TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-Konferenz 2023

29.06.2023, Berlin

Impulsvortrag: Neue IT-Sicherheitskonzepte

(Die wahren Probleme der IT-Sicherheit)

Prof. Dr. (TU NN)

Norbert Pohlmann

TeleTrusT-Vorstandsvorsitzender

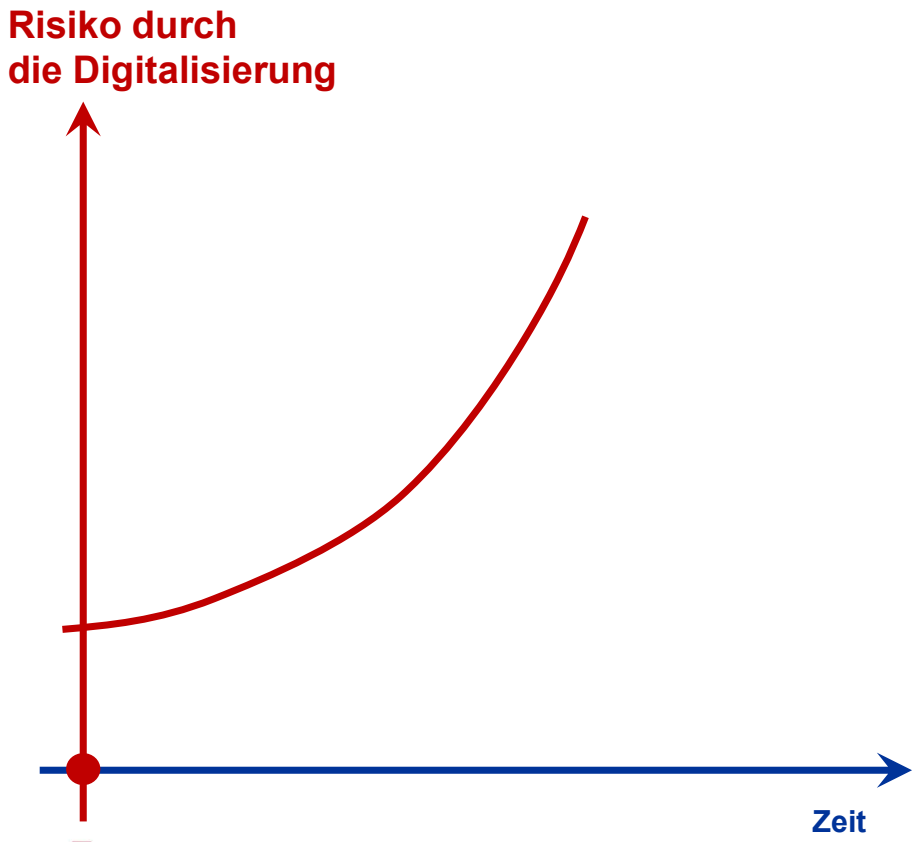
Professor für *Cyber-Sicherheit* und

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

if(is) internet-sicherheit.

Immer mehr Risiken durch die Digitalisierung

→ Eine Einschätzung



- ***IT-Systeme und -Infrastrukturen sind nicht sicher genug konzipiert, aufgebaut, konfiguriert und upgedatete***
  (… gegen intelligente Angreifer)
- ***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)

Immer mehr Risiken durch die Digitalisierung
→ Gegebenheiten

- **Investment in IT-Sicherheit sollte deutlich mehr sein**
  - 7 % vom IT-Budget ist zu wenig

- **Monopolisten ↔ Local Champions**
  - die Integration von IT-Sicherheitslösungen in Standardsoftware der Monopolisten ist schwierig
  - kein internationaler Support

- *…*

Immer mehr Risiken durch die Digitalisierung
→ Notwendigkeiten

- **Souveräne IT-Sicherheitstechnologie**
  - wie brauchen mehr innovative IT-Sicherheitstechnologien für ein Know-how-Land wie DE
  - die EU
  - mehr Förderungen für angemessene IT-Sicherheitslösungen,
  um uns souverän schützen zu können

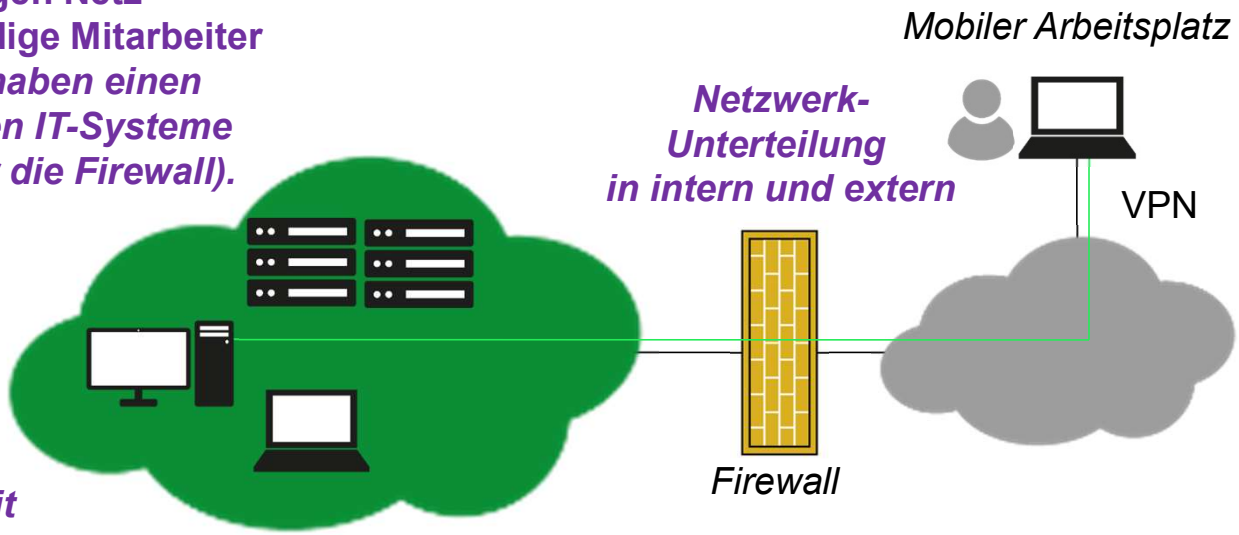
- **Erfolgreiche Ökosysteme in der EU etablieren**
  - eigene erfolgreiche Märkte generieren und internationalisieren … siehe EU-Wallet

- *…*

IT-Sicherheits-Paradigma

→ Perimeter-Sicherheit: Traditionell verwendetes Sicherheitsmodell

Alle IT-Systeme stehen im vertrauenswürdigen Netz und nur vertrauenswürdige Mitarbeiter des Unternehmens haben einen Zugriff auf die internen IT-Systeme (zum Internet nur über die Firewall).



Netzwerk-Unterteilung in intern und extern

Zugang zum internen Unternehmensnetzwerk mittels VPN

Weniger IT-Sicherheit im internen Netz und deren IT-Systemen, weil als vertrauenswürdig eingestuft.

Unternehmensnetzwerk
(intern)

Internet
(extern)

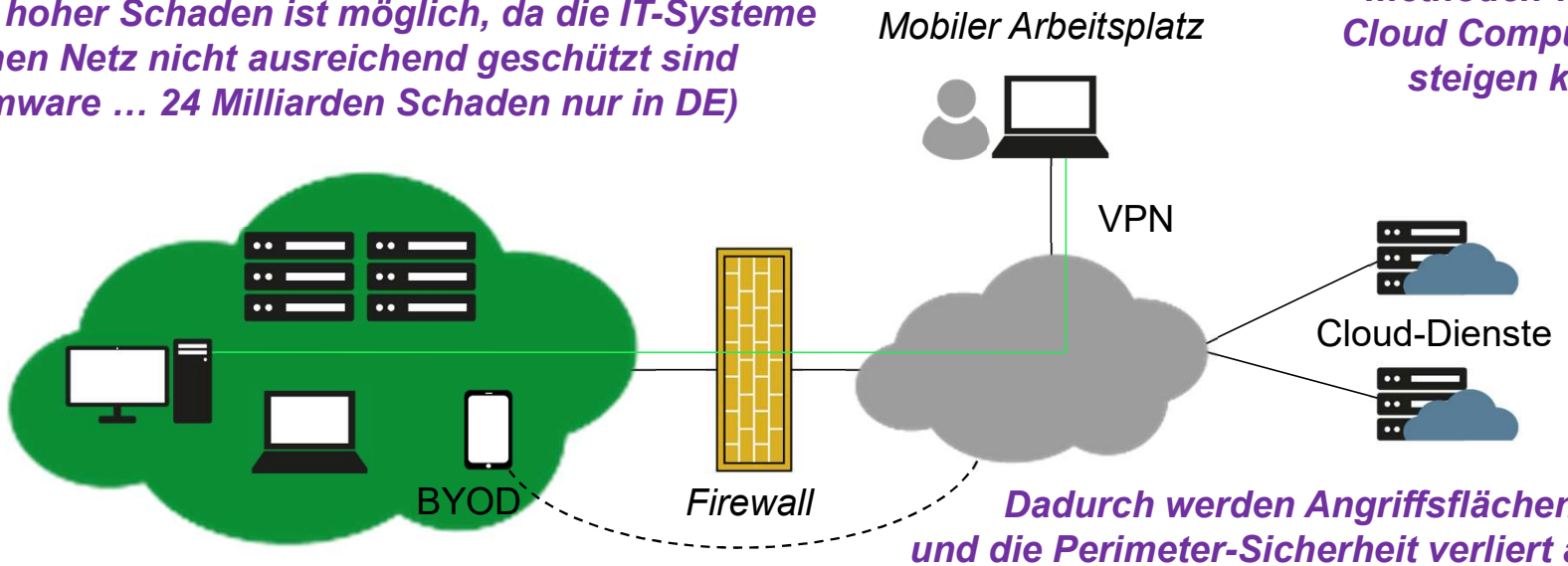
Fokus auf Schutz vor externen Angriffen - Abschottung, Abgrenzung (Firewall, Intrusion Detection Systems (IDS) …)

IT-Sicherheits-Paradigma

→ Perimeter-Sicherheit: Die Probleme

Sobald ein Angreifer in das interne Netz eingedrungen ist, hat dieser leichtes Spiel.
Ein hoher Schaden ist möglich, da die IT-Systeme im internen Netz nicht ausreichend geschützt sind (Ransomware … 24 Milliarden Schaden nur in DE)

Moderne Arbeitsweisen und -methoden wie Homeoffice, Cloud Computing und BYOD steigen kontinuierlich



Dadurch werden Angriffsflächen größer und die Perimeter-Sicherheit verliert an Bedeutung

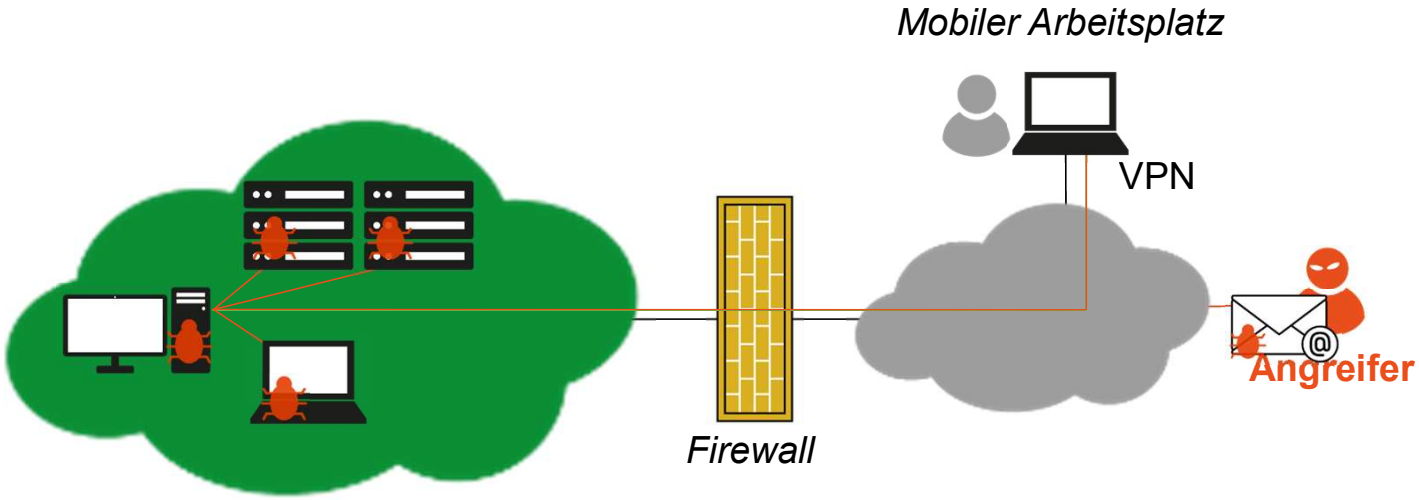
Unternehmensnetzwerk
(intern)

Internet
(extern)

IT-Sicherheits-Paradigma

→ Perimeter-Sicherheit: Problem VPN-Zugang

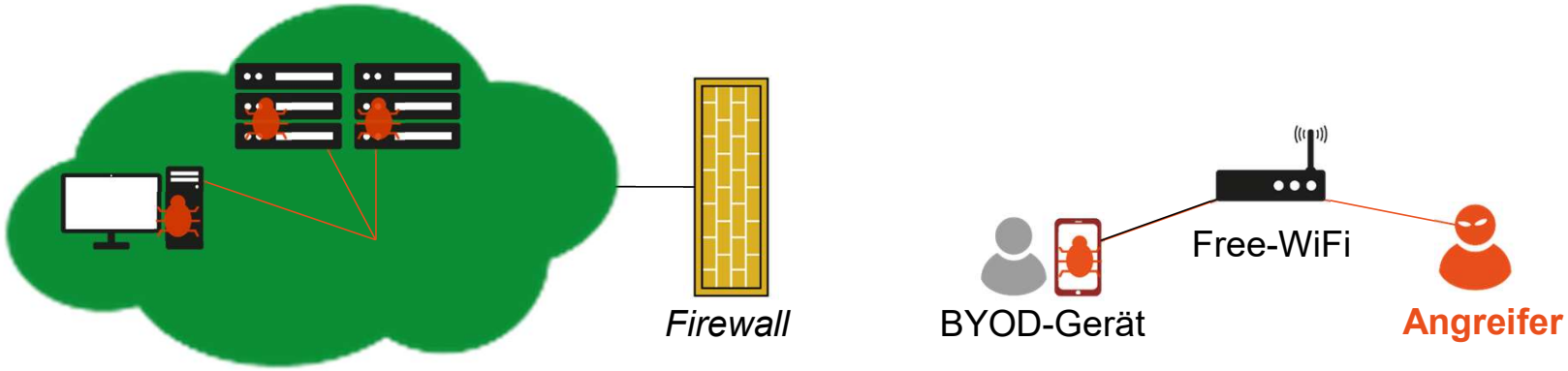
Angreifer erlangt VPN-Zugang mithilfe von Social Engineering / Phishing / Malware
(Typischer Angriffsvektor: Ransomware)



IT-Sicherheits-Paradigma

→ Perimeter-Sicherheit: Problem BYOD-Geräte

BYOD-Geräte können infiziert und damit Malware in das interne Unternehmensnetzwerk eingeschleust werden, Kommunikation an der zentralen Firewall vorbei.

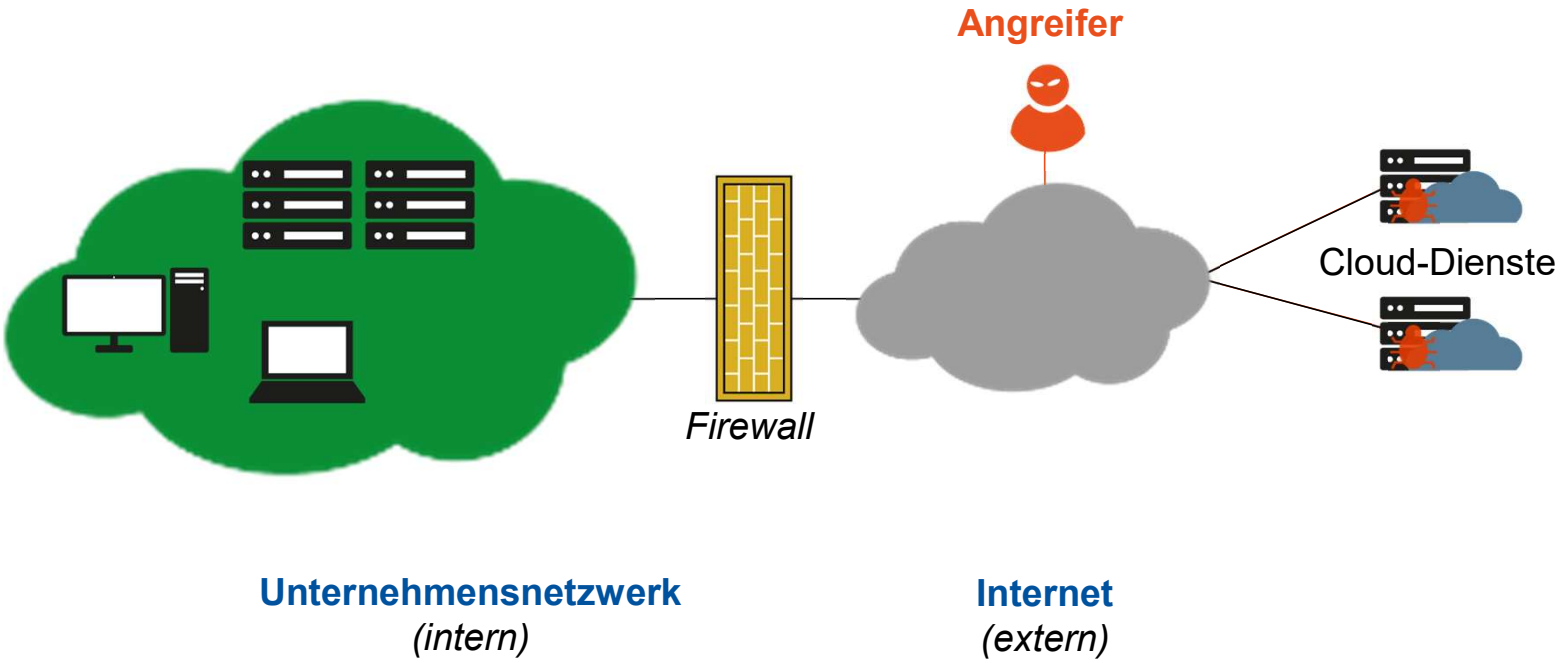


Unternehmensnetzwerk
(intern)

IT-Sicherheits-Paradigma

→ Perimeter-Sicherheit: Problem Cloud-Dienste

Cloud-Dienste werden nicht durch den eigentlichen Perimeter geschützt



IT-Sicherheits-Paradigma

→ Perimeter-Sicherheit: Bewertung

Perimeter-Sicherheit
hat *deutlich an Wirkung* und
damit an *Bedeutung verloren*

IT-Sicherheits-Paradigma

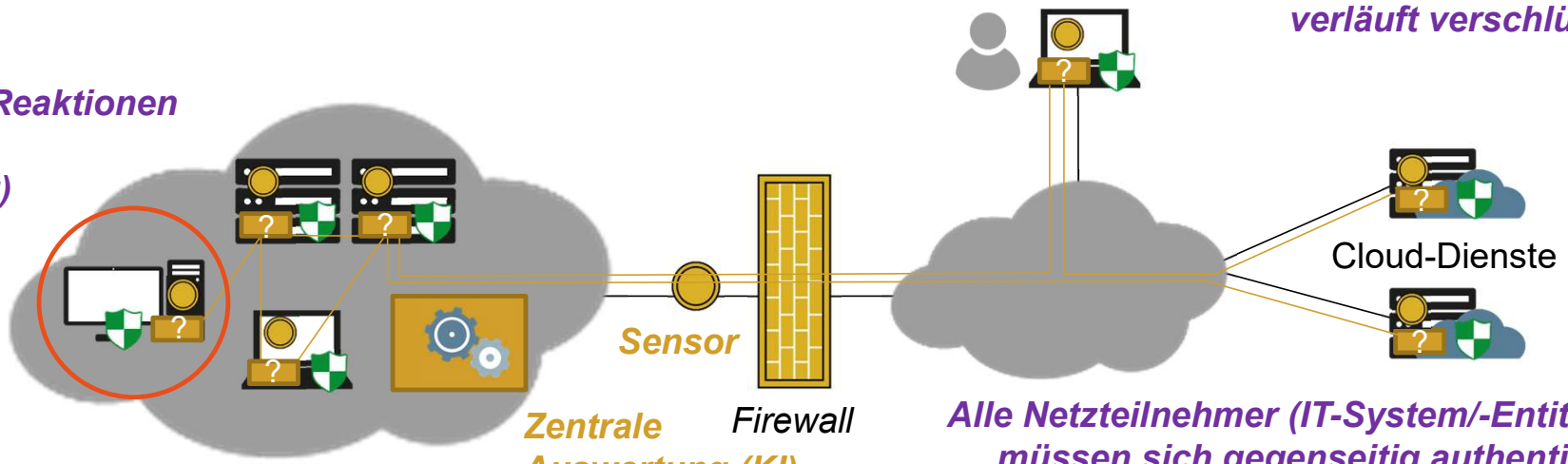
→ Zero Trust Konzept – mehr Sicherheit gegen innovative Angriffe

Moderne End-Point-Security (Sensoren bei den Netzteilnehmern und zentrale KI-Auswertung)

Automatische Reaktionen (Isolierung, falls notwendig)

Mobiler Arbeitsplatz

Jegliche Kommunikation verläuft verschlüsselt



Alle Netzteilnehmer (IT-System/-Entität, Nutzer) müssen sich gegenseitig authentifizieren

Unternehmensnetzwerk
(intern)

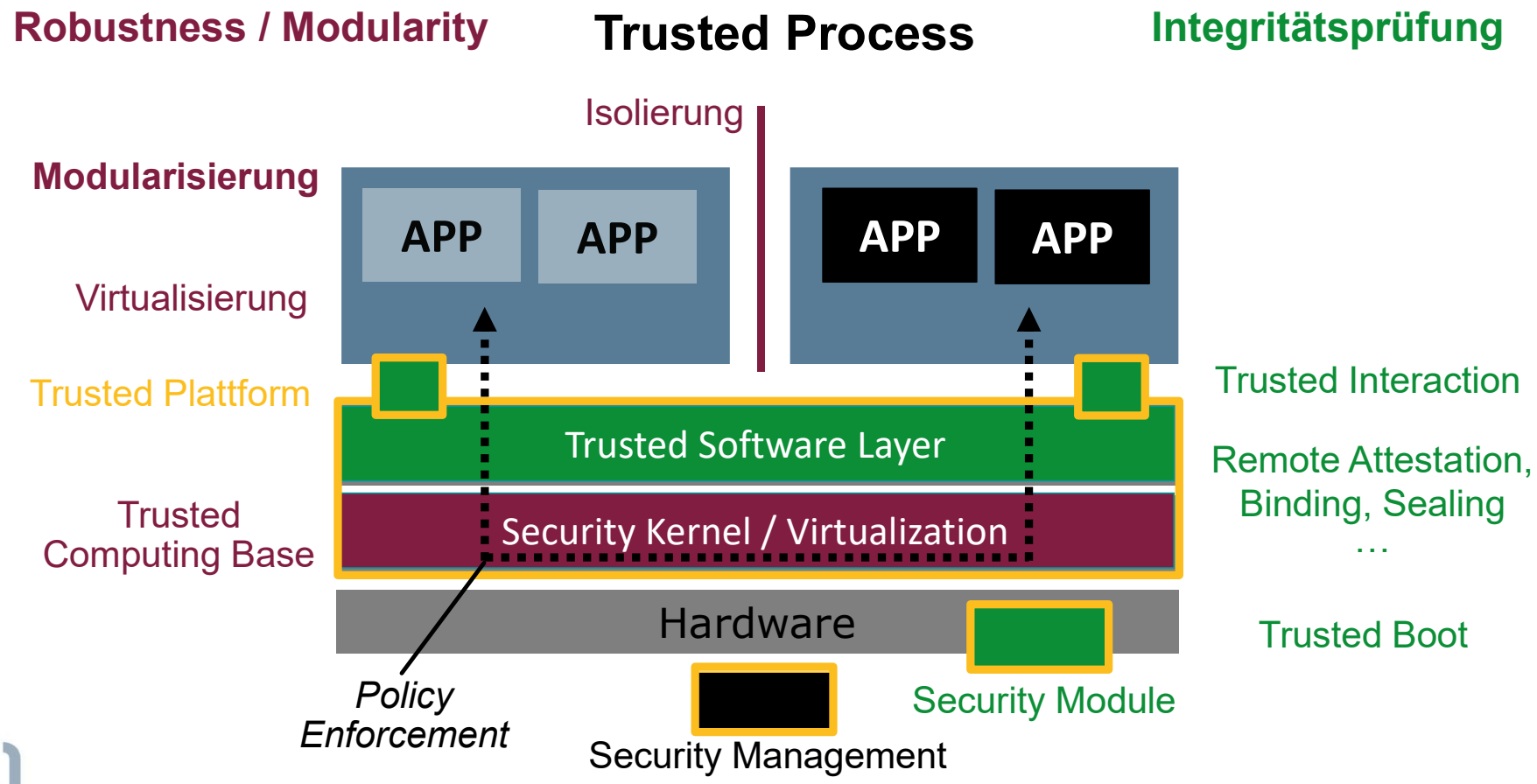
Internet
(extern)

Minimalprinzip: Netzteilnehmer erhalten so wenig Rechte wie möglich (Vermeidung von Überberechtigungen)

Alle IT-Systeme werden robust aufgebaut (Trusted und Confidential Computing)

Robustheit von IT-Systemen (Trusted Computing+)

→ Reduzierung von Problemen - Softwarequalität / Malware



IT-Sicherheits-Paradigma
→ Zero Trust Konzept

Die Ideen von Zero Trust sind sehr gut,
nur die Umsetzungen hat viele Herausforderungen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-Konferenz 2023

29.06.2023, Berlin

Impulsvortrag: Neue IT-Sicherheitskonzepte

(Die wahren Probleme der IT-Sicherheit)

Prof. Dr. (TU NN)

Norbert Pohlmann

TeleTrusT-Vorstandsvorsitzender

Professor für *Cyber-Sicherheit* und

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

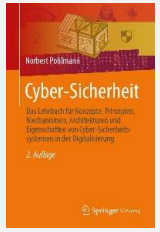
if(is) internet-sicherheit.

Anhang / Credits

→ Übersicht

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

CYBER SCHUTZRAUM

Master Internet-Sicherheit
https://it-sicherheit.de/master-studieren/

(M) MASTER internet-sicherheit.

Glossar Cyber-Sicherheit
https://norbert-pohlmann.com/category/glossar-cyber-sicherheit/

Cyber-Sicherheit GLOSSAR

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/

Der Marktplatz IT-Sicherheit

https://www.it-sicherheit.de/

if(is) internet-sicherheit.