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

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyber-Resilienz
→ Idee und Umsetzung

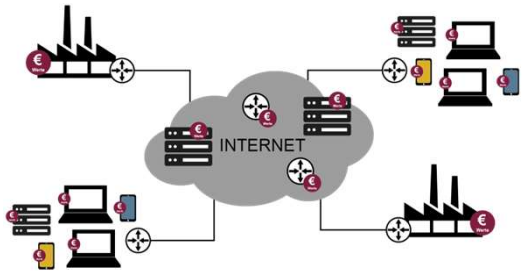
Prof. Dr. (TU NN)
Norbert Pohlmann

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

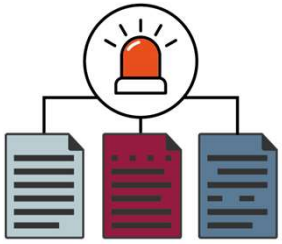
if(is)
internet-sicherheit.

Cyber-Resilienz
→ Definition (1/2)

- **Cyber-Resilienz**, **Cyber-Widerstandsfähigkeit** oder **Cyber-Anpassungsfähigkeit** ist eine ganzheitliche Strategie zur Stärkung der Widerstandskraft der IT-Systeme und IT-Infrastruktur eines Unternehmens gegenüber Cyber-Angriffen.



- **Cyber-Resilienz** beinhaltet unter anderem die Konzepte der
  - **Cyber-Sicherheit** *und des*
  - **Business Continuity Management (BCM)**, *aber auch*
  - **digitale Forensik** *und*
  - **Incident Response**.



- **Cyber-Resilienz** soll **Cyber-Angriffe** auf die IT **verhindern** ***sowie*** den sicheren **Weiterbetrieb der Geschäftsprozesse** *und* die **schnelle Wiederaufnahme** des Betriebs der IT-Systeme sowie der IT-Infrastruktur **bei einem Ausfall sicherstellen**.

Cyber-Resilienz
→ Definition (2/2)

- **Je größer** die zu schützenden **Werte** eines Unternehmens sind und damit das **Risiko** eines finanziellen **Schadens**, **desto höher** muss die **Cyber-Resilienz** sein.

- **Ziel** ist es, eine **hohe Robustheit** der IT-Systeme sowie der IT-Infrastruktur eines Unternehmens **gegenüber den verschiedenen Bedrohungen** zu schaffen und **Risiken für Betriebsausfälle** zu **minimieren.**

→ Letztendlich soll der **Fortbestand** des Unternehmens **gesichert werden**.

→ Sofern ein Unternehmen bereits über eine gute Cyber-Sicherheit verfügt, ist die Weiterentwicklung hin zu einem **cyber-resilienten Unternehmen** in der Regel gut zu bewältigen.

→ Es geht darum, wie schnell man sich nach einem Angriff **davon erholt**.

Cyber-Resilienz

→ Aspekt: Business Continuity Management (BCM)

- Business Continuity Management (BCM) besteht aus Strategien, Plänen, Maßnahmen und Prozessen, um ernsthafte **Schäden** durch die **Unterbrechung des IT-Betriebs** eines Unternehmens zu **minimieren**.

- Mit Hilfe eines Präventions- und Wiederherstellungssystems soll die Sicherstellung des **Fortbestands eines Unternehmens** im Sinne ökonomischer Nachhaltigkeit in Bezug auf Cyber-Sicherheitsrisiken mit hohem Schadensausmaß **gewährleistet werden**.

→ Dies soll sowohl den **optimalen Betrieb** der IT-Systeme und IT-Infrastrukturen unter Krisenbedingungen garantieren als auch den **problemlosen** und **schnellen Wiederanlauf** der IT-Prozesse nach einem Ausfall ermöglichen.

→ Das allgemeine Ziel ist, sowohl den **Fortbestand** eines Unternehmens zu **sichern** als auch den Erhalt der **wirtschaftlichen Tätigkeit aufrecht erhalten**.

Cyber-Resilienz

→ Aspekt: Digitale Forensik

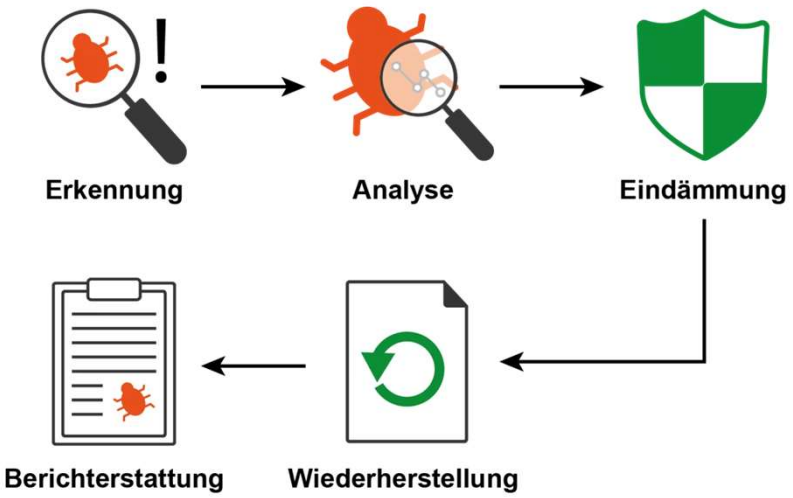
- Digitale Forensik ist eine streng methodisch vorgenommene **Datenanalyse** *auf Datenträgern*, *von IT-Systemen* und *Kommunikationsnetzwerken* **zur Aufklärung von Vorfällen** durch forensische Sicherung von digitalen Beweisen sowie der Analyse der digitalen Beweismittel.

→ Die Analyse der gesammelten Daten hilft, den Vorfall aufzuklären, um gegebenenfalls vorhandene **IT-Sicherheitsmaßnahmen zu optimieren** oder **Schwachstellen zu schließen**.

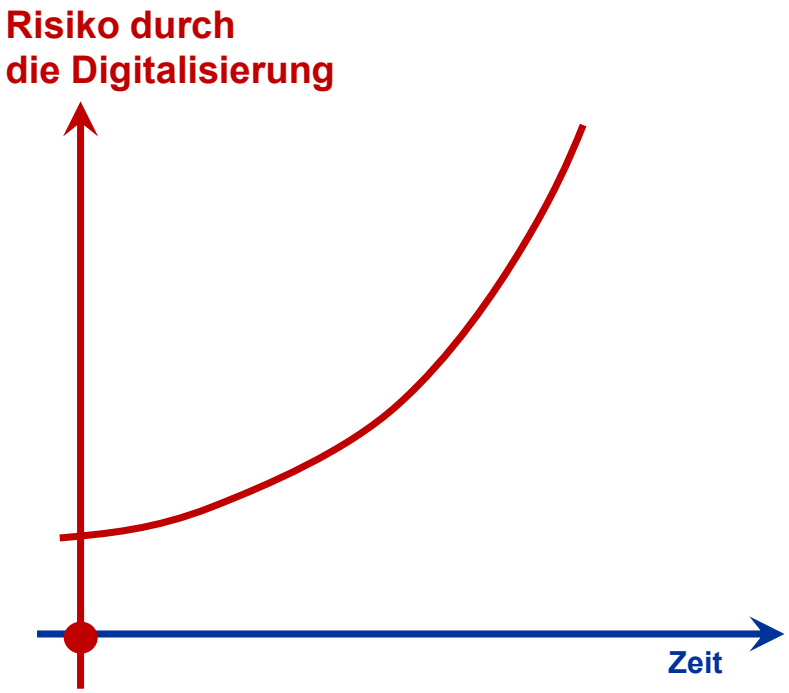
→ Viele **Angriffe werden wiederholt**, weil der Zugang offen bleibt (von derselben oder einer anderen Gruppe).

Cyber-Resilienz
→ Aspekt: Incident Response

- **Incident Response** auf einen Cyber-Sicherheitsvorfall bezeichnet einen formalen Prozess, der in Unternehmen implementiert wird, um auf **Cyber-Sicherheitsvorfälle schnell** und **angemessen** zu **reagieren**.
- Es handelt sich um eine strukturierte Methodik oder Vorgehensweise, die darauf abzielt, **potenzielle Cyber-Sicherheitsgefahren sicher zu erkennen**, ausführlich zu analysieren und darauf schnell zu reagieren, **um die negativen Auswirkungen** auf die IT-Infrastruktur **zu minimieren**.



Warum Cyber-Resilienz wichtig ist
→ Übersicht

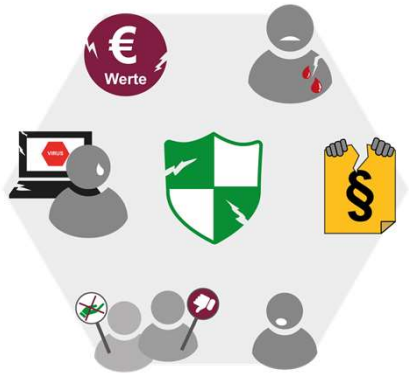


- **Zunehmende Cyber-Bedrohungen:**
  Ransomware, Supply-Chain-Angriffe, KI-basierte Attacken, Fake-Informationen (CEO-Fraud), DDoS-Angriffe …
- **100% Cyber-Sicherheit ist unrealistisch**
  → Fehler und Ausfälle sind unvermeidlich
  → Ein Restrisiko muss immer eingeplant werden
- **Ziel:**
  Betriebsfähigkeit** trotz Cyber-Angriffen und Ausfälle **erhalten

Softwarefehler - Update - CrowdStrike
→ Beispiel für zu wenig Cyber-Resilienz

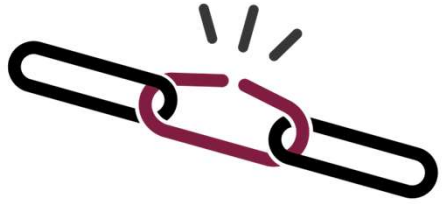
- **Ein Softwarefehler** in einem Update der IT-Sicherheitsfirma Crowdstrike hat im Juli 2024 dafür gesorgt, dass nicht nur deren End Point-Sicherheit, sondern auch **8,5 Millionen Microsoft-Systeme** und daraus resultierend flächendeckend kritische Anwendungen **nicht mehr funktioniert haben**.
  - **Notrufe** ließen sich **nicht abzusetzen**,
  - Krankenhäuser mussten **Operationen verschieben**,
  - vielerorts wurde der **Flugbetrieb eingestellt**,
  - **Zahlungen** konnten **nicht durchgeführt** werden und
  - **tausende Mitarbeiter konnten nicht arbeiten.**

➢ Ein **Softwarefehler in einem Update** hat einen **Schaden** von mehr als **1,5 Milliarden Euro Schaden** verursacht!



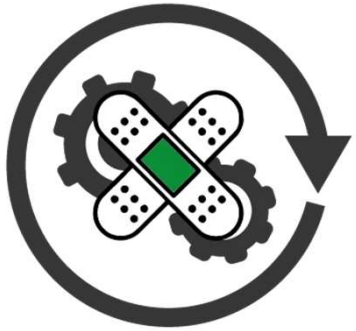
Software-Fehler – Ursache
→ Blickwinkel: CrowdStrike

Nicht gut genug getestet, *fasche Update-Strategie*



Die Zurverfügungstellung von **qualitativer Software** liegt in der **Verantwortung des Herstellers** – aber,
Software wird praktisch **nie 100% fehlerfrei** sein können.

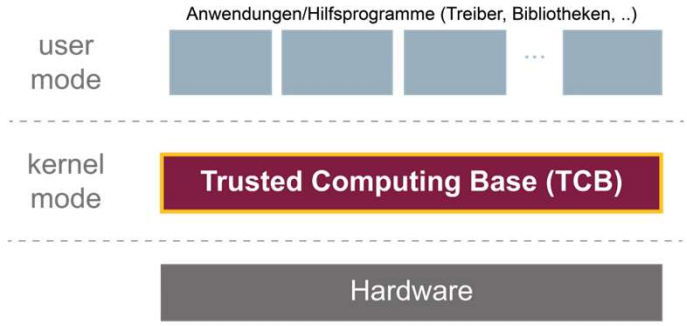
- Aus diesem Grund muss das **Vorhandensein von Fehlern immer** in den IT-Sicherheitskonzepten mit **eingeplant werden**.
- Trotzdem müssen die Software-Hersteller:
  - Deutlich **umfangreich testen**, um möglichst viele **Fehler** zu **finden**, **bevor** ein **Update** verteilt wird.
  - **Gestaffelte Updates** umsetzen, um die Risiken und damit die Schäden bei fehlerhaften Updates zu minimieren.



Software-Fehler – alte Betriebssysteme
→ Blickwinkel: Microsoft

IT-Sicherheitsarchitektur müssen so aufgebaut werden, dass Fehler von einem Drittanbieter nicht zum Ausfall von Millionen (8,5 Mio.) von IT-Systemen führen.

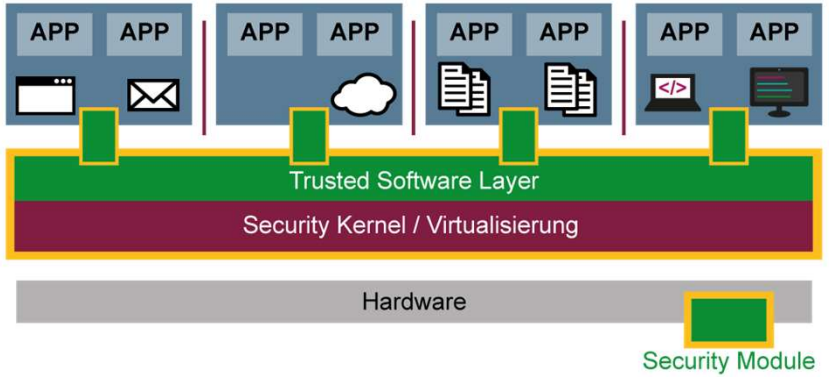
Wir benötigen sichere IT-Sicherheitsarchitekturen



- **Wenige Lines of Code:**
  kleine vertrauenswürdige Softwarebasis (TCB)
  (besonders sicher umgesetzt – keine Angriffsfläche)

- **Isolierung:**
  Anwendungen werden **isoliert** voneinander in virtuellen Maschinen **zur Ausführung** gebracht
  (Fehler bleiben isoliert)

- **Modularisierung / Robustheit:**
  Ein **Softwarefehler**, der bei einer solchen IT-Sicherheitsarchitektur auftreten würde, **beeinflusst keine anderen Anwendungen** auf dem gleichen IT-System
  (eingeschränkte Auswirkung)

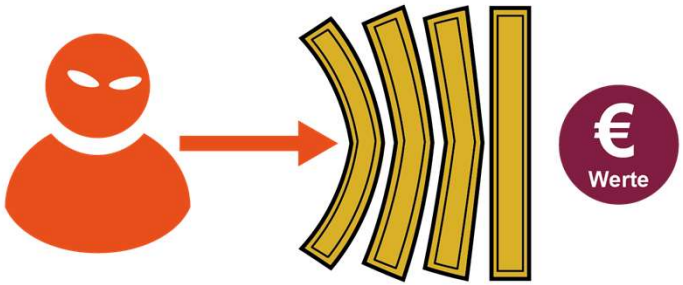


Software-Fehler – keine Redundanz

→ Blickwinkel: Anwender (Flughäfen, Banken …)

Anwendungen müssen deutlich robuster geplant und aufgebaut werden.

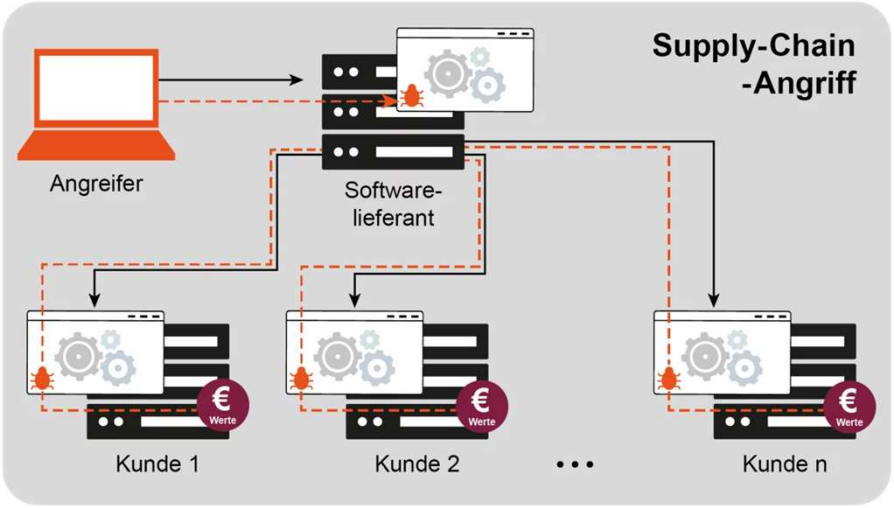
Wir brauchen redundante IT-Lösungen für deutlich mehr Resilienz



- **Cloud-Anwendungen**
  (über zentrale Cloud-Dienste)
- **Aktive Redundanz** mit **unterschiedlichen Zulieferern**
  (schnelles umswitchen, wenn ein Dienst ausfällt)
- ***Moderne Konzepte***
  - z.B. mit Confidential Computing flexible auf Cloud-Infrastrukturen

IT-Supply Chain-Security
→ Cyber-Resilienz wird komplexer

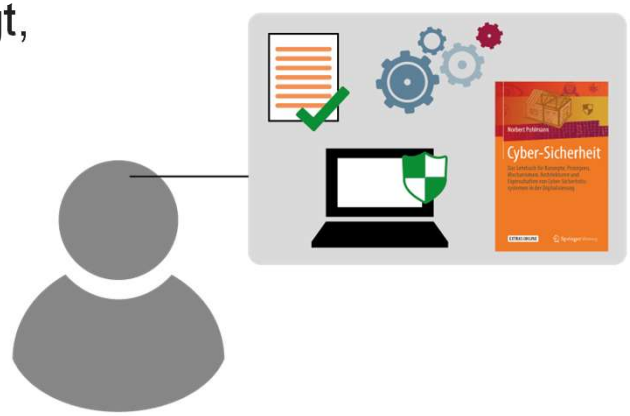
- Unternehmen sind durch **die umfassende Digitalisierung** immer stärker auf **externe Dienstleister** und **digitale Lieferketten** angewiesen.
- Das Problem dabei ist, Angreifer nutzen zunehmend Schwachstellen bei Drittanbietern, um **indirekt** auf die IT-Systeme von Unternehmen zuzugreifen.



- **IT-Supply Chain-Angriffe** sind in den letzten Jahren **deutlich gestiegen**.

Resiliente Mitarbeiter
→ Einordnung

- Das **Ziel von Awareness** darf ***nicht nur*** in der Fehlervermeidung liegen, sondern darin, **Menschen zu befähigen**, mit *Unsicherheit*, *Stress* und *Abweichungen* souverän umzugehen.
- Das beschreibt resiliente Mitarbeiter:
  die Fähigkeit, **Störungen zu absorbieren**, **sich anzupassen** und **aus Erfahrung zu lernen**.
- In der Cyber-Sicherheit bedeutet das auch, **unter Druck handlungsfähig zu bleiben** – ruhig, lösungsorientiert und als Team abgestimmt zu reagieren.
- **Resilienz ist** keine angeborene Eigenschaft, sondern **erlernbar**. *(siehe Serious Games)*
- Durch **Wiederholung** und **Reflexion** werden Muster gefestigt, die im Ernstfall automatisch greifen.
- In **Krisen** zeigt sich nicht, wer das meiste Wissen hat, sondern wer **handlungsfähig** bleibt.
- **Resiliente Mitarbeiter entstehen durch Erfahrung**, nicht aufgrund von theoretischer Wissensvermittlung.



Cyber-Widerstandsfähigkeit
→ Umsetzung (1/2)

- Bei der Umsetzung der Cyber-Widerstandsfähigkeit sollten acht Punkte beachtet werden:

- **1. Verantwortung auf höchster Ebene:**
  Die Cyber-Resilienz eines Unternehmens sollte von der **Geschäftsführung verantwortet**, **getrieben** und **überprüft** werden.

- **2. Interdisziplinäres Management:**
  Für das Management von Cyber-Risiken sollte ein **interdisziplinäres Team** zusammengestellt werden, um möglichst alle Aspekte zu betrachten.

- **3. Controlling des Risikos:**
  Das Cyber-Risiko-Portfolio sollte regelmäßig **überprüft** und gegebenenfalls **angepasst** werden.

- **4. Bedrohungsgetriebenes Vorgehen:**
  Die Cyber-Resilienz sollte bedrohungsgetrieben sein *sowie* von einem **durchgehend bestehenden** und sich **verändernden Risikopotenzial** ausgehen.

Cyber-Widerstandsfähigkeit
→ Umsetzung (2/2)

- **5. Realistisches Krisenmanagement:**
  Das Cyber-Krisenmanagement eines Unternehmens muss anhand realistischer Szenarien **regelmäßig trainiert werden**.

- **6. Vorbereitung im Unternehmen:**
  Cyber-Krisenreaktionsprozesse sind mit allen Unternehmensbereichen **abzustimmen** und **zu optimieren**.

- **7. Aktualität der vorhandenen Bedrohungen:**
  Die Bedrohungslandschaft muss **regelmäßig analysiert** werden, um eine realistische Einschätzung der eigenen Bedrohungssituation gewinnen zu können.
  (Attack Surface Management)

- **8. Austausch mit anderen Stakeholdern:**
  Die eigene Cyber-Widerstandsfähigkeit sollte durch den **Austausch** über aktuelle Bedrohungen **mit anderen Stakeholdern** gestärkt werden.

Cyber Resilience Act (CRA)
→ Übersicht

- **Zweck:**
  Erhöhung der IT-Sicherheit von vernetzten Produkten durch verbindliche Cybersicherheitsanforderungen (Attack Surface Management, SBOM …).
- **Geltungsbereich:**
  Betrifft ***alle Produkte mit digitalen Elementen***, die auf dem EU-Markt hergestellt, importiert oder vertrieben werden.
- **Auswirkungen:**
  Hersteller, Importeure und Händler müssen sicherstellen, dass ihre Produkte den CRA-Anforderungen entsprechen.
- **Fristen:**
  Erste Pflichten zur **Meldung von Schwachstellen** gelten ab September 2026.
  Ab Dezember 2027 dürfen nur noch konforme Produkte in der EU verkauft werden.
- **Folgen bei Nichteinhaltung:**
  Mögliche Strafzahlungen, Warnungen, Verkaufsverbote und der Verlust der CE-Kennzeichnung.

Komplexität managen
→ Zusammenfassung

- **Präventionsmaßnahmen (Reduktion der Angriffsfläche)**
  - Attack Surface Management, Patchmanagement, Awareness-Maßnahmen …
  - Informations-Sicherheits-Management-Systeme (ISMS)
  - Business-Continuity-Management-Systeme (BCMS) **…**
- **Verteidigungsfähigkeit (Konkrete Angriffe abwehren)**
  - Angriffserkennung und automatisierte Reaktion (KI-basiert)
  - End-Point-Sicherheit, Zero Trust-Konzepte (Trusted Computing, Confidential Computing) …
  - Anti-DDoS-Maßnahmen …
- **Bewältigungsfähigkeiten (Reduktion von Schaden)**
  - Notfallplan + Übungen
  - Getestete Backups
  - Digitale Kompetenz / Fähigkeit …

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

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyber-Resilienz
→ Idee und Umsetzung

„Ein Muss für robuste IT und IT-Infrastrukturen“

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/

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/

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

Der Marktplatz IT-Sicherheit

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