

**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cybernation

→ **Motivation / Definition / Vorgehensweise**

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.

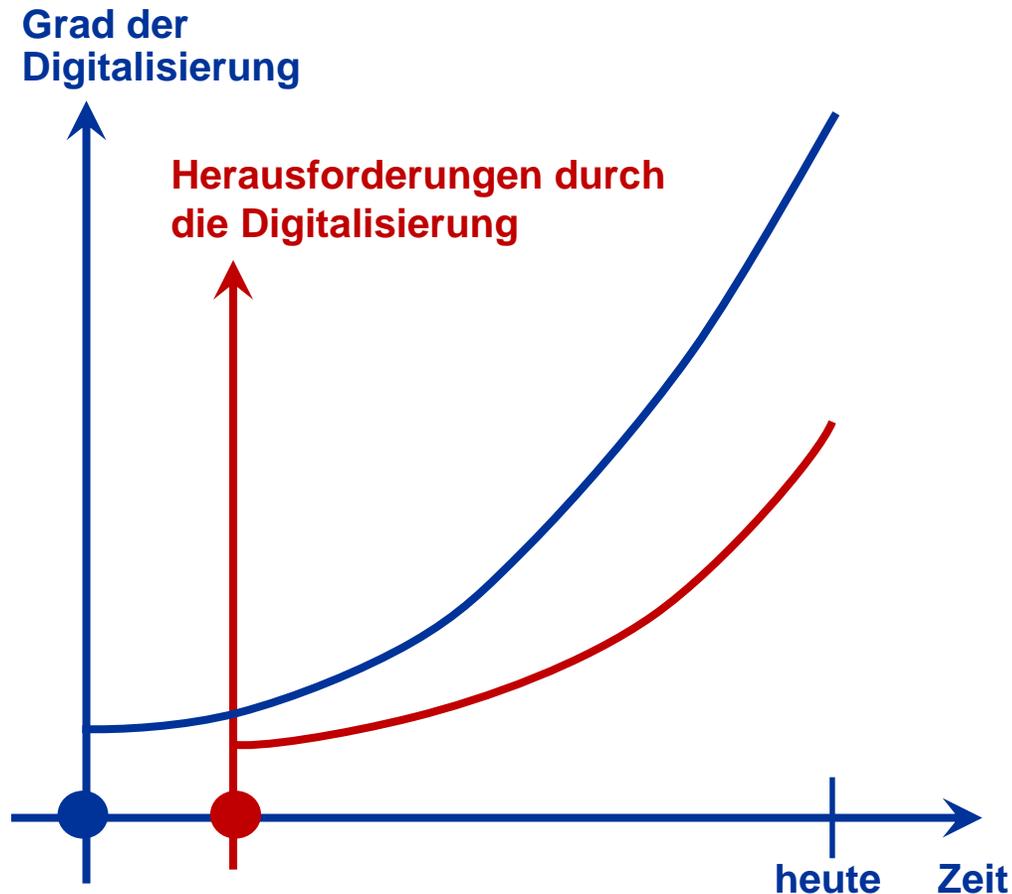
Cyber-Sicherheitslage

→ Motivation Cybernation

- *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 fortschreitenden Digitalisierung:**
 - *IT-Systeme und -Infrastrukturen werden immer komplexer (Steigerung der Abhängigkeiten... mehr Software/Schwachstellen ... Supply-Chain...)*
 - **Angriffsfläche wird größer**
 - *Die Methoden der Angreifer werden ausgefeilter*
 - **Kriminelles-Ökosystems → mehr Angriffe**
 - *Angriffsziele werden kontinuierlich lukrativer (Digitalisierung)*
 - **mehr digitale Werte**

Digitalisierung

→ Die Basis für eine Cybernation



Erfolgsfaktoren der Digitalisierung (Beispiele)

- **Kommunikationsinfrastruktur** (5/6G, Glasfaser, „NFC“ ...)
- Smartheit der Endgeräte (Watch, Phone, Book/Pad, IoT ...)
- **Leistungsfähigkeit zentraler IT-Systeme** (Cloud, Edge-Computing, Hyperscaler ...)
- **Verwendung von KI** (ML, LLM ...)
- Integration in IT-Prozesse und IT-Systeme (echtzeitorientiert+)
- **Moderne Benutzerschnittstellen** (Sprache, Gestik ...)

Herausforderungen Cyber-Sicherheit (Beispiele)

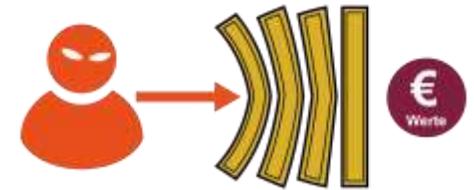
- **Softwarequalität** verbessern
- mehr Schutz vor Malware, unsichere Webseiten ...
- **Alternativen zu Passwörtern (MFA)** einführen
- verschlüsselte E-Mails, Kommunikation umsetzen
- **Umgang mit der Komplexität der IT-Systeme** managen ...
- „bessere“ IT-Sicherheitsarchitekturen motivieren
- **angemessene Verfügbarkeit** schaffen
- passenden Level IT-Sicherheit („Stand der Technik“) nutzen
- **sichere Hardware** (Sicherheitsmodule in IT-Systemen)

- Eine **Cybernation** ist ein **souveräner Staat**, der die **Möglichkeiten** und das **Potenzial** der **digitalen Technologien**
 - *umfassend*,
 - *sicher* und
 - *vertrauenswürdig*
ausschöpft.
- Das **Ziel** ist, die **Digitalisierung im Sinne der Gesellschaft** engagiert umzusetzen, um die **wirtschaftliche Leistungsfähigkeit** sowie die **Effektivität** der öffentlichen Dienstleistungen zu maximieren.
- Eine **Cybernation** bietet eine **sehr gute Voraussetzung** für eine *souveräne, sichere und vertrauenswürdige digitale Zukunft*.

Cybernation

→ Cyber-Sicherheit ist ein wichtiger Aspekt

- Wir brauchen **robuste Cyber-Sicherheitsmechanismen** auf der Basis des „**Stand der Technik**“, um uns **wirkungsvoll** gegen immer intelligentere Angriffe zu schützen.
- Alle relevanten **Cyber-Sicherheitsbedürfnisse** müssen im Cyberraum **garantiert** werden (*Vertraulichkeit, Integrität, Verfügbarkeit ...*).
- Die Cybernation muss **erhebliche Ressourcen** (*15-20 % der IT-Ausgaben*) in die Stärkung ihrer **Cyber-Sicherheit** investieren, um sich
 - **gegen Cyber-Sicherheitsrisiken zu schützen,**
 - **um Schäden zu vermeiden.**
- Dadurch kann das **Vertrauen** aller Beteiligten **in die Digitalisierung** gestärkt und so eine **notwendige Akzeptanz** erreicht werden.



- Das **Cyber-Sicherheitsniveau muss substantiell erhöht werden**, um uns deutlich wirkungsvoller zu schützen.
- **Technologiekompetenz** muss weiter **aufgebaut werden**, um **souveräner**, sicherer und vertrauenswürdiger agieren zu können.
- Vorhandenes **Know-how muss effizient gebündelt werden**, um *nicht-hilfreiche* Doppelarbeit zu vermeiden.
- Es muss ein **aktives Cyber-Ökosystem** etabliert werden, um erfolgreich und souverän wirken zu können (*Technik, Recht und Investitionen*).
- Alle **Cyber-Sicherheitsakteure** aus Wirtschaft, Wissenschaft und Staat in Deutschland müssen **eng zusammenarbeiten** und **gemeinsam handeln**.
- Wir brauchen ein gemeinsames und umfangreiches **Cyber-Sicherheitslagebild**, um schnell und gezielt aktiv zu werden.
- Die **Cyber-Resilienz muss wesentlich gesteigert werden**, um die Stärkung der Widerstandskraft aller IT-Systeme und IT-Infrastruktur zu gewährleisten.

Cybernation

→ Vorgehensweise

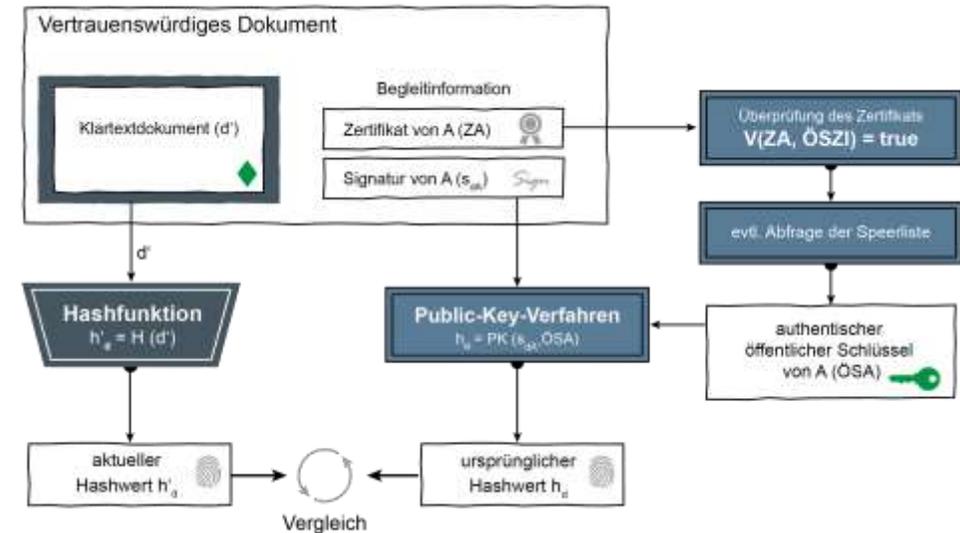
- Nur durch eine
 - **enge Zusammenarbeit** aller wichtigen Akteure,
 - die Motivation und Realisierung **passender Innovation** und
 - **gemeinsame** und **feste Entschlossenheit**

kann Deutschland eine wirkungsvolle Cybernation werden und die digitale Zukunft *souverän, sicher, vertrauenswürdig* und *erfolgreich* gestalten.

- Dazu brauchen wir **gemeinsame Ziele** und **ein Kommittent** zwischen den **wichtigen Akteuren**.
- Die Idee ist vorhanden, nur die **Umsetzung muss jetzt motiviert werden**.

Gemeinsame Umsetzung von E-Mail-Sicherheit

- **Verschlüsselung**, um die Vertraulichkeit von E-Mails zu gewährleisten
- **Digitale Signatur**, um
 - die Verbindlichkeit von Businessabläufen zu gewährleisten *und*
 - **Spear-Phishing- von echten E-Mails unterscheiden zu können**
- **Umsetzung / Aktivitäten**
 - Gemeinsam Ziele sowie den Umsetzungszeitpunkt definieren
 - Einfache Dienste und Technologien kollektiv motivieren
 - Aufklärung vereint durchführen, um die Umsetzung zu fördern ...



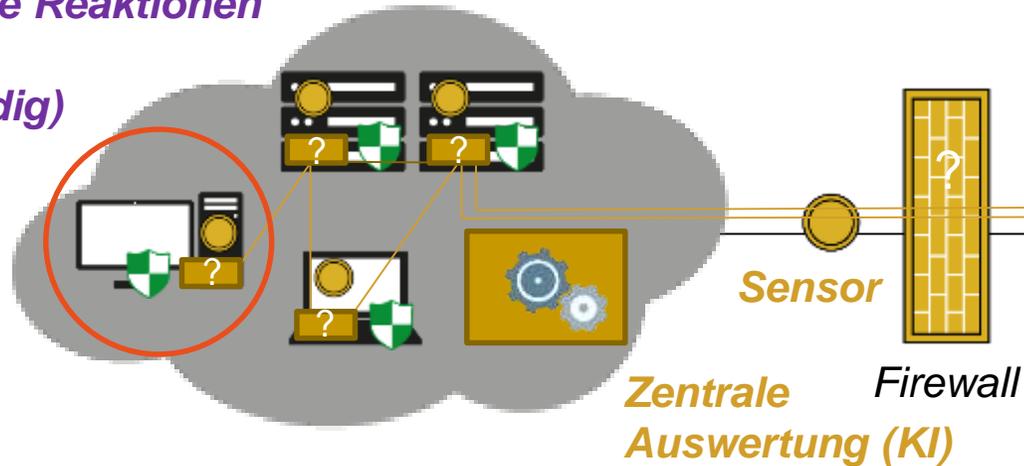
Weitere Themen: Zero Trust, sicheren Cloud-Anwendungen für kleine Unternehmen, Ressourcen-optimierte Aufteilung der notwendigen IT-Sicherheitsaktivitäten ...

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)



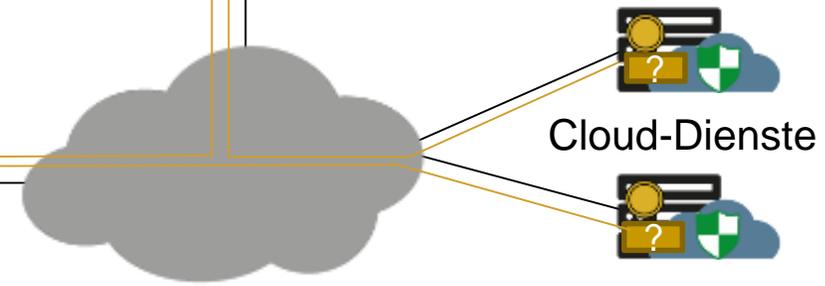
Unternehmensnetzwerk
(intern)

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)

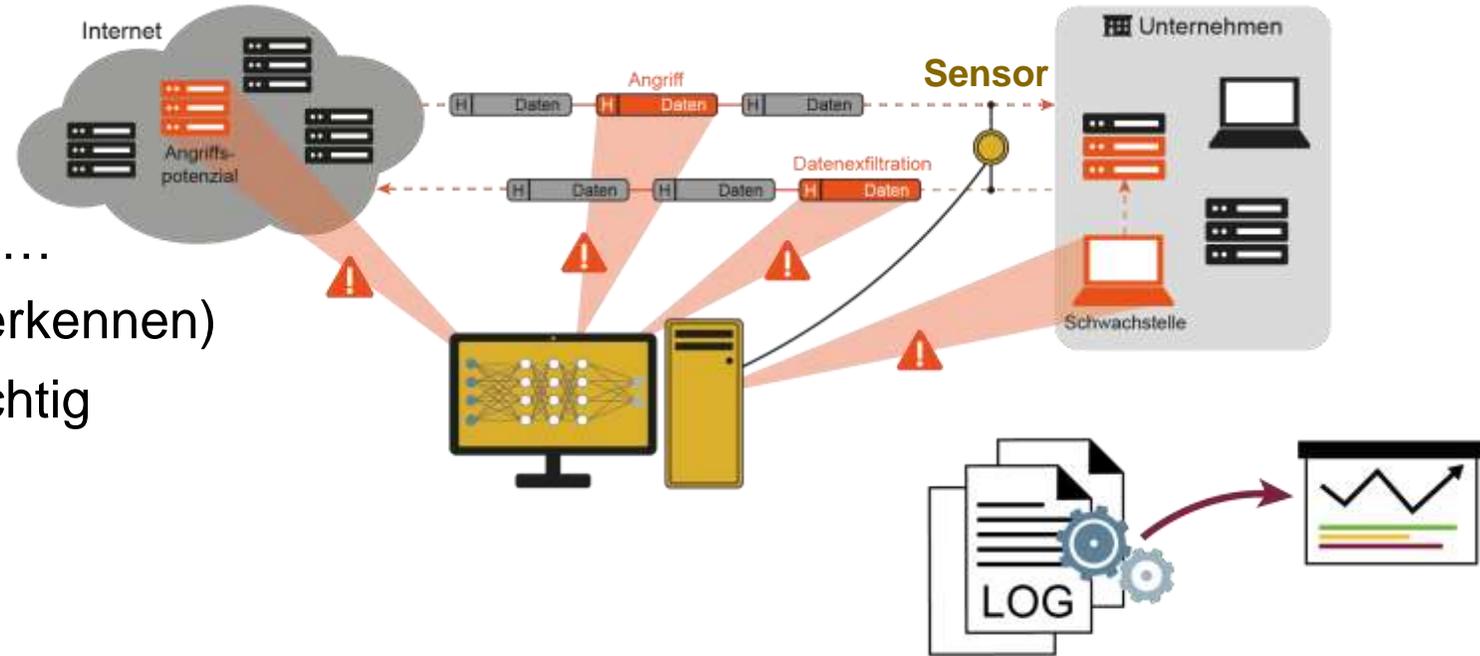
Alle IT-Systeme werden robust aufgebaut (Trusted und Confidential Computing)

Künstliche Intelligenz für IT-Sicherheit

→ Erkennen von Angriffen

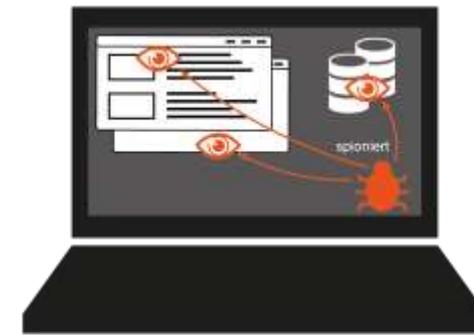
Erhöhung der Erkennungsrate von Angriffen

- Netzwerk, *IT-Endgeräte*, Server, *IoT-Geräte*, Cloudanwendungen ...
- adaptive Modelle (neue Angriffe erkennen)
- Anomalien: normal *versus* verdächtig



Weitere Bereiche, bei denen die Erkennung eine Rolle spielt:

- Netze / Internet
- *Malware*, Spam ...
- Fake-News
- *Deepfake*
- ...



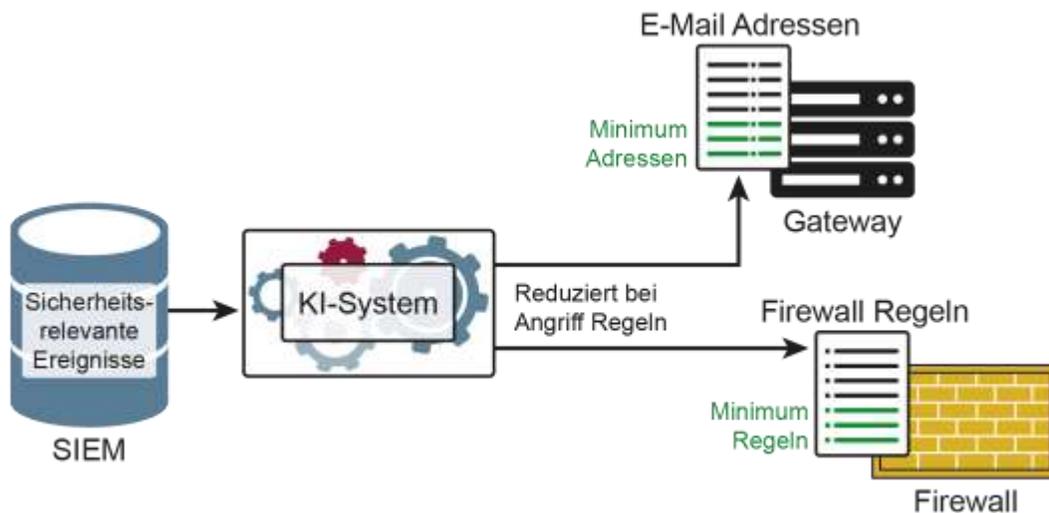
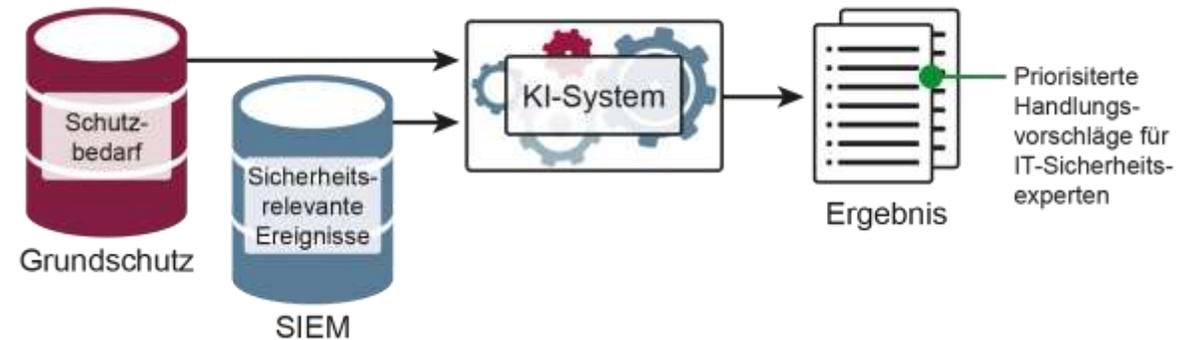
Künstliche Intelligenz für IT-Sicherheit

→ Unterstützung von IT-Sicherheitsexperten

Erkennen von **wichtigen sicherheitsrelevanten Ereignissen** mit einer **Priorisierung**

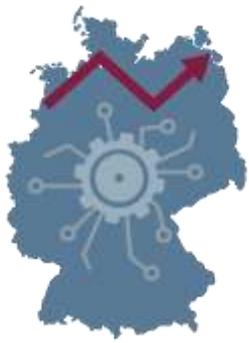
- **Idee:** IT-Sicherheitsexperten von **zeitaufwendiger Analysearbeit** zu entlasten.
- *Ein **KI-System analysiert** hunderte / tausende sicherheitsrelevante Ereignisse und zeigt, nach **welchen Prioritäten** diese **abgearbeitet** werden müssen.*

→ Dadurch wird der höchste Schutz **in der aktuellen Situation** für die Organisation erzielt.



(Teil-)Autonomie bei Reaktionen

- **Idee:** Wenn ein Angriff oder eine besondere Bedrohung erkannt wird, werden sofort die **Firewall- und E-Mail-Regeln automatisch reduziert**.
 - *Die **wichtigen Prozesse** für eine Organisation bleiben **erhalten** (Minimum Regeln).*
- Dadurch wird **Angriffsfläche** für die Angreifer deutlich **reduziert** und damit Schäden verhindert.



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cybernation

→ **Motivation / Definition / Vorgehensweise**

*Gemeinsam für eine souveräne, sichere und
vertrauenswürdige digitale Zukunft*

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.

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/>

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*



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

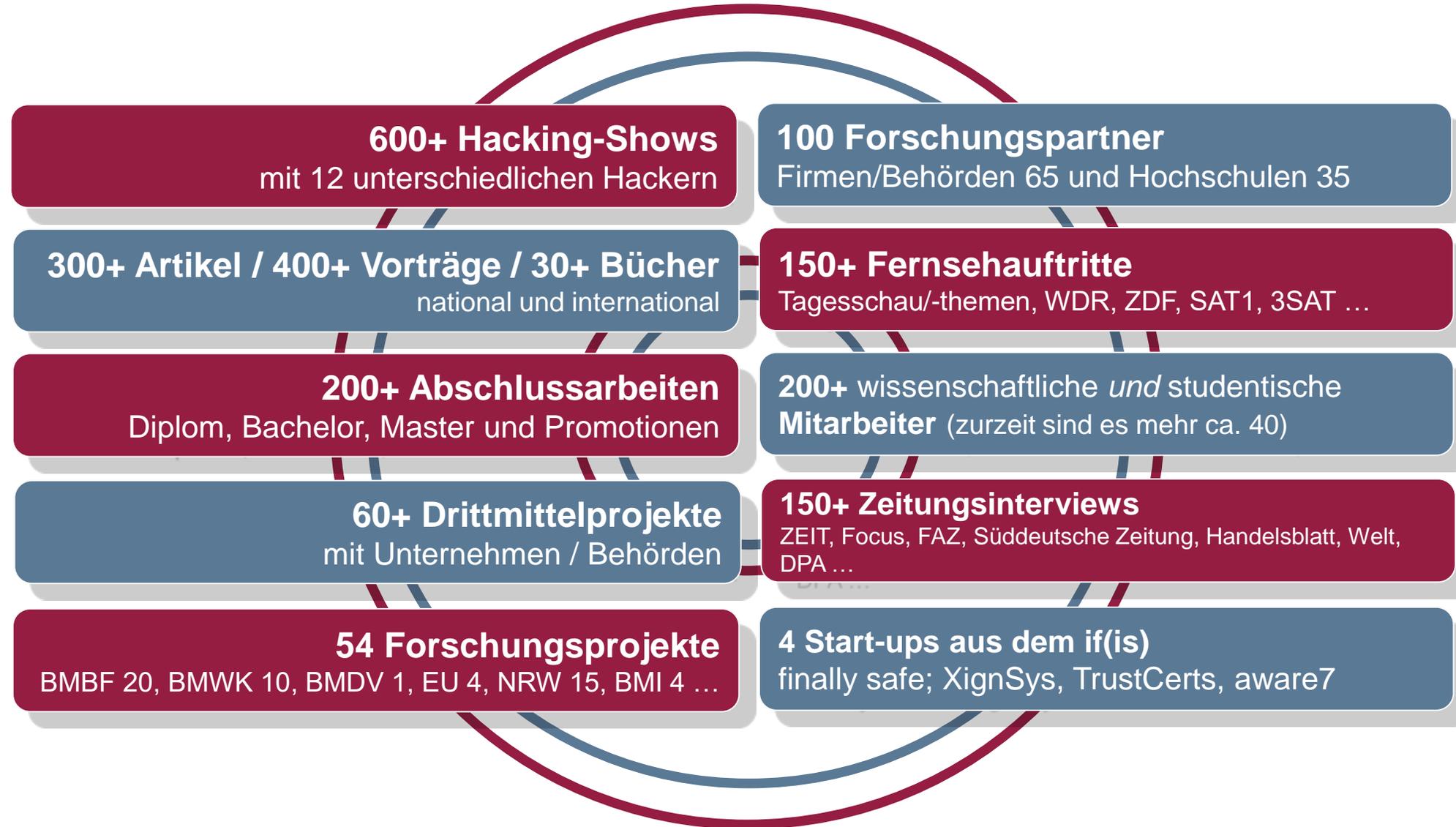
→ Übersicht

- 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