Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Immer mehr Daten
= Immer mehr (Un) Sicherheit?

Prof. Dr. (TU NN)
Norbert Pohlmann
Vorstandsmitglied eco – IT-Sicherheit
***Professor** für **Cyber-Sicherheit** und*
Leiter** des **Instituts für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen

if(is) internet-sicherheit.

These
→ Mehr Daten → mehr Unsicherheit

Ja

Daten
→ Werte

- Durch die **fortschreitende Digitalisierung** steigt die Anzahl der Daten und damit die **Werte auf unseren IT-Systemen**

- Beispiele von Daten:
  - ***Firmengeheimnisse:*** vollständige Entwicklungs- und Fertigungsunterlagen, *Geschäfts- und Betriebsergebnisse*, Kalkulationen, *Strategiepläne*, Fusionsabsichten, *Sicherheitsinformationen*, Pateninformationen, *Protokolldaten* …
  - ***Logistikinformationen:*** Lagerbestand, *Lagerort* …
  - ***Kundendaten:*** Angebote, *Preise*, Prognosen …
  - ***Persönliche Daten:*** Gehalt, *Krankheiten* …
  - ***Weitere Daten:*** Filme, *Musik*, Bücher …

Cyber-Sicherheitsbedürfnisse
→ Sichtweise Daten (1/2)

Cyber-Sicherheitsbedürfnisse sind **Grundwerte der Cyber-Sicherheit**, die mithilfe von Cyber-Sicherheitsmechanismen befriedigt werden können.

Gewährleistung der Vertraulichkeit

- Vertraulichkeit ist wichtig, damit **keine unautorisierten Personen** oder Organisationen in der Lage sind, übertragene oder gespeicherte **Daten** zu **lesen**.

Gewährleistung der Authentifikation

- Mithilfe des Cyber-Sicherheitsmechanismus Authentifikation wird verifiziert, **wer** der Partner bei der Kommunikation oder Transaktion ist beziehungsweise welcher Nutzer auf Betriebsmittel und **Daten** **zugreift**.

Gewährleistung der Authentizität

- Mithilfe des Cyber-Sicherheitsmechanismus Authentizität wird **verifiziert**, dass **Daten** oder Identitäten **echt sind**.

Cyber-Sicherheitsbedürfnisse
→ Sichtweise Daten (2/2)

Gewährleistung der Integrität

- Bei der „Gewährleistung der Integrität“ wird überprüft, ob **Daten**, die übertragen werden oder gespeichert sind, unverändert, das heißt **original sind**.

Gewährleistung der Verbindlichkeit

- „Gewährleistung der Verbindlichkeit“ sorgt für die Gewissheit, dass die Prozesse und die damit verbundenen Aktionen (auch Austausch von **Daten**) **verbindlich sind**.

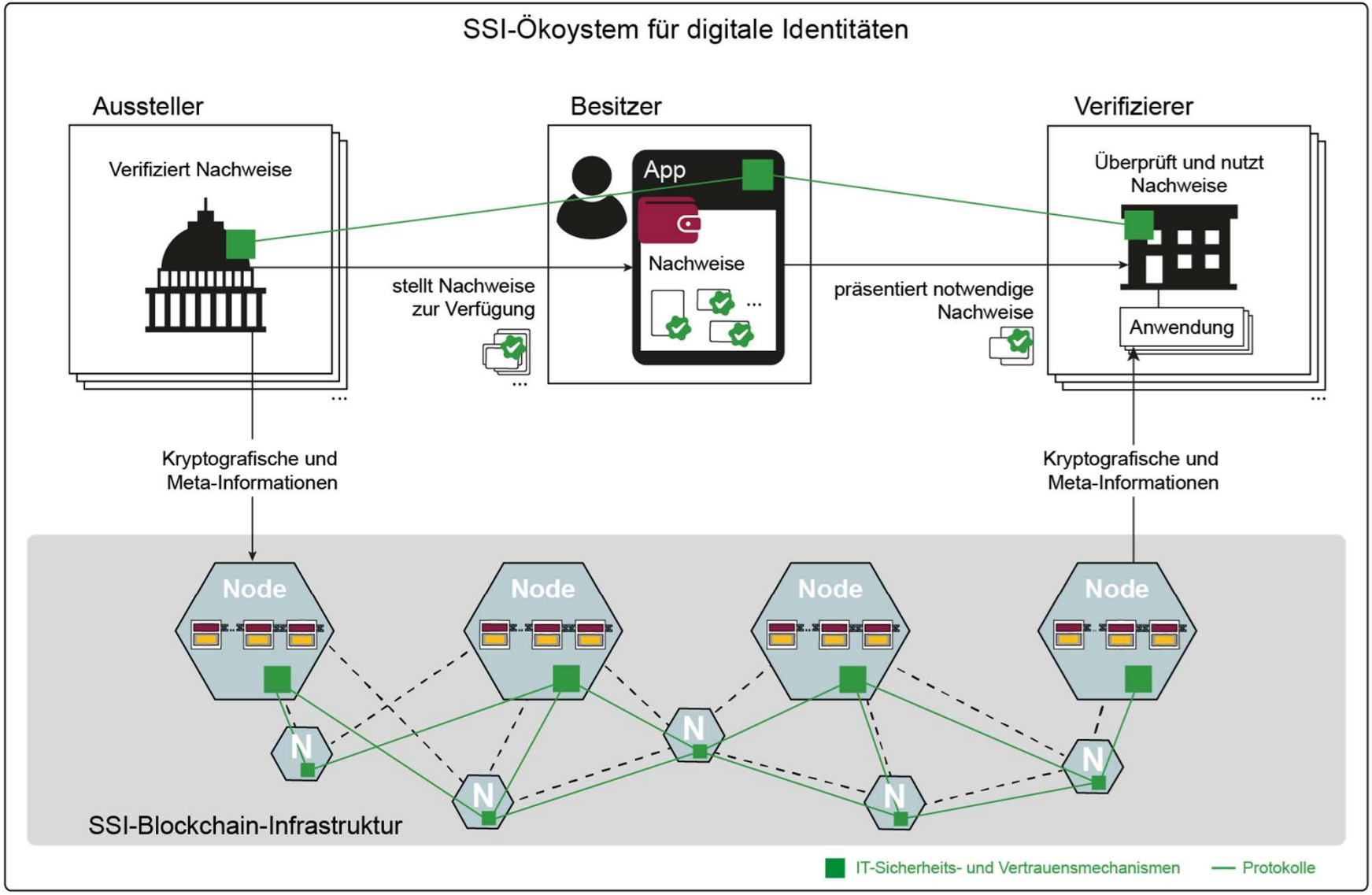
Gewährleistung der Verfügbarkeit

- Dieses Cyber-Sicherheitsbedürfnis sorgt für die Gewissheit, dass die **Daten** und Dienste auch **zur Verfügung stehen**.

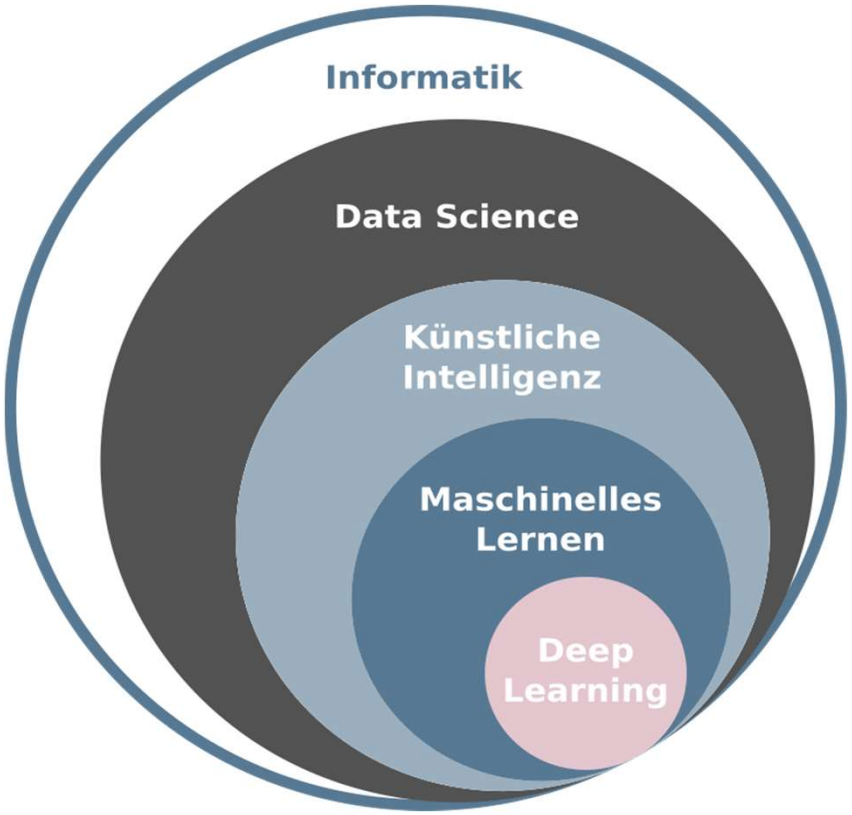
Self-Sovereign Identity

→ Daten sind beim Nutzer, nicht beim Provider

- Im SSI-Ökosystem spielen **drei Akteure eine Rolle**, die gemeinsam einen Vertrauensdienst – zum Beispiel die SSI-Blockchain-Infrastruktur - nutzen.



KI - Maschinelles Lernen
→ Einordnung



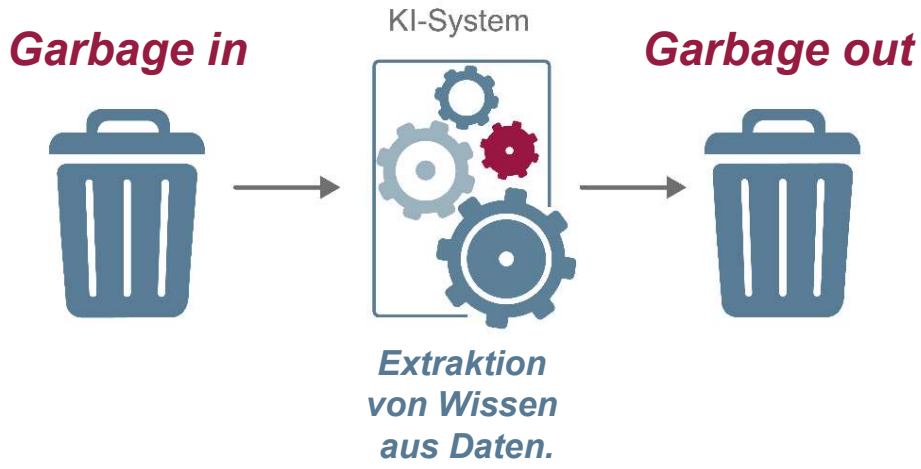
- **Data Science** bezeichnet generell die **Extraktion von Wissen** **aus Daten**.

- **Starke „Künstliche Intelligenz“** *(Zukunft)* soll automatisiert „**menschenähnliche Intelligenz“** nachbilden. **Singularität** („Maschinen“ verbessern sich selbst, sind intelligenter als Menschen)

- **Schwache „Künstliche Intelligenz“** *(heute)* **Maschinelles Lernen** ist ein Begriff für die „künstliche“ **Generierung von Wissen aus Erfahrung** (in **Daten**) durch Computer.

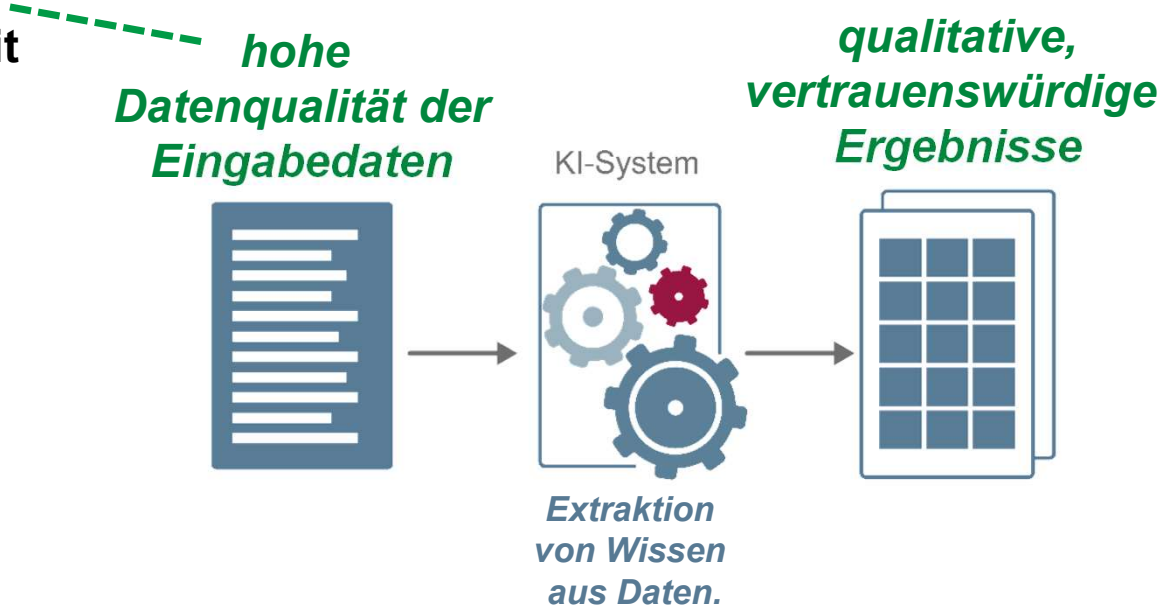
KI-Anwendungen
→ Qualität der Daten

Paradigma



Standards für die Datenqualität:

- → Inhalthöhe der **Daten** und **Korrektheit**
- → **Nachvollziehbarkeit** (Datenquellen)
- → Vollständigkeit und **Repräsentativität**
- → Verfügbarkeit und Aktualität



Risiken der KI aktiv reduzieren
→ Cyber-Sicherheitsmaßnahmen

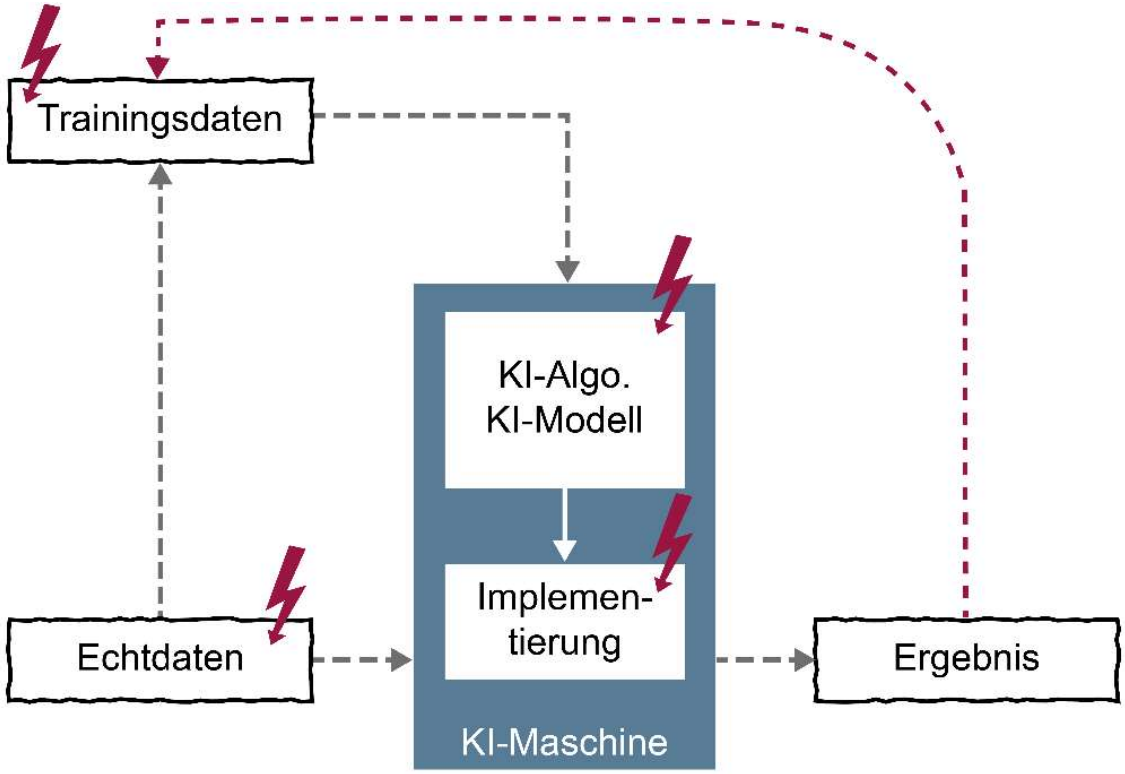
Angriffe auf KI-Systeme

→ *Poisoning Attack*

→ *Evasion Attack*

→ *Exploratory Attack*

→ *…*



Stand der Technik *an*
Cyber-Sicherheitsmaßnahmen
zum ***Schutz***

→ *der* ***Daten*** *(Training, Echt, Ergebnis),*

→ *der* ***KI-Maschine*** *und*

→ *der* ***Anwendung***

Nutzung *einer* ***qualitativ hochwertigen***
KI-Technologie
(Evaluierung / Zertifizierung / ***Souveränität / GAIA-X*****)**

Risiken der KI aktiv reduzieren
→ Schutzziele

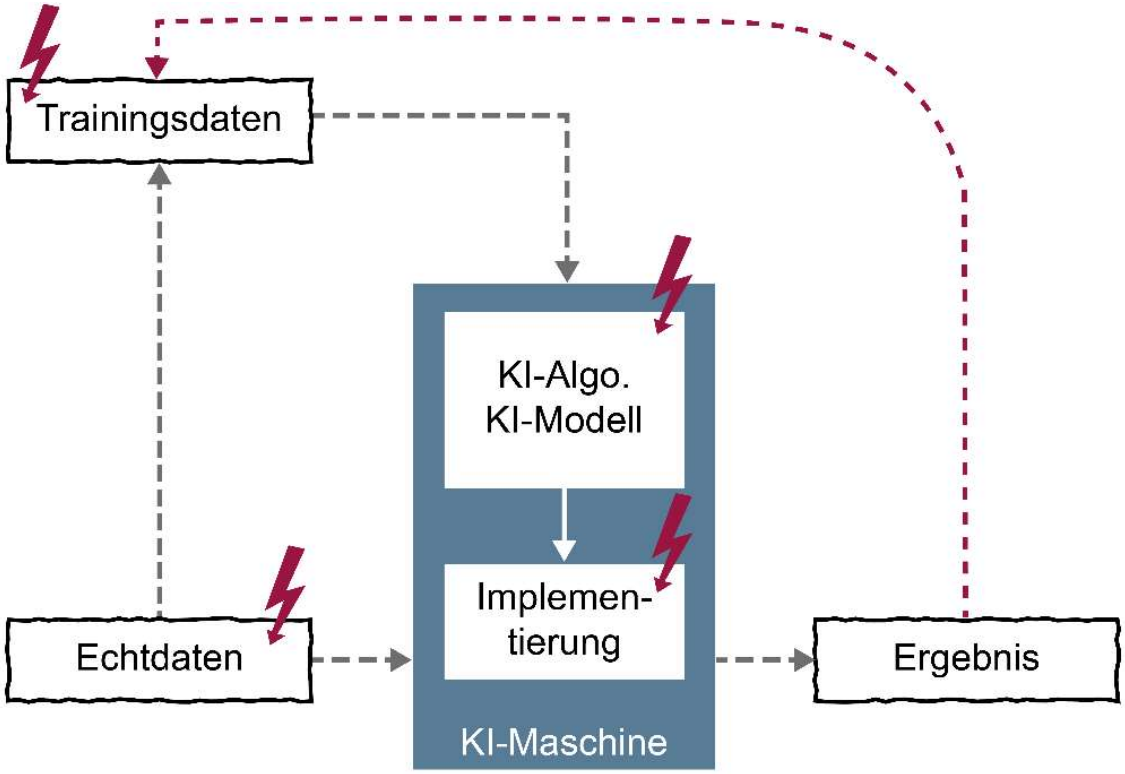
Schutzziele:

→ ***Integrität***
*(Erkennen von Manipulation der **Daten**)*

→ ***Vertraulichkeit***
*(Wahrung von Geschäftsgeheimissen - **Daten**)*

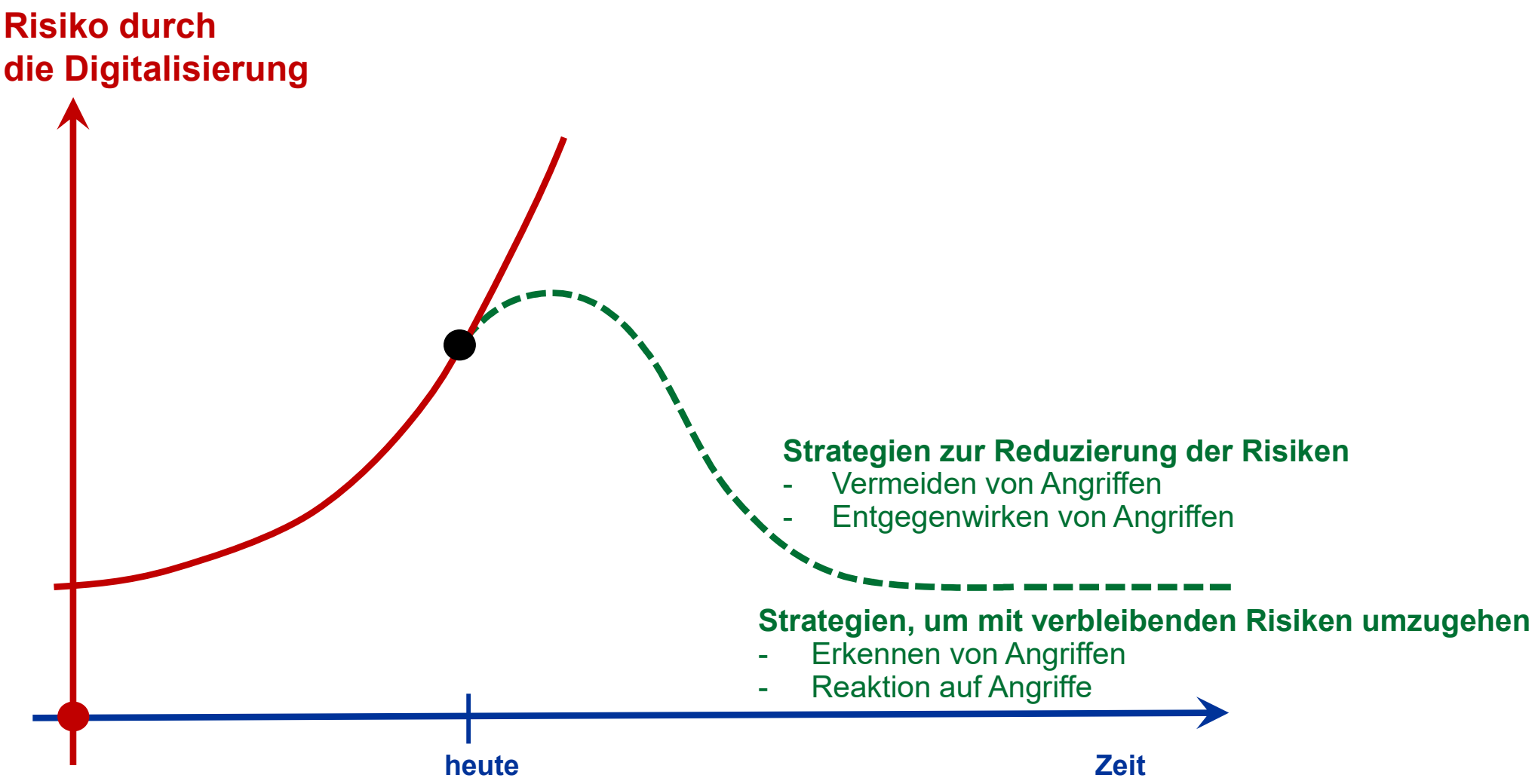
→ ***Datenschutz***
*(Schutz von personenbezogenen **Daten**)*

→ ***Verfügbarkeit***
*(der Anwendung und Ergebnisse - **Daten**)*



Zusammenarbeit** von **erfahrenen** **KI-** und **Cyber-Sicherheitsexperten
(Aufbau / Sicherstellung von Kompetenzen - Ergebnisse, Ethik, …)

Cyber-Sicherheitsstrategien
→ Übersicht



Prinzipielle IT-Sicherheitsstrategien
→ 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 das Unternehmen **alles wirklich *Notwendige*** für das Business **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 Mitarbeiter***

Prinzipielle IT-Sicherheitsstrategien
→ 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)*

Prinzipielle Sicherheitsstrategien
→ 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, Endgeräte, …) nach **Angriffssignaturen** oder **Anomalien** gesucht wird.

Cyber-Sicherheitsmechanismen

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

Prinzipielle Sicherheitsstrategien
→ 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-Dienst …) - KI*
- ***Digitale Forensik*** *(Maßnahmen optimieren, Schwachstellen schließen)*
- ***Definition von Befugnissen, Informationsflüsse, Entscheidungsprozess und Kommunikationsstrategien***
- ***Notfallplanung (Backup von Daten …)***

Mehr Data mehr Unsicherheit
→ Zusammenfassung

- Mit der **fortscheitenden Digitalisierung** haben wir **immer mehr Daten**

- **Unterschiedliche Daten haben verschiedene Cyber-Sicherheitsbedürfnisse**

- **Self-Sovereign Identity**
  → Die Identitätsdaten besitzt der Nutzer
  → Der Nutzer entscheidet die Weiterleitung und die Regel der Nutzung
  → …

- **Daten sind die Basis für KI-Anwendungen**
  → Die Qualität ist entscheidend
  → Wir müssen die rechtlichen Rahmenbedingungen beachten
  → Manipulationen müssen verhindert werden
  → …

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Immer mehr Data
= Immer mehr (Un) Sicherheit?

Die Gewährleistung der Cyber-Sicherheitsbedürfnisse unserer Daten ist entscheidet für die Sicherheit

Prof. Dr. (TU NN)
Norbert Pohlmann
Vorstandsmitglied eco – IT-Sicherheit

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

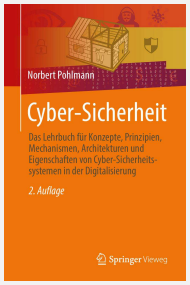
if(is) internet-sicherheit.

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

M. Hesse, N. Pohlmann: „Kryptographie (I bis VII): Von der Geheimwissenschaft zur alltäglichen Nutzanwendung“, IT-Sicherheit & Datenschutz - Zeitschrift für rechts- und prüfungssicheres Datenmanagement, Vogel-Verlag, 06/2006

N. Heibel, M. Linnemann, N. Pohlmann: „Mehr Vertrauenswürdigkeit für Anwendungen durch eine Sicherheitsplattform", in "Trusted Computing - Ein Weg zu neuen IT-Sicherheitsarchitekturen”, Hrsg.: N. Pohlmann, H. Reimer; Vieweg-Verlag, Wiesbaden 2008

J. Fischer, N. Pohlmann: „Ein Quantum Bit. Quantencomputer und ihre Auswirkungen auf die Sicherheit von morgen“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 1/2017

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: **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
Vorstandsmitglied eco – IT-Sicherheit

***Professor** für **Cyber-Sicherheit** 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 Cyber-Sicherheit *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 Cypersecurity – **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: 15+ Jahre if(is)

→ Übersicht

600+ Hacking-Shows
(mit 12 unterschiedlichen Hackern)

100 Forschungspartner
(Firmen/Behörden (65) und Hochschulen (35))

300+ Artikel / 400+ Vorträge / 30+ Bücher
(national und international)

150+ Fernsehauftritte
(Tagesschau/-themen, WDR, ZDF, SAT1, 3SAT, …)

200+ Abschlussarbeiten
(Diplom, Bachelor, Master und Promotionen)

200+ wissenschaftliche *und* studentische **Mitarbeiter** (zurzeit sind es mehr als 50)

60+ Drittmittelprojekte
mit Unternehmen / Behörden

150+ Zeitungsinterviews
(ZEIT, Focus, FAZ, Süddeutsche Zeitung, Handelsblatt, Welt, DPA, …)

53 Forschungsprojekte
(BMBF (20), BMWi (10), EU (4), NRW (15), BMI (4), …)

7 Cyber Security Challenges
Finden von IT-Sicherheitstalenten

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 Grids, -Car, -Traffic
- Cloud, Fog, Edge Computing
- Mobile Security
- Botnetz-Erkennung