Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

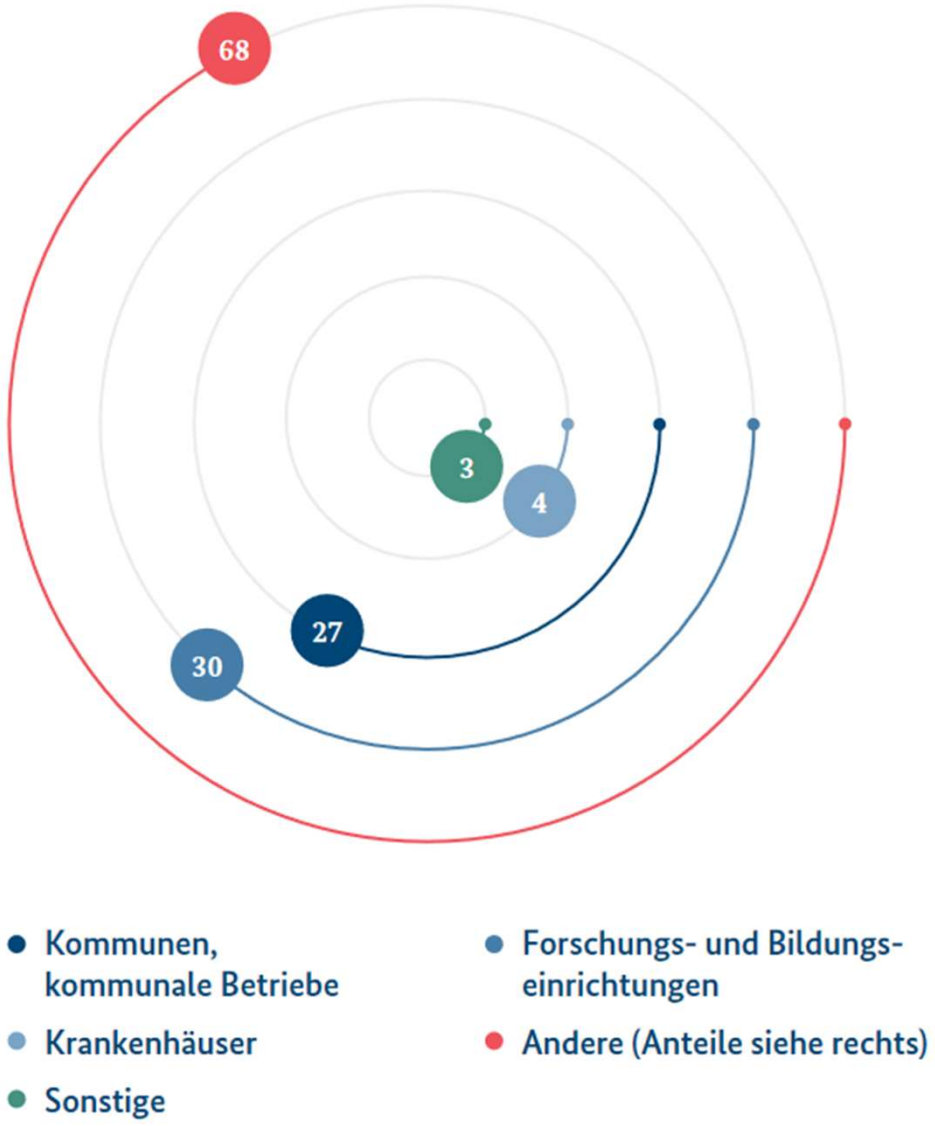
Kommunale IT-Sicherheit

Prof. Dr. (TU NN)
Norbert Pohlmann

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

Angriffe auf Kommunen
→ Wie viele Kommunen wurden angegriffen?

- Insgesamt **27 kommunale Verwaltungen** und **Betriebe** wurden Opfer von Ransomware-Angriffen
- Dabei kann es jeden treffen
  - Wie eine **ländliche Gemeinde** mit gerade mal 2.800 Einwohner
  - Oder eine **Großstadt** mit 1,8 Millionen Einwohner
- Häufig sind Stadt- oder Kreisverwaltungen betroffen
- Jedoch waren auch Unternehmen wie Nahverkehrsbetriebe, städtische Energieversorger oder Wohnungsbaugesellschaften betroffen
- Sogar der Friedhofsbetrieb einer Großstadt blieb nicht verschont



Angriffe auf Kommunen
→ Beispiele und deren Auswirkungen (1/2)

- Mit dem folgenschweren Angriff auf eine **Landkreisverwaltung in Sachsen-Anhalt** wurde wegen eines **Cyber-Angriffs** der **Katastrophenfall ausgerufen**.
- **Bürgernahe Dienstleistungen** waren **über 207** Tage lang **nicht** oder nur **eingeschränkt verfügbar**.
- Bei dem Angriff handelte es sich um eine **Ransomware** die **Dateien verschlüsselt** hat.
- Der Angriff wurde am **06.07.2021 entdeckt**, hatte aber bereits am **02.06 begonnen,** wie die Forensik feststellte

Angriffe auf Kommunen
→ Beispiele und deren Auswirkungen (2/2)

- **Ransomware legt Dienstleister Südwestfalen-IT von mehr als 70 Kommunen lahm**
- Die **Dienstleistungen** der **70 Kommunen** mit rund 1,7 Millionen Einwohner, waren praktisch lahmgelegt oder stark eingeschränkt
- **Die Auswirkungen auf die Rathäuser, die zu den Kunden von der Südwestfalen-IT zählen, waren / sind gravierend.**
- Durch schnelles **Notabschalten** der Rechner sind keine **persönlichen Daten** von Einwohnern abgeflossen

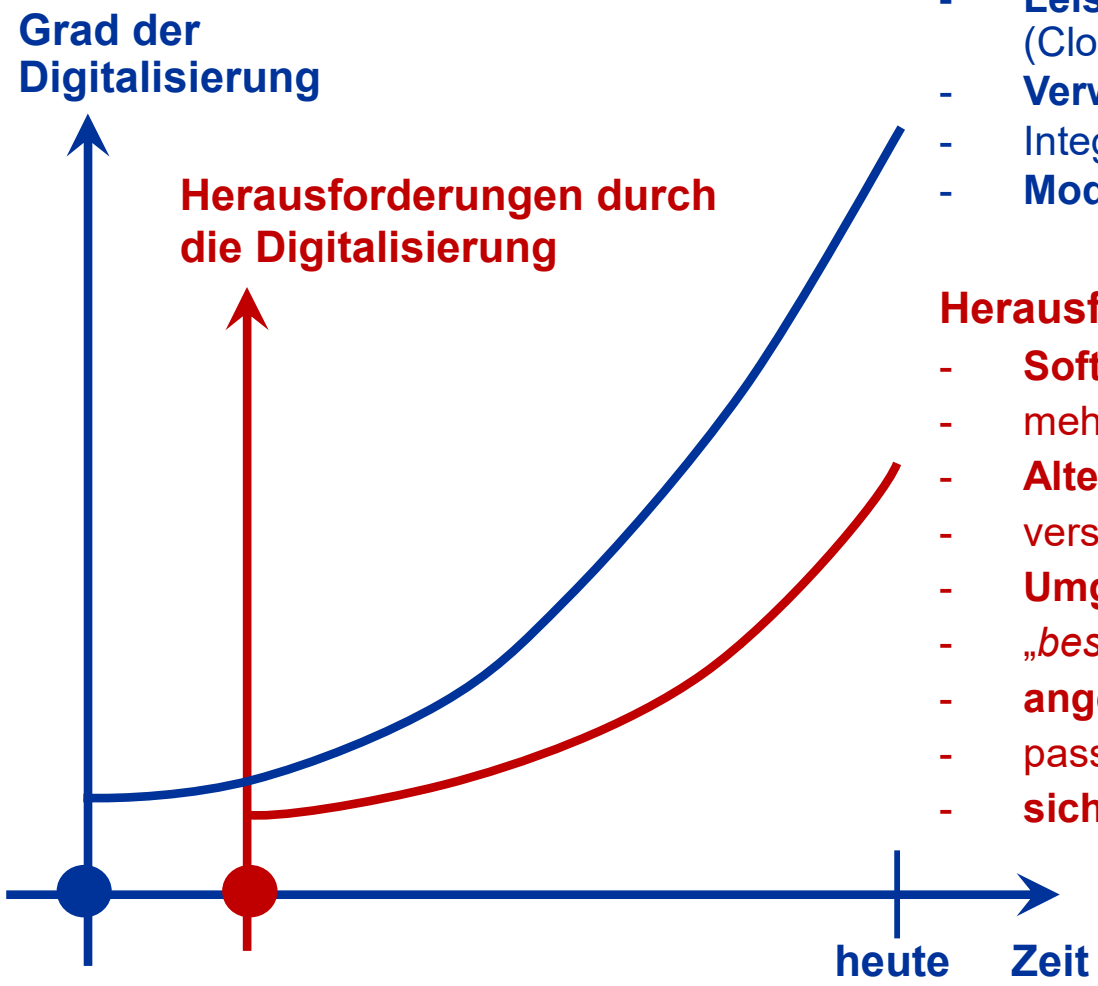
Cyber-Sicherheitslage
→ Einschätzung

- ***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/Schwachstellen … mehr Verbindungen … Supply-Chain… Facebook-Problem…)*
    - **Angriffsfläche wird größer**
  - *Die **Methoden der Angreifer** werden **ausgefeilter***
    - **Kriminelles-Ökosystem**
  - ***Angriffsziele** werden **kontinuierlich lukrativer** (Digitalisierung)*
    - **mehr digitale Werte**

Entwicklung der Digitalisierung
→ Erfolgsfaktoren und Herausforderungen



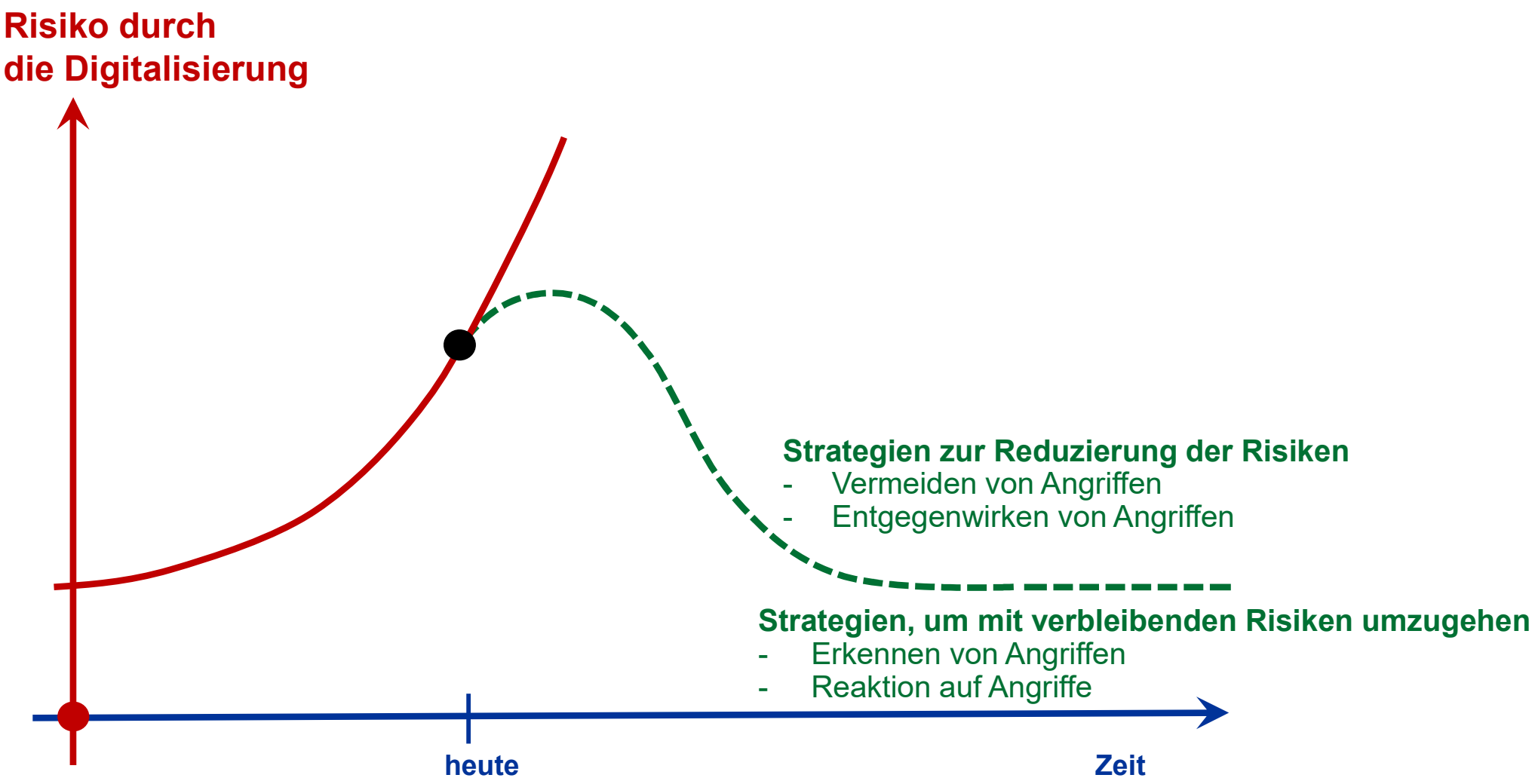
Erfolgsfaktoren der **Digitalisierung** (Beispiele)

- **Kommunikationsinfrastruktur** (**5**/6**G**, 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)

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***

Cyber-Sicherheit
→ Zusammenfassung

- Die **Cyber-Sicherheitsprobleme** im Cyberraum **sind größer** denn je und **wachsen weiter an.**

- **Cyber-Sicherheit** ist für unsere **Digitalisierung wichtig**, um die Zukunft sicher und vertrauenswürdig gestalten zu können.

- **Cyber-Sicherheitsstrategien** helfen auf verschiedenen Ebenen und Phasen, **Risiken zu reduzieren** und **verbleibende Risiken zu managen.**

Anwendungszentrum für KI in Kommunen
→ Übersicht

- Wir möchten eine Zukunft gestalten, in der unsere Städte **intelligent**, **resilient** und **nachhaltig** sind.
- Dazu werden wir *innovative* und *vertrauenswürdige* KI-Lösungen entwickeln, die das **Leben in Städten verbessern** und **die Gemeinschaft** sowie **die Wirtschaft** vor Ort in den Kommunen **stärken**.
- Die **Themenvielfalt** ist im kommunalen Umfeld und in der KI **sehr groß**: Stadt-, Mobilitäts-, Umweltplanung, *Ver- und Entsorgung*, zivile Sicherheit, *Bürgerbeteiligung* sowie KI-Technologien/Modelle, *Datenräume* und **IT-Sicherheit, *Datenschutz*** und **Vertrauenswürdigkeit.**
- Wir beschäftigen uns mit diesen Themen *für alle* und *mit allen* Kommunen **bundesweit**.
- Dieses Projekt ist die Basis, um das **Anwendungszentrum** für KI in Kommunen **langfristig zu etablieren**.

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Kommunale IT-Sicherheit

IT-Sicherheit
wird in der Zukunft immer wichtiger

Prof. Dr. (TU NN)
Norbert Pohlmann

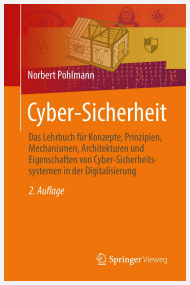
***Professor** für **Informationssicherheit** und*
Leiter** des **Instituts für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen

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/