pro_ digital

European Digital Innovation Hub

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

Wildauer Verwaltungstag

Workshop IT-Sicherheit – Einleitung

Prof. Dr. Benjamin Fabian

Professor für Verwaltungsinformatik, Wissenschaftlicher Leiter EDIH pro_digital
benjamin.fabian@th-wildau.de

Workshop IT-Sicherheit: Agenda

pro_ digital
European Digital Innovation Hub

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

- **Einführung in die Informationssicherheit**

  Referent: **Ben Fabian**
  Prof. Verwaltungsinformatik VIBB & EDIH pro_digital

- **Informationssicherheit in der Praxis**

  Referent: **Bernd Heimer**
  Leiter Hochschulrechenzentrum TH Wildau & Leiter DCC

- **Ransomware (Demonstration)**

  Referent: **Hendrik Wolf**
  Bachelor Verwaltungsinformatik VIBB THWi

- **Kurze Umfrage zu Informationssicherheit**

  Referentin: **Gizem Dur**
  Master Wirtschaftsinformatik THWi

EDIH pro_digital: Eine kleine Werbeseite ☺

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

pro_ digital

European Digital Innovation Hub

https://edihprodigital.eu

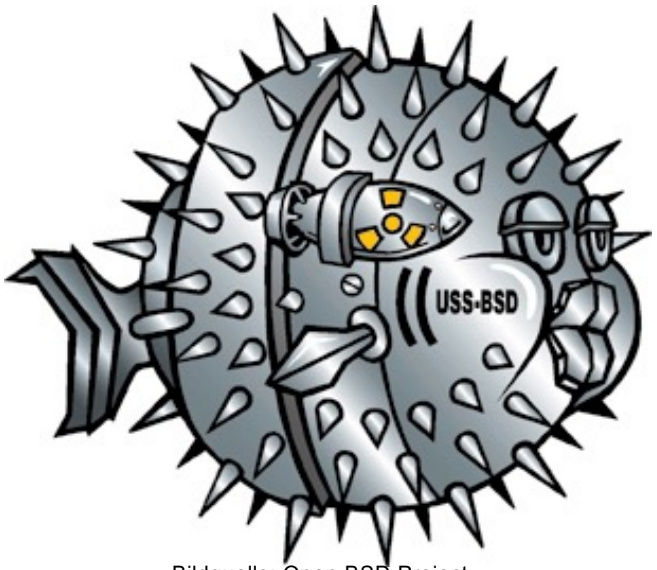
Co-funded by the European Union

- Anfang 2023 startete der **EDIH pro_digital**, einer von Hunderten von europaweiten **European Digital Innovation Hubs**, die durch das EU DIGITAL Programm gefördert werden.
- Wir engagieren uns im **Land Brandenburg** und zusammen in ganz **Europa** für die **Transformationsprozesse der Digitalisierung und Nachhaltigkeit** in kleinen und mittelständischen Unternehmen (KMU), Midcaps, Start-Ups und in der öffentlichen Verwaltung.
- Konsortialpartner: TH Wildau & BTU Cottbus-Senftenberg
- Neutral & Not-for-profit!

Was bedeutet Informationssicherheit?

Working Definition:

Verteidigung von **Informationen und IT-Systemen** gegen **Angreifer**.



Bildquelle: Open BSD Project

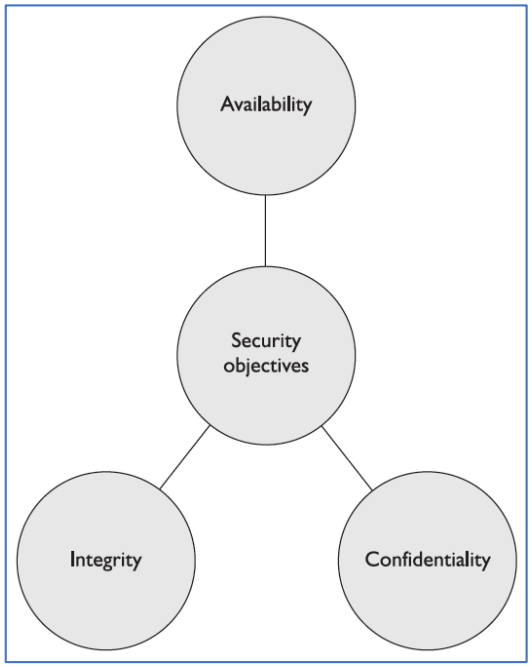
vs.

Bildquelle: Free BSD-Projekt

Ziele der Informationssicherheit: „CIA“ ;-)

- **Vertraulichkeit (Confidentiality):**
  Verhindern einer unbefugten **Weitergabe** von Informationen.
- **Integrität (Integrity):**
  Verhindern einer unbefugten **Änderung** von Informationen.
- **Verfügbarkeit (Availability):**
  Verhindern eines unbefugten **Vorenthaltens** von Informationen (oder von System-Ressourcen).

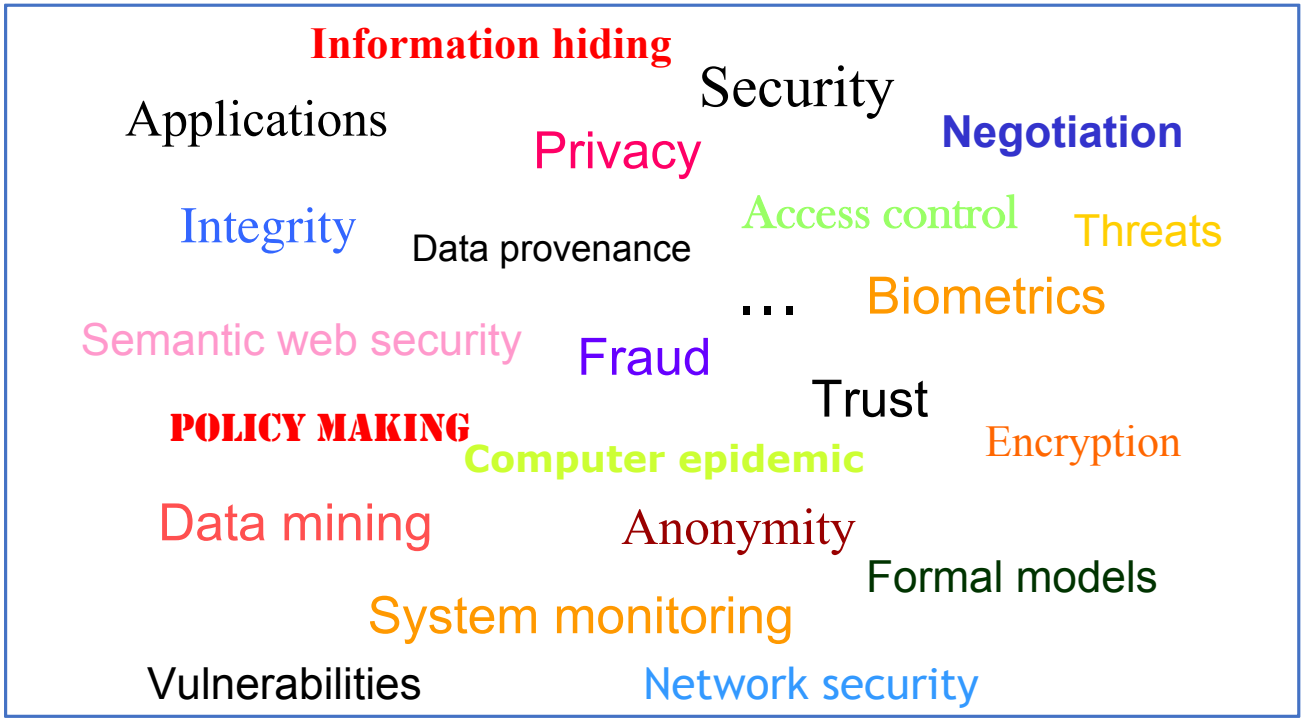
- Merkhilfe „CIA“:



Bildquelle:
Shon Harris, CISSP Certification Guide, 2007

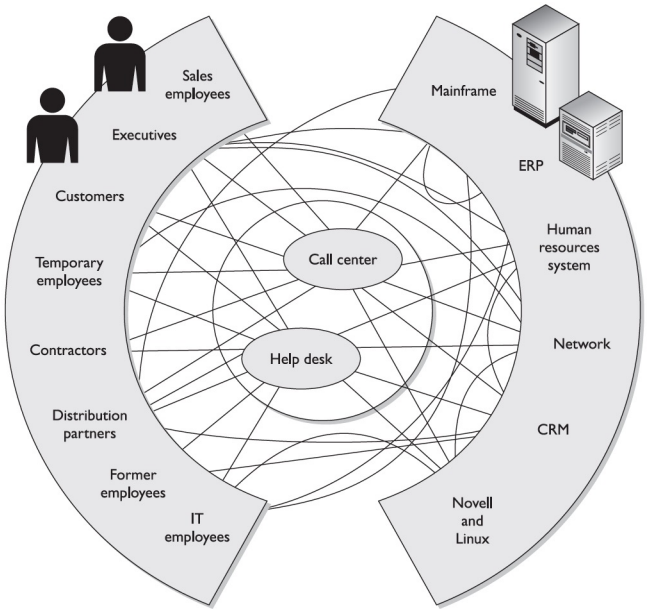
- Dieter Gollmann: *Computer Security*, Wiley, 2. Aufl., 2006 (S. 18-25).
- ITSEC, Europäische Kriterien für die Bewertung der Sicherheit von Informationstechnologie, 1991.
- IETF: Internet Security Glossar, RFC 2828 (Request for Comments #2828). http://www.ietf.org/rfc/rfc2828.txt (zuletzt abgerufen 09/2023).

Informationssicherheit: Thematische Komplexität in Praxis und Forschung

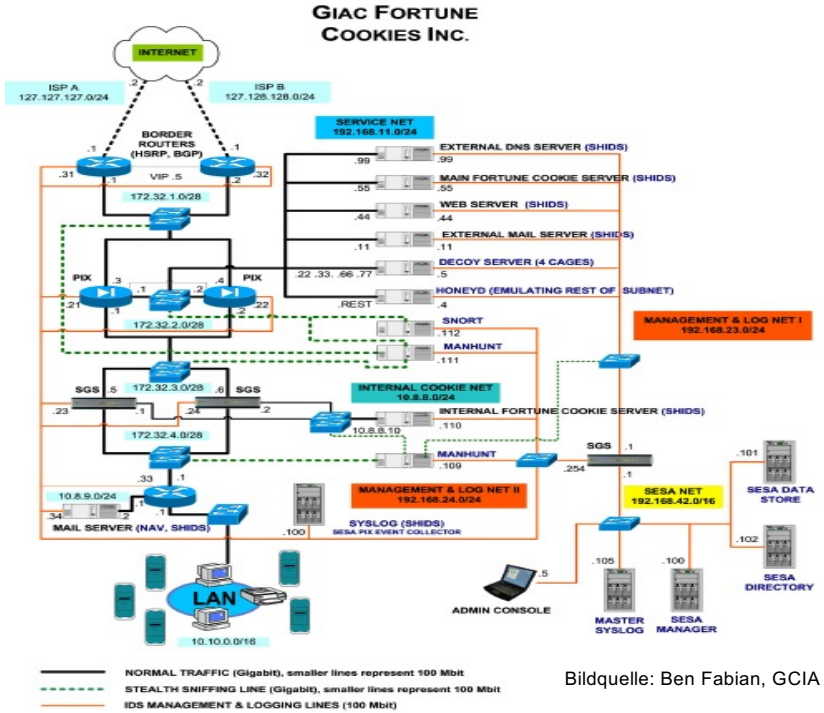


Bildquelle: Csilla Farkas, o.J.

Kontext: Vernetzte Informationssysteme & User



Bildquelle: Shon Harris, CISSP Certification Guide, 2007



Bildquelle: Ben Fabian, GCIA Practical, 2004

- Hohe **organisatorische** und **technische Komplexität!**

Komplexität von Software

- **Software ist komplex** (auch bereits ohne Netzwerke).
  - Heuristische und simple Metrik:

    Anzahl von Fehlern ~ Anzahl der Codezeilen

  - Für kommerzielle Software-Qualitätsmessungen siehe z.B. *Secure Software Engineering* Studien und *DevSecOps* Services, z.B. https://www.coverity.com/
- Beispiel: **Betriebssysteme**
  - Dutzende Millionen Codezeilen.
  - Regelmäßig werden neue "kritischer" Sicherheitsfehler angekündigt.
  - Das MS "Secure Development" Programm hat dies mit großem Aufwand etwas abgemildert.
- **Unbeabsichtigte** Sicherheitsmängel bleiben aber in der Praxis unvermeidlich.
- **Beabsichtigte** Sicherheitslücken sind nahezu unentdeckbar.

Informationsseiten zu Schwachstellen

(Aber nur die öffentlich bekannten …)

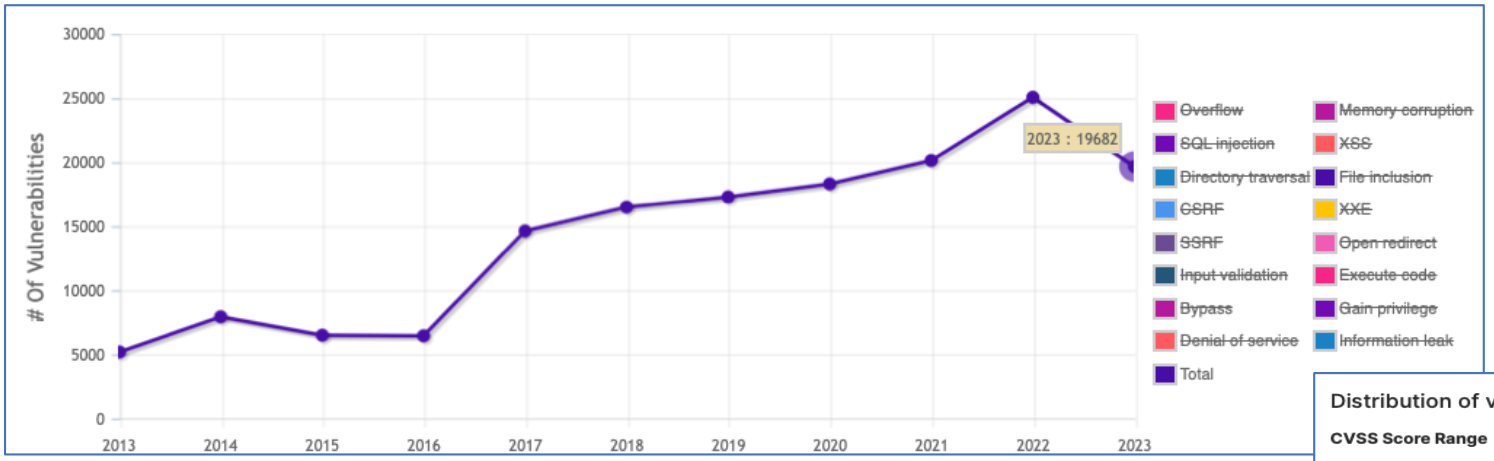
- CVE (Common Vulnerabilities and Exposures):
  - "Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities".
  - Klassisch: https://cve.mitre.org
  - Ab 2024: https://www.cve.org
  - Visualisierungen: https://www.cvedetails.com

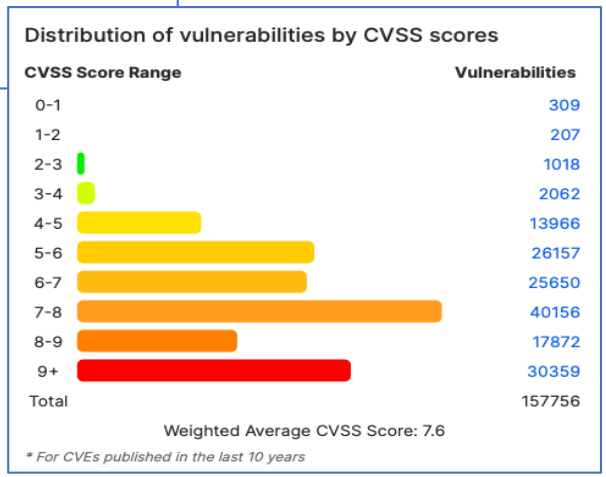
- CWE (Common Weakness Enumeration) TOP 25 Most Dangerous Software Errors
  - https://www.sans.org/top25-software-errors/
  - https://cwe.mitre.org/top25/
- OWASP Top Ten (Web Application Security):
  - https://owasp.org/www-project-top-ten/

- Coordinated Vulnerability Disclosure (CVD) Richtlinie des BSI
  - https://www.bsi.bund.de/dok/schwachstellenmeldung

Historische Trends (publizierte Schwachstellen)

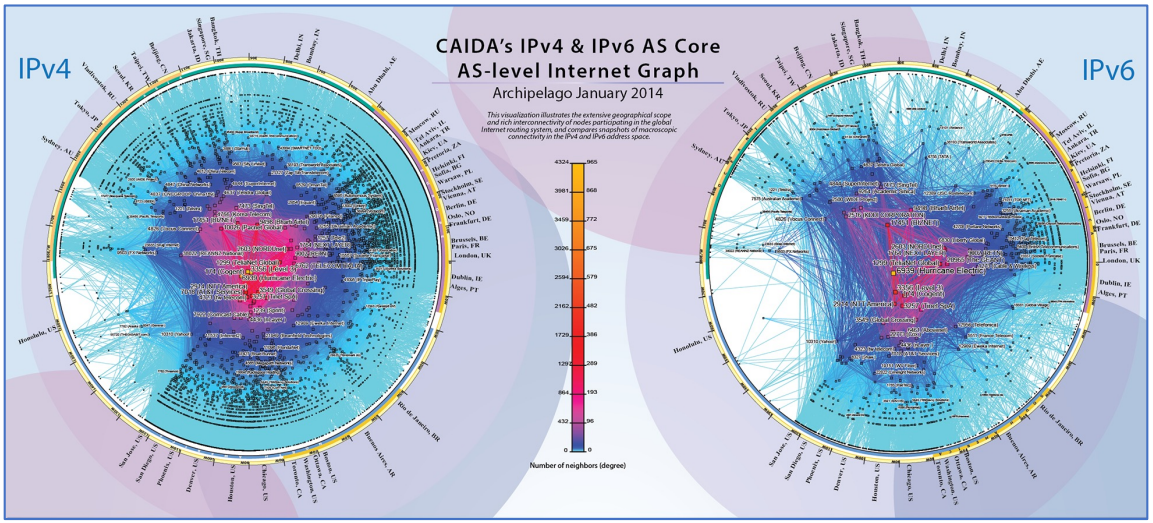
https://www.cvedetails.com (Abruf 08.09.2023, 12:30)

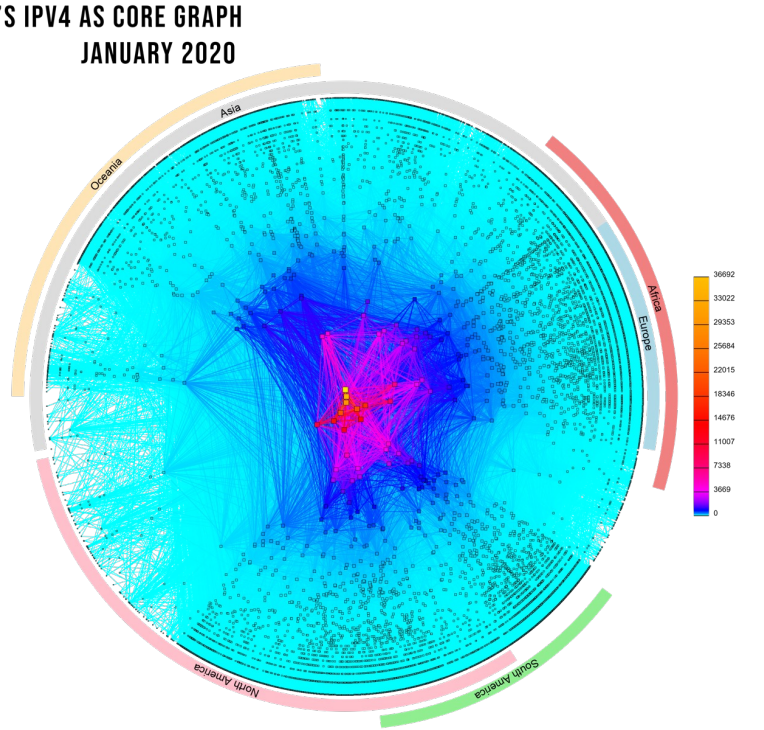




- Ansteigende Tendenz
- Im Schnitt mittlere bis hohe Gefährlichkeit

Das Internet ▷ Weltweite Vernetzung ▷ Weltweite Ausnutzbarkeit von Schwachstellen

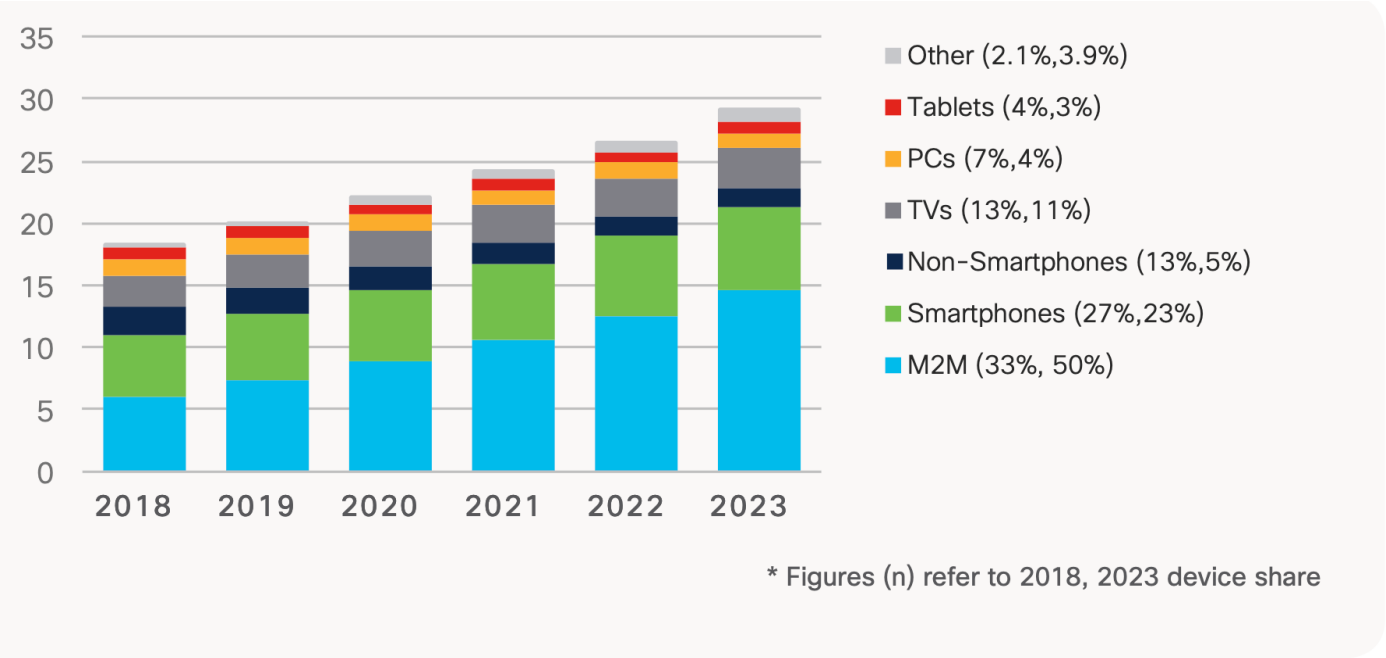




"Starting from 2013 we have made two major refinements to how we create the graph, including how we rank individual ASes, improving our AS Core visualization.
1.First, we now rank ASes based on their transit degree rather then their outdegree.
2.Second, we now infer links across **I**nternet e**X**change (IX) point address space, rather than considering the IX itself a node to which various ISPs attach."

Quelle: Center for Applied Internet Data Analysis (CAIDA) https://www.caida.org/ https://www.caida.org/projects/as-core/

Das Internet der Dinge (IoT) ▷ Zahlreiche ungesicherte Systeme dienen als Angriffsplattformen



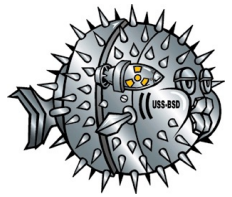
Source: Cisco Annual Internet Report, 2018–2023

2023:

Fast **30 Milliarden** Geräte im IoT!

- Y-Achse: **Milliarden** von Geräten im IoT [M2M: Machine-to-Machine]
- Ähnliche Schätzungen von Statista.

Netzwerksicherheit: Notwendigkeit technischer Maßnahmen



- Schutz von Netzwerken und Servern vor bösartigem Datenverkehr:
  - **Firewalls**
- Überwachung von Netzwerken und Systemen auf bösartige Aktivitäten:
  - **Anti-Virus & Intrusion Detection**
  - **Auditing & Pen Testing**
- Gegenmaßnahmen gegen Abhören und unbefugten Zugriff:
  - **Verschlüsselung und Authentifizierung** des Datenverkehrs (Krypto, TLS, VPN)
  - **Zugangskontrolle** (*Access Control*, physisch und zu Software-Diensten)

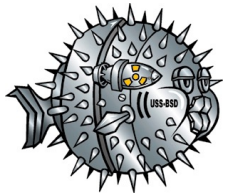
Einige fundamentale Herausforderungen hierbei:
- Komplexität und Dynamik von Technik und Infrastrukturen
- Prozesse
- „Faktor Mensch“

Vielen Dank für Ihre Aufmerksamkeit ☺

benjamin.fabian@th-wildau.de

pro_ digital
European Digital Innovation Hub

Technische Hochschule Wildau
Technical University of Applied Sciences



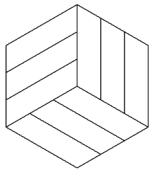
Diskussion & Umfrage (auch für eine Masterarbeit)

Gizem Dur (gidu9769@th-wildau.de)

Hat nach Ihrer Erfahrung das Onlinezugangsgesetz (OZG) zu behebende Schwachstellen in Bezug auf Cybersicherheit?

Können Sie drei solche Schwachstellen kurz beschreiben?

Werden bei Verwaltungen in Sachen Cybersicherheit „best practice“s gelebt?



Unterscheiden sich darin Bund, Land und Kommunen?

Wollen Sie zu dem Thema noch etwas sagen / hinzufügen?

https://survey.lamapoll.de/Schwachstellen-Cybersicherheit-

https://survey.lamapoll.de/Umfrage-Onlinezugangsgesetz/de