



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Zero Trust: Allheilmittel oder fauler Zauber?

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

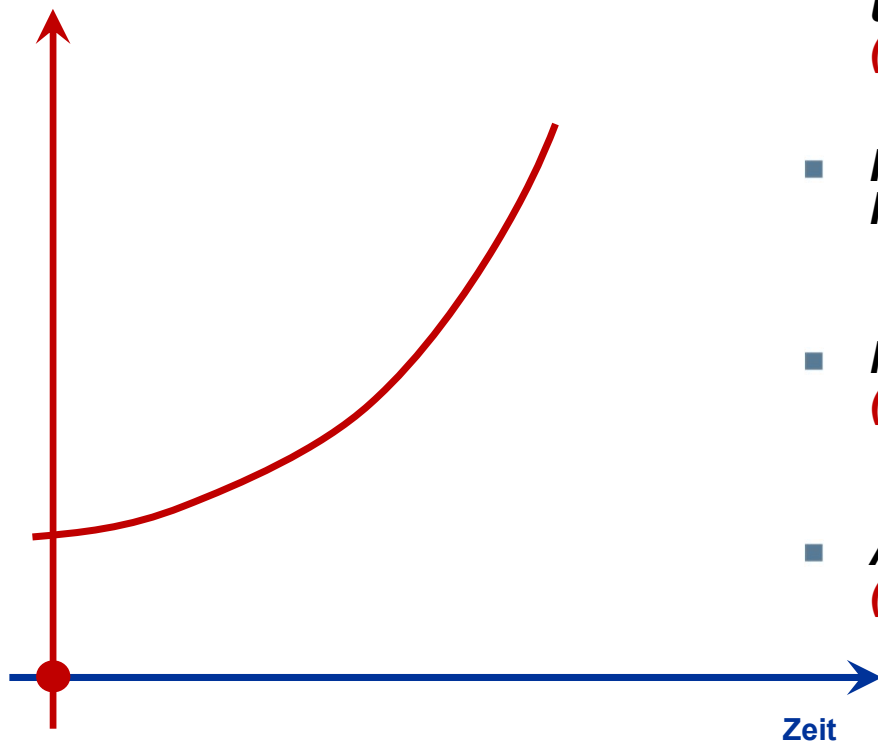
Vorstand im Verband der Internetwirtschaft - eco

if(is)
internet-sicherheit.

Immer mehr Risiken durch die Digitalisierung

→ Eine Einschätzung der Lage der IT-Sicherheit

Risiko durch
die Digitalisierung



- **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)

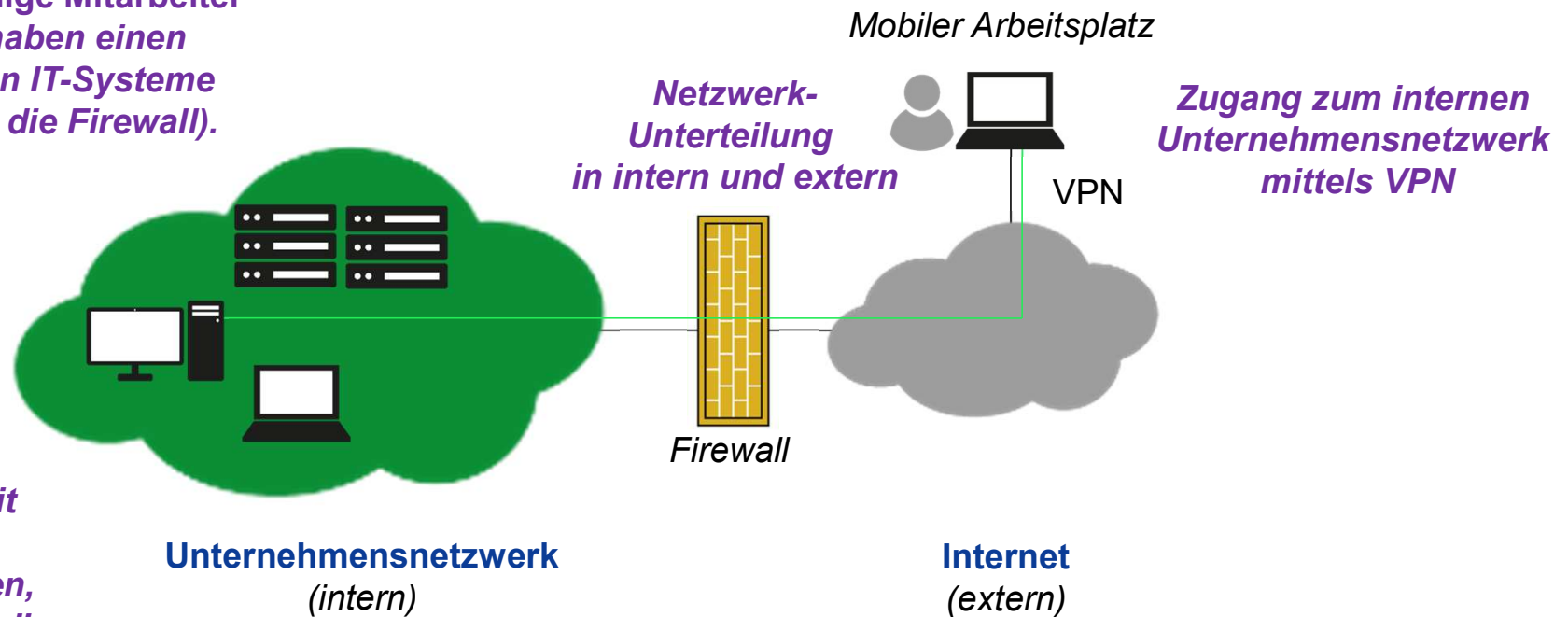
Immer mehr Risiken durch die Digitalisierung → Gegebenheiten / Notwendigkeiten

- **Investment in IT-Sicherheit sollte deutlich mehr sein**
- 7 ... 13 % vom **IT-Budget** ist zu wenig
- **Etablierung eines angemessenen IT-Sicherheitslevel**
- Dazu brauchen wir den **Stand der Technik** - die am Markt verfügbare Bestleistung einer IT-Sicherheitsmaßnahme
- **Wir nutzen die falschen IT-Sicherheit-Paradigmen**
- **Zero Trust** statt *Perimeter-Sicherheit*

IT-Sicherheits-Paradigma

→ Perimeter-Sicherheit: Traditionelles 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).



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

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

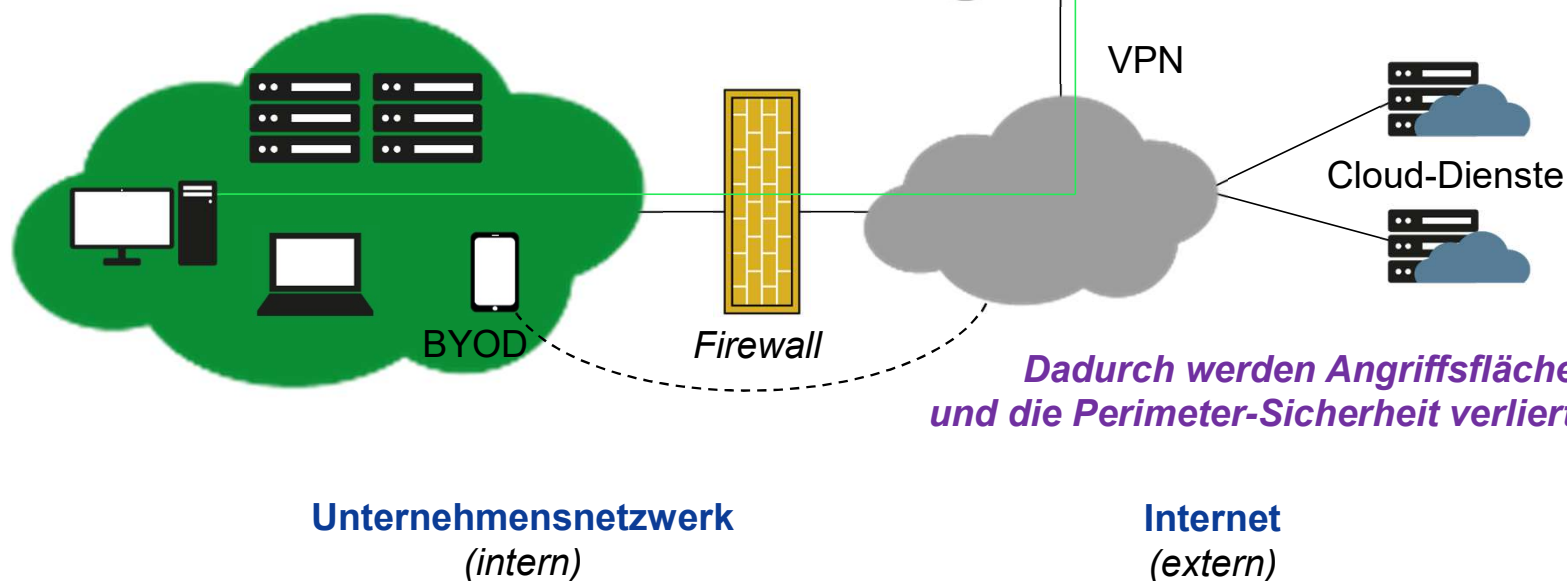
IT-Sicherheits-Paradigma

→ 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

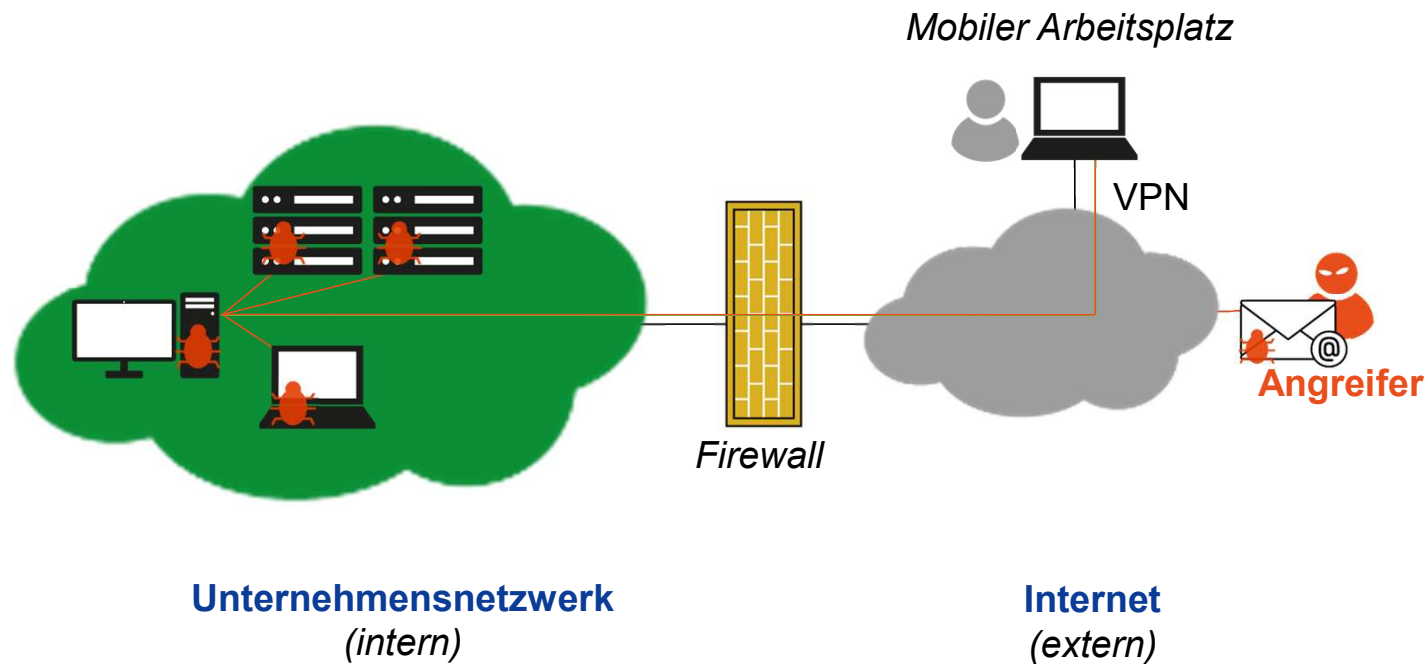


Dadurch werden Angriffsflächen größer und die Perimeter-Sicherheit verliert an Bedeutung

IT-Sicherheits-Paradigma

→ Perimeter-Sicherheit: Problem VPN-Zugang

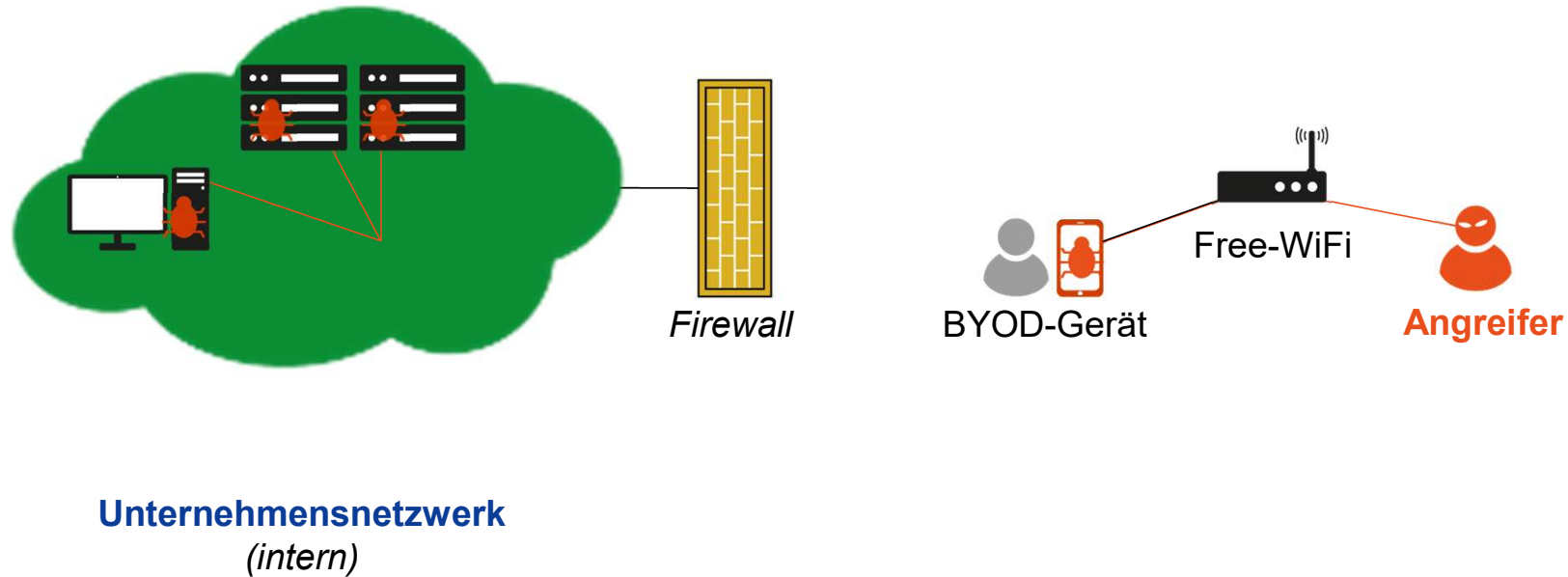
Angreifer erlangt VPN-Zugang mithilfe von **Social Engineering / Phishing / Malware**
(Typischer Angriffsvektor: Ransomware)



IT-Sicherheits-Paradigma

→ Perimeter-Sicherheit: Problem BYOD-Geräte

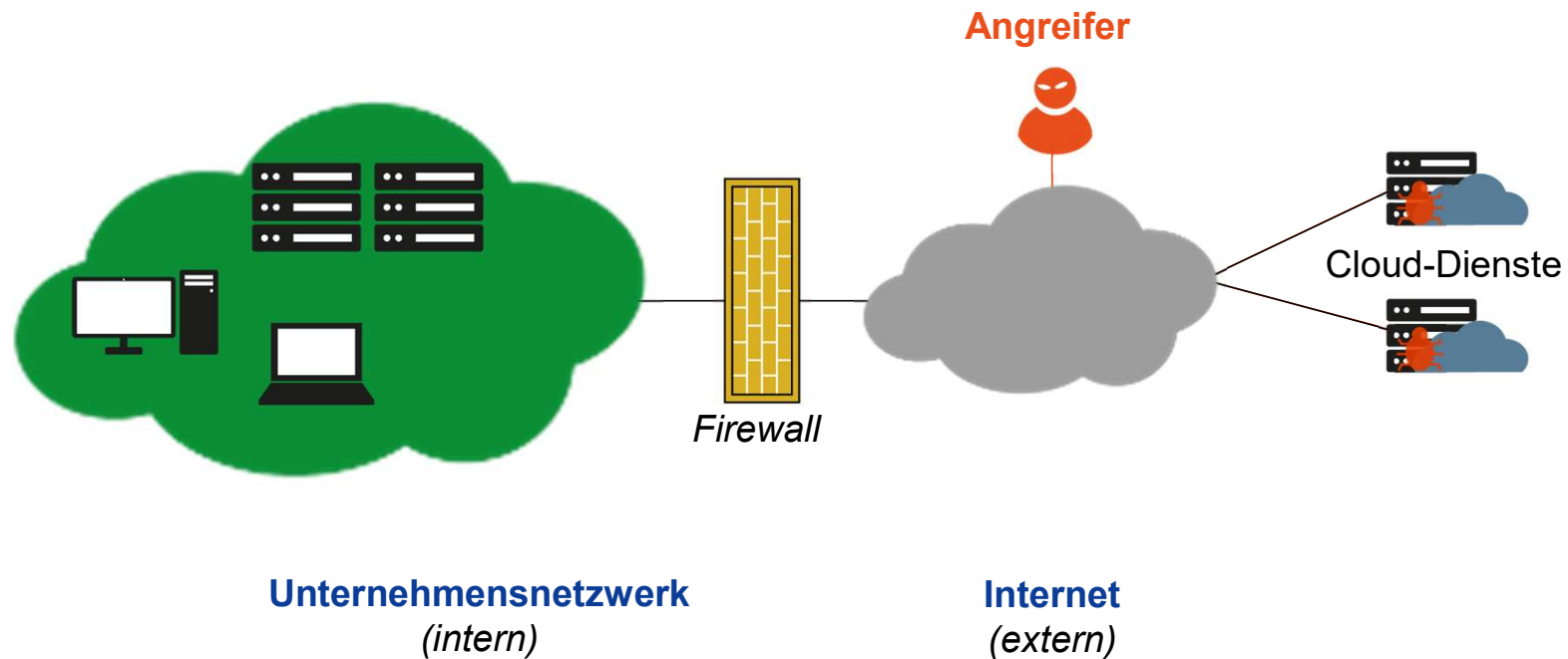
BYOD-Geräte können infiziert und **damit Malware** in das interne Unternehmensnetzwerk eingeschleust werden, „Kommunikation“ an der zentralen Firewall vorbei.



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***

Grundlegende Definition

→ Zero Trust

IT-Sicherheits-Paradigma von Zero Trust: „Vertraue nie, überprüfe immer“

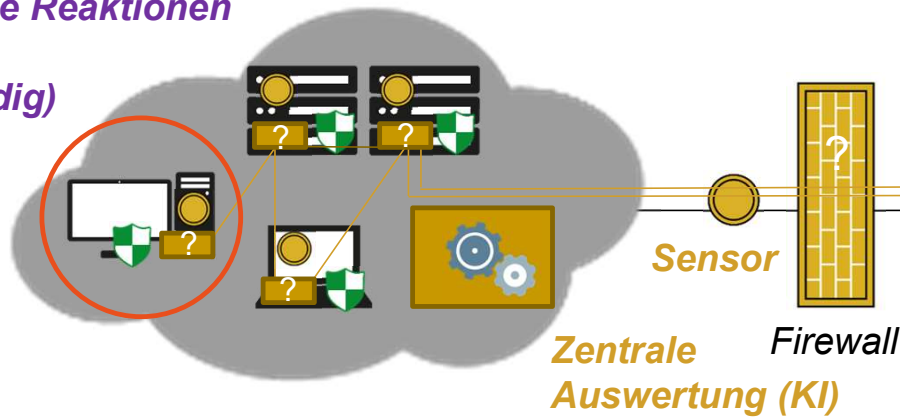
- Alle **Ressourcen** (IT-Systeme, IT-Entities) müssen **validiert** werden
- **Zugänge** müssen **limitiert** und **strikt geregelt** werden
- Jeglicher **Netzwerkverkehr** muss **überprüft** und **geloggt** werden

IT-Sicherheits-Paradigma

→ Zero Trust Konzept – gegen innovative Angriffe

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

Automatische Reaktionen (Isolierung, falls notwendig)



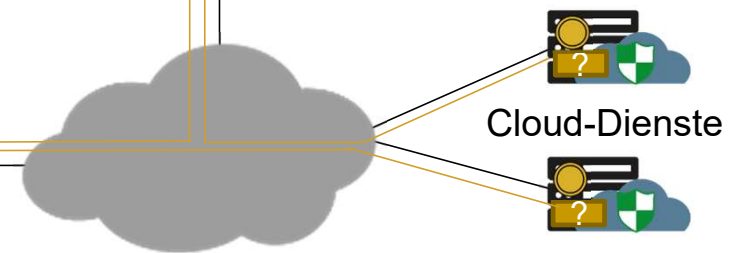
Unternehmensnetzwerk
(intern)

Least-Privilege-Prinzip
Minimalprinzip: Netzteilnehmer erhalten so wenig Rechte wie möglich (Vermeidung von Überberechtigungen)

Mobiler Arbeitsplatz



Jegliche Kommunikation verläuft verschlüsselt und Integritäts-gesichert



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

Internet
(extern)

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

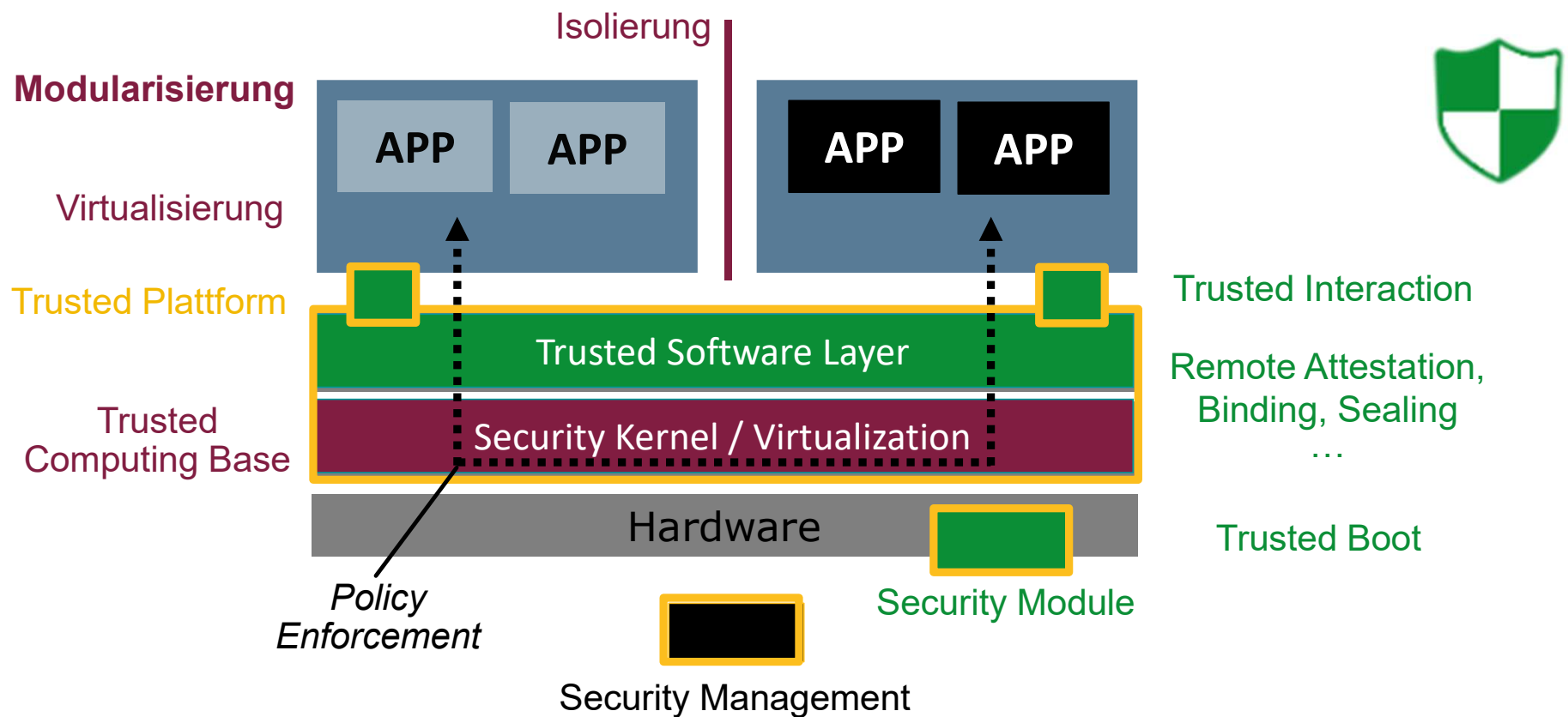
Robustheit von IT-Systemen (Trusted Computing+)

→ Reduzierung von Problemen - Softwarequalität / Malware

Robustness / Modularity

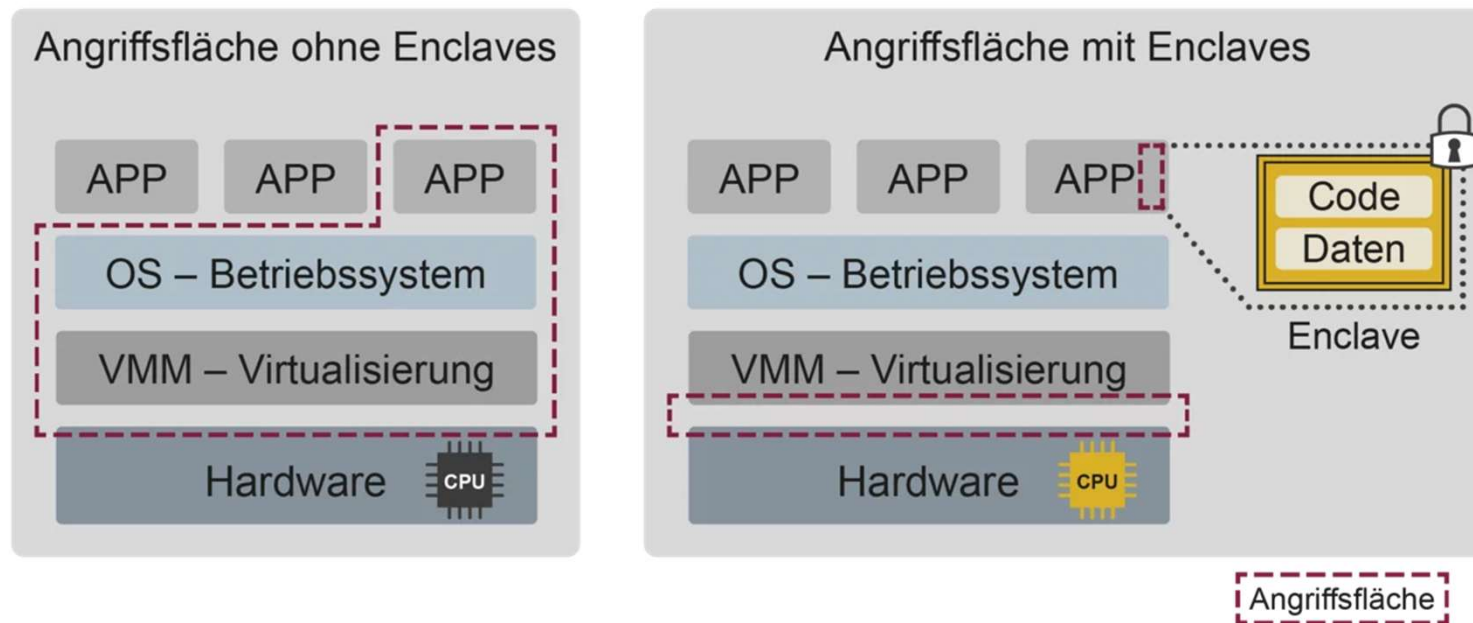
Trusted Process

Integritätsprüfung



Robustheit von IT-Systemen (Cloud Infrastrukturen)

→ Confidential Computing



- Mithilfe von **Confidential Computing** ist es möglich, remote die Daten und den Code einer Anwendung vertrauenswürdig im **verschlüsselten Zustand** als Enclaves auf einem fremden IT-System wie Cloud-Infrastrukturen sicher zu verarbeiten.
- Alle dafür notwendigen Sicherheitsfunktionen sind in der CPU implementiert.

IT-Sicherheits-Paradigma

→ Zero Trust Konzept

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



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Zero Trust:

Allheilmittel oder fauler Zauber?

***„Weder ... noch“ wir brauchen neue
IT-Sicherheitskonzepte für einen besseren Schutz ...
Zero Trust Prinzipien helfen dabei***

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 - TeleTrustT

Vorstand im Verband der Internetwirtschaft - eco

if(is)
internet-sicherheit.

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/>

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
<https://www.it-sicherheit.de/>

Literatur

N. Pohlmann: „Eine vertrauenswürdige Zusammenarbeit mit Hilfe der Blockchain-Technologie“, Buch: „Cybersecurity Best Practices - Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden“, Herausgeber: M. Bartsch, S. Frey; Springer Vieweg Verlag, Wiesbaden 2018

M. Mollik, N. Pohlmann: „Trust as a Service – Vertrauen als Dienstleistung – Validierung digitaler Nachweise mit der Blockchain“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 3/2019

N. Pohlmann: „Wertschöpfung der Digitalisierung sichern - Vier Cybersicherheitsstrategien für den erfolgreichen Wandel in der IT“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 1/2020

N. Pohlmann: „Chancen und Risiken von Smart Home“, DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 2/2021

U. Coester, N. Pohlmann: „Vertrauenswürdigkeit schafft Vertrauen - Vertrauen ist der Schlüssel zum Erfolg von IT- und IT-Sicherheitsunternehmen“, DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 2/2022

N. Pohlmann: **Lehrbuch „Cyber-Sicherheit“**, Springer Vieweg Verlag, Wiesbaden 2022
Druckausgabe (ISBN 978-3-658-36242-3) und eBook (ISBN 978-3-658-36243-0).

Weitere Artikel siehe: <https://norbert-pohlmann.com/artikel/>



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Institut für Internet-Sicherheit

→ Vorstellung und Übersicht

Prof. Dr. (TU NN)

Norbert Pohlmann

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

if(is)
internet-sicherheit.

Institut für Internet-Sicherheit

→ Prof. Norbert Pohlmann

Berufliche Erfahrungen: Unternehmer im Bereich IT-Sicherheit

- Geschäftsführender Gesellschafter der **KryptoKom** GmbH (1988-1999)
- Vorstandsmitglied der **Utimaco Safeware** AG (1999-2003)

Hauptamtliche Tätigkeiten: seit 2003

- **Informatikprofessor** für Informationssicherheit *und*
- Geschäftsführender **Direktor des Instituts für Internet-Sicherheit** – if(is) an der Westfälische Hochschule

Ehrenämter:

- Vorstandsvorsitzender des **Bundesverbands IT-Sicherheit** – TeleTrusT
- Vorstandsmitglied des eco – **Verband der Internetwirtschaft** e.V.
- Vorstandsmitglied **EuroCloud** Deutschland_eco e.V.
- Mitglied des wissenschaftlichen Beirates der **GDD**
- Mitglied im Lenkungskreis Initiative „**IT-Sicherheit in der Wirtschaft**“ des BMWi
- Mitglied der Advisory Group der European Union Agency for Cybersecurity – **ENISA**
- ...

Institut für Internet-Sicherheit

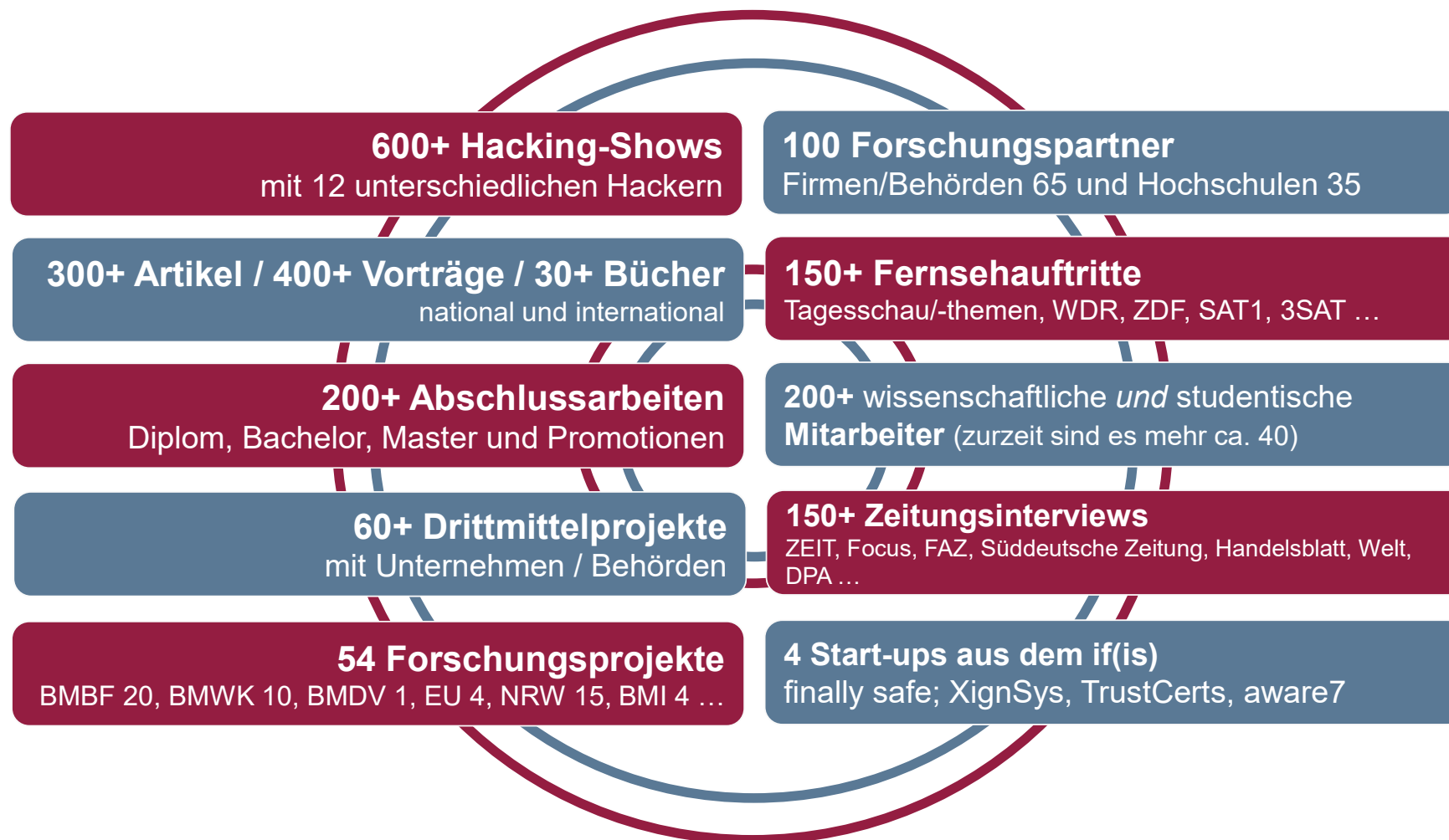
→ Übersicht

- Das Institut für Internet-Sicherheit - if(is) ist eine Fachbereich übergreifende, **wissenschaftliche Einrichtung der Westfälischen Hochschule**, im Fachbereich Informatik
- Gründung: 2005
- Wir haben uns zu dem **führenden Institut für Internet-Sicherheit** entwickelt!
- Seit WS10/11: **Master** „Internet-Sicherheit“
- Ca. 50 Mitarbeiter
- Unser **Ziel** ist es, einen Mehrwert an **Vertrauenswürdigkeit** und **Sicherheit** im Internet herzustellen.



Zahlen des if(is)

→ Übersicht



Forschungsschwerpunkte im



Internet Frühwarnsysteme



(Internet-)Kennzahlen-Sys.



KI + Cyber-Sicherheit



Zahlungssysteme und Banktransaktionen



Blockchain

Identity Management



IoT Security



Gesundheitswesen

Vertrauenswürdige IT-Systeme



Smart City, -Car, -Traffic

Cloud, Fog, Edge Computing



Mobile Security

Botnetz-Erkennung



Vertrauenswürdigkeit