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

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Bedrohungslage & Sicherheitsprinzipien für souveräne Datenräume

Prof. Dr. (TU NN)

Norbert Pohlmann

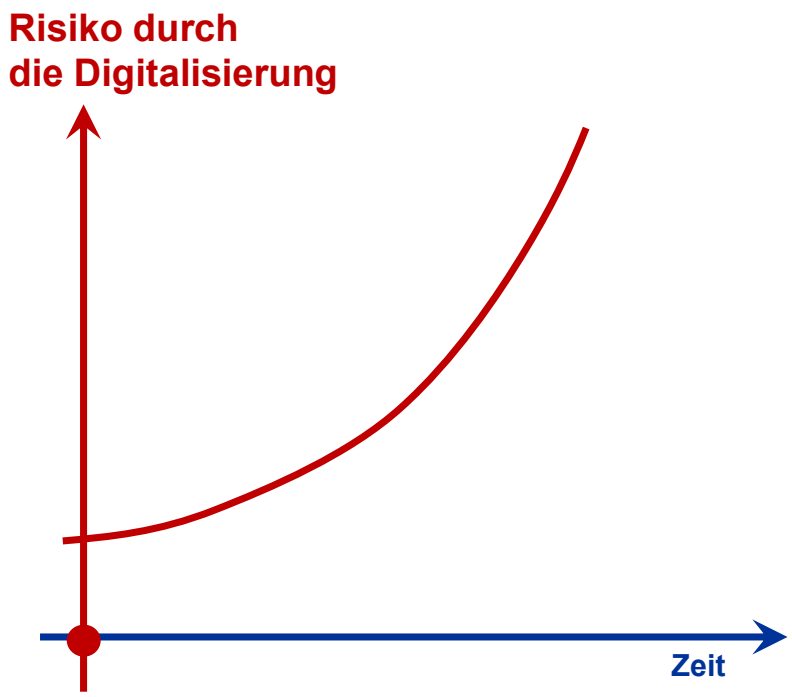
Professor** für **Cyber-Sicherheit** und **Leiter** des **Instituts für Internet-Sicherheit** – **if(is), Westfälische Hochschule, Gelsenkirchen

Vorstandsvorsitzender Bundesverband IT-Sicherheit - TeleTrusT

Vorstand im Verband der Internetwirtschaft - eco

if(is) internet-sicherheit.

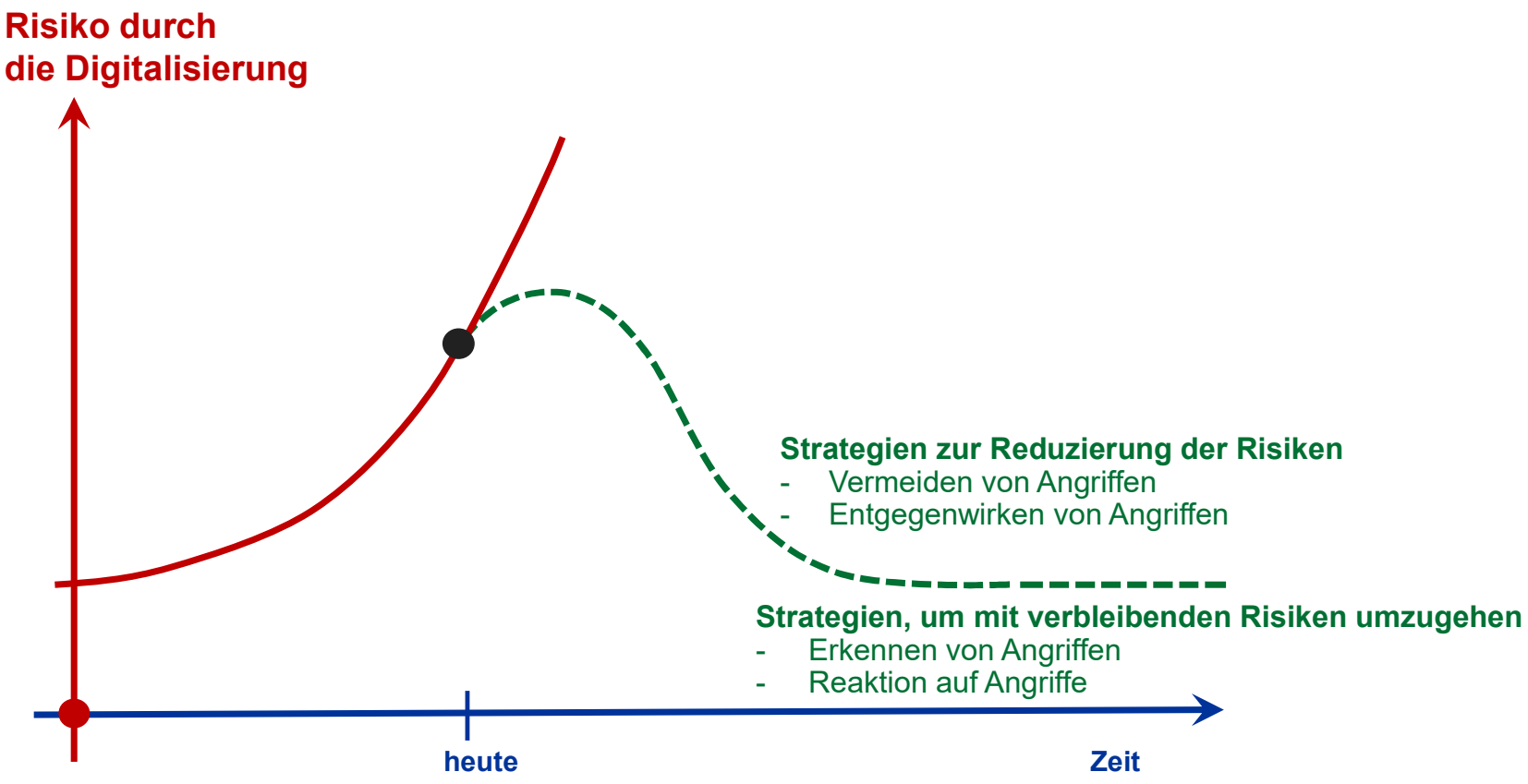
Cyber-Sicherheitslage
→ Eine Einschätzung



- *IT-Systeme und -Infrastrukturen sind nicht sicher genug konzipiert, aufgebaut, konfiguriert und upgedatet*
  (… gegen zunehmend intelligente Angriffe)
- *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)

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsstrategien
→ Übersicht



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Bedrohungslage
→Gefahren für Datenräume

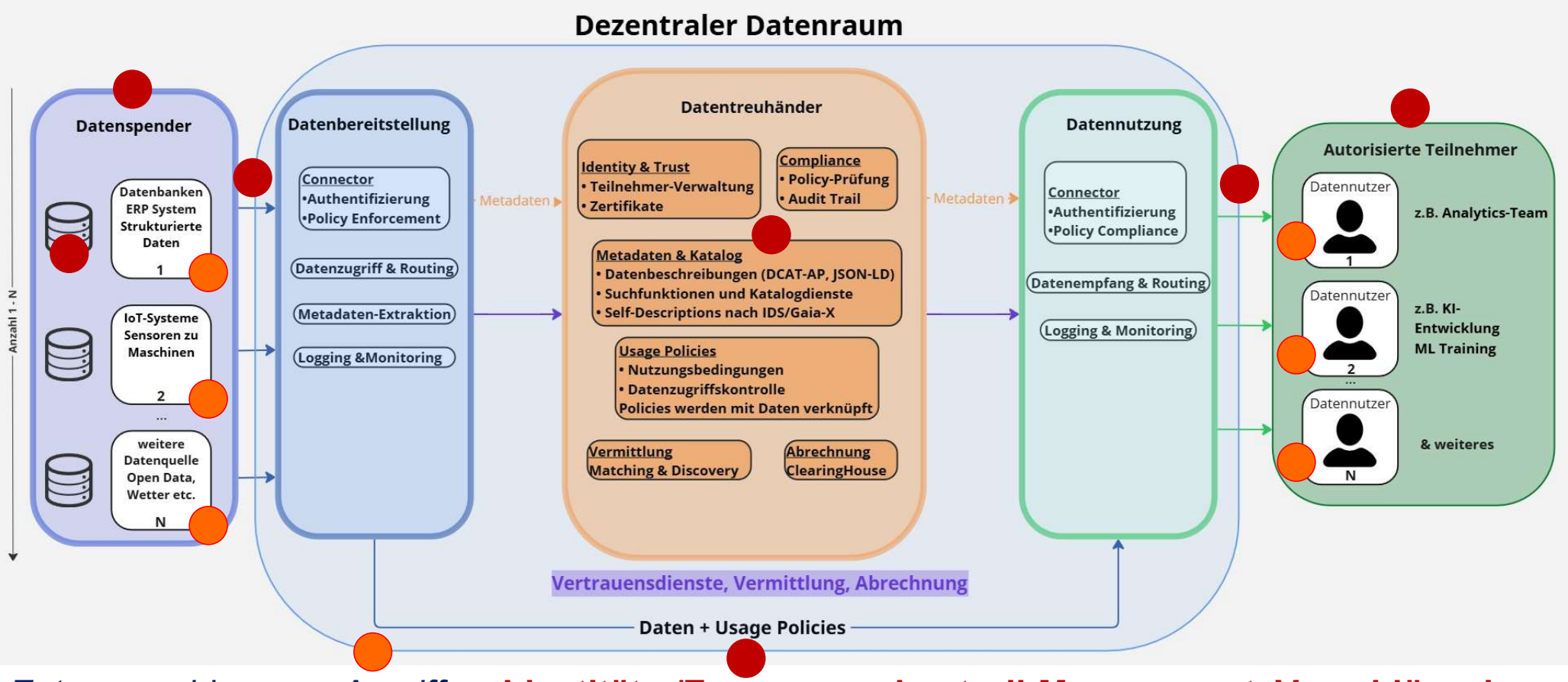
Angriffsvektor	*Beschreibung & Ziele*	*Verletztes Schutzziel*
Cyberkriminalität (z.B. Ransomware-as-a-Service)	Erpressung, finanzielle Gewinne, Datenabfluss, Systemblockade.	Verfügbarkeit, Vertraulichkeit
Advanced Persistent Threats (APT)	Gezielte Spionage oder Sabotage (oft staatlich gesteuert); Einschleusen von Malware.	Vertraulichkeit, Integrität
Phishing & Social Engineering	Einfallstor für Malware und Zugangsdatenmissbrauch durch menschliche Unzulänglichkeiten.	Vertraulichkeit
Schwachstellen (z.B. Zero-Day-Exploits)	Ausnutzung unbekannter oder ungepatchter Softwarelücken für unautorisierten Zugriff.	Integrität, Vertraulichkeit
Menschliches / Organisatorisches Versagen	Unzureichende Passwörter, Fehlkonfiguration, unautorisierte Tools (Schatten-IT).	Vertraulichkeit, Integrität, Verfügbarkeit
Distributed Denial of Service (DDoS)	Datenräume durch Erschöpfung (Bandbreite, CPU, RAM) lahmlegen.	Verfügbarkeit

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Datenraum
→ Übersicht

Vermeiden von Angriffen: **geschulte Mitarbeiter**

Reaktion auf Angriffen: **Notfall planen und trainieren**



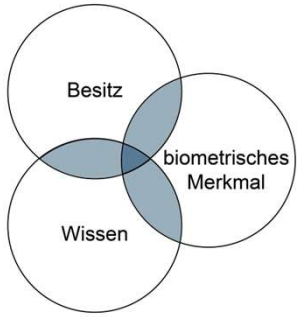
Entgegenwirken von Angriffen: **Identitäts-/Zugangangskontroll-Management, Verschlüssel. …**

Erkennen von Angriffen: **z.B. gemeinsames Attack Surface, *Angriffs* Management**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

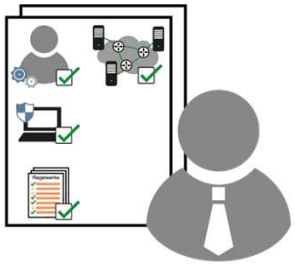
Sicherheitsprinzipien
→ Verifizierte Identitäten & Zugriffskontrolle

Dieses Prinzip gewährleistet, dass nur berechtigte Personen (oder Systeme) auf die Daten zugreifen dürfen.

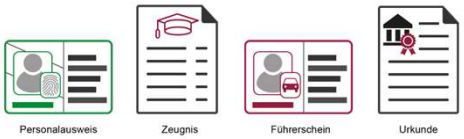


- **Zwei-Faktor-Authentifizierung (2FA / MFA):** Erhöhte Sicherheit beim Login.

- **Attributbasierte Berechtigungen (ABAC):** Feingranulare Steuerung, wer welche Daten sehen, bearbeiten … darf.



- **Protokollierung / Audit-Trails:** Lückenlose Aufzeichnung jeder Aktion (Wer? Was? Wann? Wo?).
- **Verifiable Credentials (VC):**



  - Digitale, kryptografisch gesicherte und fälschungssichere Nachweise von Dritten (Issuer), die ein Holder (Nutzer) kontrolliert und einem Verifier (Datenraum) vorlegen kann.
  - VCs werden primär zur Verifizierung der Identität und der Berechtigungen (z.B. Qualifikationen, Status) der Teilnehmer eines Datenraums verwendet. Sie ersetzen traditionelle, zentrale Identitätsnachweise durch selbstbestimmte, dezentrale.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Sicherheitsprinzipien
→ Schutz der Daten durch Verschlüsselung (1/2)

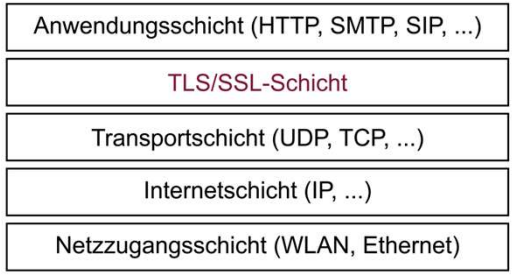
Dieses Prinzip gewährleistet, dass nur berechtigte Personen (oder Systeme) Daten lesen dürfen.

In Motion

- **Ende-zu-Ende-Verschlüsselung (E2EE):**
  Daten sind vom Absender bis zum Empfänger geschützt (wichtig für Datenräume, die besonders hohe Vertraulichkeit erfordern).

S/MIME

- **Transportverschlüsselung (TLS/SSL):**
  Schutz der Daten während der Übertragung (z.B. HTTPS).



At Rest

- **Festplattenverschlüsselung, Datenbankverschlüsselung …**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Sicherheitsprinzipien
→ Schutz der Daten durch Verschlüsselung (2/2)

In Use

- **Confidential Computing:**
  Mithilfe von Confidential Computing ist es möglich, die Daten und den Code einer Anwendung vertrauenswürdig im verschlüsselten Zustand als Enclaves auf einem fremden IT-System wie Cloud-Infrastrukturen sicher zu verarbeiten.

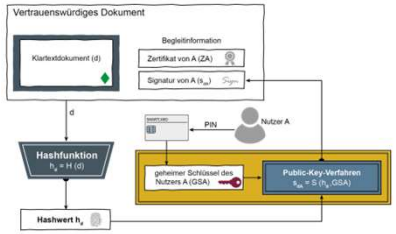
Gesetzesebene

- **Datenspeicherung in der EU/Deutschland:**
  Gewährleistung der DSGVO-Konformität und Datenresidenz.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Sicherheitsprinzipien
→ Asset Authentifizierung & Kontrolle

Dieses Prinzip konzentriert sich auf die Sicherung der Daten-Assets selbst.



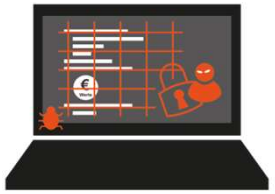
- **Asset Authentifizierung:** Sicherstellung, dass die im Datenraum abgelegten Daten echt, vollständig und unverändert sind (Integrität). Dies kann durch digitale Signaturen oder Hash-Prüfsummen z.B. beim Upload erfolgen.
- **Dynamische Wasserzeichen:** Personengebundene, nicht entfernbare Markierungen von Daten, um die Weitergabe nachvollziehbar zu machen.
- **Hardware-Sicherheitsmodule (Smartcards, TPMs, High-Level Security Modules):** Mithilfe von Hardware-Sicherheitsmodulen wird der unerlaubte Zugriff und die unerlaubte Nutzung von Sicherheitsinformationen unterbunden.

- **Compute to Data:**
  Anstatt die Daten an eine Anwendung zu übertragen, sendet die Anwendung einen Verarbeitungsauftrag an den Datenraum (wird dort berechnet)
- **Zertifizierungen:** Nachweis der Sicherheit des Datenraums (z.B. ISO 27001, SOC 2 Type II).

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

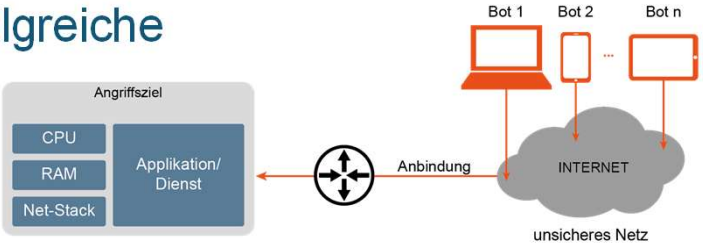
Sicherheitsprinzipien
→ System-Sicherheit (1/2)

Dieses Prinzip konzentriert sich auf die Sicherung der genutzten IT-Infrastruktur.



- **Anti-Malware-Lösungen / End-Point-Sicherheit** sorgen dafür, dass illegales Aufspielen und kriminelles Nutzen von Malware nicht umgesetzt werden kann.

- Mithilfe von **Anti-DDoS-Verfahren** wird die erfolgreiche Umsetzung von DDoS-Angriffen verhindert.



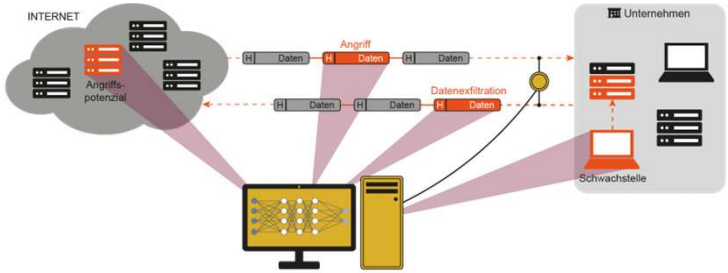
- **Zero Trust**
  Sämtliche Kommunikation zwischen den IT-Entitäten wird **kontrolliert**, reglementiert sowie **auf Angriffsversuche untersucht**.
  Zudem werden alle IT-Entitäten robust aufgebaut und müssen sich **gegenseitig authentifizieren**.
  Dazu ist es notwendig, dass alle IT-Entitäten eine **eindeutige digitale Identität** haben.

…

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Sicherheitsprinzipien
→ System-Sicherheit (2/2)

- **Erkennen von Angriffen:** Angriffe müssen führzeitig erkannt werden, um zu versuchen, den Schaden so schnell wie möglich zu minimieren.
  …



- **Notfallplanung:** Wichtig ist auch, dass es bereits getestete Reaktionskonzepte (Notfallplanungen) gibt, in denen definiert ist, was im Krisenfall die richtige Vorgehensweise ist und welche Personen die Rechte haben, die entsprechenden Reaktionen im Angriffsfall auszulösen.
  …

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

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

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Bedrohungslage & Sicherheitsprinzipien für souveräne Datenräume

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

Master Internet-Sicherheit

https://it-sicherheit.de/master-studieren/

Glossar Cyber-Sicherheit

https://norbert-pohlmann.com/category/glossar-cyber-sicherheit/

Vertrauenswürdigkeits-Plattform - Trust4Good

https://vertrauenswürdigkeit.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

Alles rund um IT-Sicherheit: Wissensaustausch, Unterstützung, IT-Sicherheitsanbieter & -Lösungen, News/Artikel/Blogs, Veranstaltungen.
https://www.it-sicherheit.de/

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen