Alive and Hacking

Sichere Digitalisierung im Krankenhaus

Fachvereinigung Krankenhaustechnik e.V. – Webinar 26. Oktober 2021

Darf ich mich vorstellen?

Jan-Tilo Kirchhoff

- Country Manager Compass Security Deutschland GmbH
- verheiratet, zwei Kinder
- Werdegang: Von der TK-Security zur IT-Security
- Kompetenzen
  - Netzwerk Sicherheitsprüfungen
  - ICT- Security (VoIP, PSTN, GSM …)
  - IT-Forensik

CISSP® Certified Information Systems Security Professional

OFFENSIVE security (OSCP)®

Hobbys

- Meine Familie
- Musik (Trompete und Chor)
- Electronic Jazz, Jazz Funk
- Laufsport
- ICT-Security

Compass Crew

Was macht Compass?

seit 1999

Penetration Tests

Als Angreifer untersuchen wir Geräte, Netze, Dienste und Anwendungen auf Schwachstellen. Mittels Social Engineering und Red Teaming testen wir das Verhalten der gesamten Organisation.

Digital Forensics

Unsere Forensik-Experten helfen bei der Koordination von Vorfällen und Sofortmassnahmen sowie bei der gerichtsfesten Bearbeitung von Daten. Zudem bieten wir eine unkomplizierte und schnelle Ursachenforschung.

Security Reviews

Erfahrene IT Analysten unterstützen Sie mit Zweitmeinungen zu Security-Konzepten und prüfen nach Wunsch den Aufbau, die Konfiguration und den Quellcode Ihrer Lösung.

Security Trainings

Profitieren auch Sie vom Wissen unserer Analysten zu Penetration Testing, Netzwerkanalyse, sichere Apps und Anwendungen, Digitale Forensik und trainieren Sie in einem eigens dafür erstellten Labor.

Wir sind “nette” Hacker

Bild von Free-Photos auf Pixabay

Aktuelle Meldungen

Industrie.de

Berliner Morgenpost

CORONA-KRISE

Homeoffice bietet Angriffsfläche – so oft schlagen Hacker zu

DW Made for minds.

PRESSE

Iranische Hacker geben sich als Journalisten aus

Zum wiederholten Mal versucht eine Hackergruppe aus dem Iran durch die Vortäuschung falscher Identitäten, Informationen für das iranische Regime zu sammeln. Auch die DW ist betroffen.

mdr SACHSEN

StN.DE STUTTGARTER NACHRICHTEN

Hackerangriff auf SRH-Kliniken

Sieben Kliniken in Baden-Württemberg offline

Hacker haben die IT-Infrastruktur des SRH Klinikverbunds angegriffen. Aus Sicherheitsgründen wurden deutschlandweit Kliniken vom Netz genommen. Auch im Südwesten.

Frankfurter Allgemeine ZEITUNG FAZ.NET

CYBERCRIME

Computer-Hacker kapern die Rechner eines Wasserwerks

Die amerikanischen Behörden untersuchen den Fall von Oldsmar in Florida. Wurde ein Programm der deutschen Teamviewer AG als Einfallstor missbraucht?

Hacker greifen Logistikfir

Telefon-Betrüger er

Düsseldorf: Massiver Netzwerkausfall

Universitätsklinikum Düsseldorf

Düsseldorf. Das Krankenhaus ist derzeit nur sehr eingeschränkt erreichbar. Die Patientenversorgung ist ebenfalls eingeschränkt.

Unbekannte Hacker verüben einen Angriff auf ein

Schlechte und Gute Neuigkeiten

F+ PODCASTS BLOGS THEMEN TICKER ARCHIV STELLENMARKT PRODUKTE NEWSLETTER

Wirtschaft > Digitec > Solarwinds-Hack: Massiver Cyberangriff gefährdet deutsche Behörden

Frankfurter Allgemeine

ZEITUNG FAZ.NET

Politik Wirtschaft Finanzen Feuilleton Karriere Sport Gesellschaft Stil Rhein-Main Technik Wissen Reise Abo

SOLARWINDS-HACK

Massiver Cyberangriff gefährdet deutsche Behörden

VON BASTIAN BENRATH - AKTUALISIERT AM 07.01.2021 - 16:46

Eine gravierende Cyberattacke hat Hackern Zugriff auf mehr als 250 amerikanische Behörden und Unternehmen verschafft. Nun wird klar: Auch zahlreiche deutsche Behörden haben die kompromittierte Software eingesetzt.

tagesschau

Sendung verpasst?

Wirtschaft ▸ Bundeskriminalamt : Schadsoftware "Emotet" zerschlagen

Bundeskriminalamt

Schadsoftware "Emotet" zerschlagen

Stand: 27.01.2021 14:16 Uhr

Deutsche Ermittler haben die Infrastruktur der weltweit als am gefährlichsten geltenden Schadsoftware "Emotet" übernommen und zerschlagen. Die Software hatte auch die IT-Infrastruktur von Behörden und Kliniken angegriffen.

Lagebilder des BSI und des BKA (Deutschland)

1 Cybercrime 2020

- Die Anzahl erfasster Cyberstraftaten steigt weiter an.
- Der Fokus von Cyberkriminellen liegt vermehrt im Bereich „Big Game Hunting".
- Die Täter sind global vernetzt und agieren zunehmend professioneller.
- Ransomware bleibt weiterhin die Bedrohung für öffentliche Einrichtungen und Wirtschaftsunternehmen.
- Die Anzahl an DDoS-Angriffen steigt weiter an – auch ihre Intensität nimmt zu.
- Die Underground Economy wächst – sie stellt eine kriminelle, globale Parallelwirtschaft dar, die maßgeblich auf finanziellen Profit aus ist.

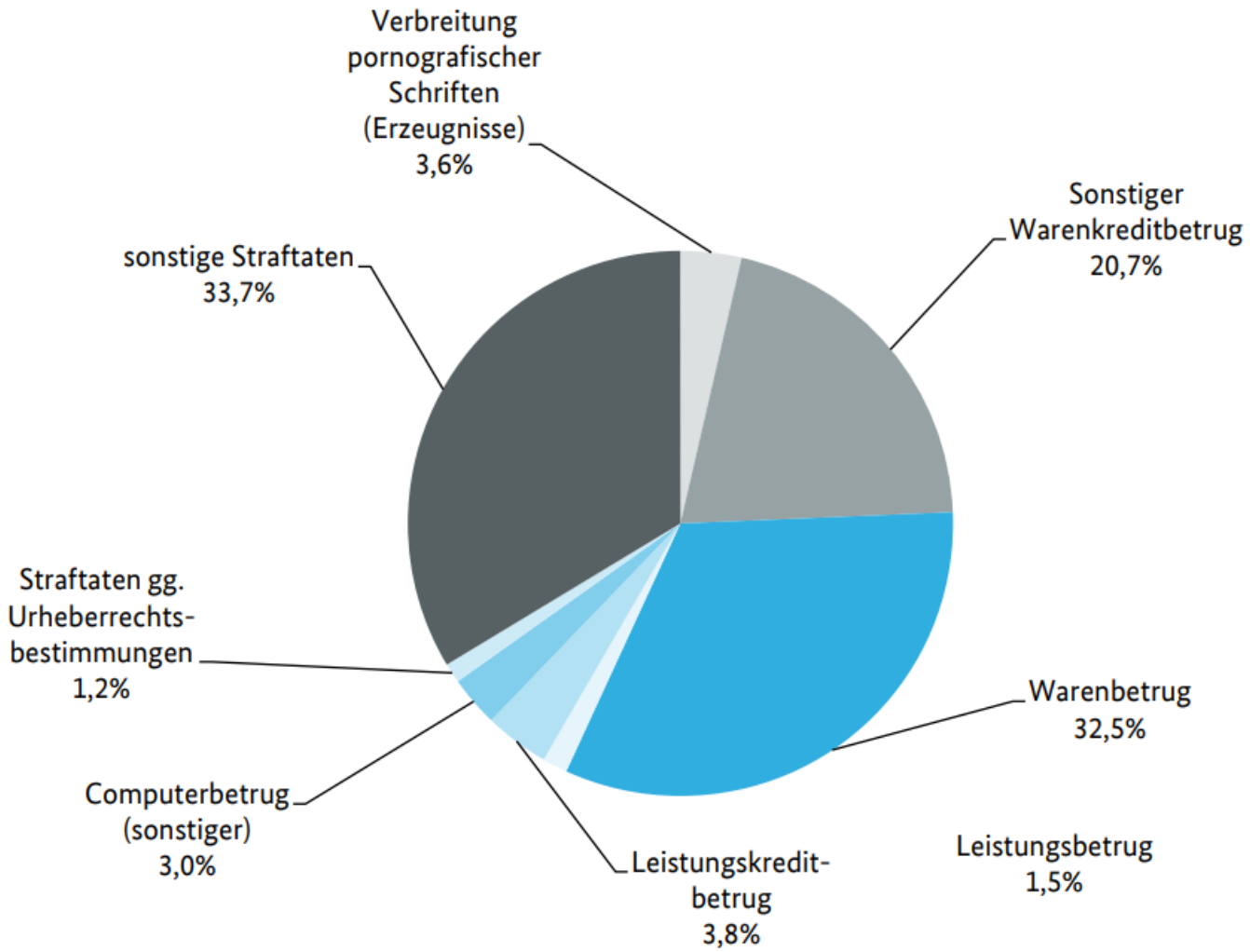
Abbildung 1: Die wesentlichen Aspekte der Cybercrime in Deutschland 2020

Bundeslagebild | Cybercrime 2020 3

Polizeiliche Kriminalstatistik (Deutschland) 2019

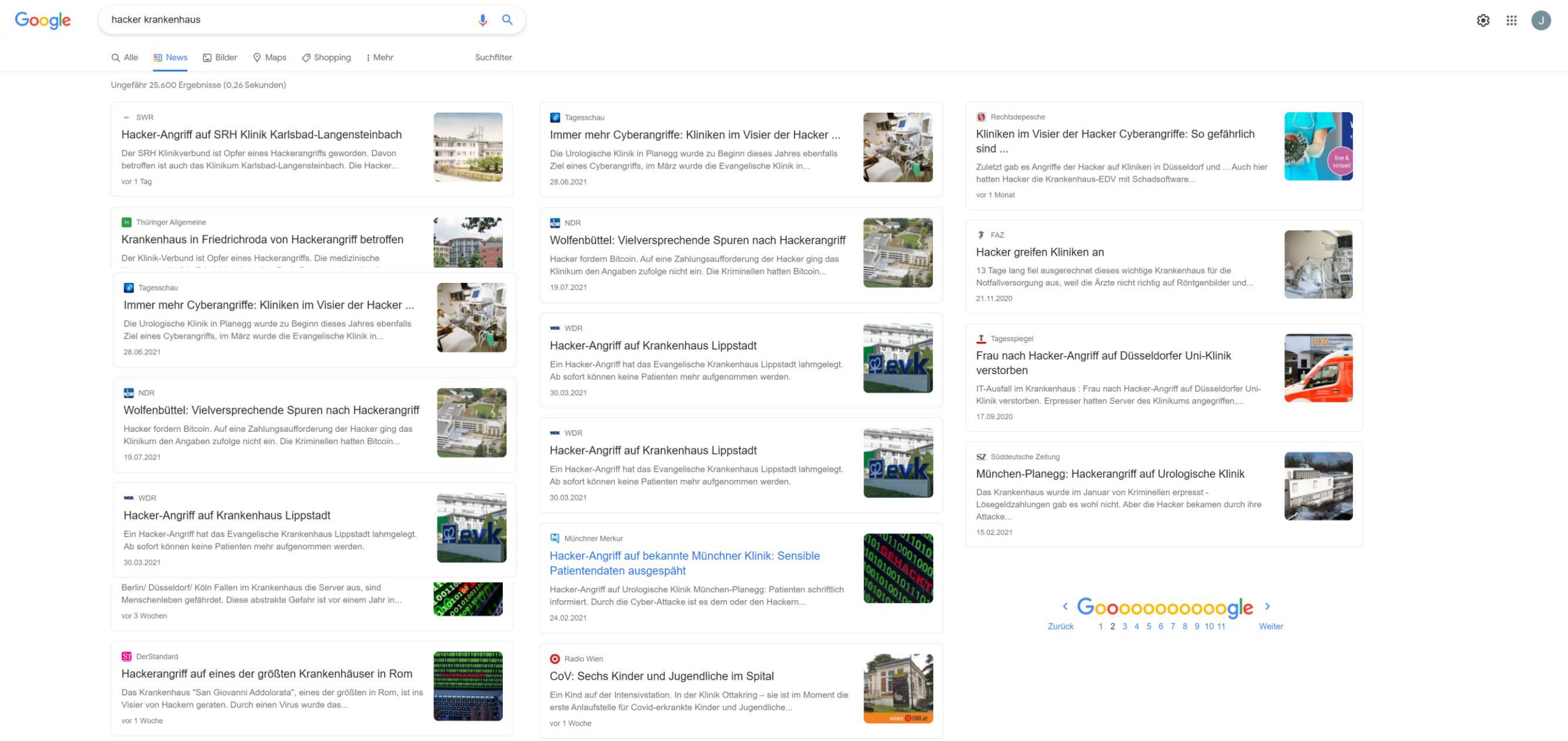
Straftatenanteile an Straftaten mit Tatmittel „Internet“ = 251.617 Fälle

1 - 2.4.2 – G01



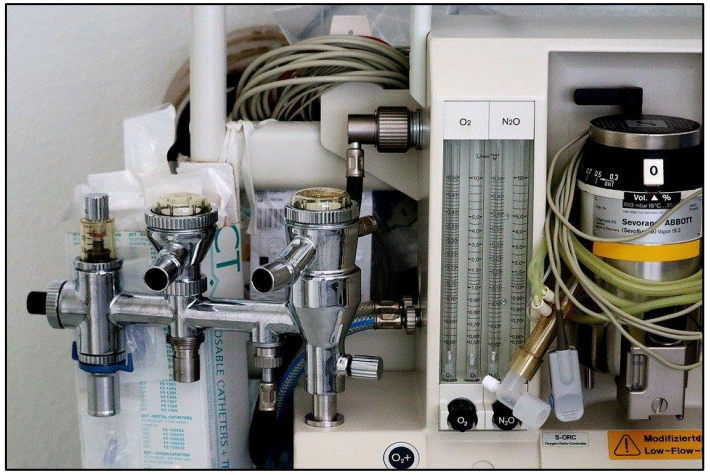
Quelle: BKA

Meldung zu Krankenhäusern



Digitalisierung im Krankenhaus

Mehr als nur ein IT Thema



Bilder: https://pixabay.com/

Automatisierung im Alltag

Fertigung

http://www.youtube.com/watch?v=Kpvr2MVZjws&feature=plcp

http://www.youtube.com/watch?v=YFbBVzYaH_E

Qualität
Produktivität

Prozesse

Bikinger, „Raffinerie Schwechat“, CC-Lizenz (BY 2.0)

Paul-Gerhard Koch, „Kaprun“Bikinger, CC-Lizenz (BY 2.0)

Gebäude

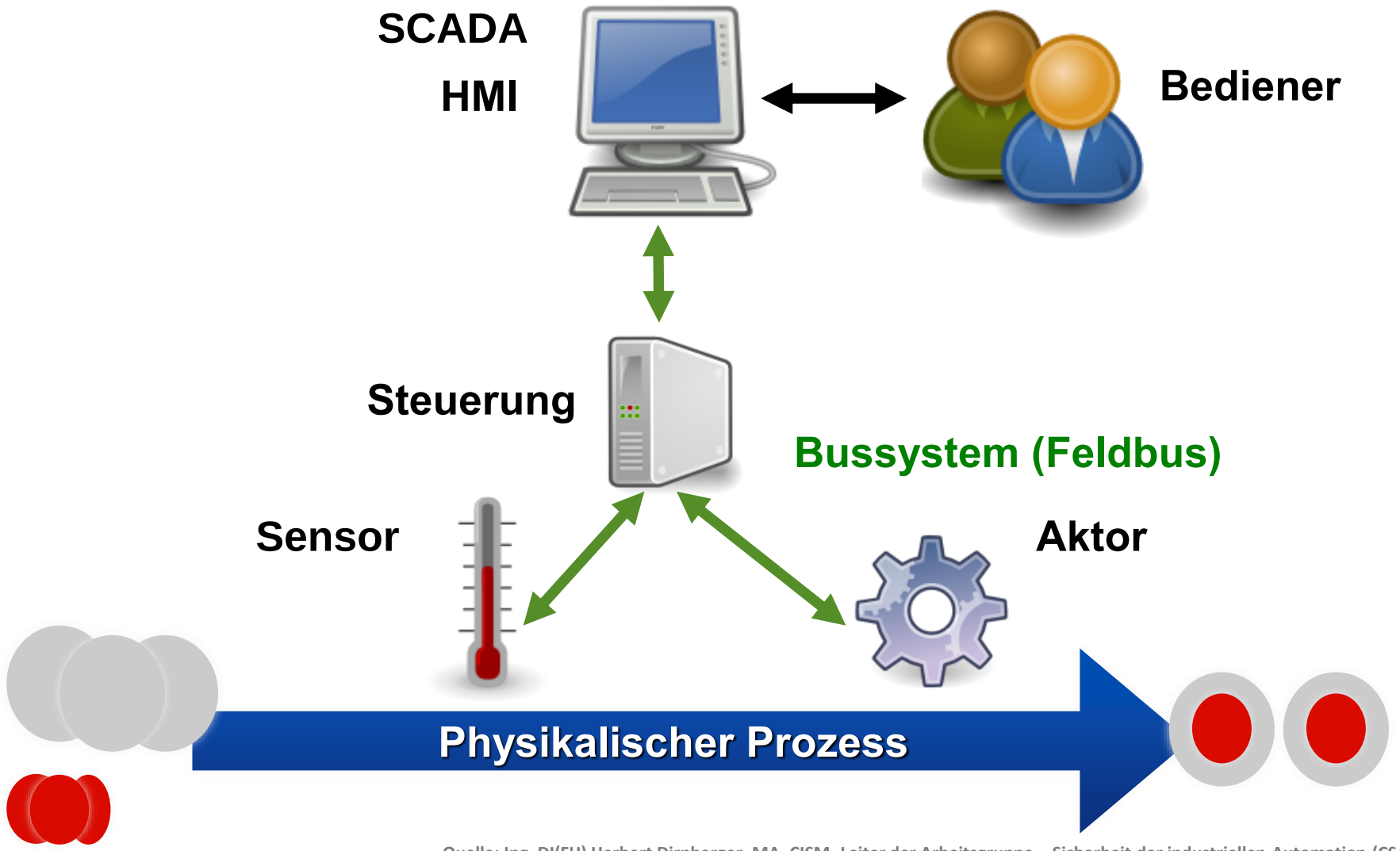
teakettle, „u1“, CC-Lizenz (BY 2.0)

Transport

kritische Infrastruktur

Quelle: Ing. DI(FH) Herbert Dirnberger, MA, CISM- Leiter der Arbeitsgruppe – Sicherheit der industriellen Automation (CSA)

Automatisierung in 2 min.



Quelle: Ing. DI(FH) Herbert Dirnberger, MA, CISM- Leiter der Arbeitsgruppe – Sicherheit der industriellen Automation (CSA)

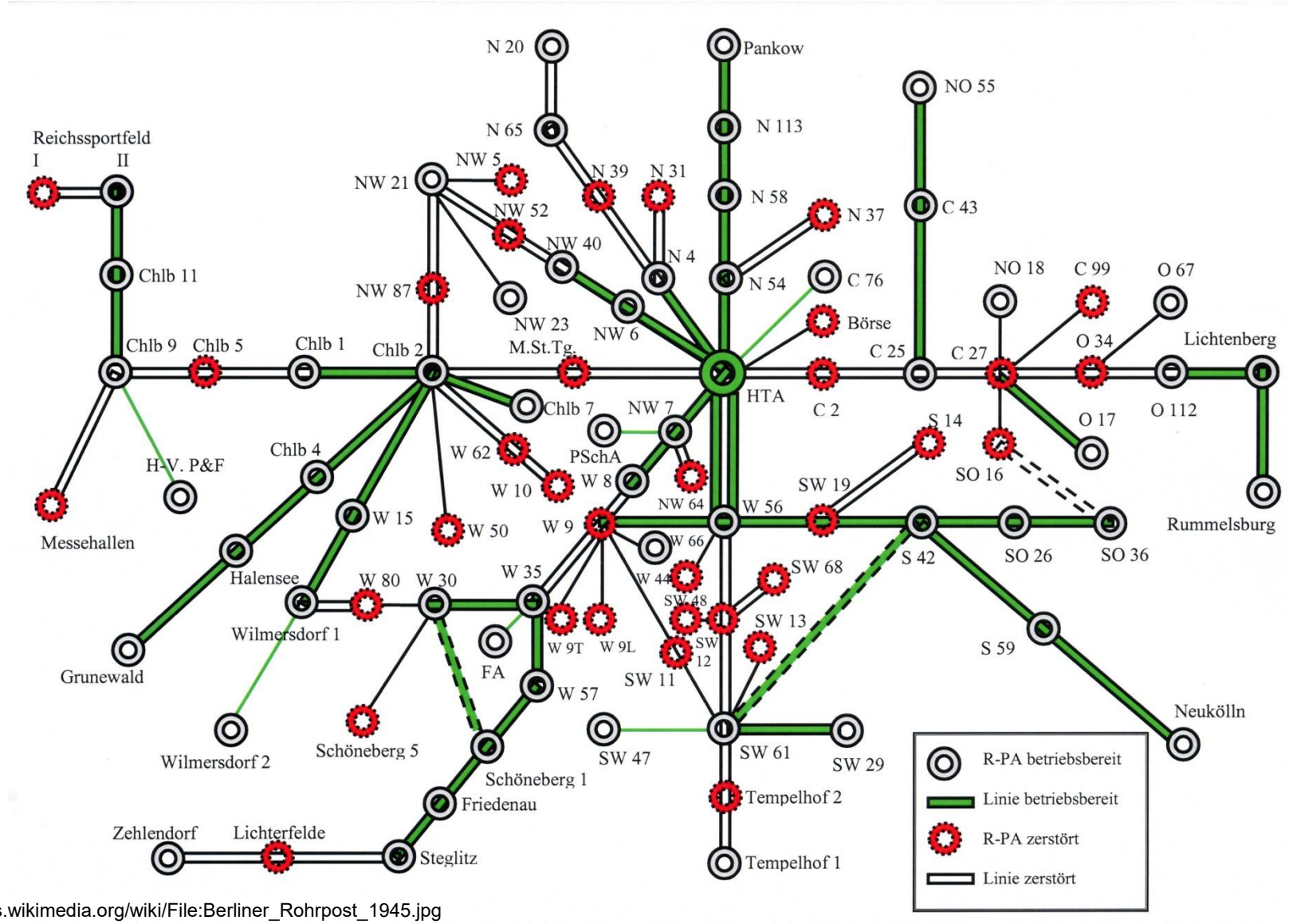
Bei wem sieht es so aus?

https://www.vamed.com/media/4691/akh_leitwarte_000_3410.jpg

Bei wem eher so?

https://www.helios-gesundheit.de/fileadmin/_processed_/5/0/csm_DSC_8072_16c347df07.jpg

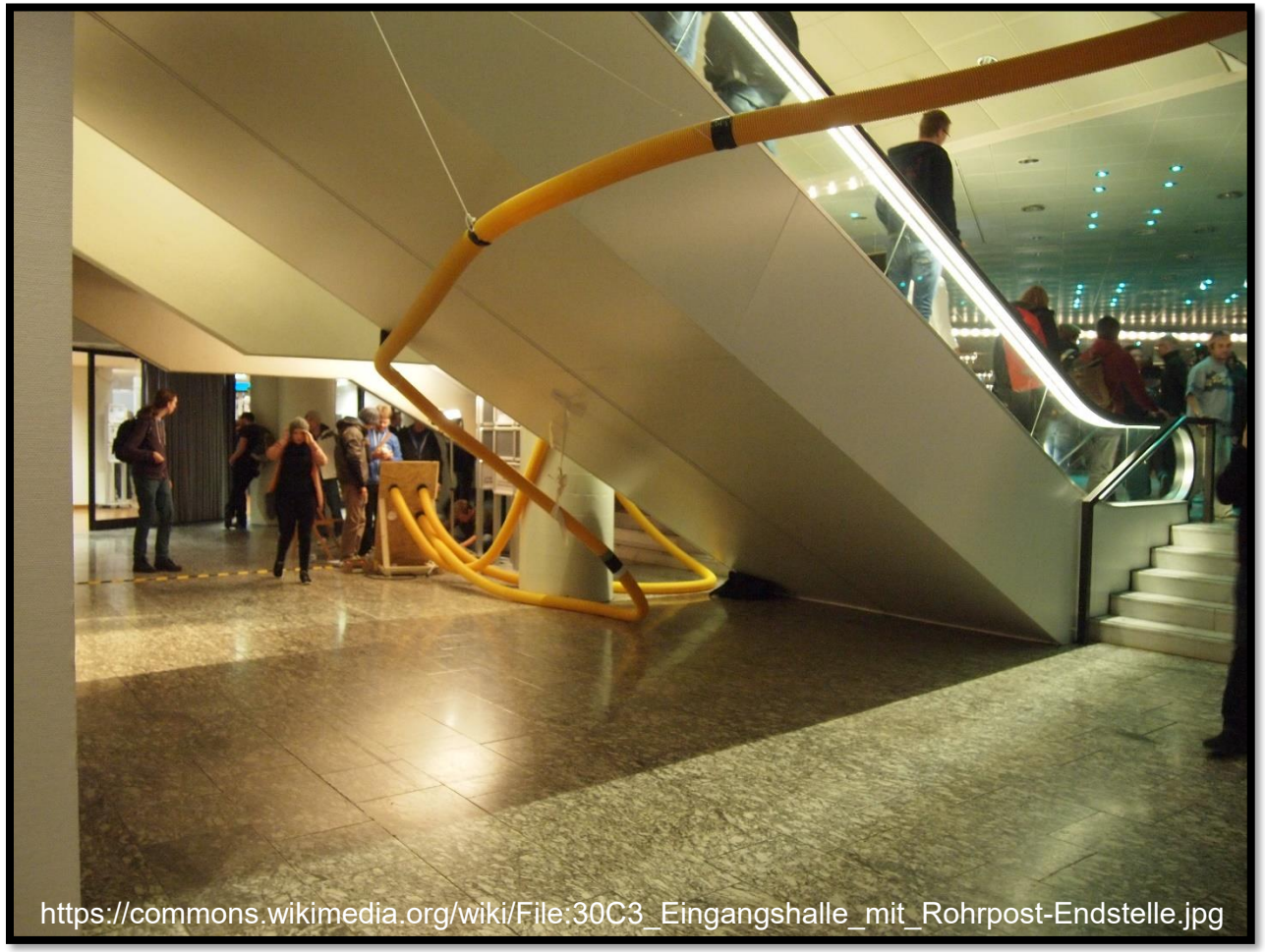
Unerwartete Technologien

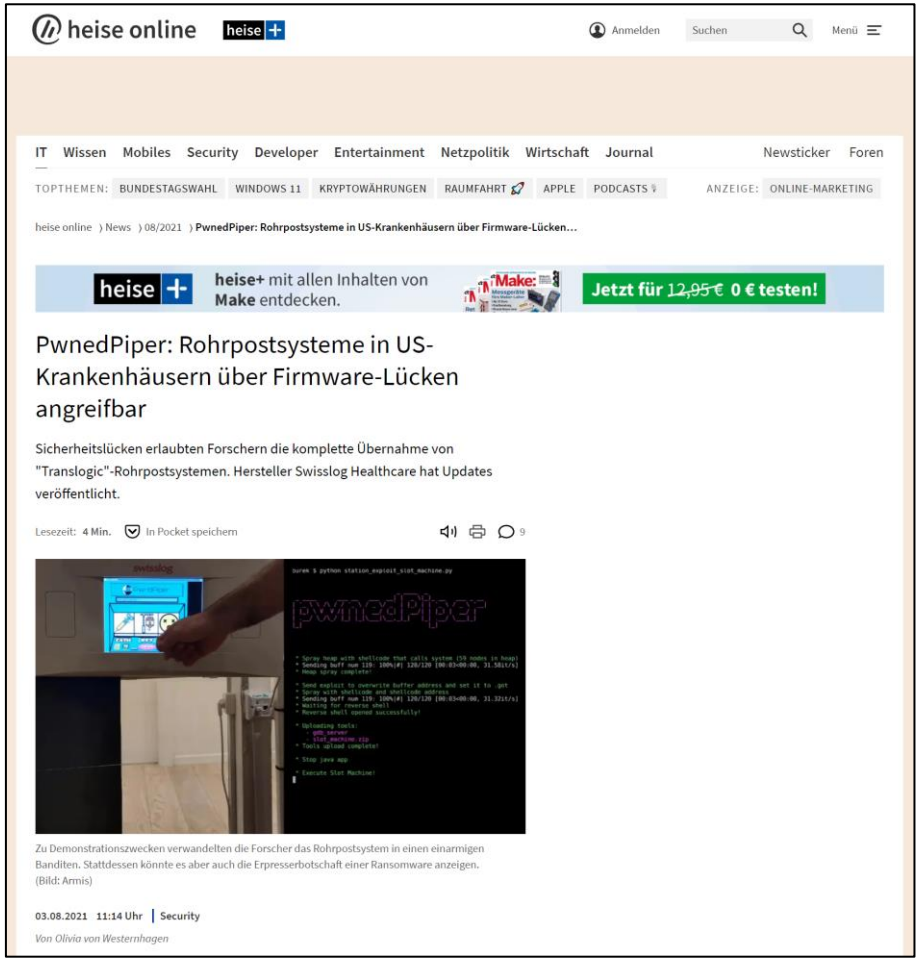


Quelle: https://commons.wikimedia.org/wiki/File:Berliner_Rohrpost_1945.jpg

Unerwartete Technologien

Die auch Hacker faszinieren

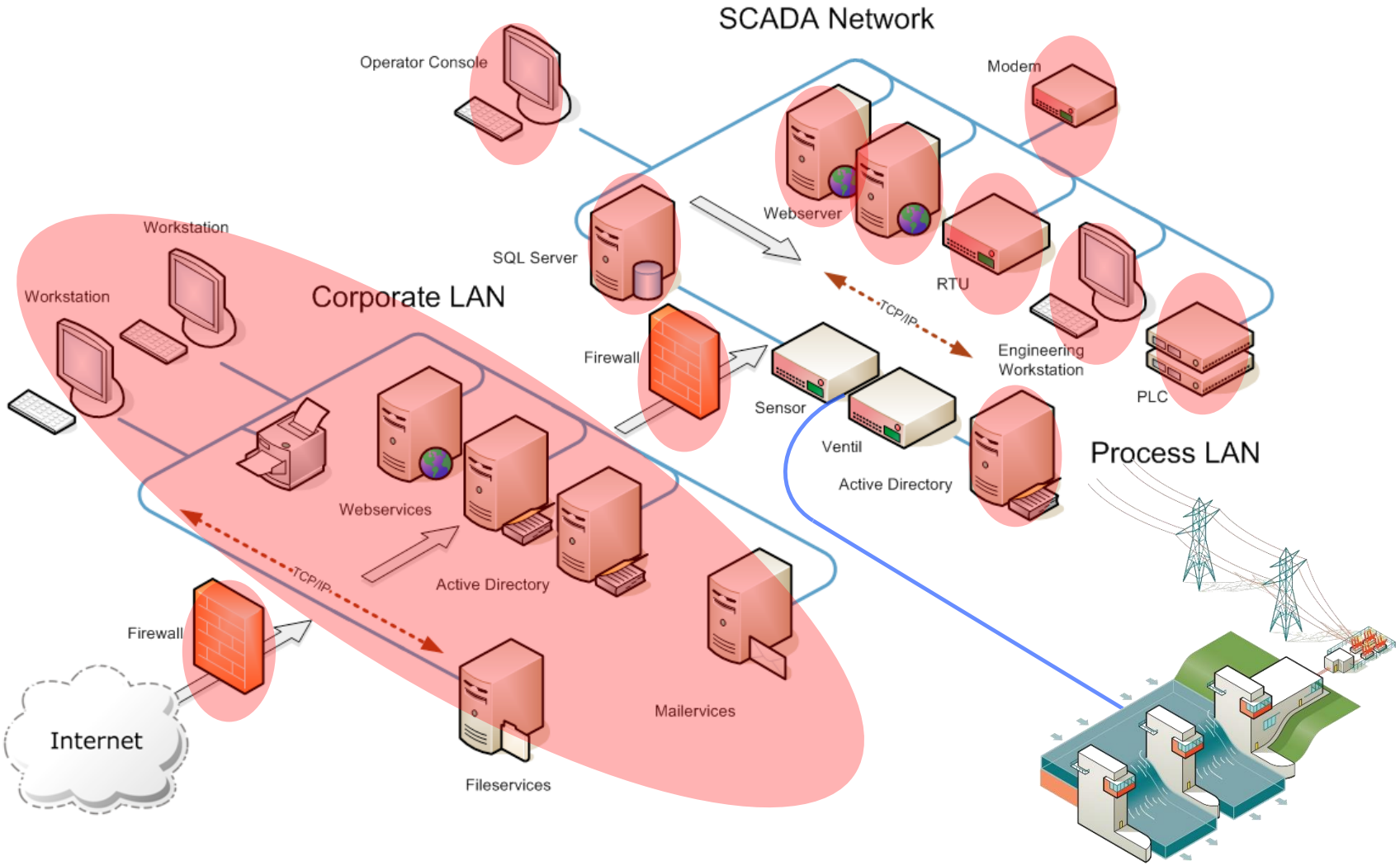

https://commons.wikimedia.org/wiki/File:30C3_Eingangshalle_mit_Rohrpost-Endstelle.jpg



Angriffsflächen

Industrial Network Architecture

Ansatzpunkte möglicher Angriffe

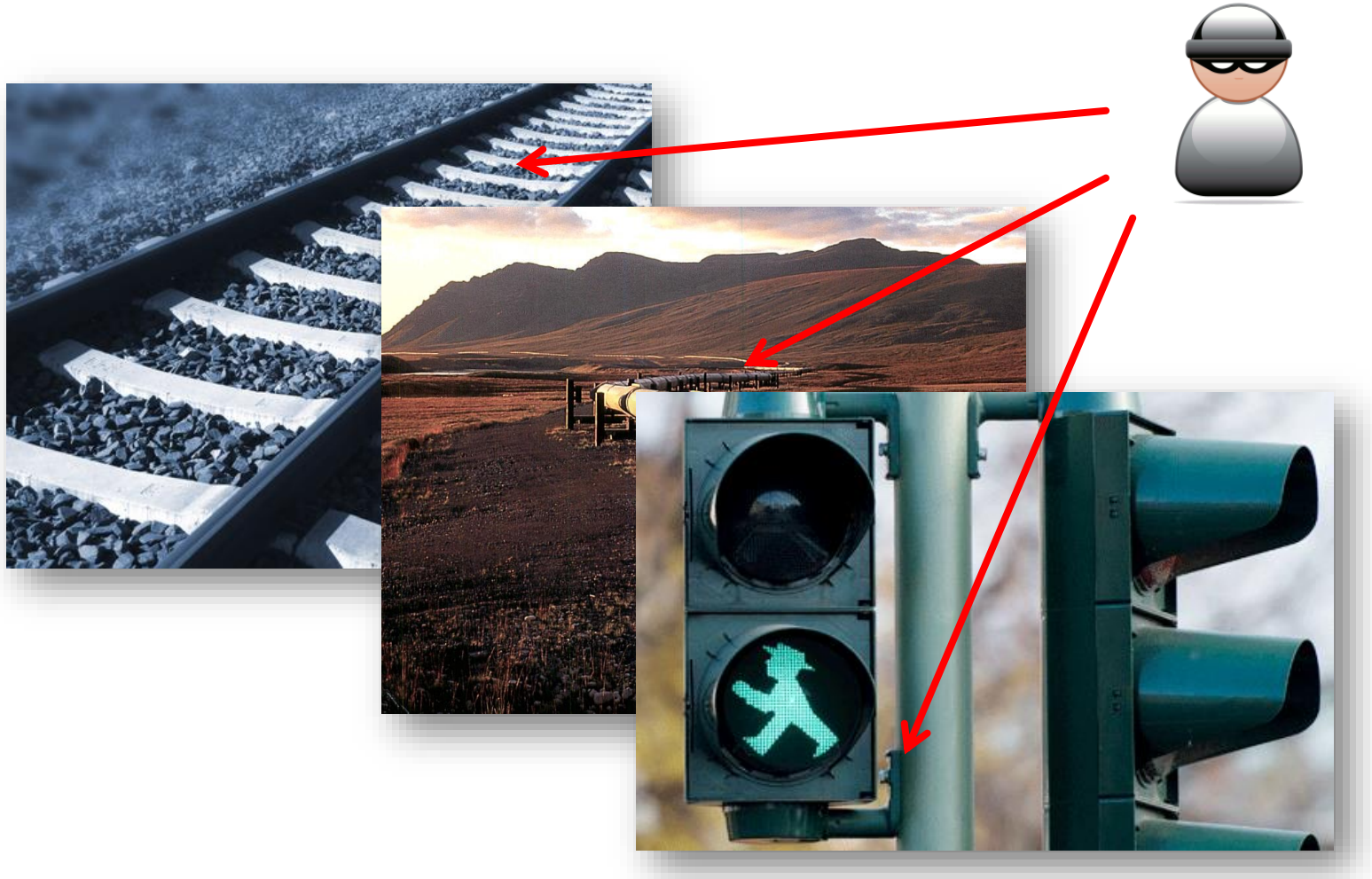


Industrial Network Architecture

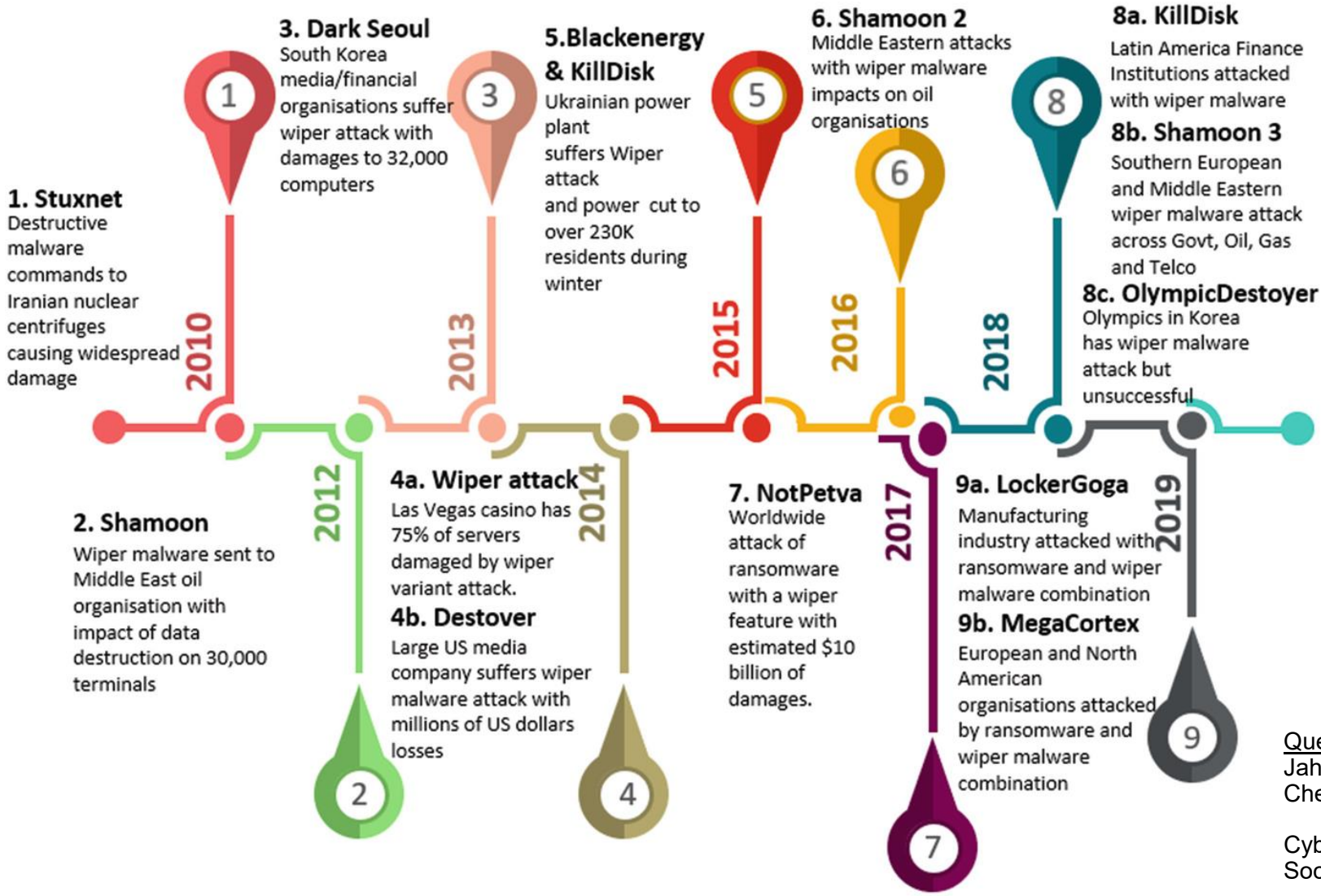
The Real World...

Industrial Network Architecture

The Real World...



Eine kurze Geschichte der ICS Sicherheit



Quelle:
Jahankhani, Kendzierskyj, Chelvachandran, Ibarra (Hrsg.)

Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity

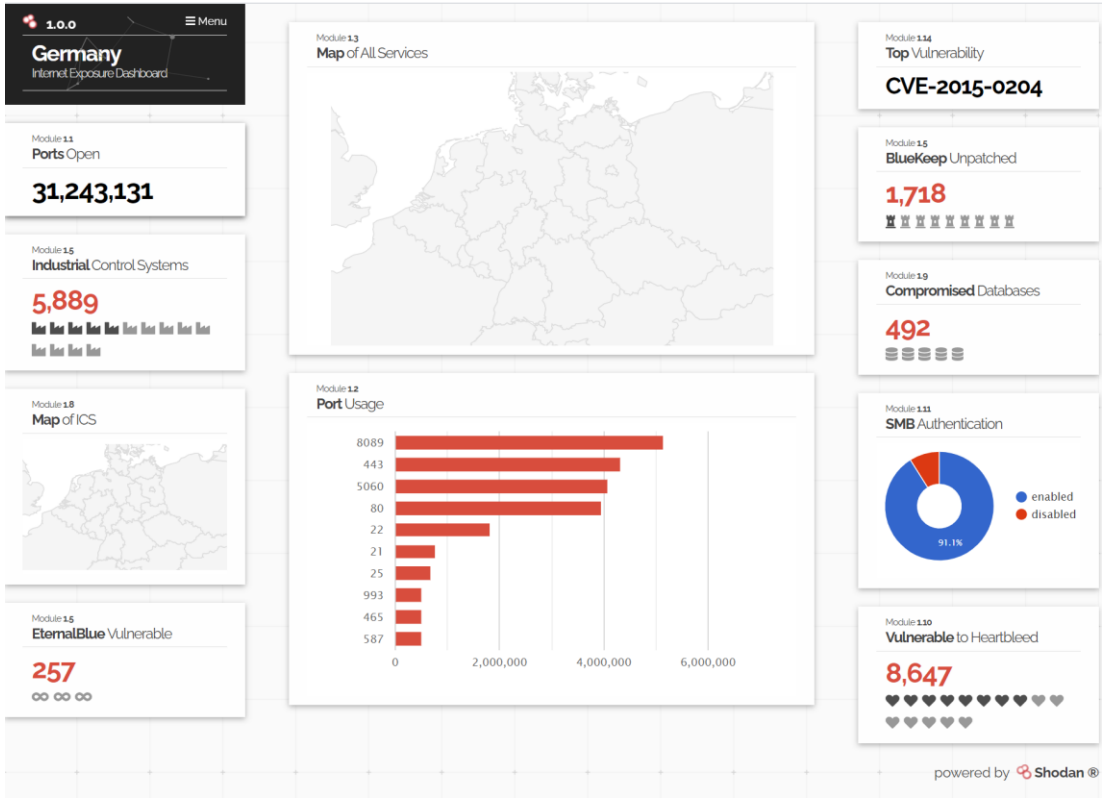
Springer Verlag 2020

Industrial Network Architecture

Was (aktuell) tatsächlich passiert.

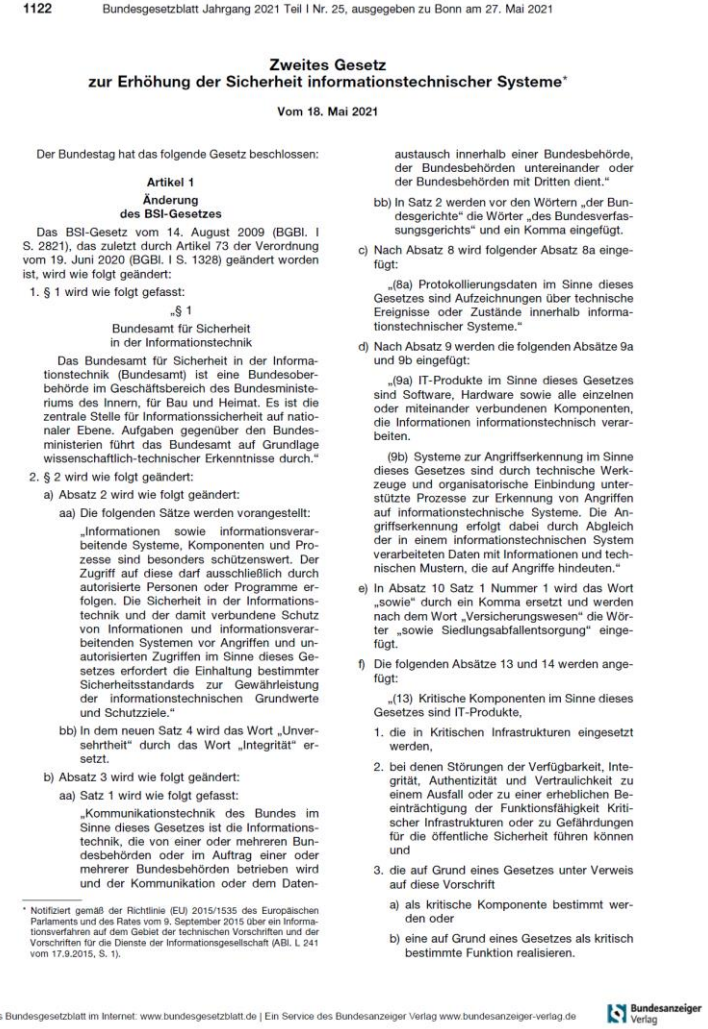
Gute Gründe

Offene Geheimnisse



https://exposure.shodan.io/#/DE

Regulierung



1122 Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 25, ausgegeben zu Bonn am 27. Mai 2021

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*

Vom 18. Mai 2021

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des BSI-Gesetzes

Das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 73 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

1. § 1 wird wie folgt gefasst:

„§ 1

Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch."

2. § 2 wird wie folgt geändert:

a) Absatz 2 wird wie folgt geändert:

aa) Die folgenden Sätze werden vorangestellt:

„Informationen sowie informationsverarbeitende Systeme, Komponenten und Prozesse sind besonders schützenswert. Der Zugriff auf diese darf ausschließlich durch autorisierte Personen oder Programme erfolgen. Die Sicherheit in der Informationstechnik und der damit verbundene Schutz von Informationen und informationsverarbeitenden Systemen vor Angriffen und unautorisierten Zugriffen im Sinne dieses Gesetzes erfordert die Einhaltung bestimmter Sicherheitsstandards zur Gewährleistung der informationstechnischen Grundwerte und Schutzziele."

bb) In dem neuen Satz 4 wird das Wort „Unversehrtheit" durch das Wort „Integrität" ersetzt.

b) Absatz 3 wird wie folgt geändert:

aa) Satz 1 wird wie folgt gefasst:

„Kommunikationstechnik des Bundes im Sinne dieses Gesetzes ist die Informationstechnik, die von einer oder mehreren Bundesbehörden oder im Auftrag einer oder mehrerer Bundesbehörden betrieben wird und der Kommunikation oder dem Datenaustausch innerhalb einer Bundesbehörde, der Bundesbehörden untereinander oder der Bundesbehörden mit Dritten dient."

bb) In Satz 2 werden vor den Wörtern „der Bundesgerichte" die Wörter „des Bundesverfassungsgerichts" und ein Komma eingefügt.

c) Nach Absatz 8 wird folgender Absatz 8a eingefügt:

„(8a) Protokollierungsdaten im Sinne dieses Gesetzes sind Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme."

d) Nach Absatz 9 werden die folgenden Absätze 9a und 9b eingefügt:

„(9a) IT-Produkte im Sinne dieses Gesetzes sind Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten.

(9b) Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten."

e) In Absatz 10 Satz 1 Nummer 1 wird das Wort „sowie" durch ein Komma ersetzt und werden nach dem Wort „Versicherungswesen" die Wörter „sowie Siedlungsabfallentsorgung" eingefügt.

f) Die folgenden Absätze 13 und 14 werden angefügt:

„(13) Kritische Komponenten im Sinne dieses Gesetzes sind IT-Produkte,

1. die in Kritischen Infrastrukturen eingesetzt werden,
2. bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können und
3. die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift
   a) als kritische Komponente bestimmt werden oder
   b) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren.

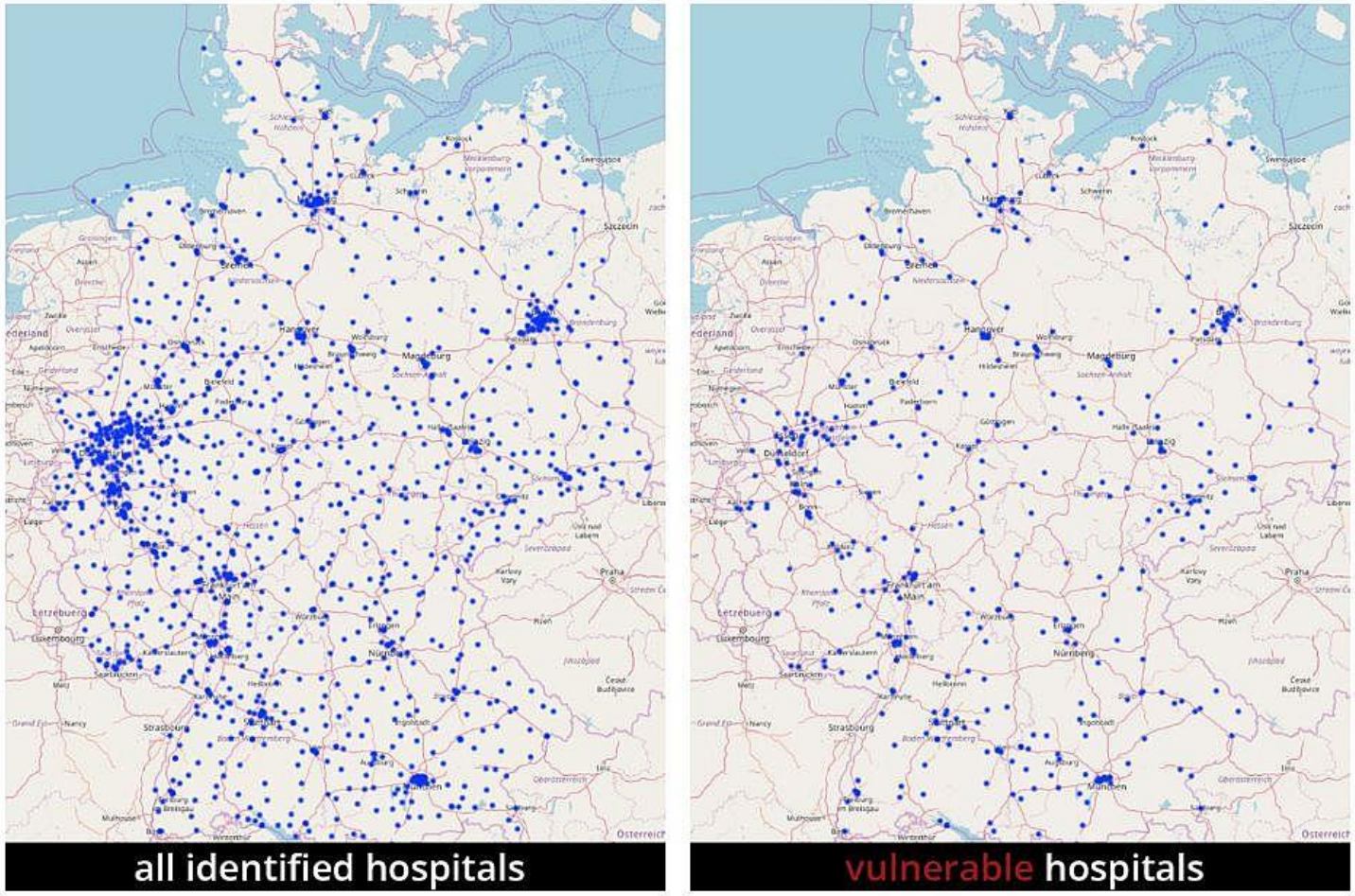
* Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

Das Bundesgesetzblatt im Internet: www.bundesgesetzblatt.de | Ein Service des Bundesanzeiger Verlag www.bundesanzeiger-verlag.de

Die Situation in den Krankenhäuser

Aktuelle Studie (2021) von alphastrike labs

- 1500 deutsche Krankenhäuser
- >900 kritische Schwachstellen
- Große Häuser starker betroffen
  - KRITIS >30.000 vollstationäre Behandlungen pro Jahr



Quelle: https://e-health-com.de/details-unternehmensnews/it-sicherheitsrisiko-krankenhaus/

Gute Gründe für Industrial Security

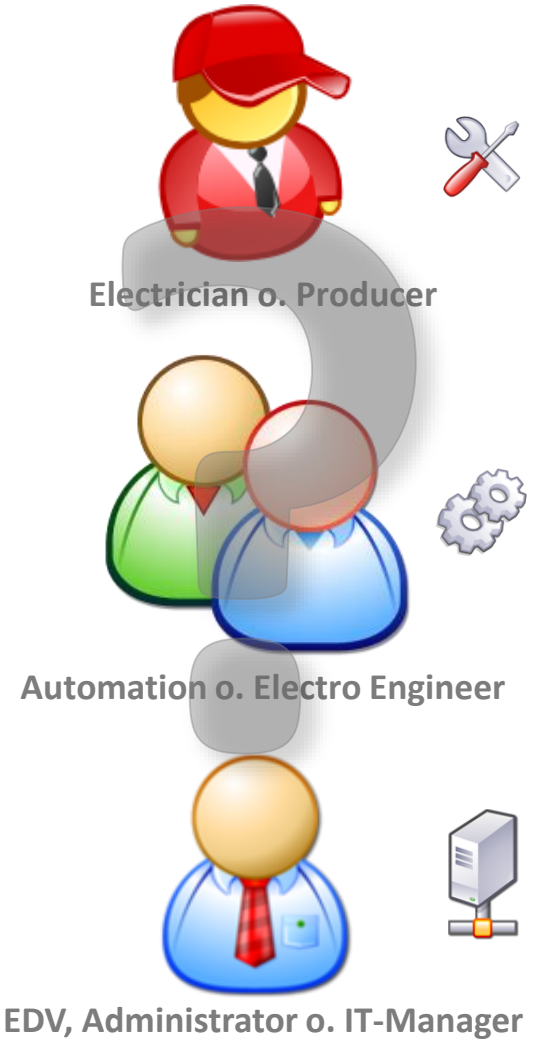
Aber wie?

- Netzwerk
  - Segmentierung des Produktionsnetzes
  - Fernwartungskonzept
  - Perimeter Security Gateway (Firewalls, IDS/IPS)
  - Security Information and Event Management (SIEM)
- Schnittstelle
  - Geräte- und Daten-Management (Device Control)
- System
  - Systemsicherheit durch Härtung durch Whitelisting-Technologie (nicht scan-basierende Technologie)
    - API Aufrufe von Prozessen, die sich nicht auf der Whitelist befinden werden unterbunden
    - Schutz vor Buffer Overflows

Verständigung

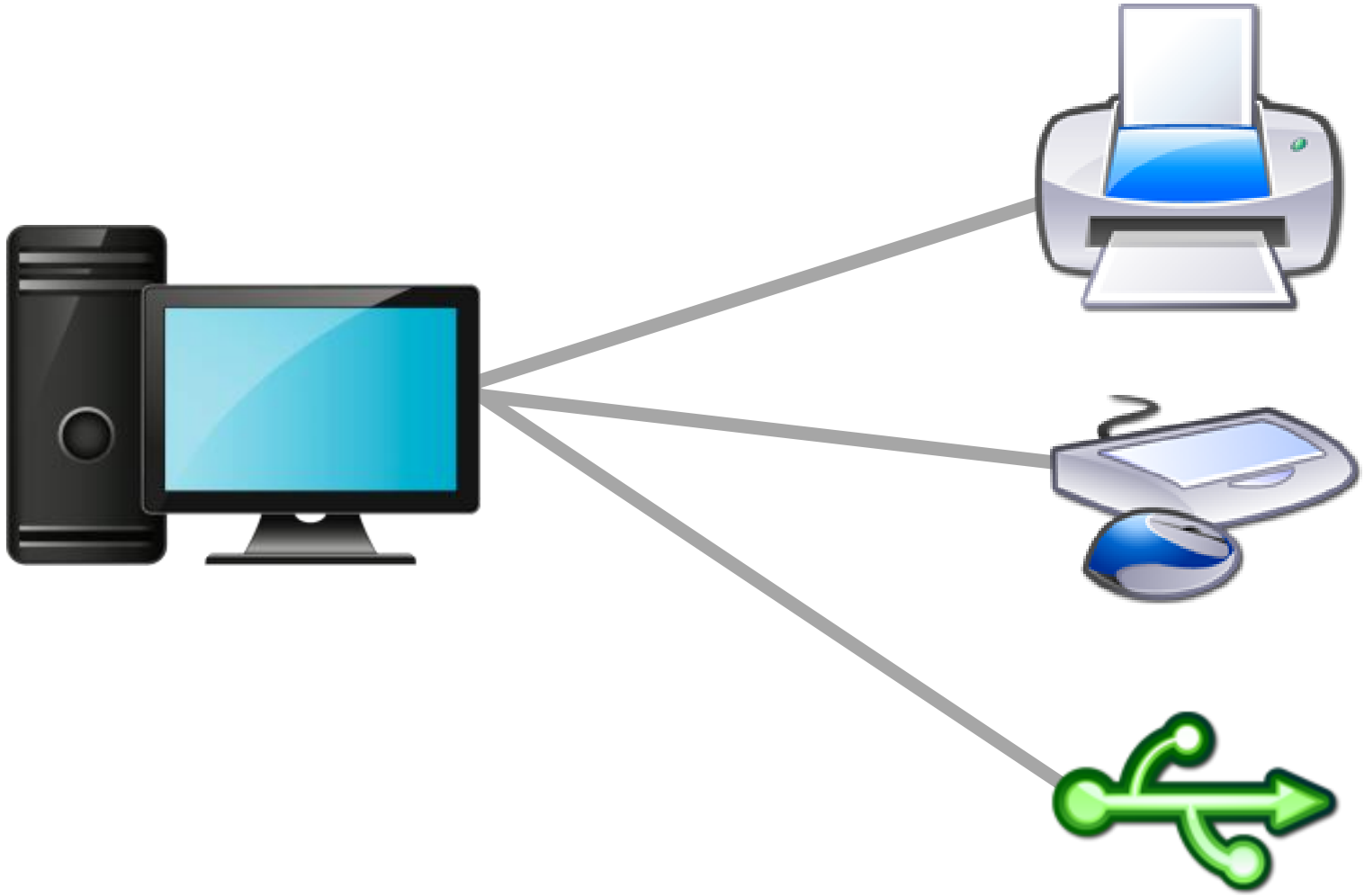
Gegenseitiges Verständnis

Verantwortlichkeit



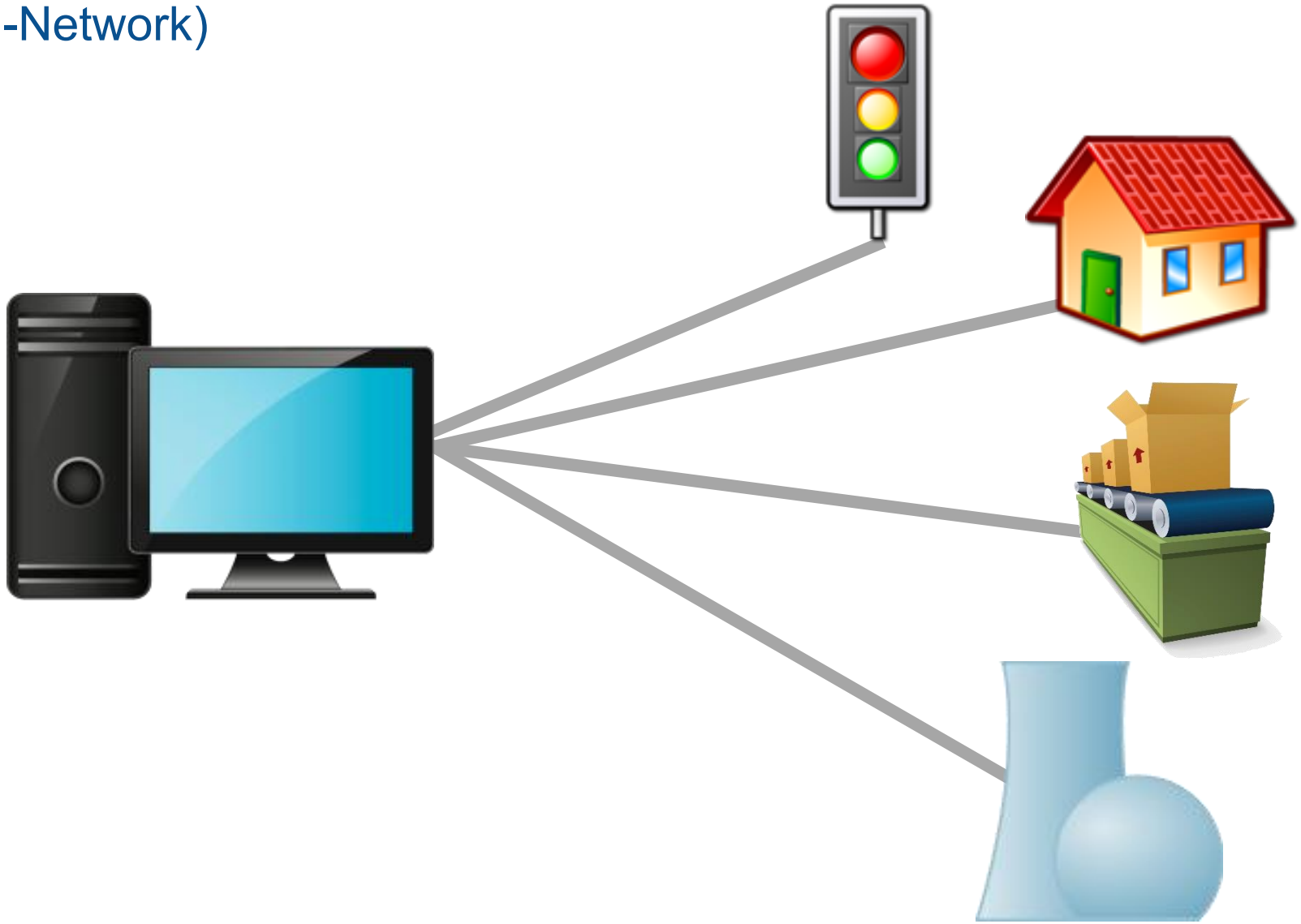
Gegenseitiges Verständnis

Peripherie (Office-Network)



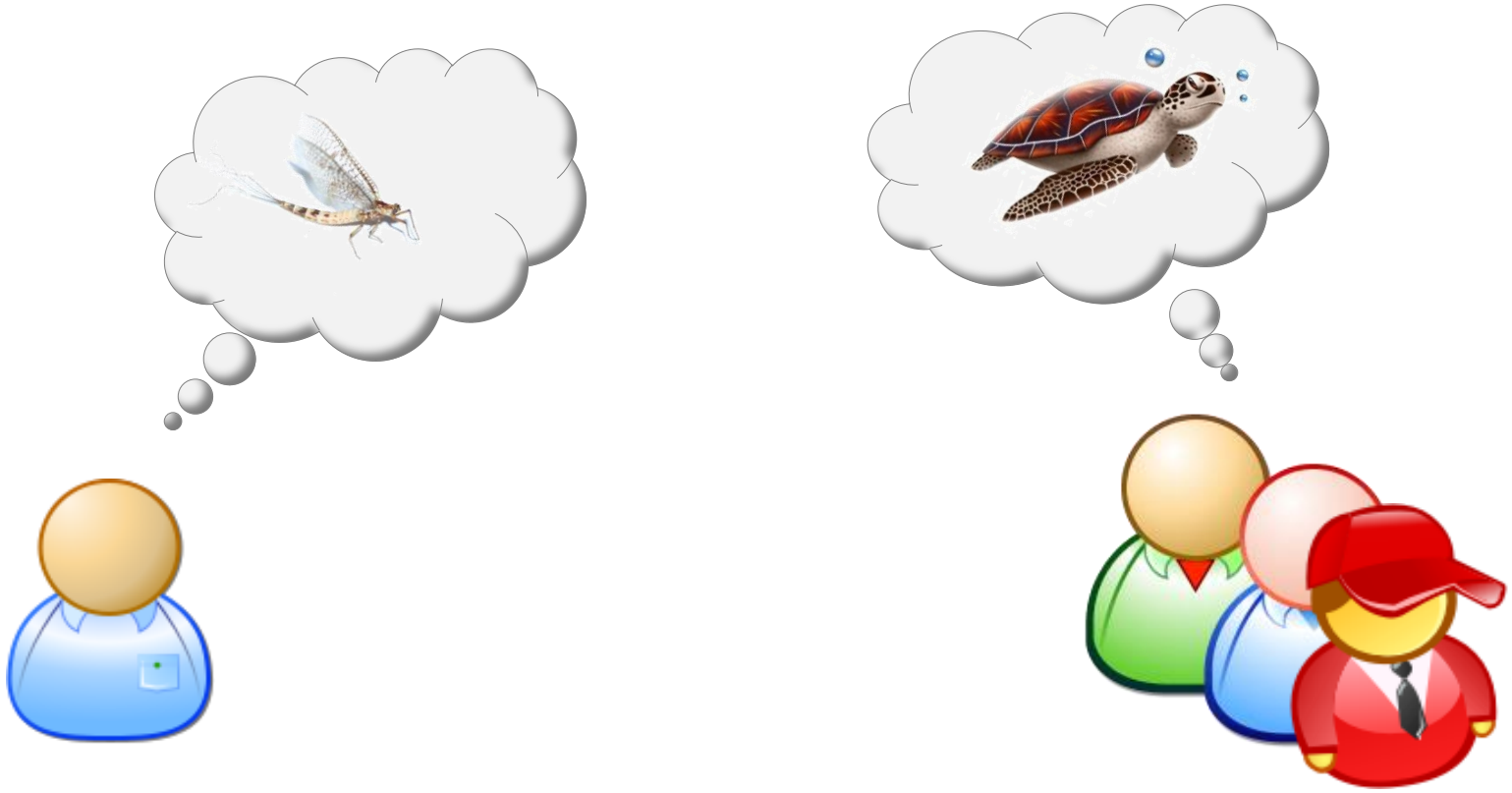
Gegenseitiges Verständnis

Peripherie (ICS-Network)



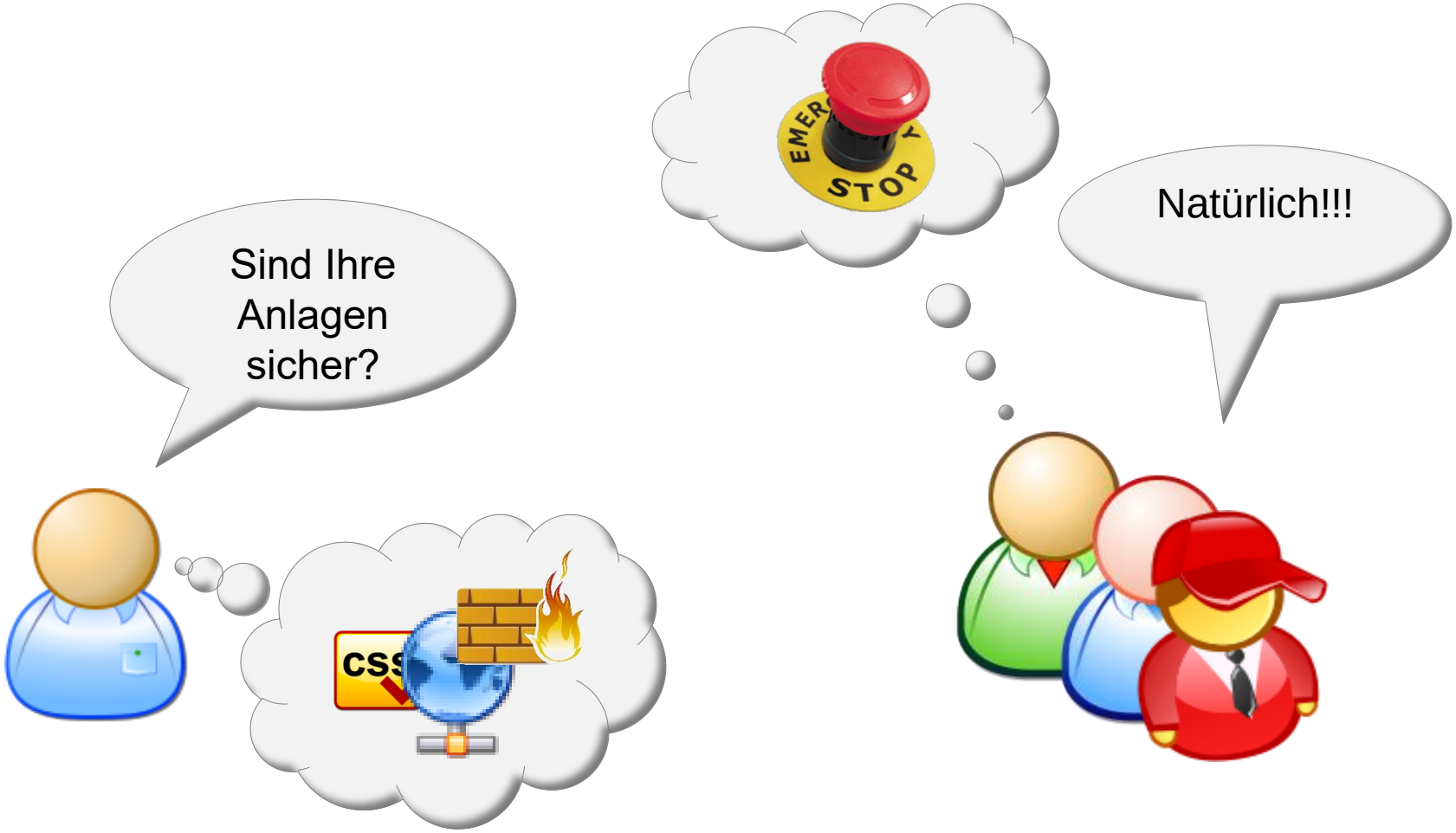
Gegenseitiges Verständnis

Lebenszyklen



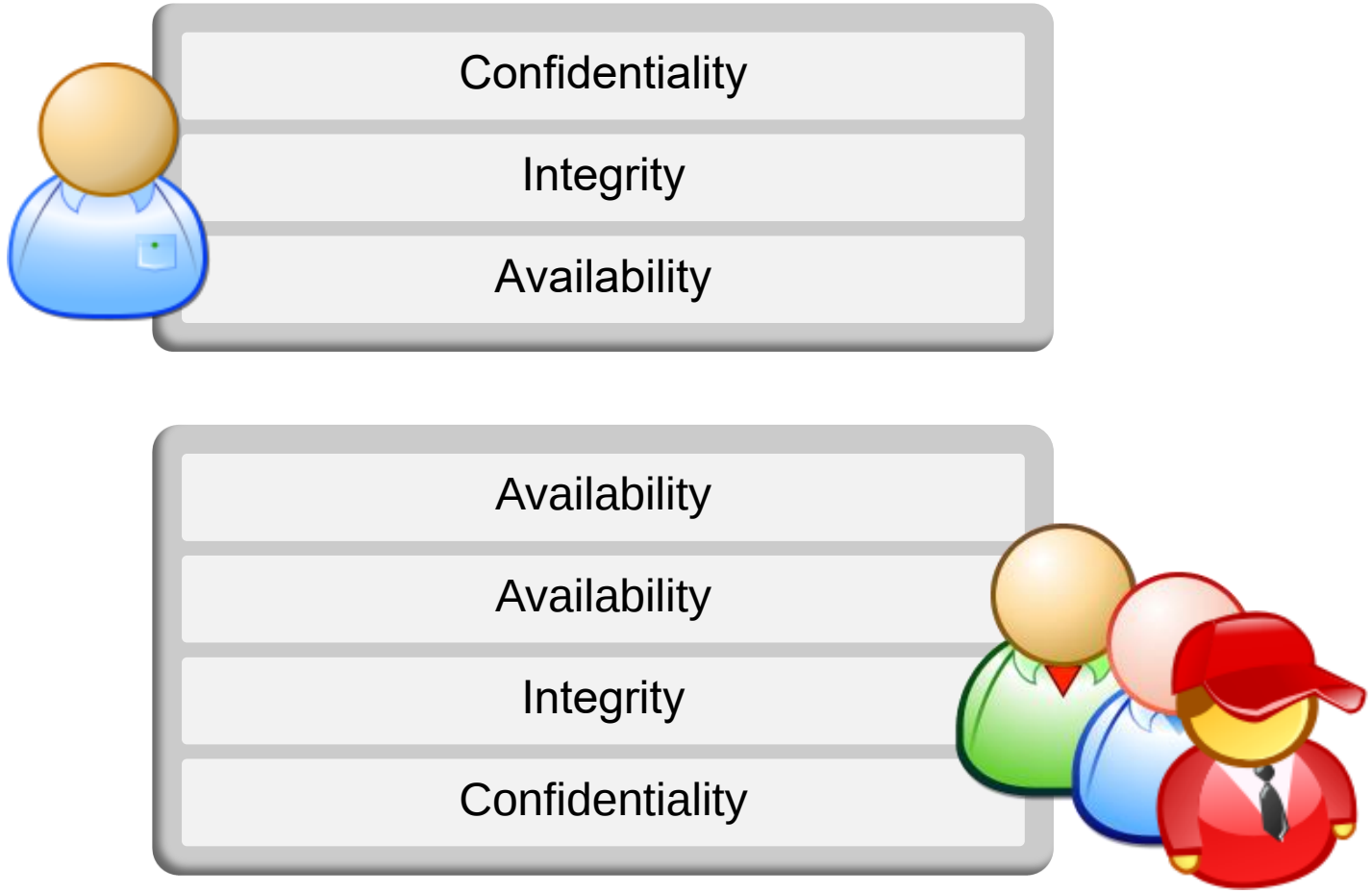
Gegenseitiges Verständnis

Security vs. Safety



Gegenseitiges Verständnis

Schutzzielpriorisierung



Vielen Dank!

Vielen Dank für Ihre Aufmerksamkeit!

Compass Security Deutschland GmbH
Tauentzienstraße 18
10789 Berlin

+49 30 2100 253 0
Team.CSDE@compass-security.com