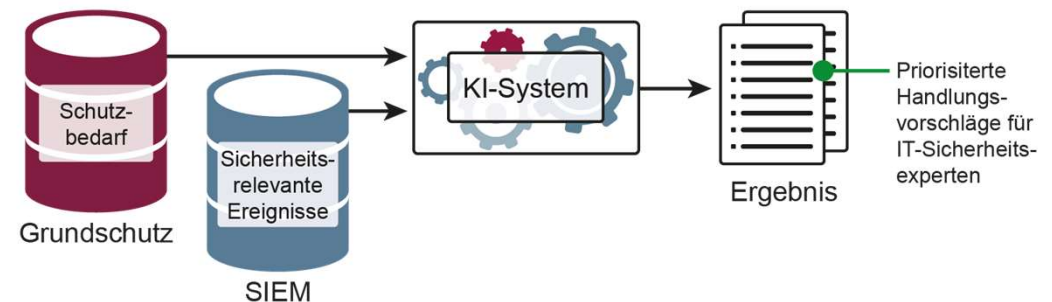
→ Erkennen von Angriffen

- 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)**



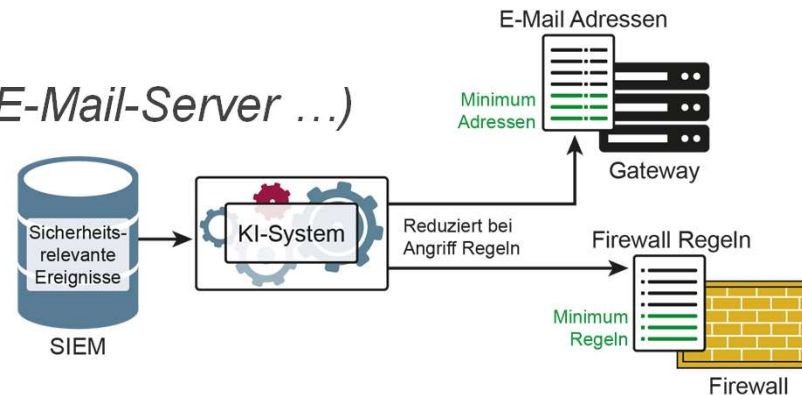
Cyber-Sicherheitsstrategie

→ 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**

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

Der Marktplatz IT-Sicherheit

Alles rund um IT-Sicherheit: Wissensaustausch, Unterstützung, IT-Sicherheitsanbieter & -Lösungen, News/Artikel/Blogs, Veranstaltungen.

Suchen nach (Unternehmen, News, Ratgebern,...)



Gemeinsam für mehr IT-Sicherheit

- Ziel: *alle 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*.

Aktuelle Cybersicherheitslage und Cyber-Sicherheitsstrategien zur Reduzierung der Risiken

„Gemeinsam für mehr IT-Sicherheit“

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

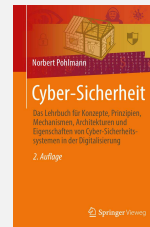
Vorstand im Verband der Internetwirtschaft - eco

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://vertrauenswuerdigkeit.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/ProfPohlmann>

YouTube

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

Prof. Norbert Pohlmann

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

www.it-sicherheit.de
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/>