Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

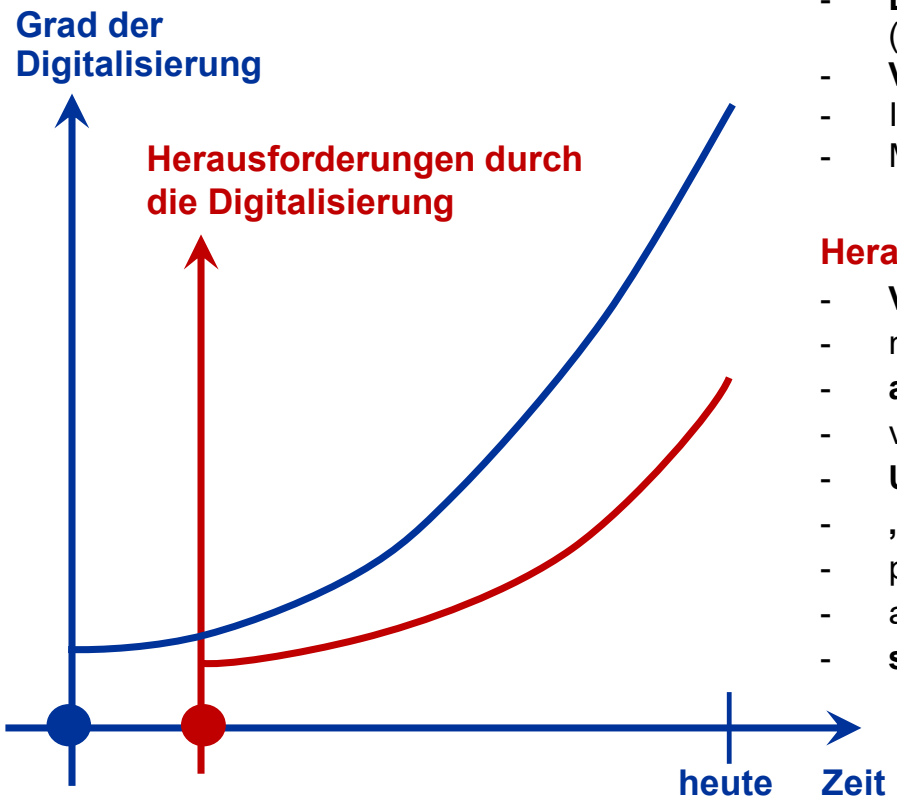
Cyber-Sicherheit *und* Vertrauenswürdigkeit *für* Smart-Cities

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.

Entwicklung der Digitalisierung
→ Erfolgsfaktoren und Herausforderungen



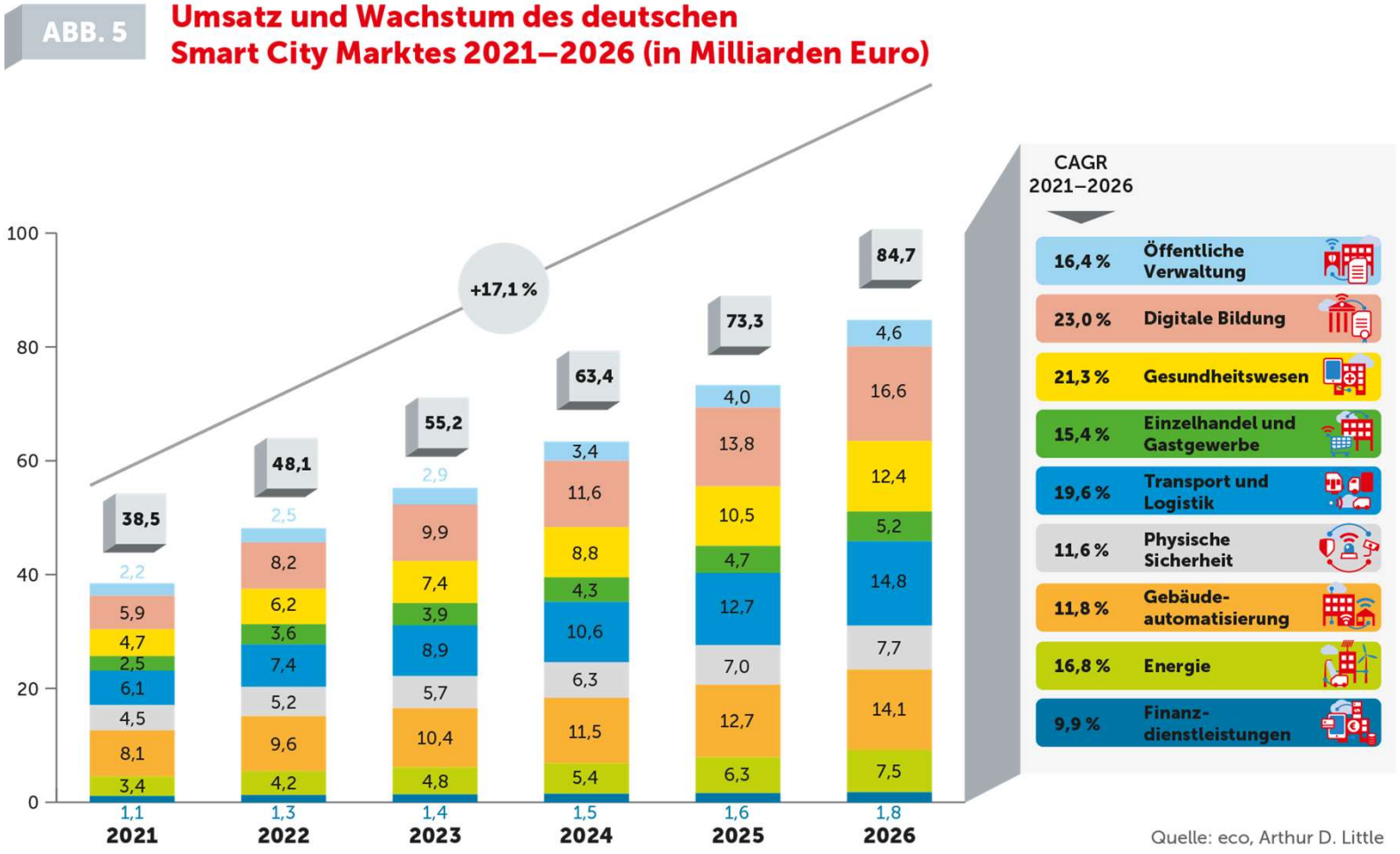
Erfolgsfaktoren der **Digitalisierung** (Beispiele)

- **Kommunikationsinfrastruktur** (5G, Glasfaser, NFC, BT …)
- Smartheit der Endgeräte (Watch, Phone, Book/Pad, IoT …)
- **Leistungsfähigkeit zentraler IT-Systeme** (Cloud, Edge-Computing, Hyperscaler ...)
- **Verwendung von KI** (ML …)
- Integration in IT-Prozesse und IT-Systeme (echtzeitorientiert+)
- Moderne Benutzerschnittstellen (Sprache, Gestik …)

Herausforderungen Cyber-Sicherheit (Beispiele)

- **Verbesserung der Softwarequalität**
- mehr Schutz vor Malware, unsichere Webseiten …
- **alternativen zu Passwörtern (MFA)**
- verschlüsselte E-Mails, Kommunikation (IPSec, TLS …)
- **Umgang mit der Komplexität der IT-Systeme**
- **„*bessere*“ IT-Sicherheitsarchitekturen**
- passenden Level IT-Sicherheit (z.Z. nicht „Stand der Technik“)
- angemessene Verfügbarkeit
- **sichere Hardware** (Sicherheitsmodule in den Komponenten)

Smart City
→ Umsatz und Wachstum



https://norbert-pohlmann.com/gutachten/smart-city-markt/

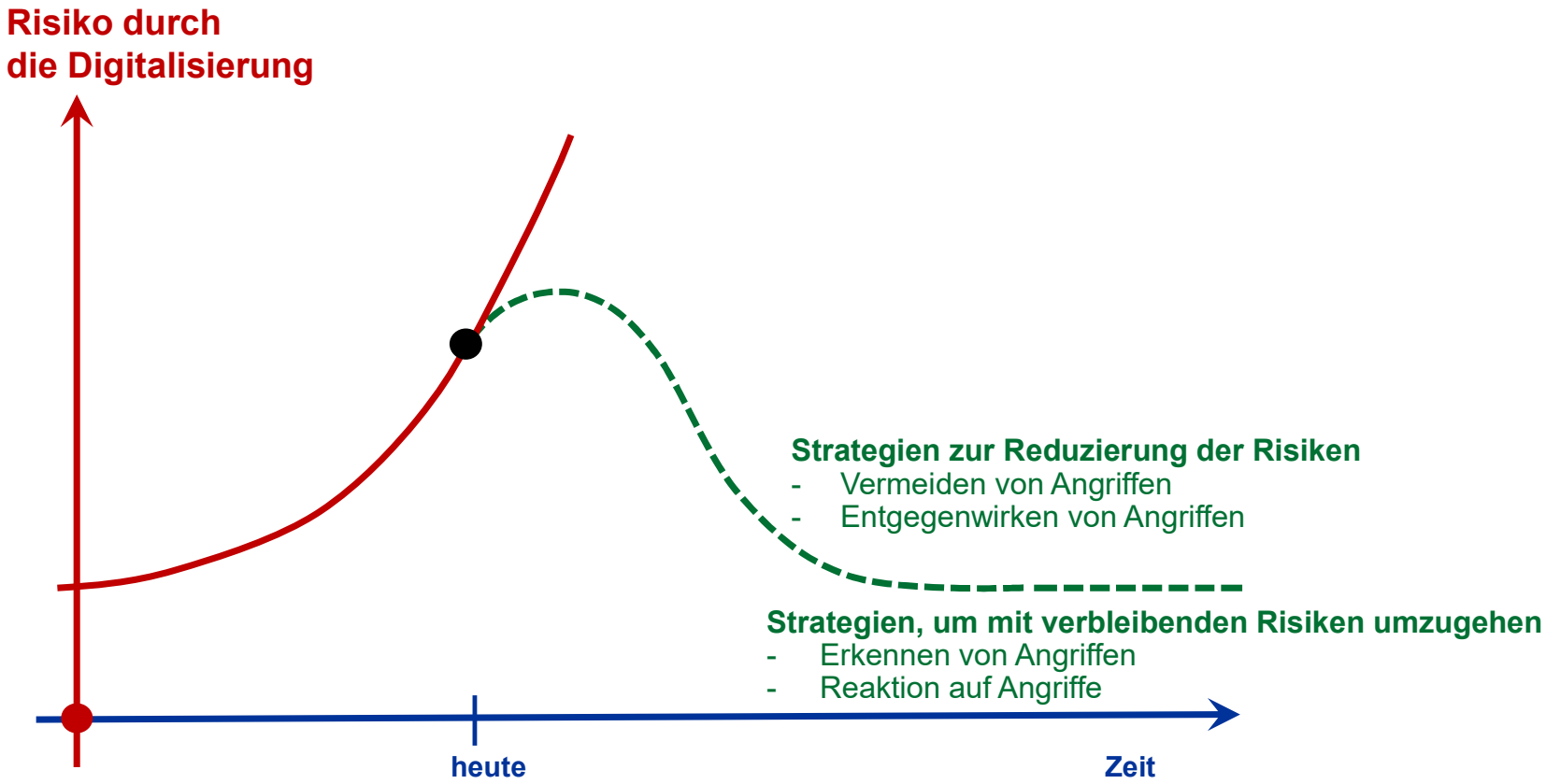
Cyber-Sicherheitslage
→ Einschätzung

- ***Die Cyber-Sicherheitsprobleme werden immer größer***

- **IT-Systeme** und **-Infrastrukturen** sind **nicht sicher genug konzipiert, aufgebaut, konfiguriert** und **upgedatete**
  um den Angriffen intelligenter Hacker erfolgreich entgegenzuwirken.

- **Weitere Herausforderungen mit der fortscheitenden Digitalisierung:**
  - *IT-Systeme und -Infrastrukturen werden **immer komplexer** (Steigerung der Abhängigkeiten… mehr Software … mehr Verbindungen … Supply-Chain… Facebook-Problem…)*
    - **Angriffsfläche wird größer**
  - *Die **Methoden der Angreifer** werden **ausgefeilter***
    - **Kriminelles-Ökosysteme**
  - ***Angriffsziele** werden **kontinuierlich lukrativer** (Digitalisierung)*
    - **mehr digitale Werte**

Cyber-Sicherheitsstrategien
→ Übersicht



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* umsetzen** kann, aber **alles andere *aktiv* vermieden wird**.

Cyber-Sicherheitsmechanismen

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

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)*
- ***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)*

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, dass in einem definierten Bereich
  (IT- und Kommunikationsinfrastruktur, IT-Endgeräte, …)
  nach **Angriffssignaturen** oder **Anomalien** gesucht wird.

Cyber-Sicherheitsmechanismen

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

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 …) - KI*
- ***Digitale Forensik*** *(Maßnahmen optimieren, Schwachstellen schließen)*
- ***Definition von Befugnissen, Informationsflüsse, Entscheidungsprozess und Kommunikationsstrategien***
- ***Notfallplanung für Smart City Anwendungen***

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

- Theorie ist gut, aber jetzt müssen wir ins Handeln kommen.
- Dazu haben wir den Marktplatz IT-Sicherheit als zentrale und vertrauenswürdige Anlaufstelle für alle Unternehmen – vom Startup bis zum gehobenen Mittelstand – sowie Institutionen aufgebaut.
- Der **Marktplatz IT-Sicherheit** bietet in Fragen der IT-Sicherheit folgendes
  - Artikel, Blogeinträge und News sowie pragmatische und aktuelle Ratschläge
  - ein Forum für die Möglichkeit zum Austausch zwischen Experten, Anwendern und Anbietern.
- Unsere Zielstellung lautet:
  "Gemeinsam lässt sich eine sichere digitale Zukunft gestalten".

www. it-sicherheit.de
Der Marktplatz IT-Sicherheit

Digitale Zukunft
→ Vertrauen

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

- **Folge:**
  Das macht den Menschen **Angst** und schränkt sie in ihrer Handlungsfähigkeit ein.

- **Risiko:**
  Die Bürger wollen keine Digitalisierung.

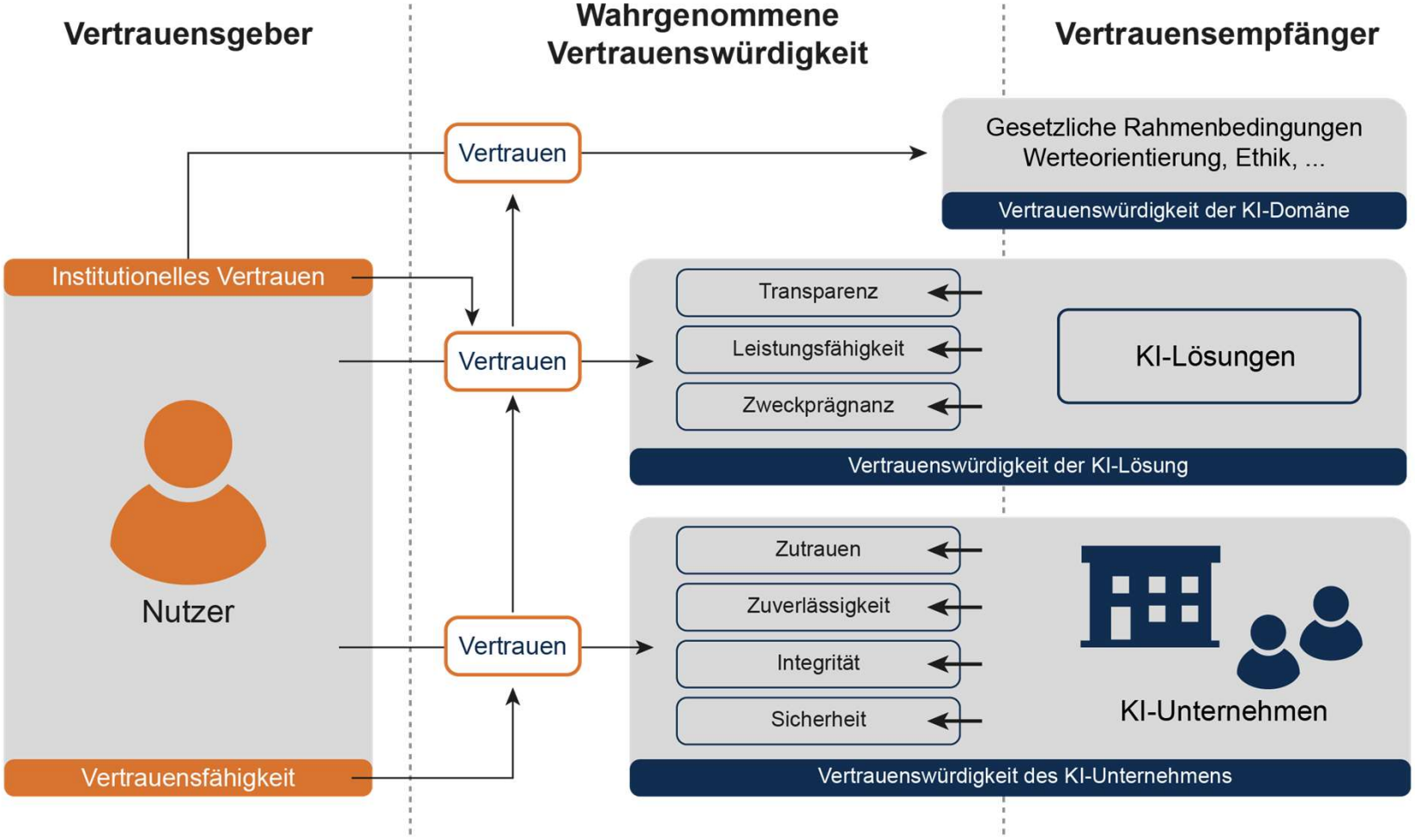
- **Lösung:**
  Vertrauen ist notwendig, um **handlungsfähig** sein zu können.

Digitale Zukunft
→ Vertrauenswürdigkeit

- **Wichtig: Nutzer / Bürger wollen Vertrauen können.**
  Aus diesem Grund müssen **Unternehmen / Städte** alles tun,
  damit es dem Nutzer / Bürger möglich ist, sowohl IT-Lösung als auch
  dem Unternehmen / den Städten zu vertrauen – das bedeutet, **vertrauenswürdig agieren**.

- **Fazit:**
  Vertrauenswürdigkeit schafft Akzeptanz und damit loyale Kunden / Bürger.

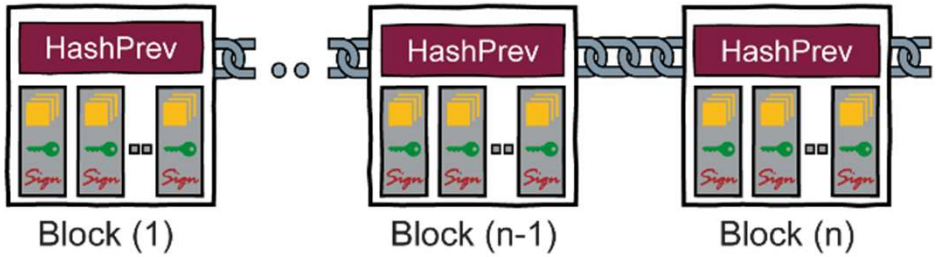
Vertrauenswürdigkeit
→ Modell

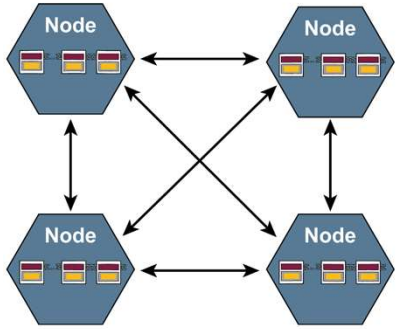


Smart City
→ Cyber-Sicherheit

- Die zunehmende Vernetzung sorgt in **Smart Cities** dafür, dass die **IT-Landschaften zunehmend komplexer** werden.
- Städte, Dienstleister und Bürger **tauschen Daten** über immer mehr IT-Systeme und Schnittstellen hinweg aus.
- IoT-Geräte, Sensoren und Plattformen für den Datenaustausch und die Datenanalyse mit ganz unterschiedlichen Sicherheitsleveln erhöhen das **Risiko** für **Sicherheitsschwachstellen** und **Cyberangriffe**.
- Verantwortlichen in den Kommunen sollten beim Entwurf smarter Lösungen für Verwaltung und Bürgerservices **Cyber-Sicherheit** **von Anfang an mitdenken**.

Blockchain-Technology
→ Sicherheitseigenschaften





Blockchain

- ist eine **fälschungssichere**,
- **verteilte**, **redundante** Datenstruktur
- in der **Transaktionen** **in der Zeitfolge protokolliert**
- **nachvollziehbar**, **unveränderlich** und
- **ohne zentrale Instanz** abgebildet sind.

kryptographische Verfahren (Hashfunktionen / Public-Key-Verfahren)

Vielzahl von Teilnehmern gespeichert (jede Note hat die Blockchain gespeichert)

Art der Verkettung (HashPrev)

jeder kann Kryptographie überprüfen (Hashwert, Signatur)

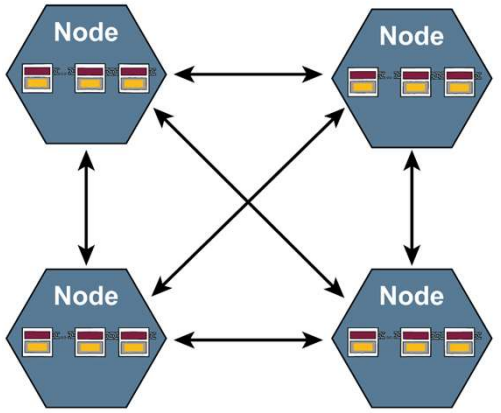
geeignete Konsensfindungsverfahren (Proof of Work, Proof of Stake …)

*(**Sicherheitseigenschaften** einer **Blockchain**)*

Blockchain-Infrastruktur
→ Eigenschaft: ohne zentrale Instanz

- Die Blockchain-Technologie bietet "**programmiertes Vertrauen**" mit Hilfe verschiedener IT-Sicherheits- und Vertrauensmechanismen.

- Alle IT-Sicherheits- und Vertrauensfunktionen sind inhärent als "**Security-by-Design**" in die Blockchain-Technologie integriert.



Vertrauenswürdigkeitsmechanismen

- **Verteilte Konsensfindungsverfahren**

- **Verteilte Validierung**
  - Echtheit der Transaktionen (Überprüfung der Hashwerte/Signatur)
  - Korrektheit der Blöcke (Überprüfung der Hashwerte/Konsens)
  - Syntax, Semantik … (Schutz gegen Fremdnutzung)

Smart City Projekt
→ Ruhrvalley

- Mithilfe der **Blockchain-Technologie** wird im **Smart City Projekt** innerhalb von Ruhrvalley an einer dezentralen digitalen Plattform für Mobilitäts- und Energiedienste geforscht.
- Untersuchung des **Use Cases** einer dezentralen, Blockchain-basierten Plattform zur Verknüpfung von Mobilitäts- und Energiediensten für **Light Electric Vehicles (LEV)**
- Untersuchung eines **Token-Economy-System** zur transparenten Abbildung der Stromherkunft und der damit einhergehenden CO2 Einsparung (**Carbon-Token**)
- Und zur Incentivierung von **nachhaltigem Nutzerverhalten** (**User Incentivize-Token**) innerhalb der Blockchain-Plattform

CS u. Vertrauenswürdigkeit für SC
→ Zusammenfassung und Ausblick

- **Neue Technologien** bringen **neue Herausforderungen** mit sich
- **Cyber-Sicherheit** und **Vertrauenswürdigkeit** haben eine entscheidende Rolle bei der Digitalisierung bzw. Entwicklung von **innovativen Smart-City Anwendungen**
  - **Cyber-Sicherheit schützt** vernetzte IT-Systeme und IT-Infrastrukturen **vor Angriffen**
  - **Vertrauenswürdigkeit** als Schlüsselfaktor, um **das Vertrauen** der Bürger und Unternehmen in die Smart-City-Technologien und -Dienstleistungen **zu gewinnen**
- **Bedeutung** von Cyber-Sicherheit und Vertrauenswürdigkeit in Smart-Cities **wird in Zukunft weiter zunehmen**, da die Abhängigkeit von vernetzten IT-Systemen und IoT-Geräten weiter wächst
- Robuste **Sicherheitsmaßnahmen** und -protokolle zu implementieren, wird entscheidend sein, um die **Smart-City-Infrastrukturen** vor realen Angriffen zu **schützen**

Cyber-Sicherheit *und* Vertrauenswürdigkeit *für* **Smart-Cities**

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyber-Sicherheit *und* ***Vertrauenswürdigkeit***
werden *in der Zukunft* ***immer wichtiger***

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.

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

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

It‘s all about Trust!

https://vertrauenswürdigkeit.com/

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/

Quellen Bildmaterial

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

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:

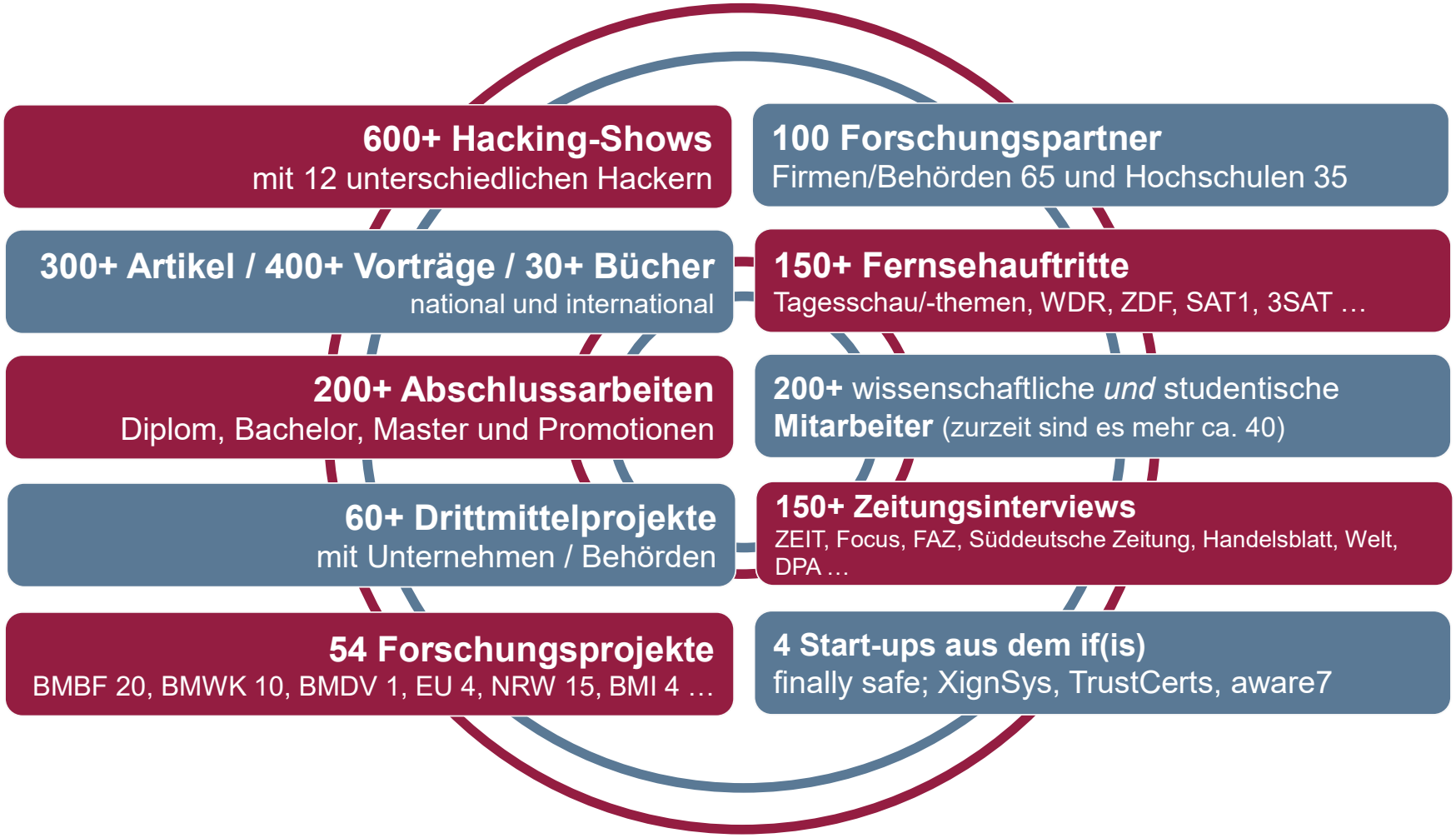
- Vorstandsvorsitzender des **Bundesverbands IT-Sicherheit** – TeleTrusT
- Vorstandsmitglied des eco – **Verband der Internetwirtschaft** e.V.
- Vorstandsmitglied **EuroCloud** Deutschland_eco e.V.
- Mitglied des wissenschaftlichen Beirates der **GDD**
- Mitglied im Lenkungskreis Initiative „**IT-Sicherheit 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 if(is) internet-sicherheit.

- 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