Cybersicherheit in der Wasserwirtschaft

ACQUA360 – Lugano - 26. September 2019

rittmeyer BRUGG

Patrick Erni

5 Jahre Leiter IT-Services bei Rittmeyer
- Studium HSLU Information Security
- Studium HSLU Digital Business Innovation
- ISO 27001 Security Officer zertifiziert - TÜV

12 Jahre Leiter Informatik bei Rittmeyer
- Studium HSLU IT-Management
- ITIL Foundation zertifiziert

9 Jahre ICT-Projektleiter
Banken, Versicherung und KMU Umfeld
- MCSE Microsoft zertifiziert
- NCSE Novell zertifiziert

6 Jahre Hardware System Engineer
- IBM HW zertifiziert

Das Unternehmen Rittmeyer AG

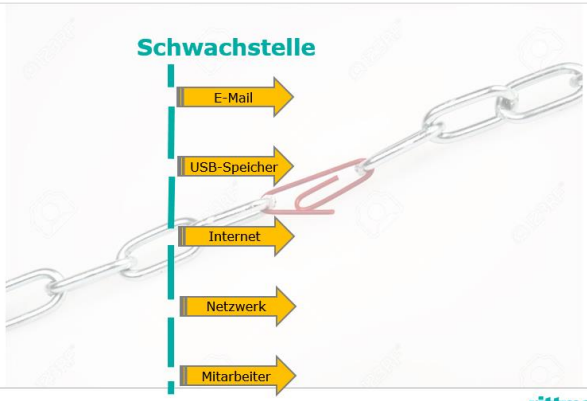
Gründungsjahr: 1904
Unternehmensform: Aktiengesellschaft
Hauptsitz: Baar (Schweiz)
Anzahl der Mitarbeitenden: 300
Weltweit installierte Systeme: über 20’000

Inhalt

Grundlagen der IT/OT Sicherheit

Bedrohungen

Schwachstellen



Gefahren

Gefahr

- Manipulation
- Diebstahl
- Erpressung
- Ausfall
- Zerstörung
- Verlust

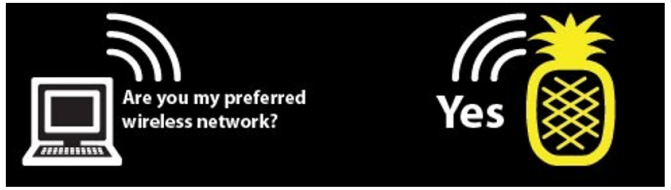
Schützen

Wie müssen wir uns schützen?

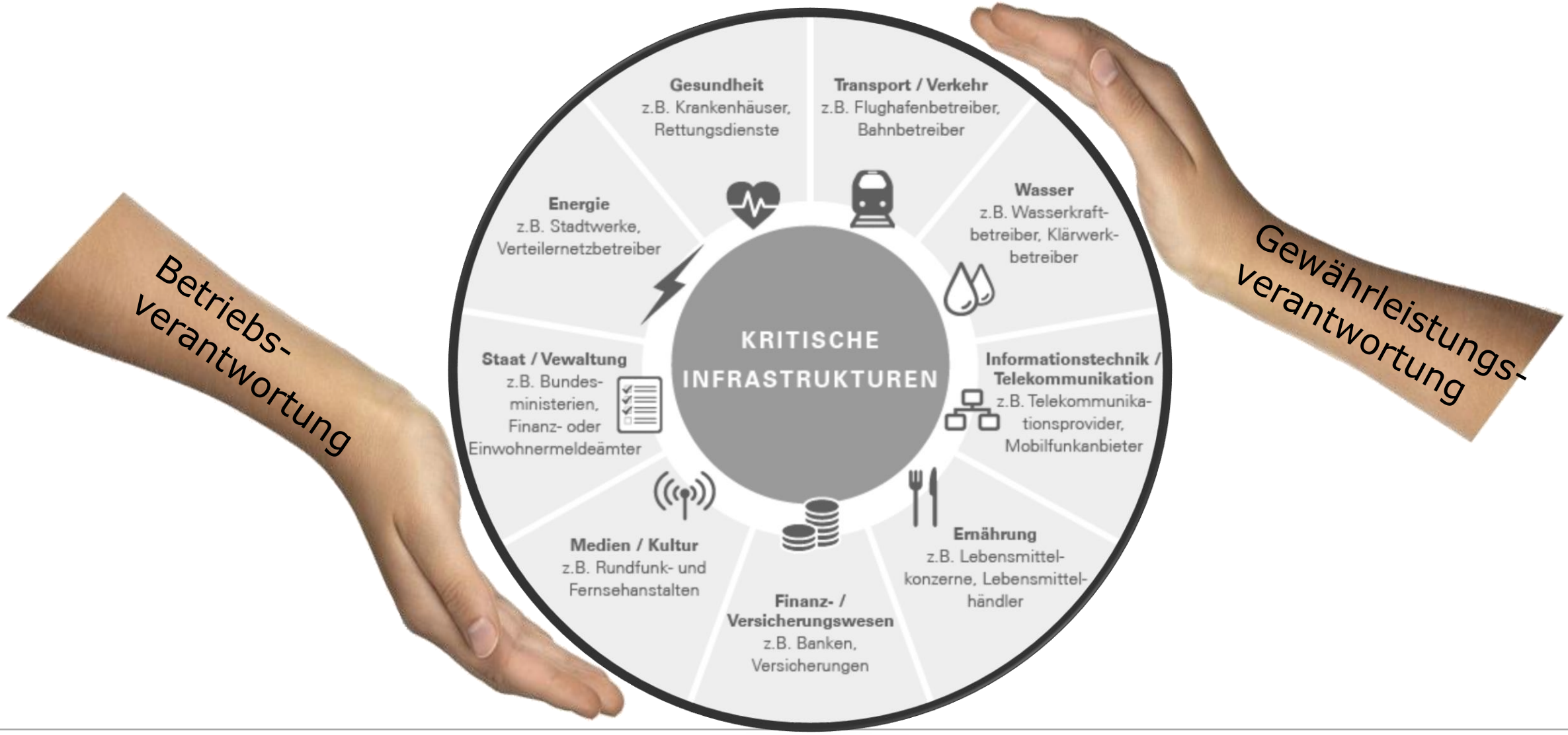
*Sicherheit besteht aus **75% Mensch** (Organisatorisch) und nur **25% Technologie***

Demo

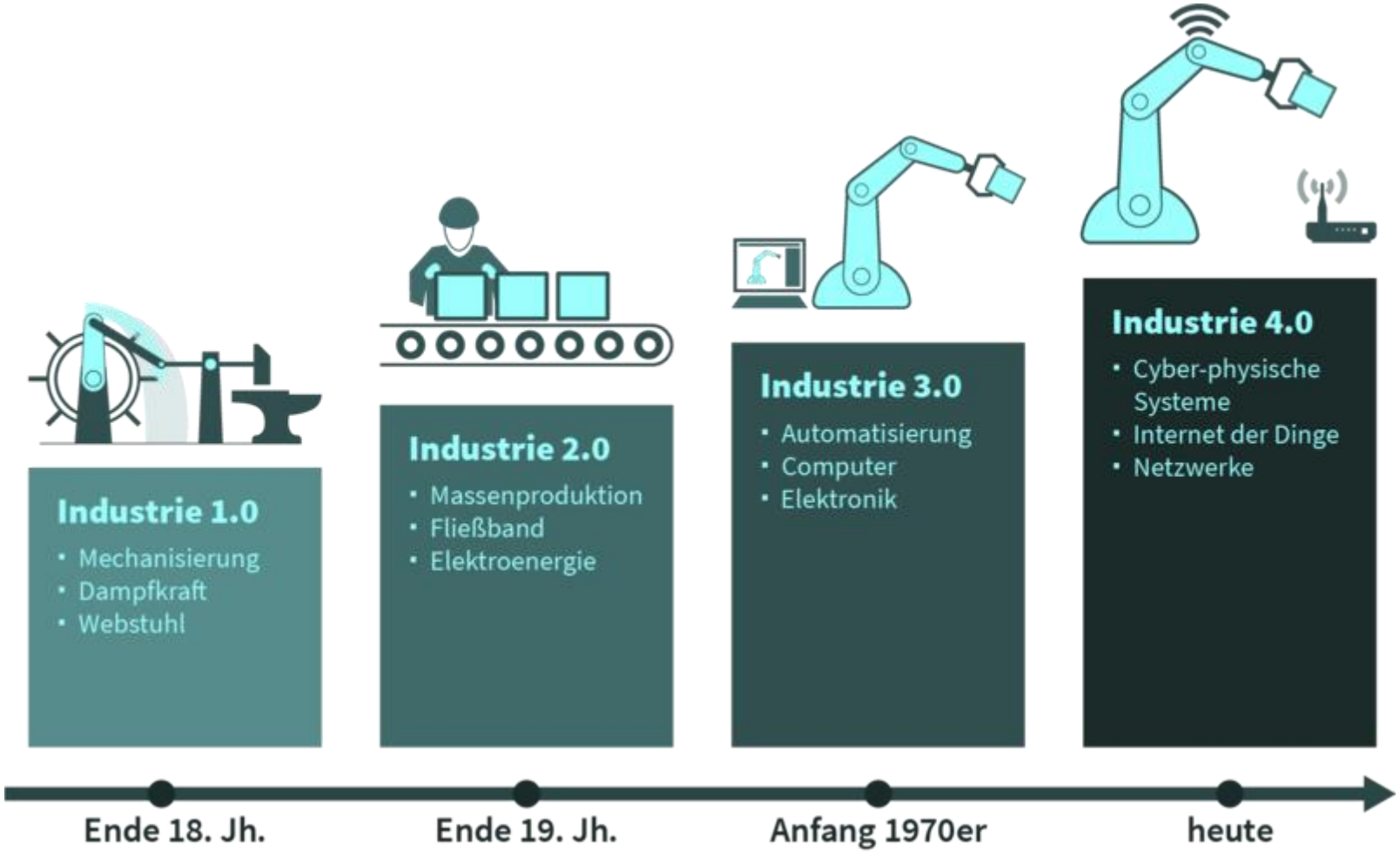
Demo



Kritische Infrastrukturen



Warum Cybersicherheit in der Industrie OT (Wasserwirtschaft)?



- Internet
- Firewall
- Virus
- Hacker
- Update
- VPN

rittmeyer BRUGG

Ooops, your files have been encrypted!

English

Payment will be raised on

5/15/2017 16:50:06

Time Left

02:23:34:22

Your files will be lost on

5/19/2017 16:50:06

Time Left

06:23:34:22

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Copy

About bitcoin

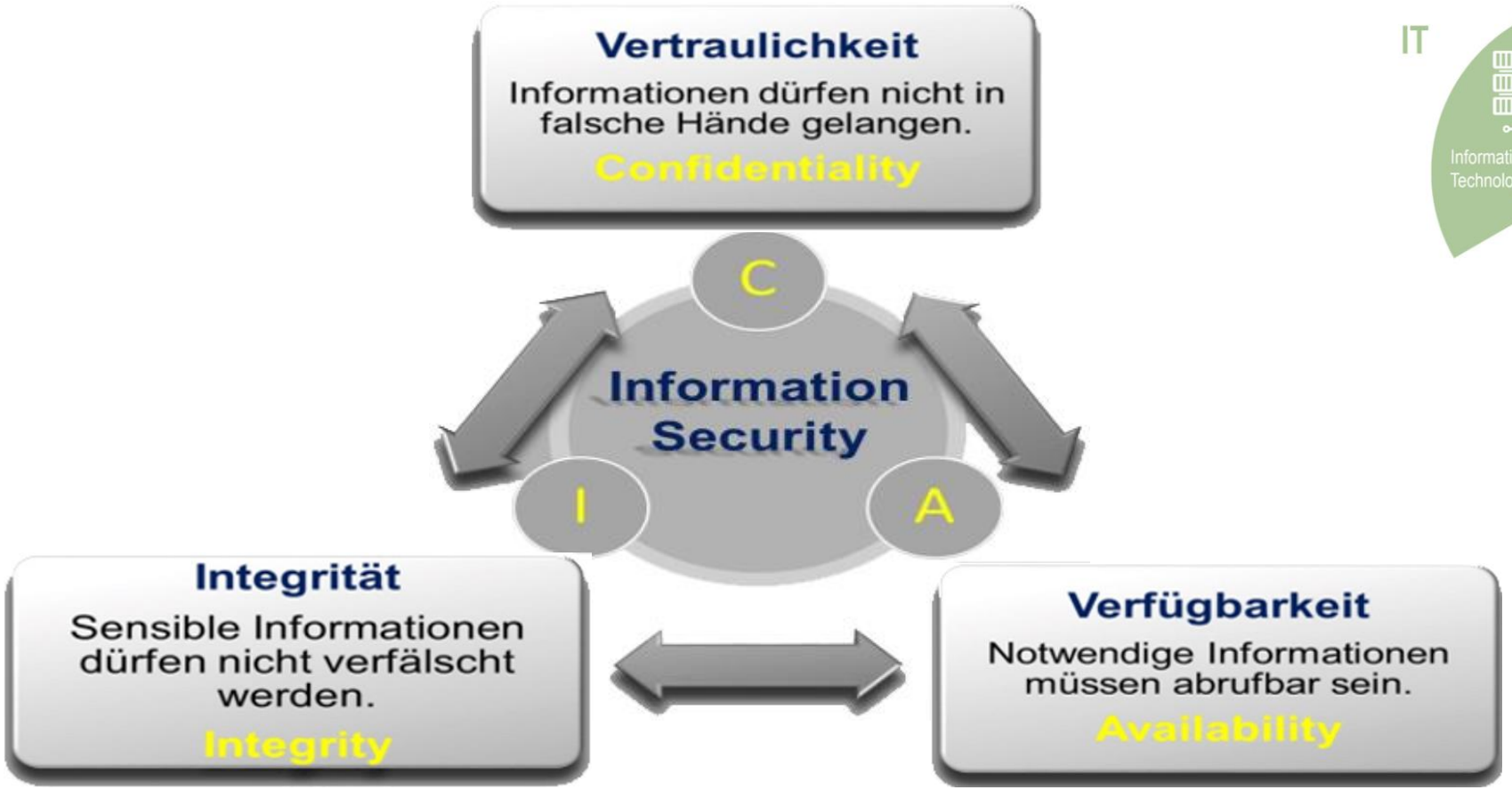
How to buy bitcoins?

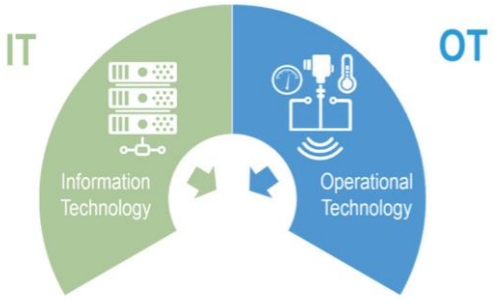
Contact Us

Check Payment

Decrypt

Definition von Informations-Sicherheit mit dem Unterschied zwischen **IT** (Information Technology) und **OT**(Operational Technology)





Definition von Informations-Sicherheit mit dem Unterschied zwischen **IT** (Information Technology) und **OT**(Operational Technology)

Vertraulichkeit
Informationen dürfen nicht in falsche Hände gelangen.
Confidentiality

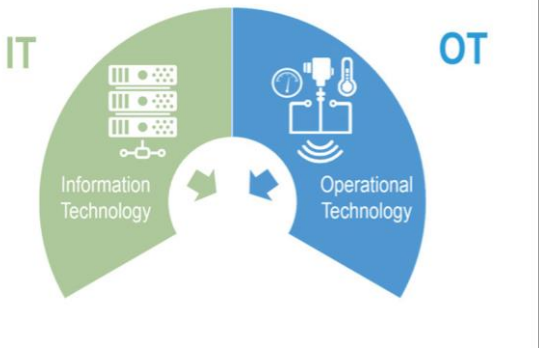
50%

Verfügbarkeit
Notwendige Informationen müssen abrufbar sein.
Availability

30%

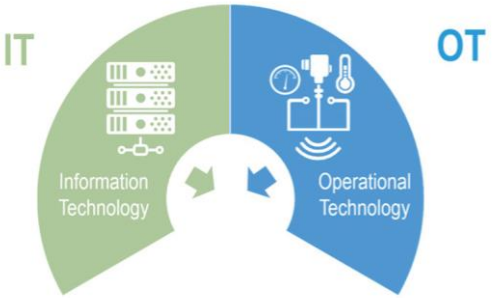
Integrität
Sensible Informationen dürfen nicht verfälscht werden.
Integrity

20%



rittmeyer BRUGG

Definition von Informations-Sicherheit mit dem Unterschied zwischen **IT** (Information Technology) und **OT**(Operational Technology)



Verfügbarkeit
Notwendige Informationen müssen abrufbar sein.
Availability

50%

Integrität
Sensible Informationen dürfen nicht verfälscht werden.
Integrity

30%

Vertraulichkeit
Informationen dürfen nicht in falsche Hände gelangen.
Confidentiality

20%

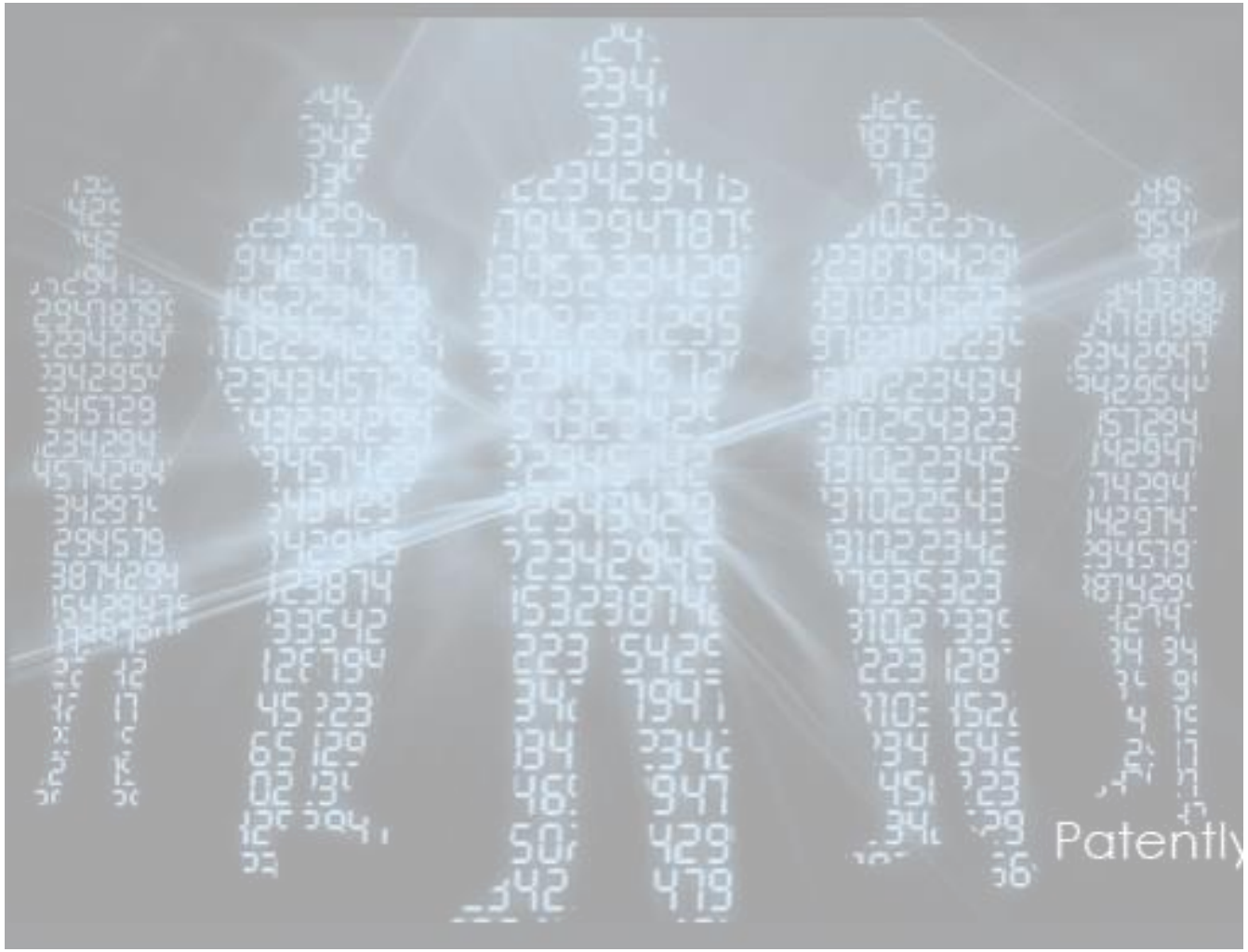
Bedrohung + Schwachstelle = Gefahr

- E-Mail
- USB-Speicher
- Internet
- Netzwerk
- Mitarbeiter

- Manipulation
- Diebstahl
- Erpressung
- Ausfall
- Zerstörung
- Verlust

An der Bedrohung können wir nichts ändern - Schwachstellen können jedoch vermieden werden

Bedrohung



Bedrohung Angreifer-Typologie

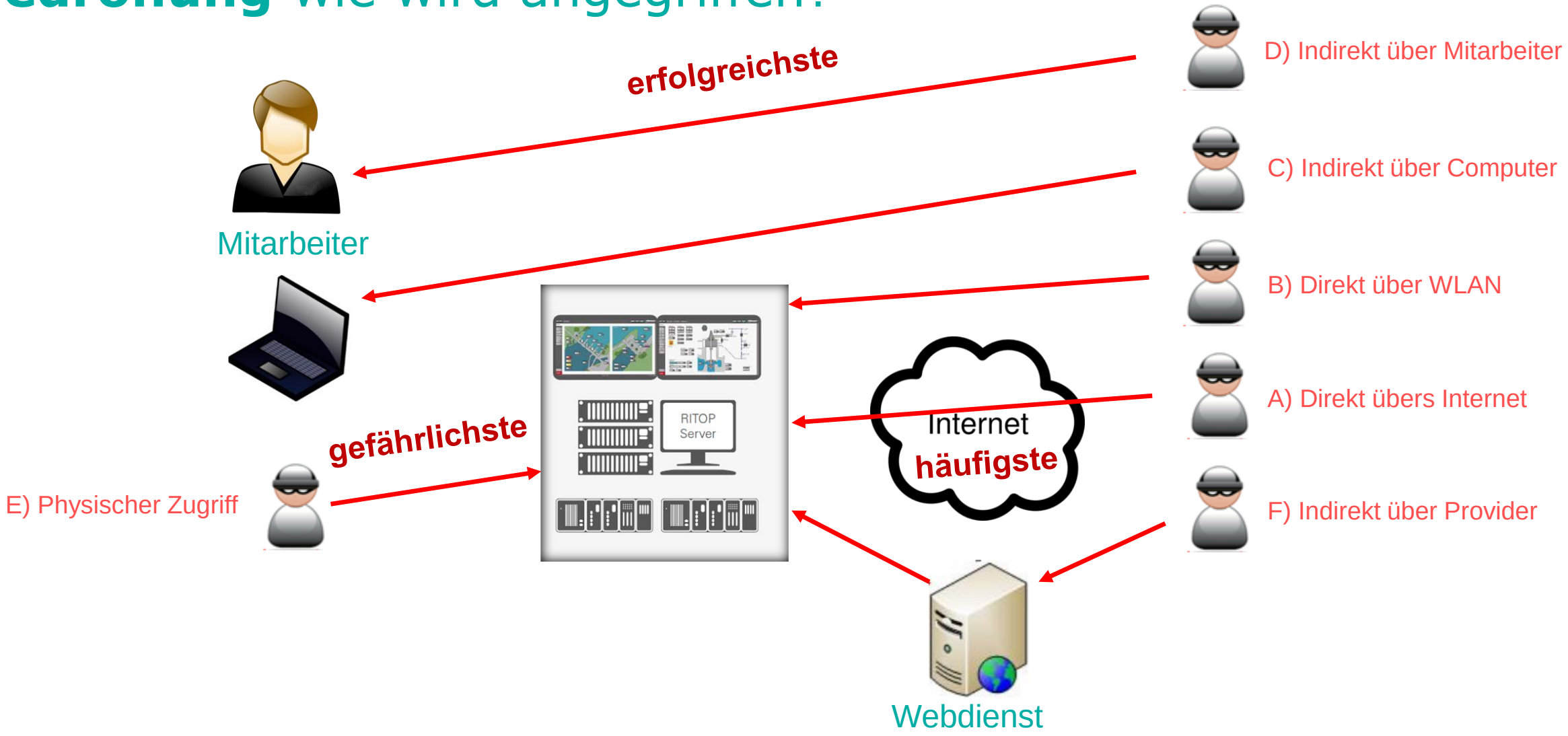
- Cyber-Kriminelle
  versuchen mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen

- Nachrichtendienste
  Spionage und Wirtschaftsspionage

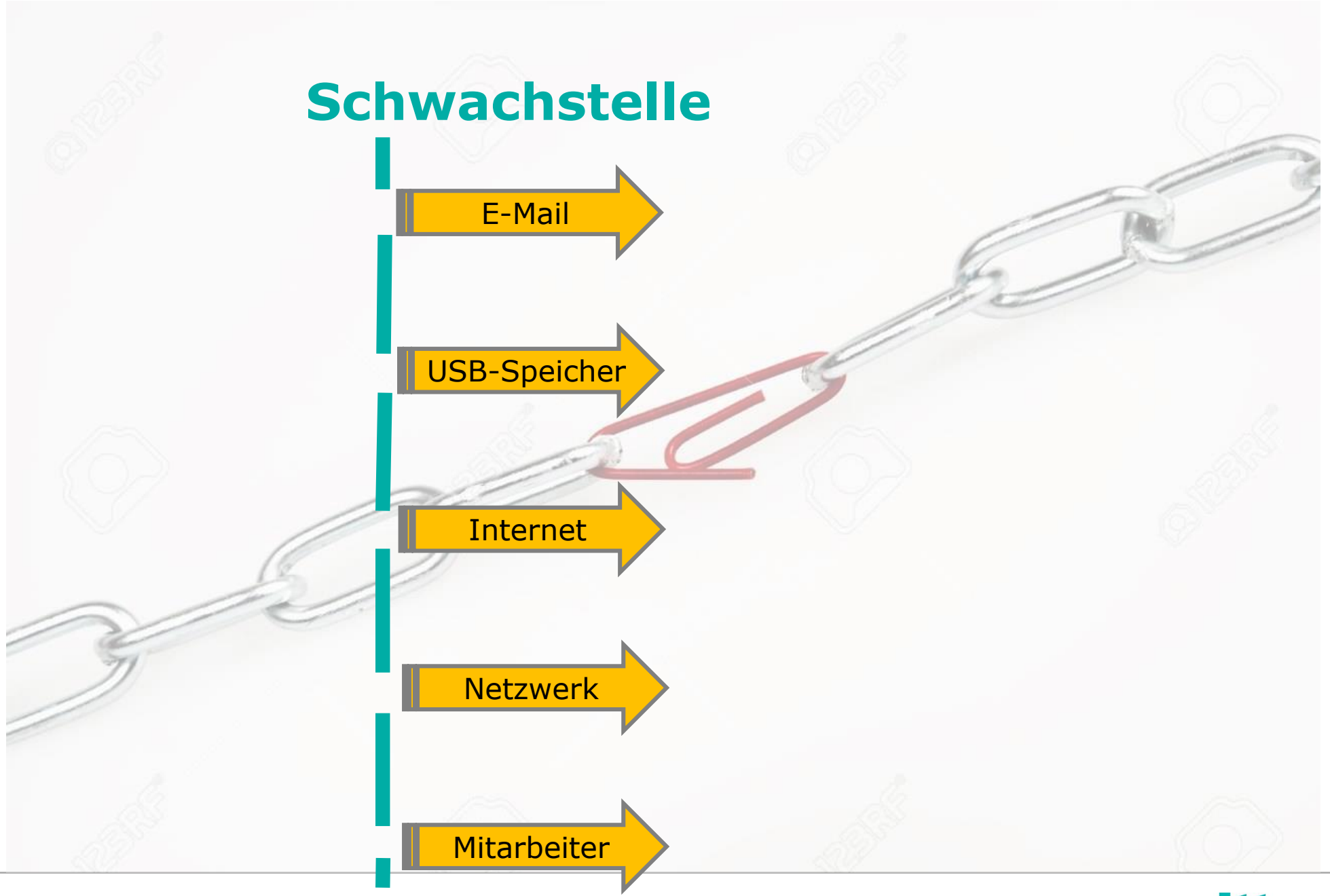
- Hacktivismus und Cyber-Aktivisten
  nutzen Computersysteme und Netzwerke vorgeblich als Protestmittel, um politische oder ideologische Ziele zu erreichen

- Innentäter
  Tätergruppe, die für Angriffe auf firmeninterne oder vertrauliche Informationen sowie Sabotage in Frage kommt

Bedrohung wie wird angegriffen?

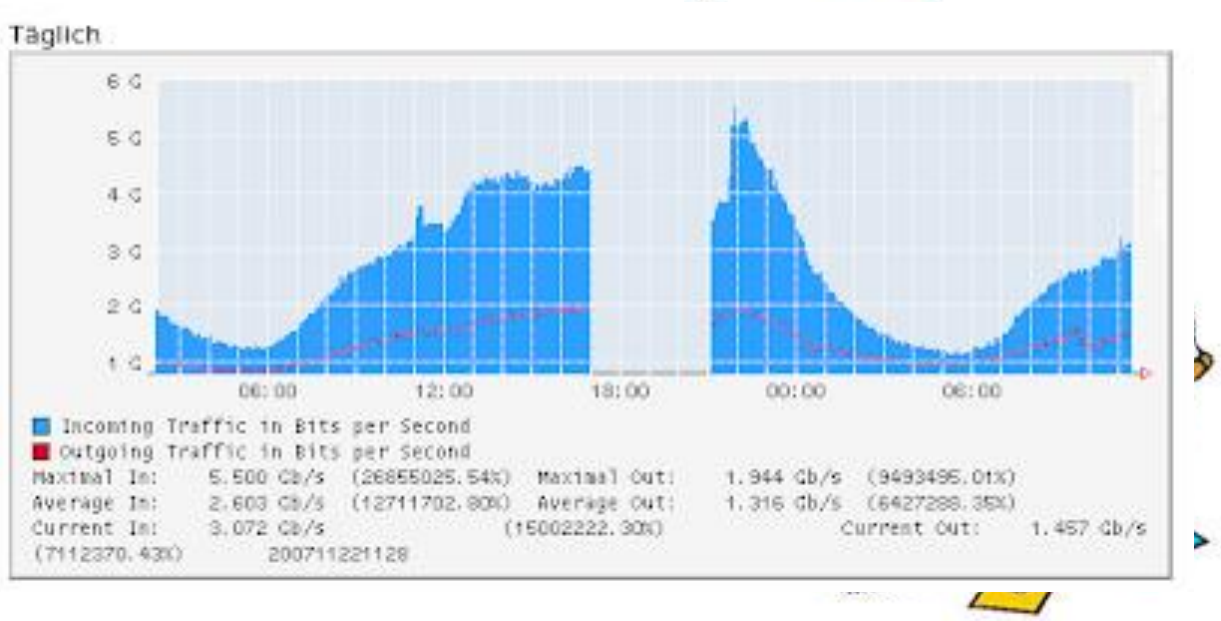


Schwachstelle



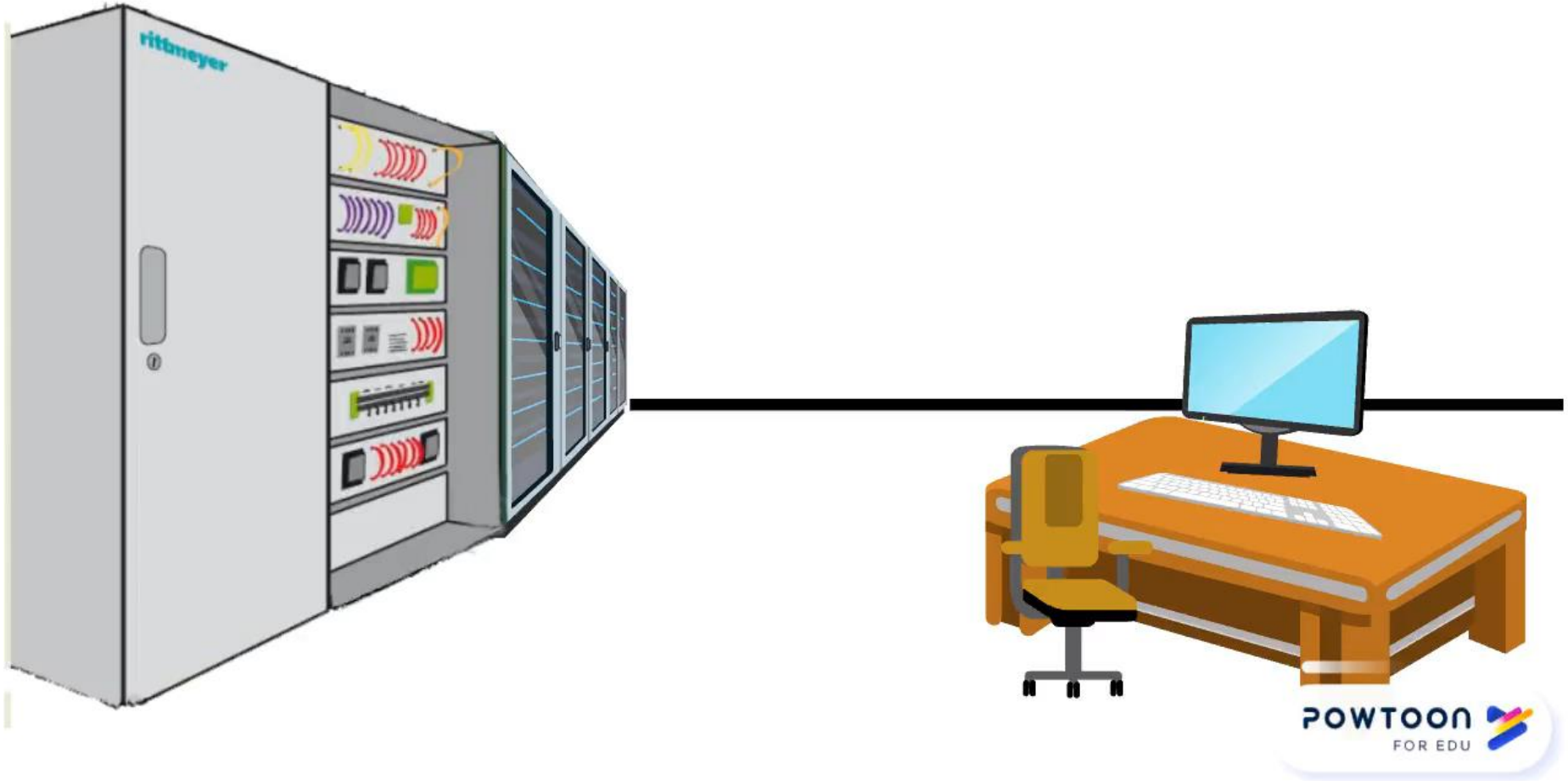
rittmeyer BRUGG

Schwachstelle physischer Zugriff - Netzwerkausfall



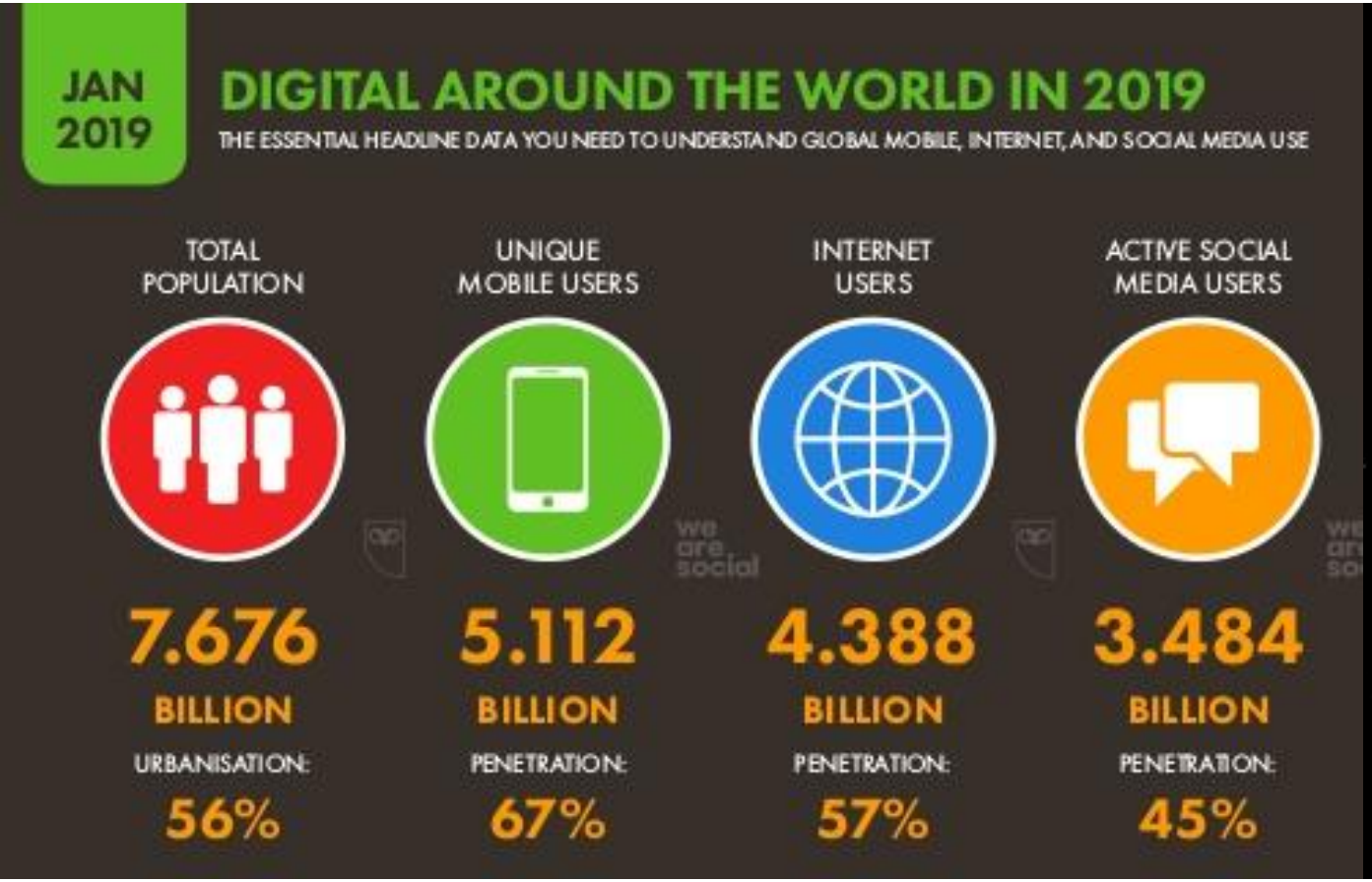
- überall Zugang
- unverdächtig
- unterbezahlt ☺

Schwachstelle physischer Zugriff



rittmeyer BRUGG

Schwachstelle Internet



z.B. der Gesamterlös durch die Nordkorea Hacker-Raubzüge wird auf bis zu zwei Milliarden Dollar geschätzt

rittmeyer BRUGG

Schwachstelle Internet

Blick News Sport Meinung Politik Wirtschaft People Leben Digital

Urheber in London und Korea

Hacker-Attacke auf Wasserversorgung in Ebikon LU

10:55 Uhr 19.12.2018 11:32 Uhr 19.12.2018

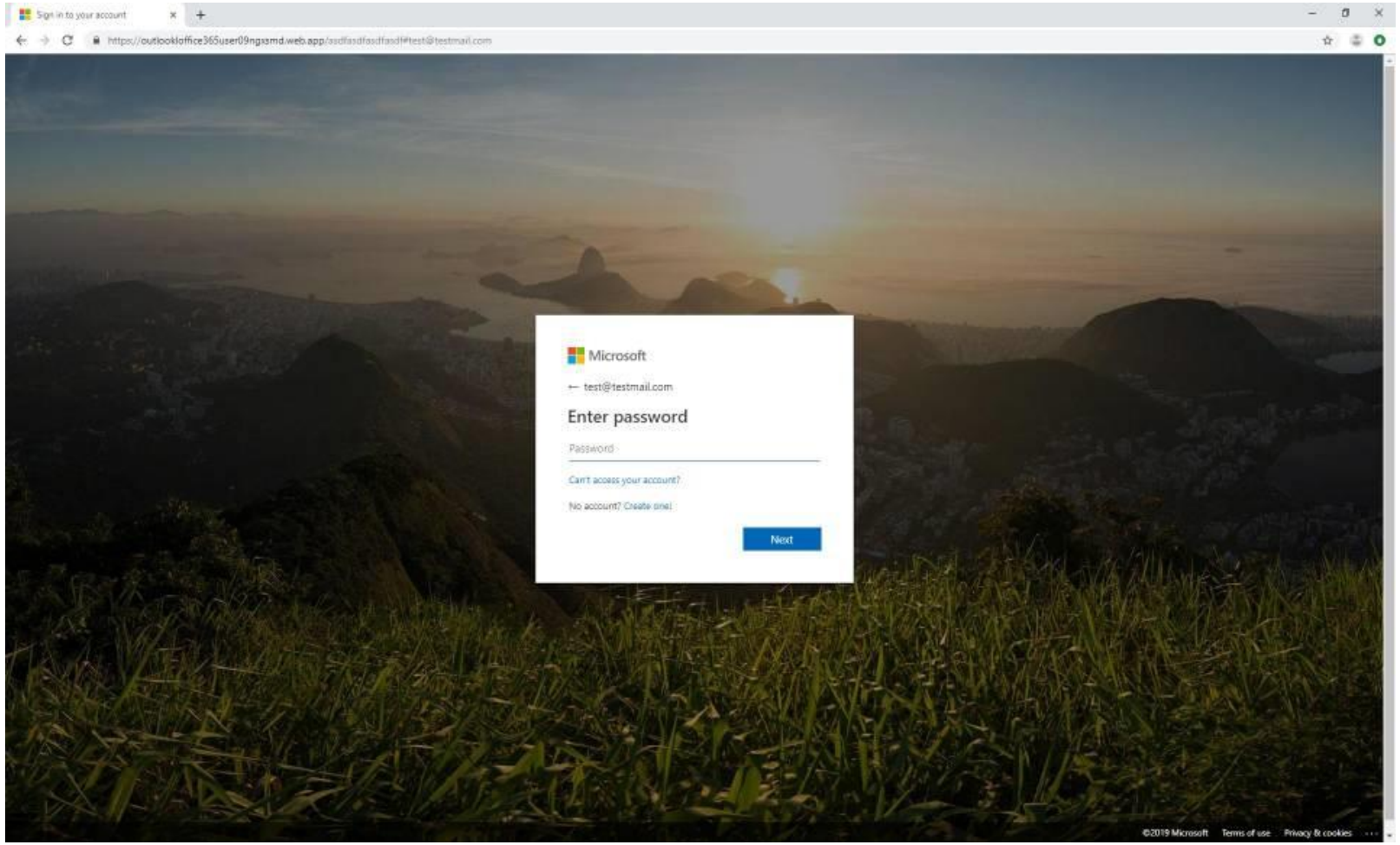
Die autonome Betriebssteuerung der Wasserversorgung der Gemeinde Ebikon LU hat im November Tausende bösartige Software-Anfragen bekommen.

SonicWALL UTM-Attacks detection

LogTime	Source Address	Source Port	Destination Address	Destination Port	Protocol	Attack Type
04/27/2016 05:58:41 PM	10.0.105.109	57353	69.171.235.48	443	TCP	TCP Xmas Tree dropped
04/27/2016 05:58:41 PM	216.177.151.110	80	10.0.105.89	58912		IPS Detection Alert: WEB-CLIENT Obfuscated HTML Code 110
04/27/2016 05:58:41 PM	10.0.105.109	57353	69.171.235.48	443	TCP	Spank attack multicast packet dropped
04/27/2016 05:58:41 PM	10.0.105.109	57353	69.171.235.48	443	TCP	Smurf Amplification attack dropped
04/27/2016 05:58:41 PM	10.0.105.109	57353	69.171.235.48	443	TCP	Senna Spy attack dropped
04/27/2016 05:58:41 PM	10.0.105.109	57353	69.171.235.48	443	TCP	Ripper attack dropped
04/27/2016 05:58:41 PM	10.0.105.109	57353	69.171.235.48	443	TCP	Probable TCP NULL scan detected
04/27/2016 05:58:41 PM	10.0.105.109	57353	69.171.235.48	443	TCP	Probable TCP XMAS scan detected
04/27/2016 05:58:41 PM	23.33.186.48	80	[illegible]	61651		Gateway Anti-Virus Alert: MalAgent.H_177 (Trojan) blocked.
04/27/2016 05:58:41 PM	10.0.105.109	57353	69.171.235.48		TCP	TCP Syn/Fin packet dropped
04/27/2016 05:58:41 PM	10.8.7.20	54465	172.26.38.1	53		IP spoof dropped
04/27/2016 05:58:41 PM	10.0.105.205	137	10.6.215.177	137		IPS Detection Alert: INFO NetBIOS Name Request Probe
04/27/2016 05:58:41 PM	216.177.151.110	80	10.0.105.89	58912		IPS Detection Alert: WEB-CLIENT Obfuscated HTML Code 110

rittmeyer BRUGG

Schwachstelle Internet



Phishing-Methode

Cyberkriminelle präsentieren eine täuschend echte, wie die regulären Seiten zum Einloggen in Office 365 oder Outlook-Online aussehen.

Über die gefälschten Einwählseite sollen die Anwender dazu gebracht werden, zunächst ihren Benutzernamen und dann ihr Passwort anzugeben.

rittmeyer BRUGG

Schwachstelle E-Mail

iTunes Rechnung

Bestellnummer: MGFWF25VGX
Lfd. Nummer: 2-12674277
Bestellung gesamt: CHF 25.00
Rechnung an: Visa ....

Artikel	Interpret	Preis pro Stück
Skype : 25 Cr	Skype	CHF 25.00
	Bestellung gesamt:	CHF 25.00

Wenn sie nicht berechtigt diese Zahlung melden Sie dies bitte in den untenstehenden Link:

Abbrechen Zahlungs

Bitte bewahren Sie eine Kopie für Ihre Unterlagen auf.
Die Bedingungen und Konditionen, die an diese Bestellung geknüpft sind, finden Sie weiter unten.

iTunes S.à r.l.
Sie finden die Verkaufsbedingungen und Verkaufsrichtlinien, indem Sie Ihr iTunes-Programm starten und auf diesen Link klicken: Verkaufsbedingungen

Antworten auf häufige Fragen zum iTunes Store finden Sie hier:
http://www.apple.com/chde/support/itunes/musicstore/

Apple-ID – Übersicht • Einkaufsstatistik

Apple respektiert Ihre Privatsphäre.
Informationen zur Verwendung Ihrer persönlichen Daten erhalten Sie hier: https://www.apple.com/chde/legal/privacy/

Copyright © 2015 iTunes S.à r.l. Alle Rechte vorbehalten
31-33, rue Sainte Zithe, L-2763 Luxembourg. UID für die Schweiz CHE-115.419.207 MWST

In einigen Bezirken wurde das Leitungswasser mit Bakterien verseucht.

Deswegen raten wir Ihnen eindringlich, auf die Nutzung des Leitungswassers zeitweilig zu verzichten.
Die Liste der Staedte mit dem vergifteten Leitungswasser finden Sie im Anhang.
Wenn Ihre Stadt in dieser Liste steht, nehmen Sie sofort Kontakt zu uns auf.

Liste_01.12.2016_admin.ch.docx (204 KB)

Hallo Patrick,

gerne lade ich Sie herzlich zu unserem größten deutschen Event, dem MuleSoft Summit am 24. Oktober in Frankfurt ein.

Unser Summit bringt Executives, IT Manager und Architekten aus der gesamten DACH-Region zusammen, um Trends der digitalen Transformation zu besprechen und Erfahrungen auszutauschen. Die Agenda beinhaltet Kundenberichte, z.B. vom Head of API & Integration von Airbus und dem CIO von Unitymedia, sowie einen Einblick in MuleSofts Product Roadmap. Außerdem gibt es spezifische Breakouts für MuleSoft Anfänger und Fortgeschrittene.

Da wir nur eine beschränkte Anzahl Plätze auf der Gästeliste haben, würden wir uns über eine zeitnahe Zu- oder Absage freuen. Hier der Link zur Anmeldung.

Gerne stehe ich Ihnen auch jederzeit für weitere Terminkoordination und als Ansprechpartner bei MuleSoft zur Verfügung. Ich freue mich auf einen persönlichen Austausch mit Ihnen!

Beste Grüße
Patrick Günther
Feel free to book 15 or 30 minutes for a call via this link

MuleSoft **Patrick Günther,** API & Integration
T: +49 1573 5995422
Im Zollhafen 18, Kranhaus 1 / 3.Etage, 50678 Köln
We're hiring!

clone phishing

rittmeyer BRUGG

Schwachstelle Mensch – Social Engineering - USB

rittmeyer
BRUGG

Schwachstelle Mensch – Social Engineering - USB

Dieses **USB-Lightning-Kabel** funktioniert normal und ein angeschlossenes iPhone wird auch aufgeladen.

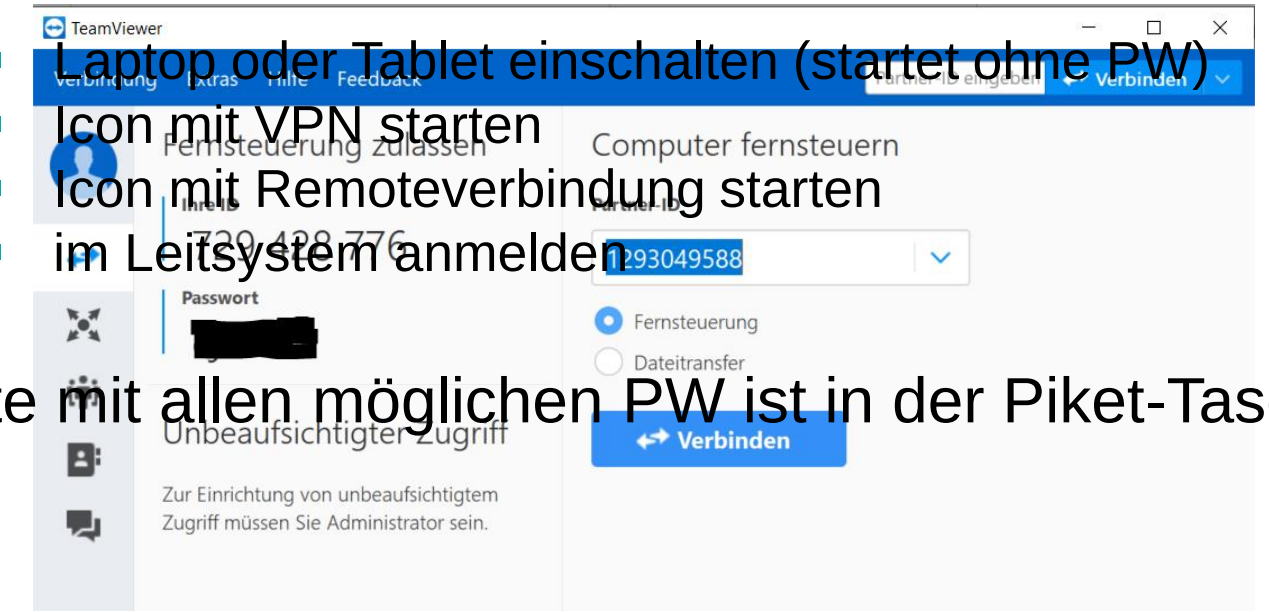
Zugleich enthält es aber eine **Mini-Platine** mit **WLAN-Chip,** über die es sich beim Einstecken am Computer als Eingabegerät ausgibt.

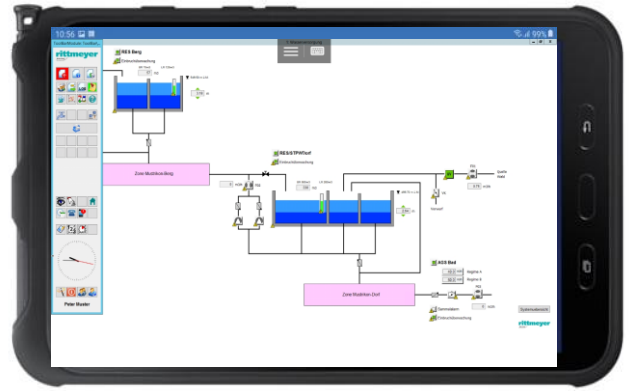
rittmeyer BRUGG

Schwachstelle Mensch & Computer - Fernwartungszugang

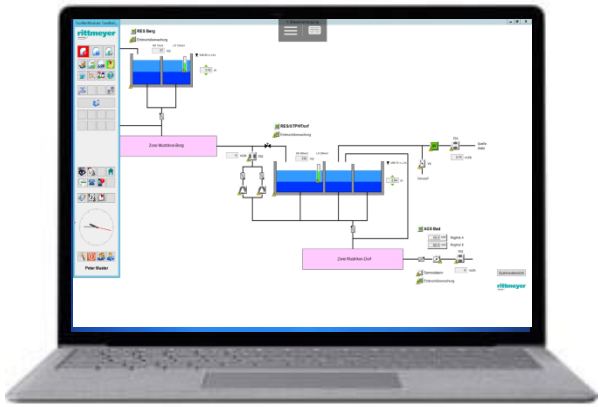
Sonntag Morgen 03:15 Uhr Alarm an Piket-Dienst

- Laptop oder Tablet einschalten (startet ohne PW)
- Icon mit VPN starten
- Icon mit Remoteverbindung starten
- im Leitsystem anmelden



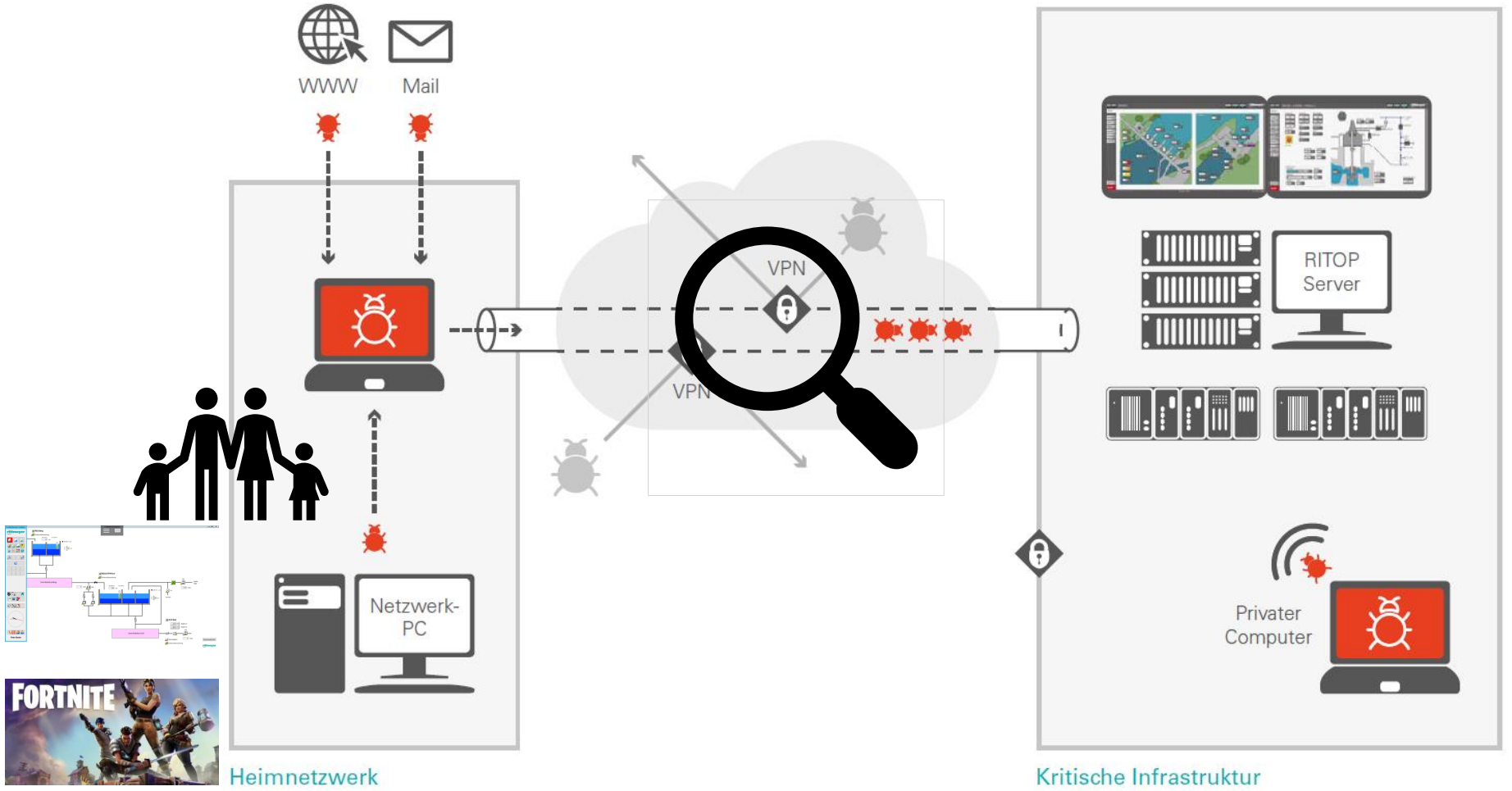


Die Liste mit allen möglichen PW ist in der Piket-Tasche...



Smartphone oder Tablet haben in der Regel kein oder ein vierstelliges Passwort ;-)

Schwachstelle Mensch & Computer - Fernwartungszugang




PRIVAT

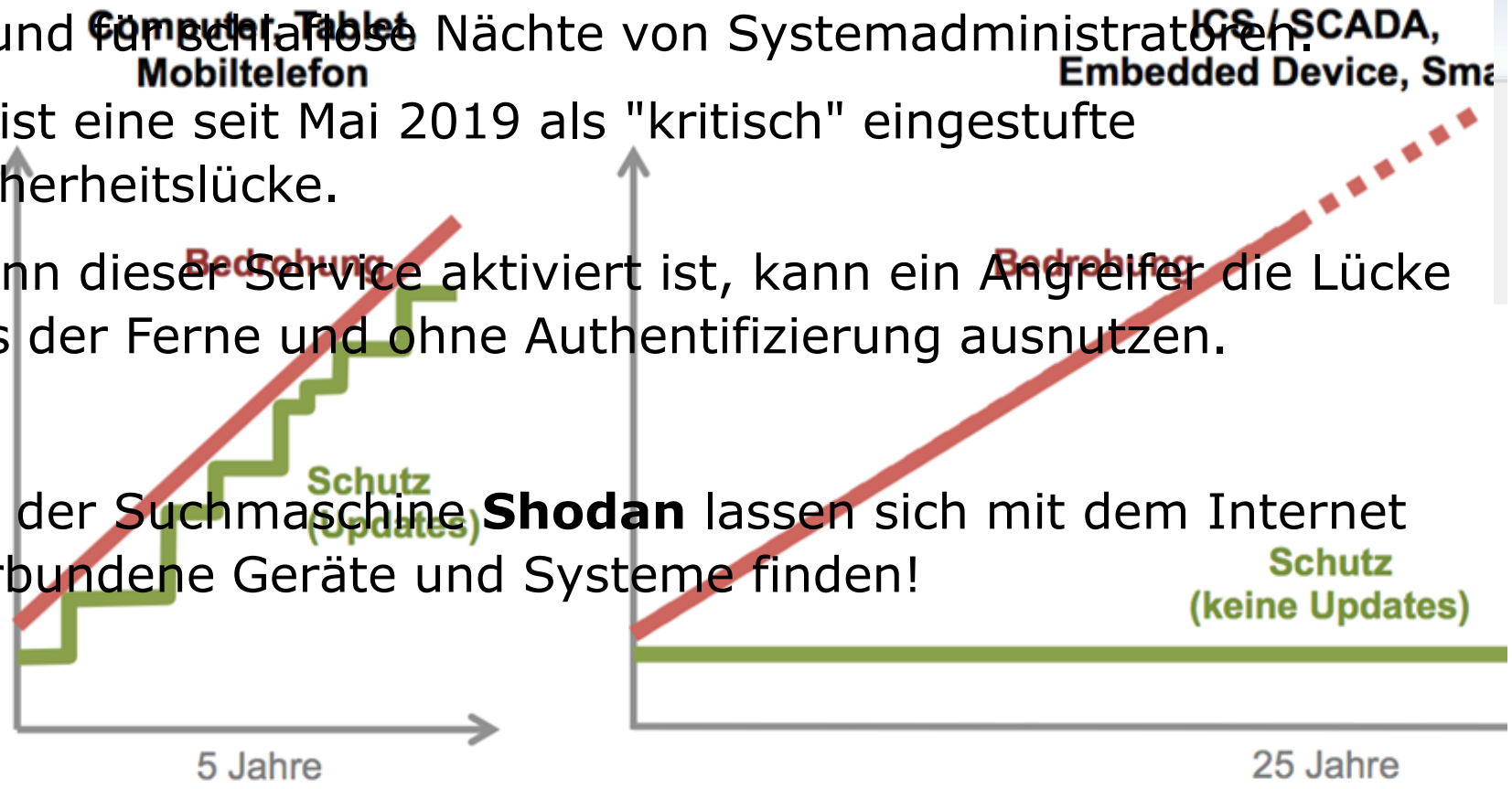
Schwachstelle Software (Update)

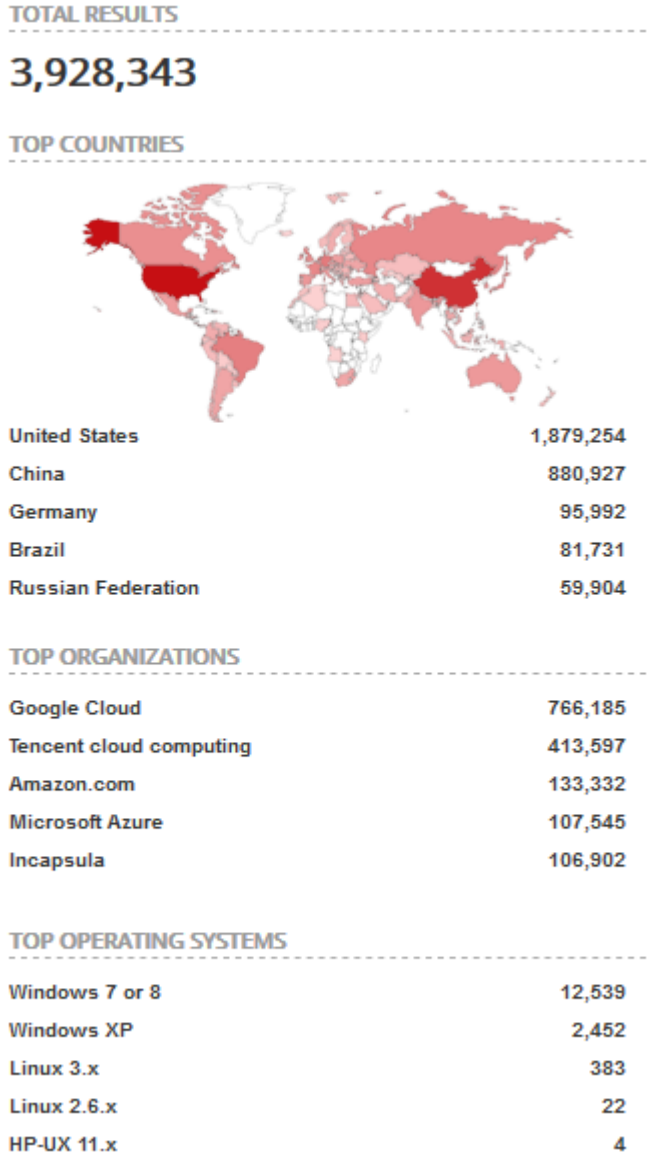
Das Remote Desktop Protocol (RDP) ist nach wie vor ein valider Grund für schlaflose Nächte von Systemadministratoren.

Es ist eine seit Mai 2019 als "kritisch" eingestufte Sicherheitslücke.

Wenn dieser Service aktiviert ist, kann ein Angreifer die Lücke aus der Ferne und ohne Authentifizierung ausnutzen.

Mit der Suchmaschine **Shodan** lassen sich mit dem Internet verbundene Geräte und Systeme finden!





Windows Server 2008/R2 / Windows 7 ab Januar 2020

rittmeyer BRUGG

Schwachstelle Passwörter

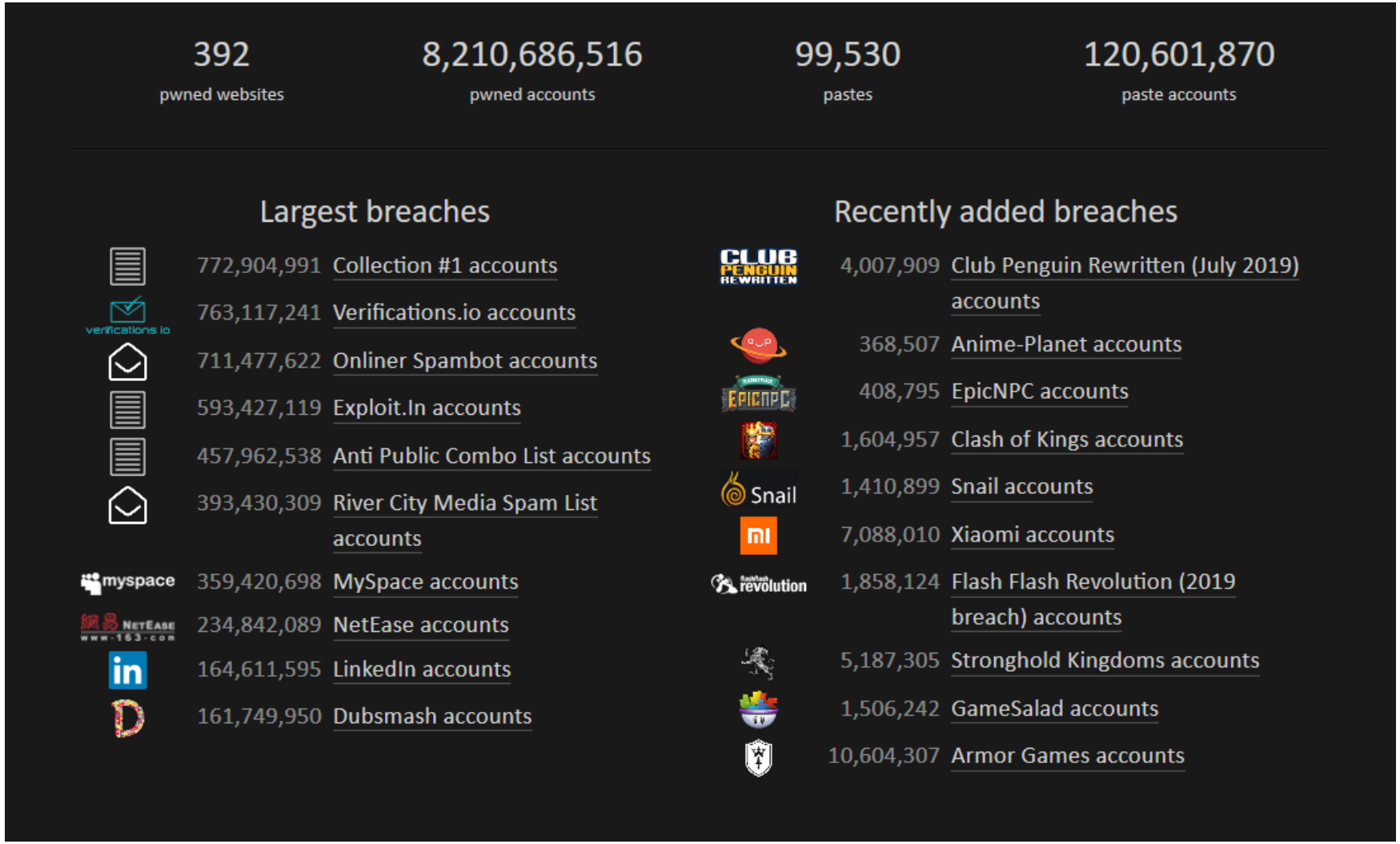
152’445’165

37’217’682

68’648’009

1’296’959

164’611’595



419’584’335

4’609’615

7’088’010

161’749’950

112’005’531

https://haveibeenpwned.com/
https://haveibeenpwned.com/Passwords

Gefahr

- Manipulation
- Diebstahl
- Erpressung
- Ausfall
- Zerstörung
- Verlust

rittmeyer BRUGG

Gefahr - Auswirkung bei einem Ausfall der Leitstelle

- manuelle Steuerung
- regelmässiger Besuch der Aussenwerke, um die Werte abzulesen
- keine Alarmierung
- Pikett muss vor Ort
- keine Abrechnung

Eine Wiederherstellung kann **Wochen dauern**!

Habe ich dafür genügend Ressourcen?

rittmeyer BRUGG

Gefahr - Auswirkung bei einem erfolgreichen Angriff

- instabile Systeme
- instabile Kommunikation
- Mitlesen von Daten / Informationen
- Systeme blockieren
- Systeme Ausfall / Zerstören
- Daten verschlüsseln / Erpressung
- Diebstahl Hardware

Datenmanipulation

- Sensoren (Überlauf)
- Sensoren (Durchfluss)
- Aufzeichnungen
- Abrechnungen

Fernsteuerung

- Software
- Hardware

Wie müssen wir uns schützen?

Technik

kaufen
konfigurieren

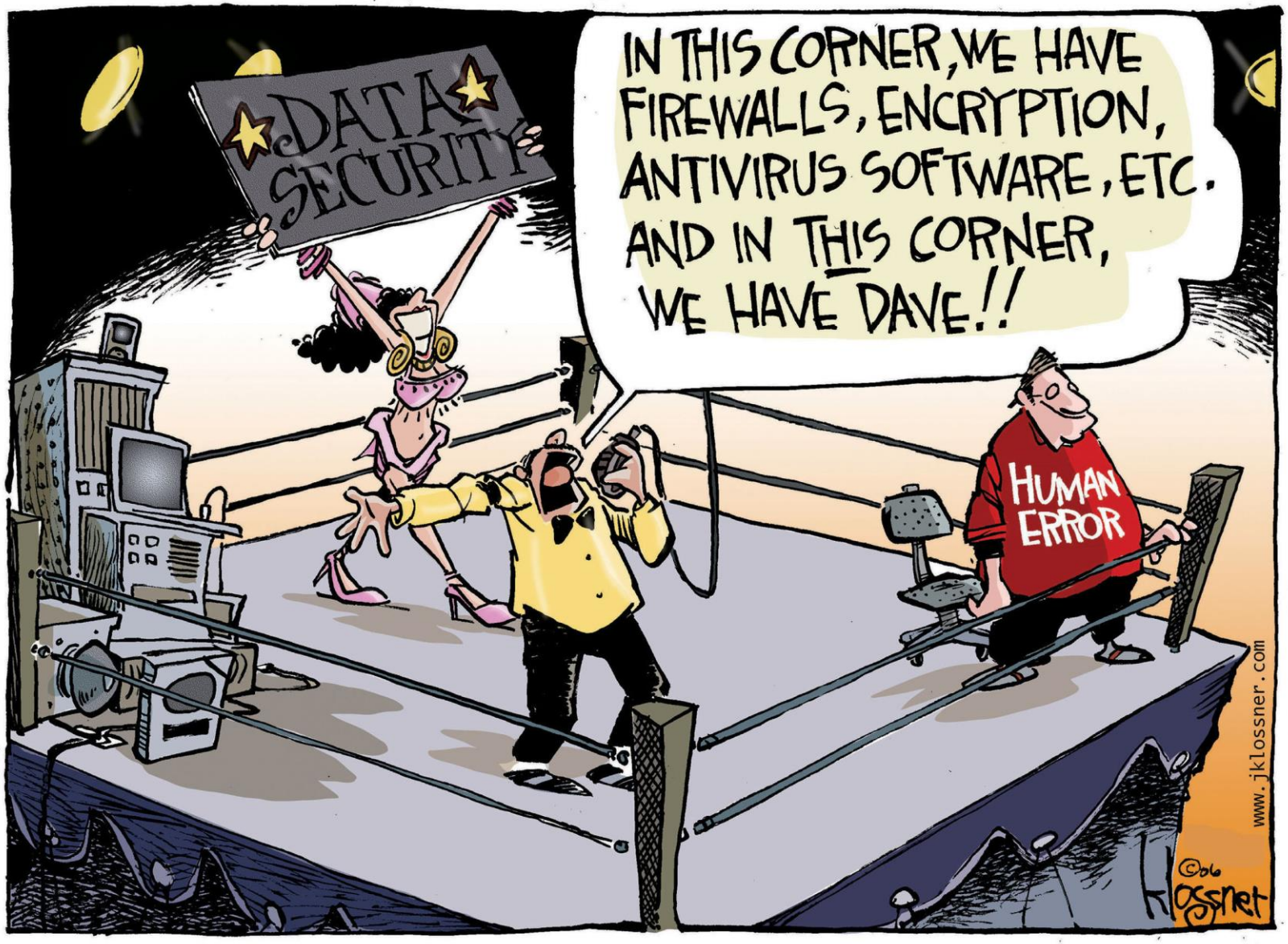
Prozesse

definieren
kontrollieren

Mitarbeitende

sensibilisieren
ausbilden

*Sicherheit besteht aus **75% Mensch** (Organisatorisch) und nur **25% Technologie***



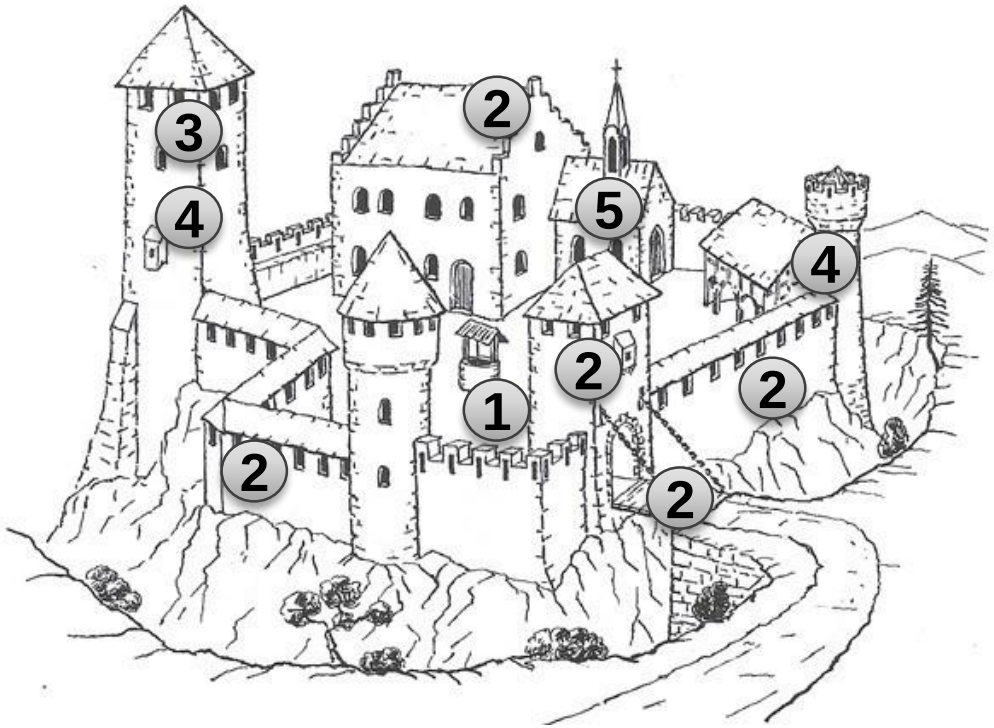
Das grösste Risiko sitzt vor dem Rechner, sagen Sicherheitsexperten in einer Umfrage

rittmeyer BRUGG

Schutzmassnahmen = Hindernisse einbauen

- **Identifizieren** (Identify)
  - Bestandsverwaltung der Anlage-Betriebsmittel
  - Schwachstellen-Analyse
- **Verhindern / Schützen** (Protect)
  - Physischer Schutz
  - Objekte verbessert schützen
    (Firewall – Passwörter – Antivirus)
  - Benutzer aufklären / schulen / sensibilisieren
  - Service Module / Unterhalt (Maintenance)
- **Überwachen / Erkennen** (Detect)
  - Überwachungssysteme
  - Feststellen von Schwachstellen
- **Alarmieren / Abwehren** (Respond)
  - Alarmsystem
  - Reagieren - Analysieren
- **Wiederherstellen** (Recovery)
  - Notfallplan / Abläufe bei Vorfällen (Backup)

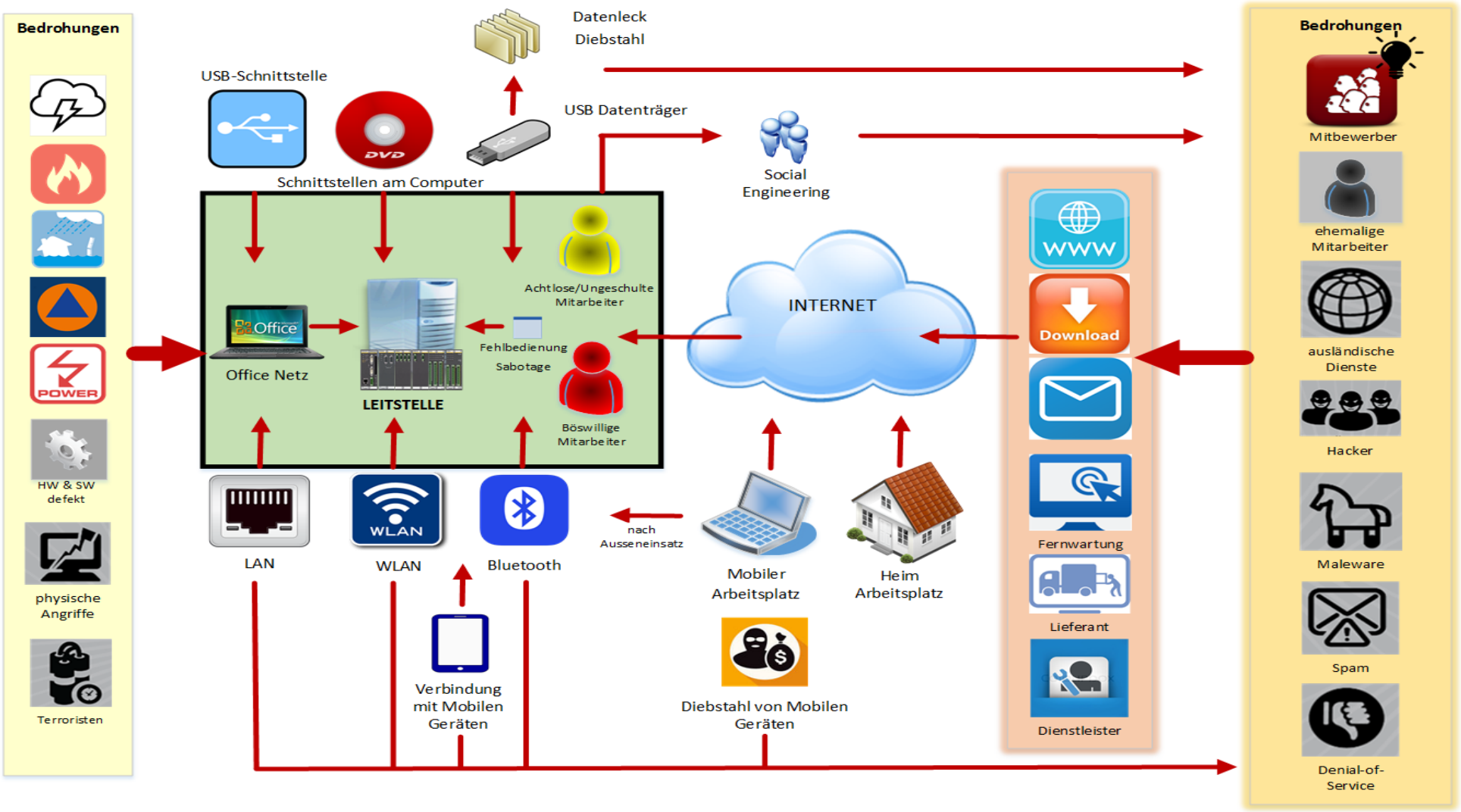
1
2
3
4
5



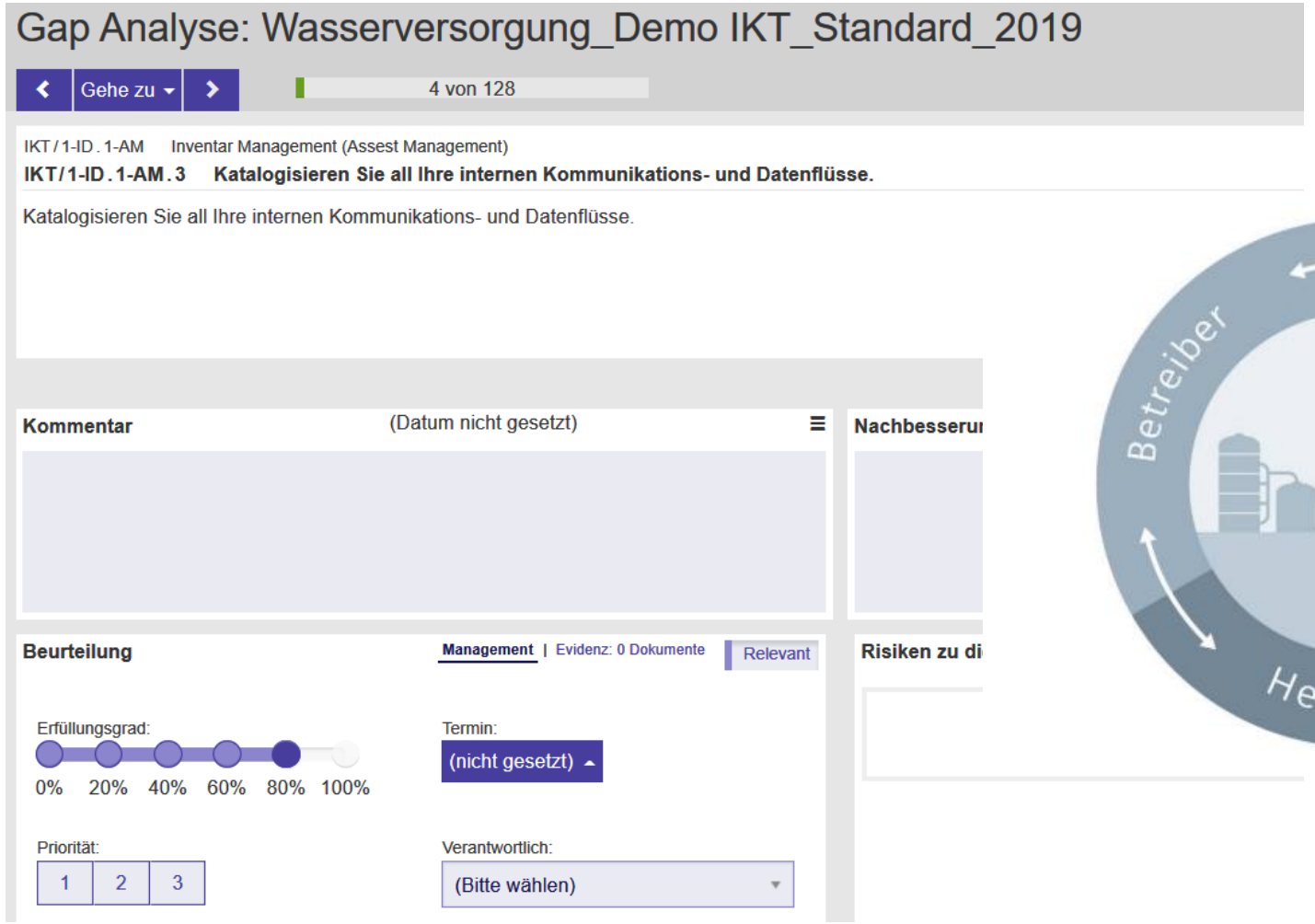
Burgarchitektur als Vorbild

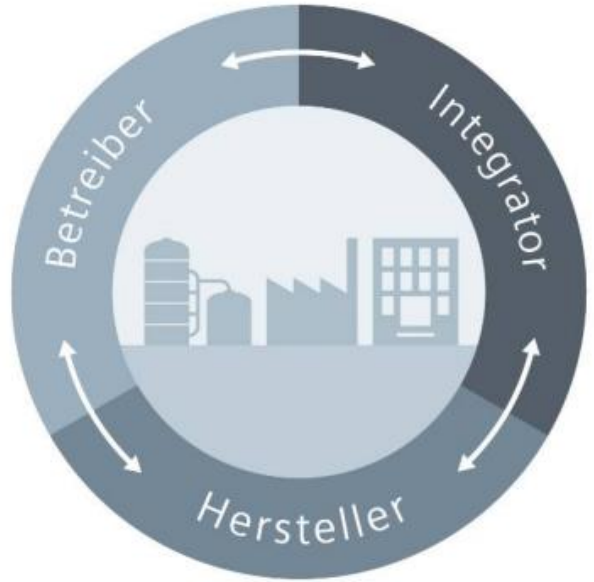
rittmeyer BRUGG

Identifizieren Schwachstellen-Analyse



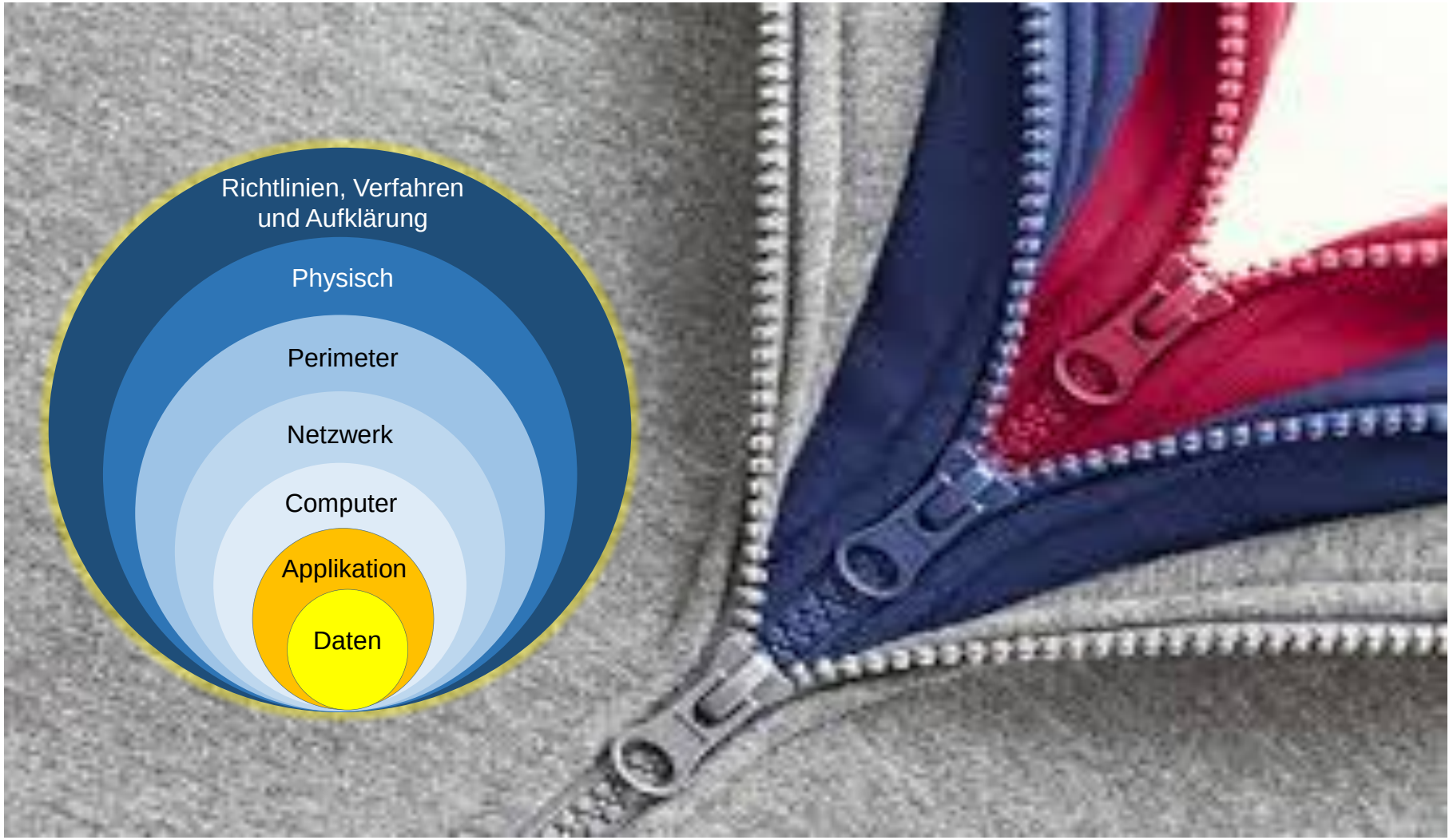
Identifizieren - festhalten im Management System



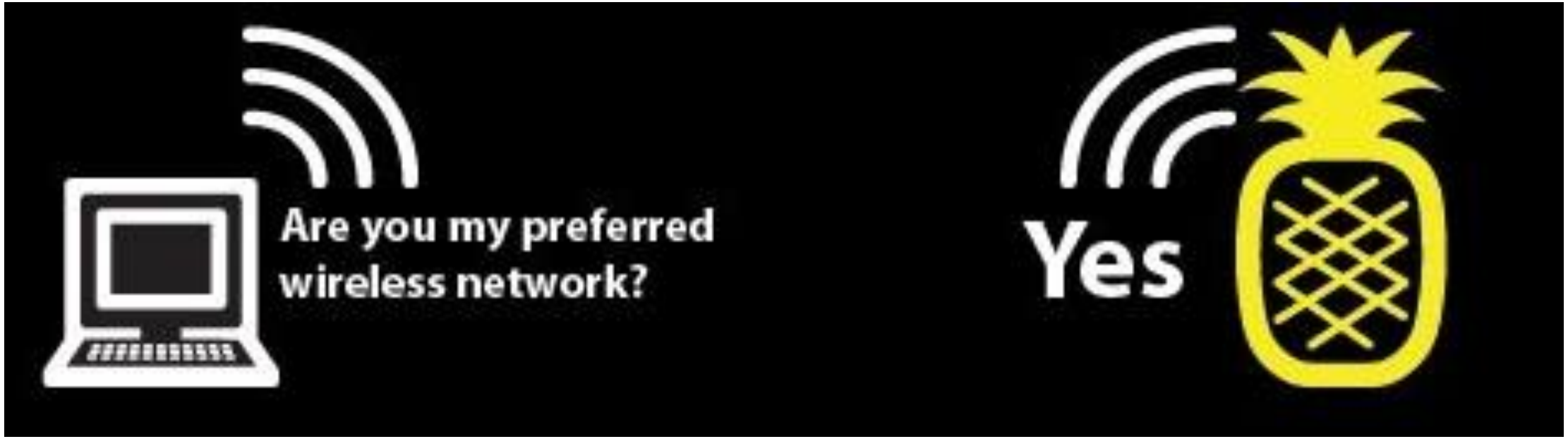


Eintragen der Massnahmen aus IKT (W1018) / ISO 27001 / BSI / IEC62443 Normen

Verhindern / Schützen mit defence in depth (Verteidigung in der Tiefe)



Demo



Tipps

- Vorsicht: Login-Seite eines unverschlüsselten Hotspots
- Auch ein Hotspot mit identischen Namen kann überlagert werden. z.B. ein WLAN-Zugang vom Restaurant → eigener Hotspot gebrauchen
- Vorsicht: bei benötigten zusätzlichen Login-Informationen
- automatische WLAN-Erkennung ausschalten, → kein automatisches Einloggen
- Keine unverschlüsselte E-Mail- oder Webseiten (HTTP) aufrufen
- Eine sichere VPN-Verbindung verwenden

Zusammenfassung

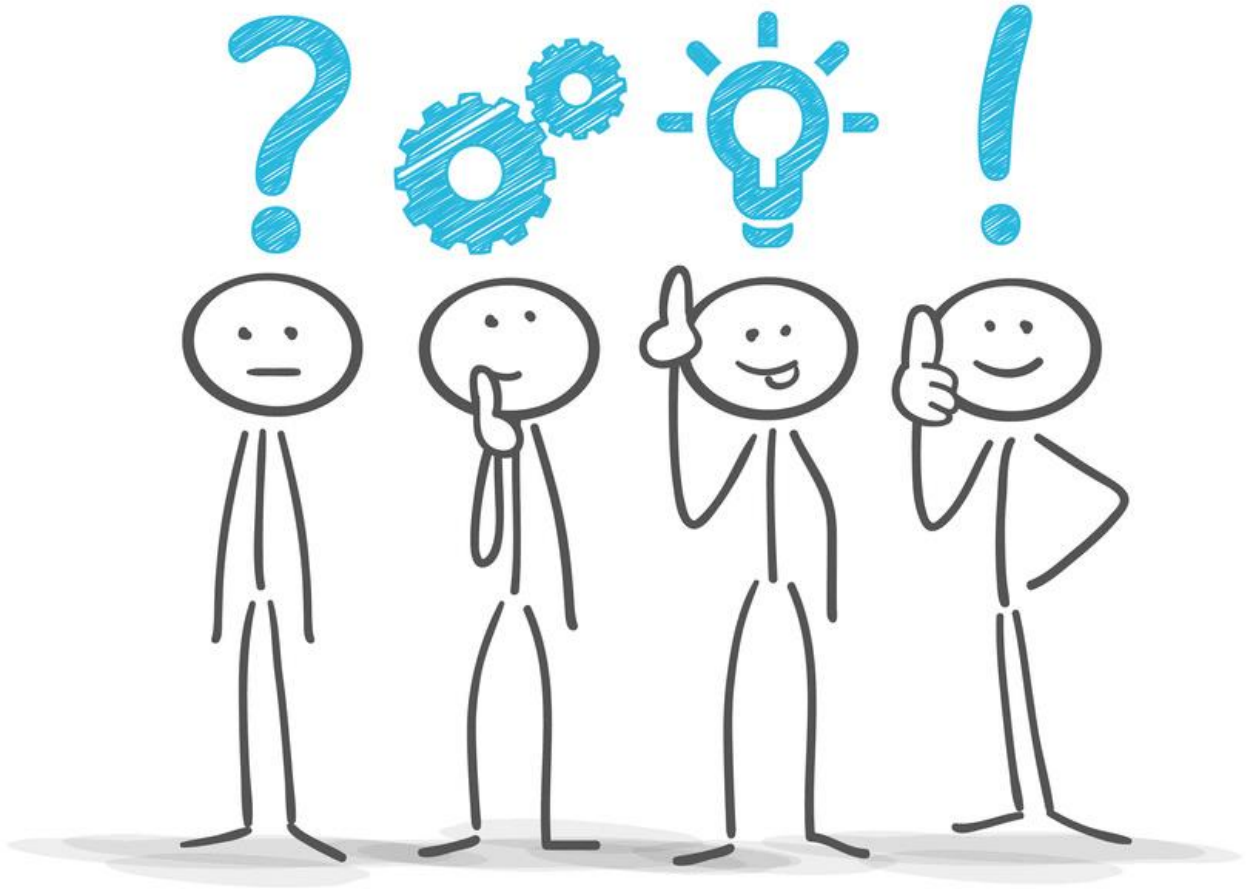
Ja - kritische Infrastrukturen werden angegriffen – ich kann mich jedoch schützen

Ich muss als Betreiber aktiv werden

- **Identifizieren**
- **Verhindern**
- **Überwachen / Erkennen**
- **Alarmieren / Abwehren**
- **Wiederherstellen**

Wir können Sie gerne dabei unterstützen!

Vielen Dank für Ihre Aufmerksamkeit



patrick.erni@rittmeyer.ch

Ein Unternehmen der Gruppe Brugg