



# Alive and Hacking

## Sichere Digitalisierung im Krankenhaus

Fachvereinigung Krankenhaus-Technik 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

## 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 [Fros-Photos](#) auf [Pixabay](#)



# Aktuelle Meldungen

**Berliner Morgenpost**  
Jobs Archiv E-Paper Tickets Leserreisen Shop Abo-Service Anzeige buchen

Home Berlin Bezirke Interaktiv Politik Wirtschaft Sport Panorama Kultur Wissen Reise Lifestyle Abo Newsletter Specials Service

Themen: Newsletter | Alle Nachrichten zum Coronavirus | Genießen in Berlin | Podcasts | Danke, Tegell | Alle Themen

Home – Aus aller Welt – Corona-Krise bringt dramatischen Anstieg von Hacker-Angriffen – auch aufs Homeoffice

**CORONA-KRISE**

## Homeoffice bietet Angriffsfläche – so oft schlagen Hacker zu

**StN.DE** STUTTGARTER NACHRICHTEN 75 JAHRE

Region & Land > Baden-Württemberg > Sieben Kliniken in Baden-Württemberg offline

## Hackerangriff auf SRH-Kliniken Sieben Kliniken in Baden-Württemberg offline

red/dpa/Isa, 22.09.2021 - 14:51 Uhr

Die IT-Systeme der Kliniken der SRH sind von Hackern angegriffen worden. (Symbolbild) Foto: imago images/Robert Poortsen/Robert Poortsen via www.imago-images.de

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

**DW** Made for minds.

ÜBER UNS KARRIERE PRESSE BUSINESS & SALES TRAVEL WERBUNG

PRESSEMITTEILUNGEN ANSPRECHPARTNER

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.

**Frankfurter Allgemeine**  
ZEITUNG • FAZ.NET

## Computer-Hacker kapern die Rechner eines Wasserwerks

VON STEPHAN FINSTERBUSCH • AKTUALISIERT AM 11.02.2021 - 17:02

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

**JKD Universitätsklinikum**  
Düsseldorf

## Düsseldorf: Massiver Netzwerkausfall

Um 12:20 Uhr | Lesedauer: Eine Minute

Das Krankenhaus hat sich derzeit von der Notfallversorgung abgemeldet. Foto: Gambarini/dpa Foto: dpa/Federico Gambarini

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

**WirtschaftsWoche**

## Hacker am Steuer

Noerpel Ulm  
Hacker greifen Logistikfirmen an

## Unbekannte Hacker verüben einen Angriff auf ein Fahrzeugpark der Bundeswehr

Das Krankenhaus hat sich derzeit von der Notfallversorgung abgemeldet. Foto: Gambarini/dpa Foto: dpa/Federico Gambarini

# Schlechte und Gute Neuigkeiten

F+ PODCASTS BLOGS THEMEN TICKER ARCHIV STELLENMARKT  
Wirtschaft > Digtac > Solarwinds-Hack: Massiver Cyberangriff gefährdet deutsche Behörden

PRODUKTE NEWSLETTER

## 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)

## Deutschland · Digital · Sicher · BSI

Die Lage der IT-Sicherheit in Deutschland 2021 im Überblick

### RANSOMWARE/DDOS

Deutliche Ausweitung cyber-krimineller Erpressungsmethoden



**13 Tage** lang konnte ein Universitätsklinikum nach einem Ransomware-Angriff keine Notfall-Patienten aufnehmen.

**144 MIO.** neue Schadprogramm-Varianten **+22%** gegenüber 2020: **117,4 MIO.**

DURCHSCHNITTLICH **394.000** neue Schadprogramm-Varianten pro Tag  
2020: 322.000

IM HÖCHSTWERT **553.000**  
2020: 470.000

**40.000** BOT-INFESTIONEN DEUTSCHER SYSTEME

**98%** aller geprüften Systeme waren durch Schwachstellen in **MS Exchange** verwundbar.

**14,8 MIO.**

Meldungen übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.



**44.000** **74.000**



**100** Zertifizierungen von Produkten, Standorten und Schutzprofilen im Bereich Common Criteria

**5.100** MITGLIEDER DER ALLIANZ FÜR CYBER-SICHERHEIT

2020: 4.400  
2019: 3.700  
2018: 2.700

**< 10%** waren nach Warnungen von BSI und Microsoft immer noch durch Schwachstellen in **MS Exchange** verwundbar.

Deutschland Digital-Sicher-BSI

## 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.

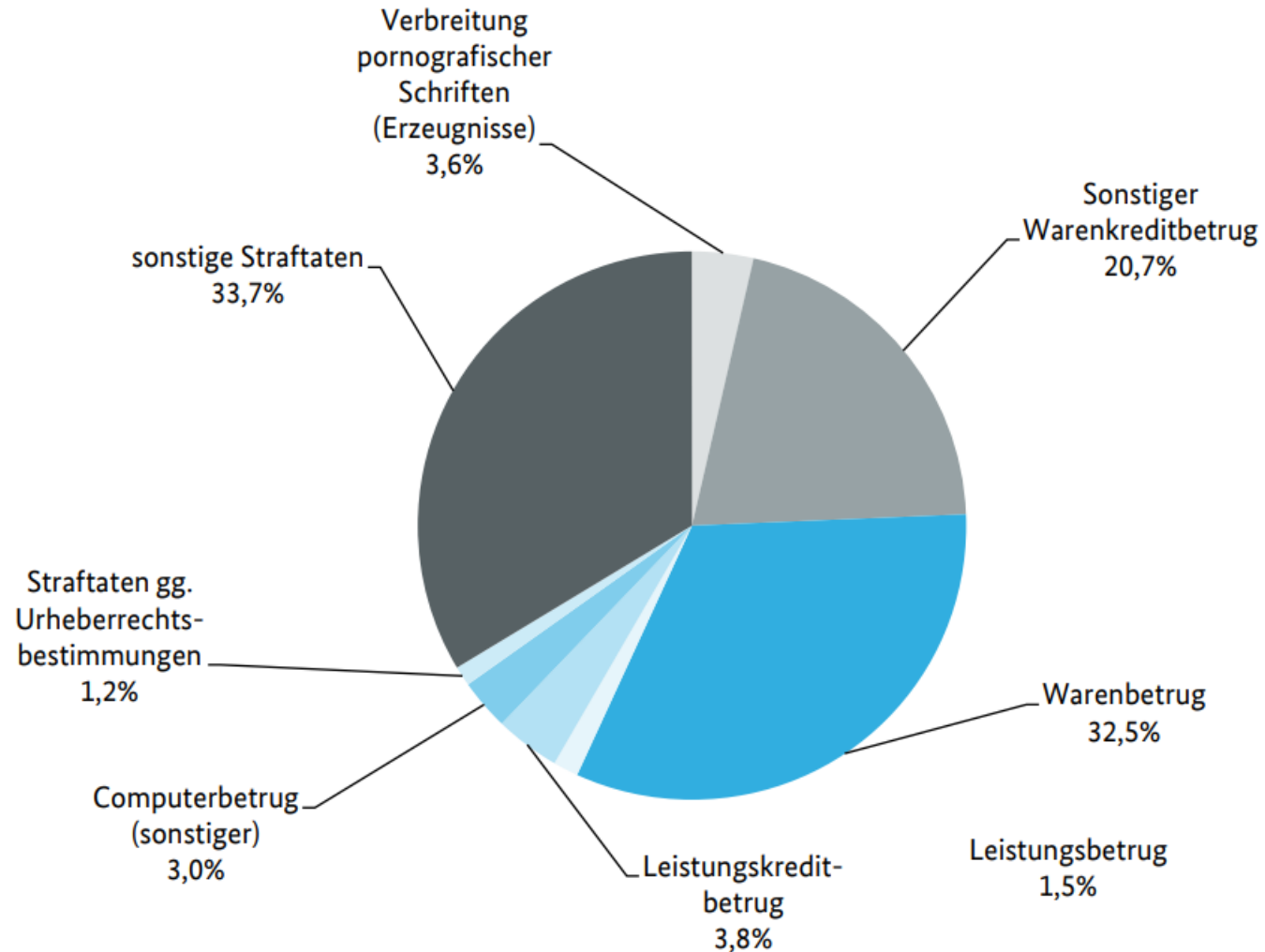
Abbildung 1: Die wesentlichen Aspekte der Cybercrime in Deutschland 2020



# Polizeiliche Kriminalstatistik (Deutschland) 2019

## Straftatenanteile an Straftaten mit Tatmittel „Internet“ = 251.617 Fälle

1 - 2.4.2 - G01



Quelle: BKA

# Meldung zu Krankenhäusern



hacker krankhaus



Alle News Bilder Maps Shopping Mehr

Suchfilter

Ungefähr 25.600 Ergebnisse (0,26 Sekunden)


SWR  
**Hacker-Angriff auf SRH Klinik Karlsbad-Langensteinbach**  
Der SRH Klinikverbund ist Opfer eines Hackerangriffs geworden. Davon betroffen ist auch das Klinikum Karlsbad-Langensteinbach. Die Hacker...  
vor 1 Tag



Thüringer Allgemeine  
**Krankenhaus in Friedrichroda von Hackerangriff betroffen**  
Der Klinik-Verbund ist Opfer eines Hackerangriffs. Die medizinische




Tagesschau  
**Immer mehr Cyberangriffe: Kliniken im Visier der Hacker ...**  
Die Urologische Klinik in Planegg wurde zu Beginn dieses Jahres ebenfalls Ziel eines Cyberangriffs, im März wurde die Evangelische Klinik in...  
28.06.2021



NDR  
**Wolfenbüttel: Vielversprechende Spuren nach Hackerangriff**  
Hacker fordern Bitcoin. Auf eine Zahlungsaufforderung der Hacker ging das Klinikum den Angaben zufolge nicht ein. Die Kriminellen hatten Bitcoin...  
19.07.2021



WDR  
**Hacker-Angriff auf Krankenhaus Lippstadt**  
Ein Hacker-Angriff hat das Evangelische Krankenhaus Lippstadt lahmgelegt. Ab sofort können keine Patienten mehr aufgenommen werden.  
30.03.2021



Berlin/ Düsseldorf/ Köln Fallen im Krankenhaus die Server aus, sind Menschenleben gefährdet. Diese abstrakte Gefahr ist vor einem Jahr in...  
vor 3 Wochen



DerStandard  
**Hackerangriff auf eines der größten Krankenhäuser in Rom**  
Das Krankenhaus "San Giovanni Addolorata", eines der größten in Rom, ist ins Visier von Hackern geraten. Durch einen Virus wurde das...  
vor 1 Woche



Tagesschau  
**Immer mehr Cyberangriffe: Kliniken im Visier der Hacker ...**  
Die Urologische Klinik in Planegg wurde zu Beginn dieses Jahres ebenfalls Ziel eines Cyberangriffs, im März wurde die Evangelische Klinik in...  
28.06.2021



NDR  
**Wolfenbüttel: Vielversprechende Spuren nach Hackerangriff**  
Hacker fordern Bitcoin. Auf eine Zahlungsaufforderung der Hacker ging das Klinikum den Angaben zufolge nicht ein. Die Kriminellen hatten Bitcoin...  
19.07.2021




WDR  
**Hacker-Angriff auf Krankenhaus Lippstadt**  
Ein Hacker-Angriff hat das Evangelische Krankenhaus Lippstadt lahmgelegt. Ab sofort können keine Patienten mehr aufgenommen werden.  
30.03.2021



WDR  
**Hacker-Angriff auf Krankenhaus Lippstadt**  
Ein Hacker-Angriff hat das Evangelische Krankenhaus Lippstadt lahmgelegt. Ab sofort können keine Patienten mehr aufgenommen werden.  
30.03.2021



Münchner Merkur  
**Hacker-Angriff auf bekannte Münchner Klinik: Sensible Patientendaten ausgespäht**  
Hacker-Angriff auf Urologische Klinik München-Planegg: Patienten schriftlich informiert. Durch die Cyber-Attacke ist es dem oder den Hackern...  
24.02.2021



Radio Wien  
**CoV: Sechs Kinder und Jugendliche im Spital**  
Ein Kind auf der Intensivstation. In der Klinik Ottakring – sie ist im Moment die erste Anlaufstelle für Covid-erkrankte Kinder und Jugendliche...  
vor 1 Woche



Rechtsdepesche  
**Kliniken im Visier der Hacker Cyberangriffe: So gefährlich sind ...**  
Zuletzt gab es Angriffe der Hacker auf Kliniken in Düsseldorf und ... Auch hier hatten Hacker die Krankenhaus-EDV mit Schadsoftware...  
vor 1 Monat



FAZ  
**Hacker greifen Kliniken an**  
13 Tage lang fiel ausgerechnet dieses wichtige Krankenhaus für die Notfallversorgung aus, weil die Ärzte nicht richtig auf Röntgenbilder und...  
21.11.2020



Tagesspiegel  
**Frau nach Hacker-Angriff auf Düsseldorfer Uni-Klinik verstorben**  
IT-Ausfall im Krankenhaus : Frau nach Hacker-Angriff auf Düsseldorfer Uni-Klinik verstorben. Erpresser hatten Server des Klinikums angegriffen...  
17.09.2020



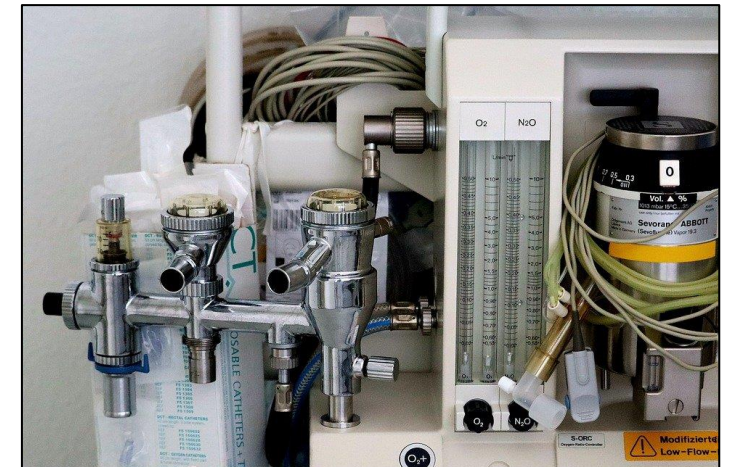
Süddeutsche Zeitung  
**München-Planegg: Hackerangriff auf Urologische Klinik**  
Das Krankenhaus wurde im Januar von Kriminellen erpresst - Lösegeldzahlungen gab es wohl nicht. Aber die Hacker bekamen durch ihre Attacke...  
15.02.2021





# Digitalisierung im Krankenhaus

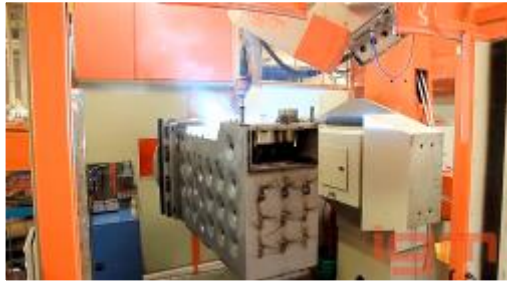
Mehr als nur ein IT Thema



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

## Qualität Produktivität

## Prozesse

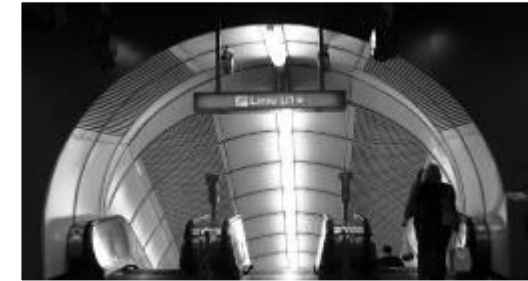


Bikinger, „Raffinerie Schwechat“, CC-Lizenz (BY 2.0)



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

## Gebäude



teakettle, „u1“, CC-Lizenz (BY 2.0)

## Transport

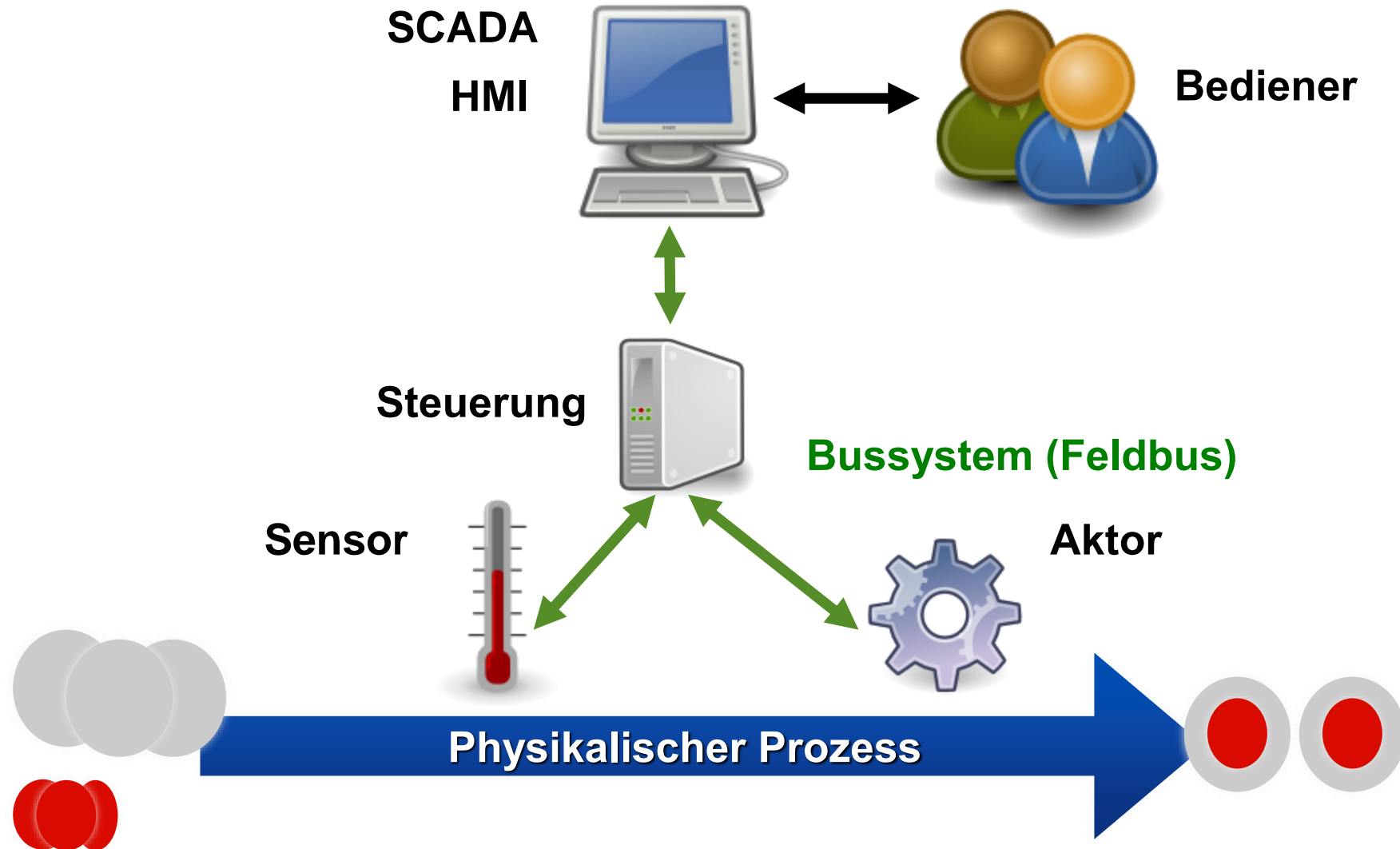
## kritische Infrastruktur

<http://creativecommons.org/licenses/by/2.0/de/deed.de>  
Alle Bilder stammen aus der kostenlosen Bilddatenbank [www.piqs.de](http://www.piqs.de)

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](https://www.vamed.com/media/4691/akh_leitwarte_000_3410.jpg)



Bei wem eher so?



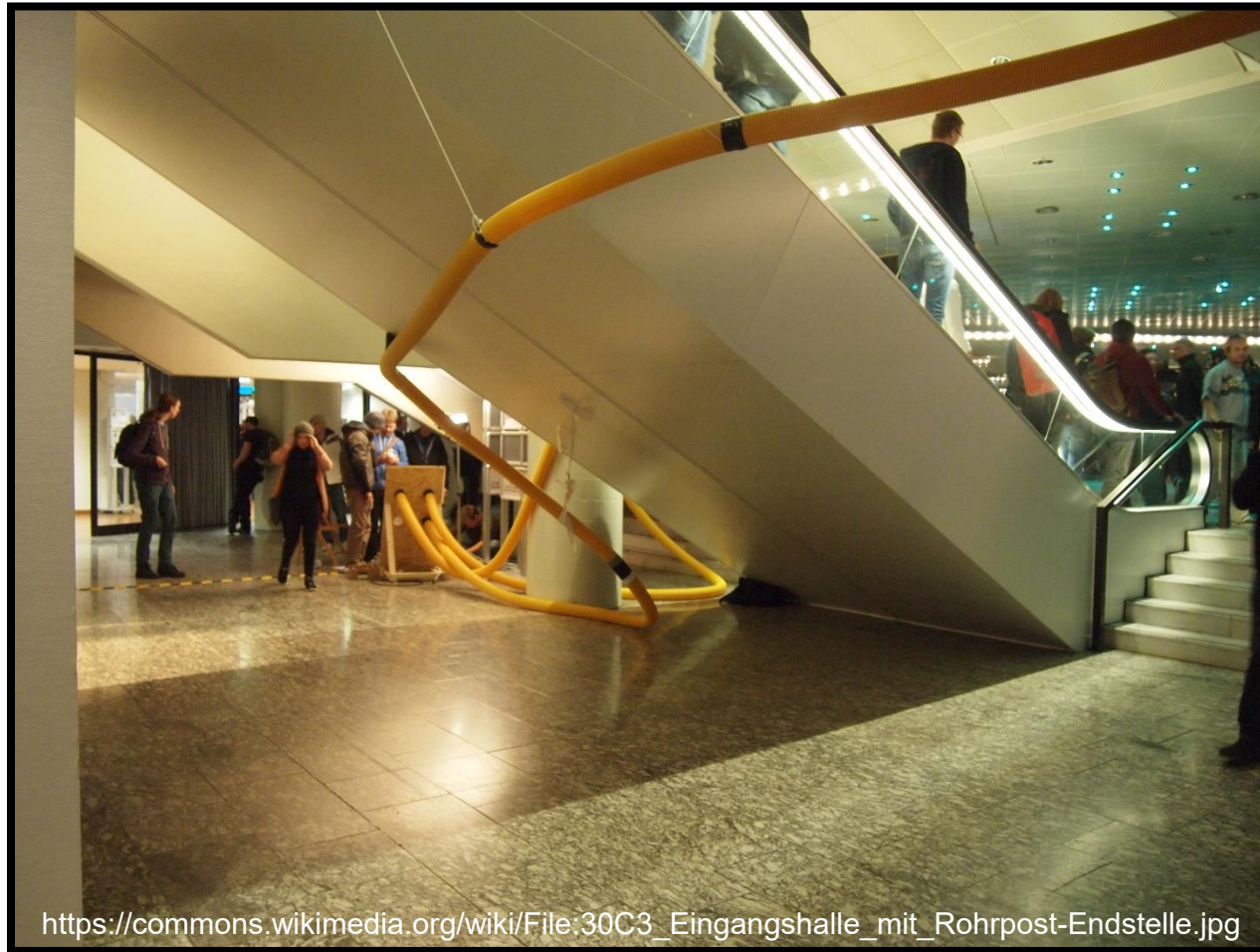
[https://www.helios-gesundheit.de/fileadmin/\\_processed\\_/5/0/csm\\_DSC\\_8072\\_16c347df07.jpg](https://www.helios-gesundheit.de/fileadmin/_processed_/5/0/csm_DSC_8072_16c347df07.jpg)





# Unerwartete Technologien

Die auch Hacker faszinieren



heise online heise+

Anmelden Suchen Menü

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN: BUNDESTAGSWAHL WINDOWS 11 KRYPTOWÄHRUNGEN RAUMFAHRT APPLE PODCASTS ANZEIGE: ONLINE-MARKETING

heise online > News > 08/2021 > PwnedPiper: Rohrpostsysteme in US-Krankenhäusern über Firmware-Lücken...

heise+ mit allen Inhalten von Make entdecken. **Jetzt für 12,95€ 0 € testen!**

## PwnedPiper: Rohrpostsysteme in US-Krankenhäusern über Firmware-Lücken angreifbar

Sicherheitslücken erlaubten Forschern die komplette Übernahme von "Translogic"-Rohrpostsystemen. Hersteller Swisslog Healthcare hat Updates veröffentlicht.

Lesezeit: 4 Min. In Pocket speichern

Zu Demonstrationszwecken verwandelten die Forscher das Rohrpostsystem in einen einarmigen Banditen. Stattdessen könnte es aber auch die Erpresserbotschaft einer Ransomware anzeigen. (Bild: Armis)

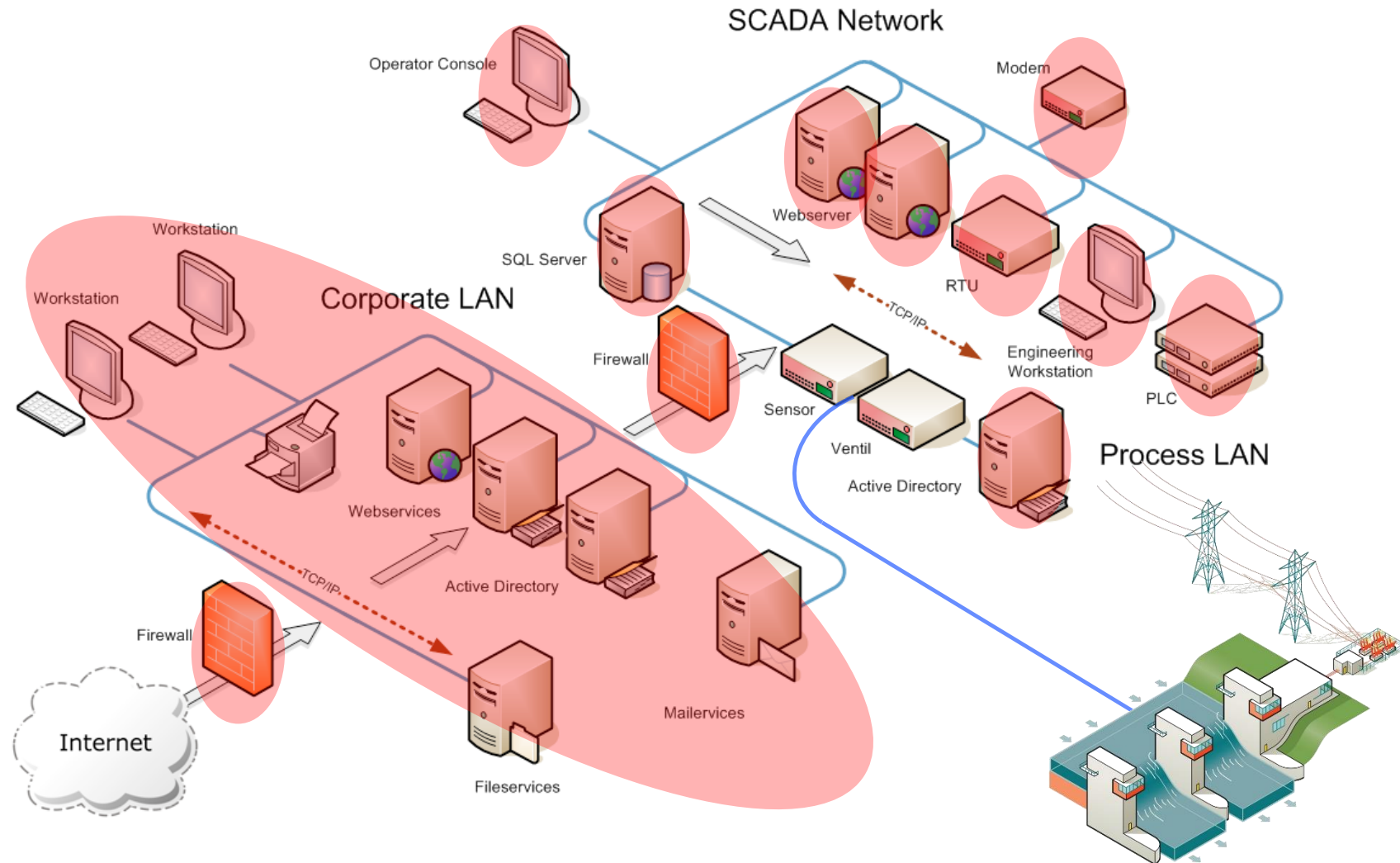
03.08.2021 11:14 Uhr | Security  
Von Olivia von Westernhagen

# Angriffsflächen



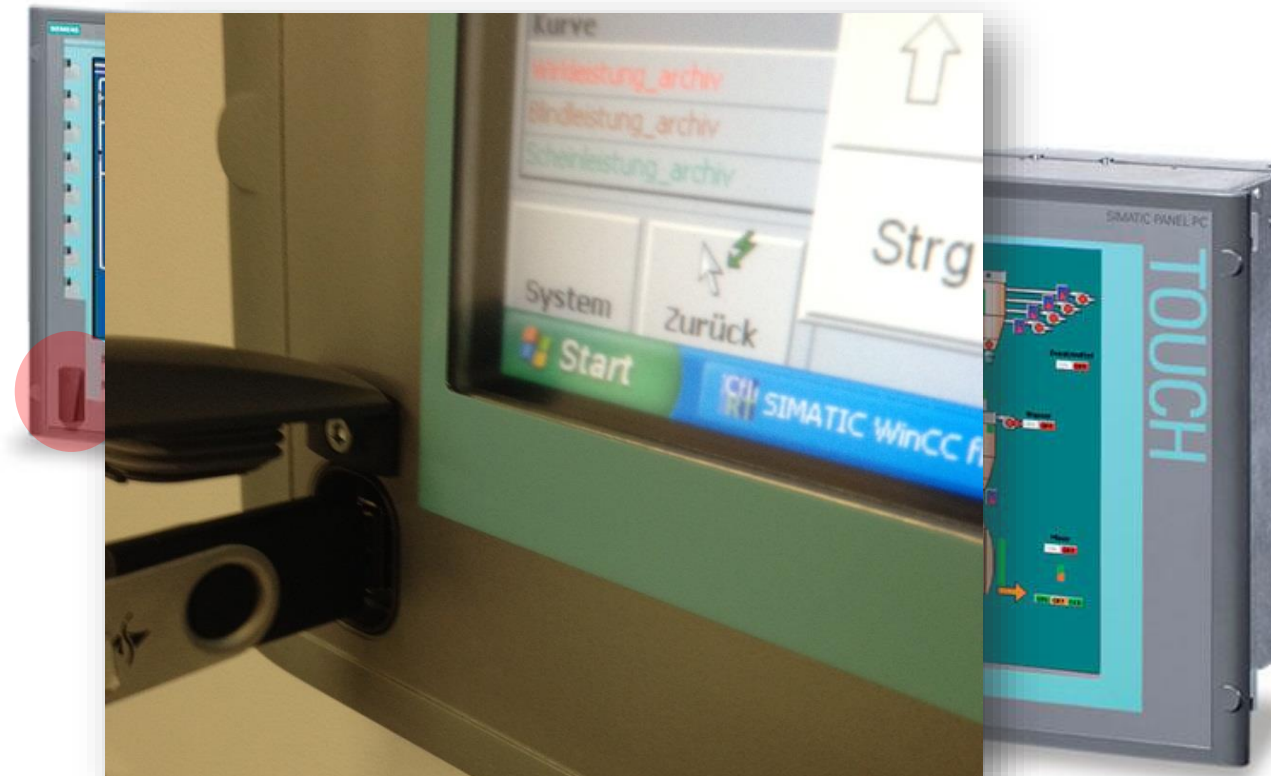
# Industrial Network Architecture

## Ansatzpunkte möglicher Angriffe



# Industrial Network Architecture

The Real World...



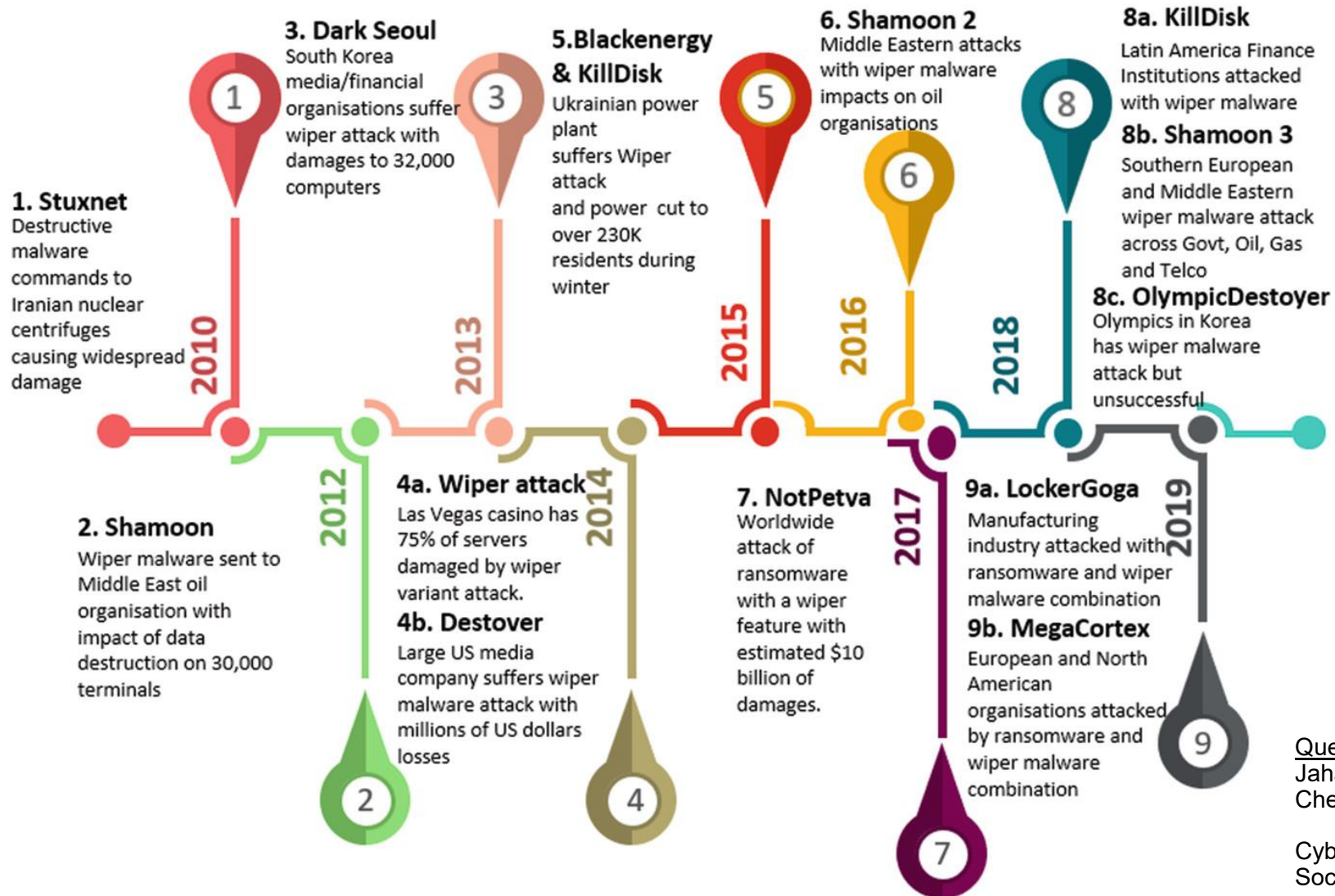


# Industrial Network Architecture

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.

tagesschau Sendung verpasst? ▶ ☰

Wirtschaft ▶ Unternehmen ▶ Nach Hackerangriff: Colonial Pipeline zahlte Lösegeld



Nach Hackerangriff

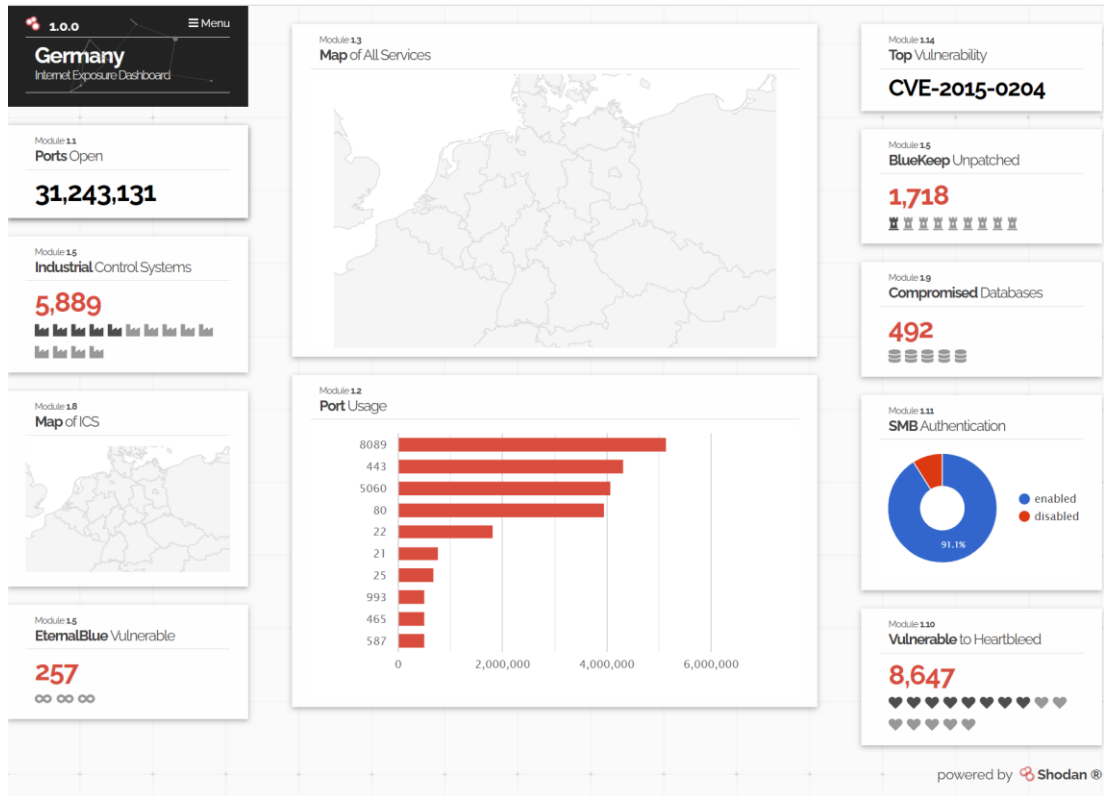
## Colonial Pipeline zahlte Lösegeld

Stand: 20.05.2021 09:31 Uhr

Vor zwei Wochen hatte ein Cyberangriff auf die Pipeline Colonial zu Engpässen bei der Benzinversorgung in Teilen der USA geführt. Nun räumte der Pipeline-Betreiber ein, den Hackern Lösegeld gezahlt zu haben.

# 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 Daten-

austausch 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 Stützinfrastruktur“ 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.“

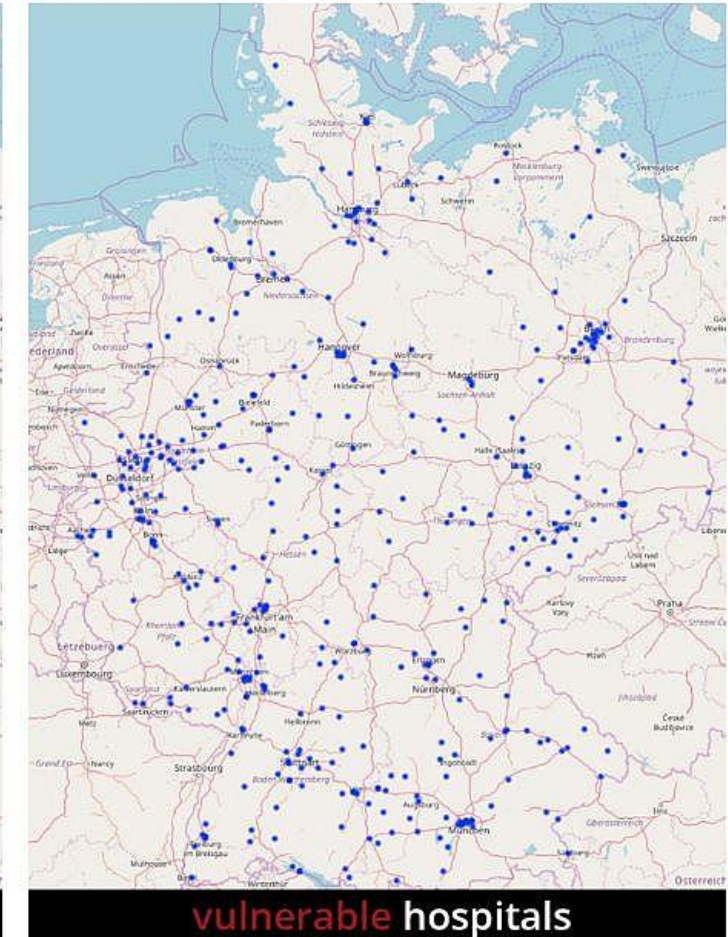
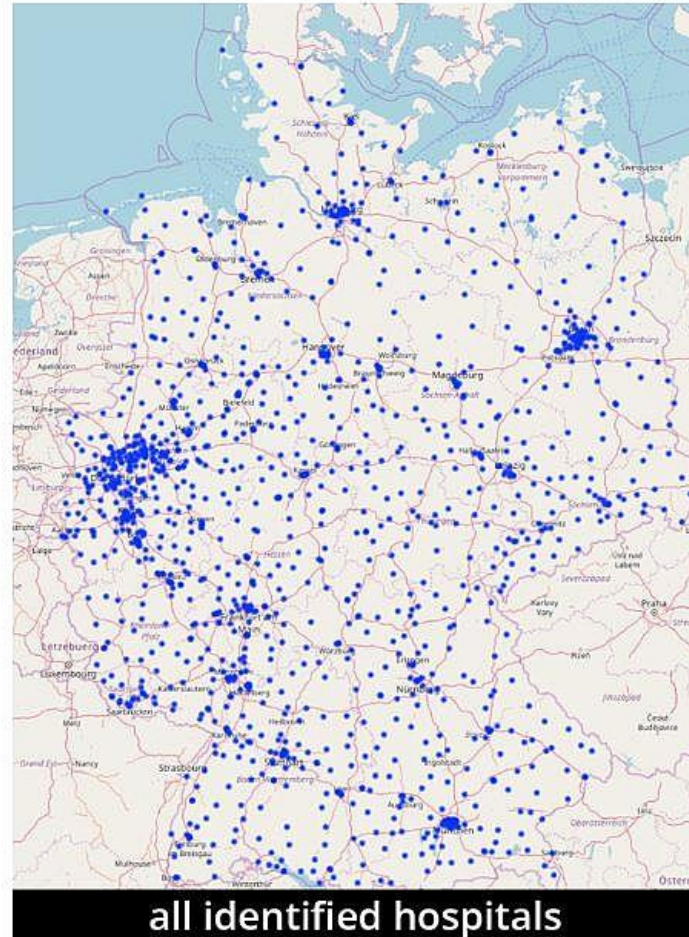
\* Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).



# 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

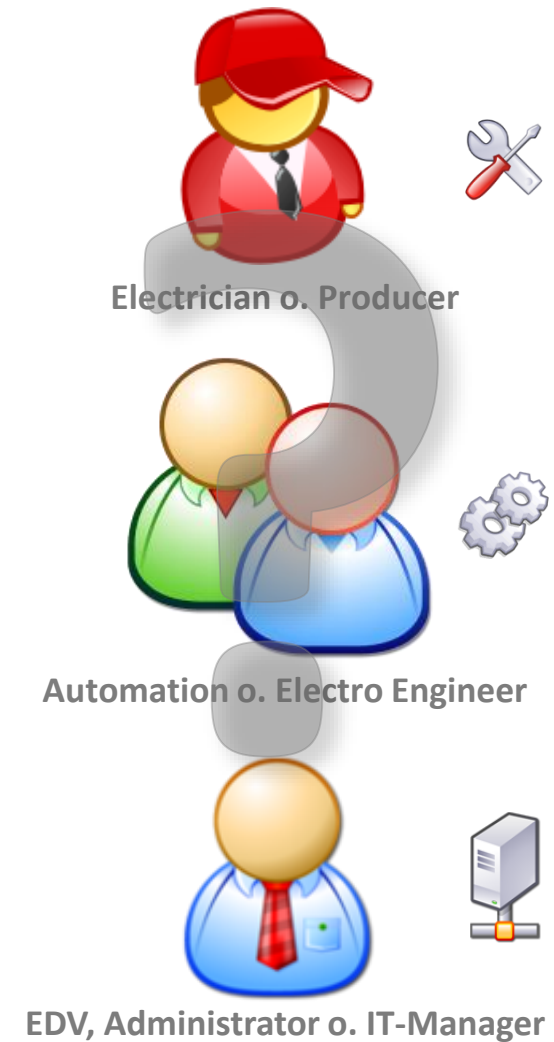




# Verständigung

# Gegenseitiges Verständnis

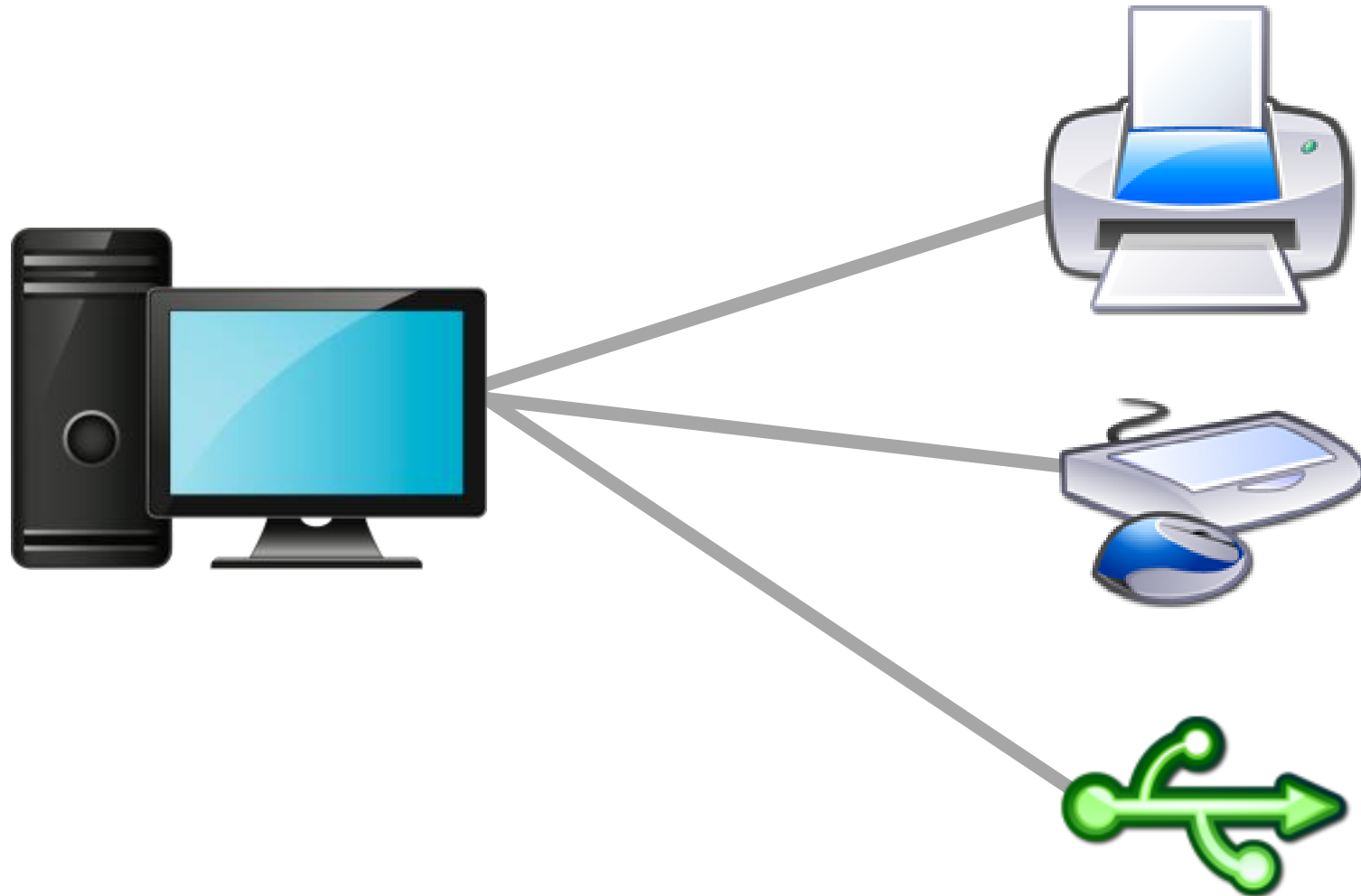
## Verantwortlichkeit





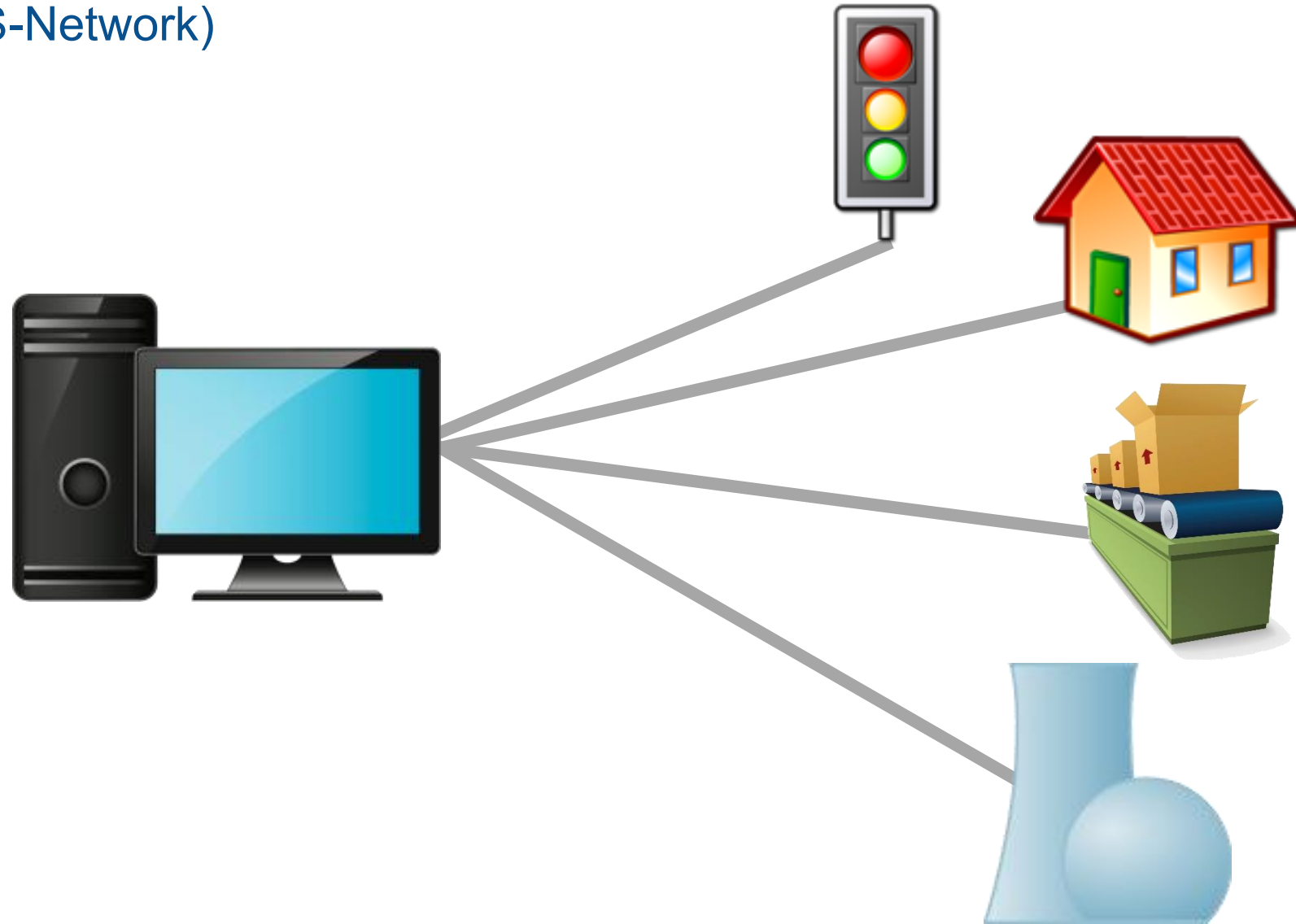
# Gegenseitiges Verständnis

Peripherie (Office-Network)



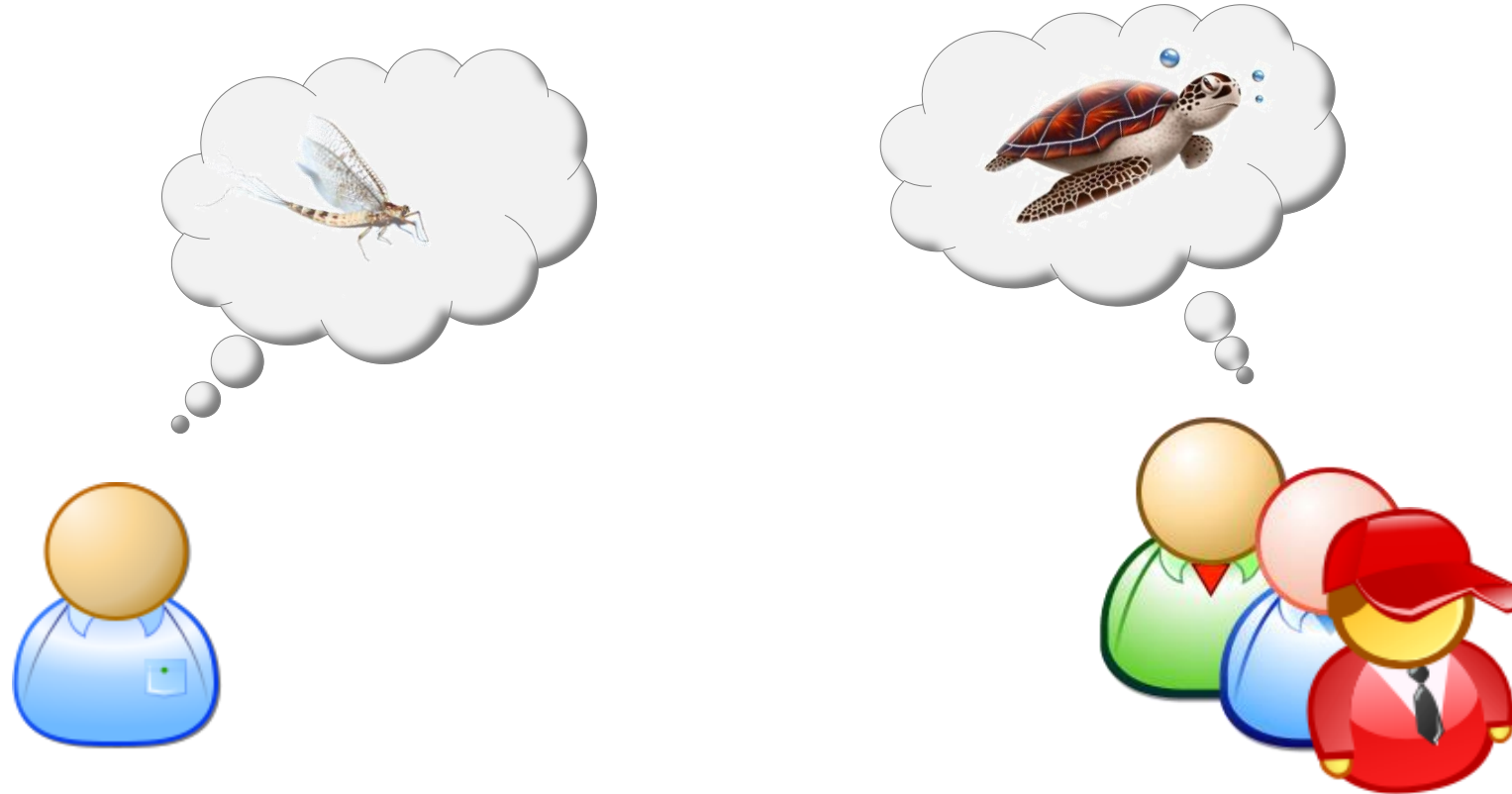
# Gegenseitiges Verständnis

Peripherie (ICS-Network)



# Gegenseitiges Verständnis

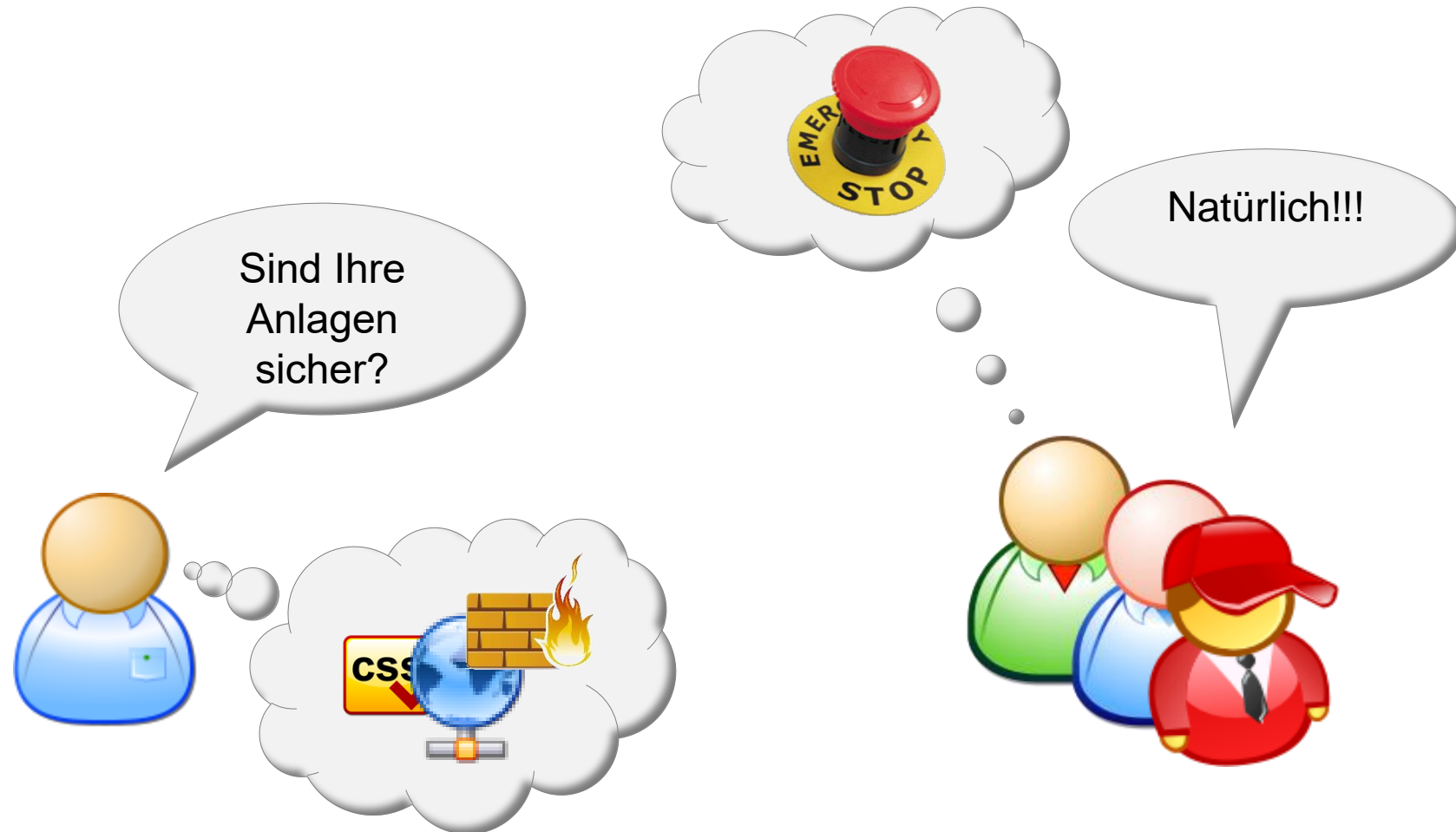
## Lebenszyklen





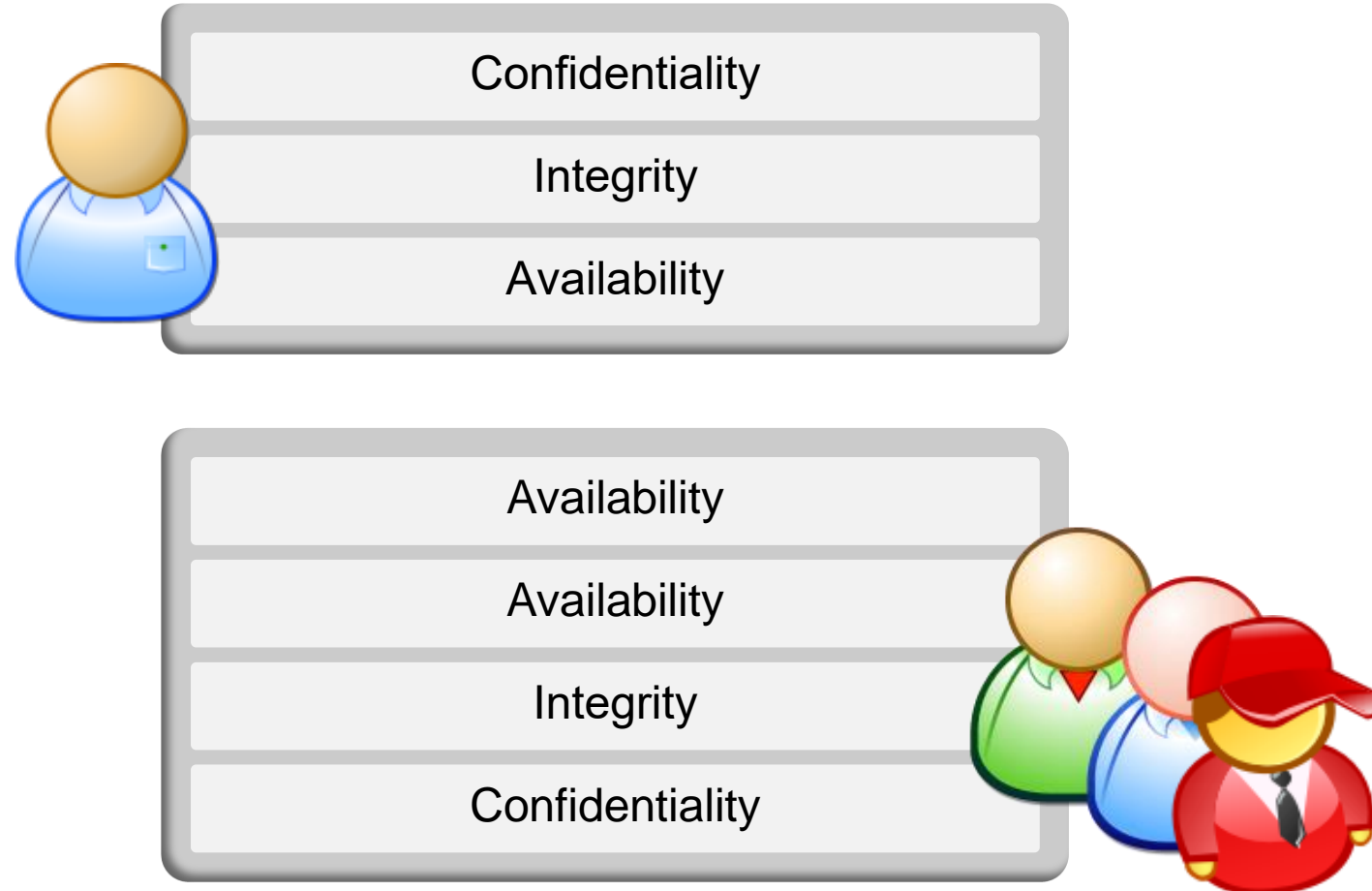
# Gegenseitiges Verständnis

## Security vs. Safety



# Gegenseitiges Verständnis

## Schutzzielpriorisierung







**Vielen Dank!**

**Vielen Dank für Ihre Aufmerksamkeit!**



Compass Security Deutschland GmbH  
Tautenzienstraße 18  
10789 Berlin

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