



Cybersicherheit

Vorstellung Brunnenmeister-Fachtagung 2022

Patrick Erni

*Team Leader Service ICT
Cyber Security Expert*

8 Jahre Leiter IT-Services bei Rittmeyer

- Studium HSLU Information Security
- Studium HSLU Digital Business Innovation
- ISO 27001 Security Officer zertifiziert – TÜV
- Ausbildung CISSP

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 Engineer zertifiziert



Das Unternehmen Rittmeyer

Gründungsjahr: 1904

Unternehmensform: Aktiengesellschaft

Hauptsitz: Baar (Schweiz)

Anzahl der Mitarbeitenden: 300

Weltweit installierte Systeme: über 20'000

ISO/IEC 27001 Zertifiziert



Angriff auf kritische Infrastrukturen

Hacker manipulieren Wasser in Aufbereitungsanlage in Florida – was ist bislang bekannt?

9. Februar 2021



Behördlichen Berichten zufolge konnten nicht nur alle Computer der Mitarbeiter auf die Steuerung des Wasserwerks zugreifen, sie waren auch alle ohne jeglichen Schutz **direkt** ans Internet angeschlossen, teilten sich **ein Passwort** für den Fernzugriff (per **TeamViewer**) und liefen mit dem längst nicht mehr unterstützten Betriebssystem **Windows 7**.

Cyberattacke trifft irische Gesundheitsbehörde und Spitäler

SECURITY, ANGRIFFE, GESUNDHEIT, EU

Von Philipp Anz, 14. Mai 2021 16:40

Letzte Aktualisierung: 14. Mai 2021 19:20



Foto: Gov.ie

Die IT-Systeme wurden abgeschaltet, es ist die Rede vom "größten Cyberangriff auf den irischen Staat". Schuld sei die Ransomware "Conti".

Cyberangriff mit Ransomware: Große Pipeline in den USA weiterhin stillgelegt

Nach einem Cyberangriff fließt weiterhin kein Treibstoff durch eine der größten Pipelines in den USA. Inzwischen wachsen die Sorgen.

Lesezeit: 1 Min.  In Pocket speichern

   25



Ein Mann wollte das Trinkwasser einer ganzen Region verseuchen

Wyatt T.* (22) hatte per Fernzugriff Teile einer Trinkwasseranlage deaktiviert. Nun steht er dafür vor Gericht. Mit der Aktion habe er die Wasserversorgung gefährdet, heisst es in der Anklageschrift. Ihm drohen bis zu 25 Jahre Gefängnis.

Man sollte meinen, dass kritische Infrastrukturen, wie die Trinkwasserversorgung einer Stadt oder einer Region, gut geschützt sind. Dass dies nicht immer so ist, zeigt erneut ein Fall aus den USA. Der 22-jährige Wyatt T.* hat im **US-Bundesstaat Kansas** auf die Computersysteme einer Trinkwasseranlage zugegriffen.

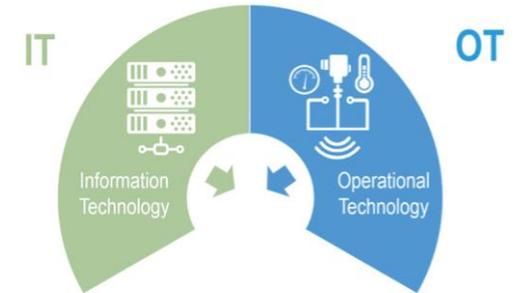
Er wird beschuldigt, das Wasserreinigungssystem der Region Ellsworth County **deaktiviert** zu haben. Dies mit der Absicht, es zu beschädigen, wie es in der Anklageschrift heisst. Der Vorfall geschah im März 2019. Publik wurde dies erst jetzt. Die Anlage versorgt rund 6000 Einwohnerinnen und Einwohner der Region mit Trinkwasser. Eine Gesundheitsgefahr bestand laut Behörden nicht. Die Wasserqualität werde permanent überwacht. Das, was T. gemacht hat, kann man aber nicht einmal als Hacking bezeichnen. Es war wohl eher eine **Fahrlässigkeit** auf Seiten der Anlagebetreiber. So war Wyatt T. ehemals beim betroffenen Post Rock Rural Water District in Ellsworth County angestellt. Auf dem Computer der Wasseranlage war eine **Fernzugriffs-Software** installiert. Er konnte sich wohl damit einloggen – und dies Monate, nachdem er den Job gewechselt hatte. Wie genau es zu dem Zugriff kam, ist jedoch nicht bekannt.

Für den 22-Jährigen könnte die Aktion weitreichende Folgen haben. Für die Manipulation eines öffentlichen Wasserversorgungssystems und das «rücksichtslose» Zerstören eines Systems könnte er zu einer Gefängnisstrafe von bis zu **25 Jahren**, sowie zu einer Geldstrafe von maximal **500'000 Dollar** verurteilt werden.

Erfolgreiche Hackerangriffe in der Schweiz

☠	Läderach	Schokoladenhersteller	September	2022
☠	Stadt Bülach	Verwaltung	Juli	2022
☠	H+	Spitalverband	Juni	2022
☠	Verkehrsbetriebe Luzern	Transport	Mai	2022
☠	Emil Frei AG	Autohändler	Januar	2022
☠	Papierfabrik Perlen	Produktion Papier	Januar	2022
☠	Treuhandbüro X	Steuererklärungen ZH/ZG/SZ	November	2021
☠	MediaMarkt/Saturn	Elektronikhändler	November	2021
☠	Bundesplattform Easygov	Corona-Kredit-Bezüge	Oktober	2021
☠	Gemeinde Montreux	Verwaltung	Oktober	2021
☠	Universität Lichtenstein	Ausbildung	September	2021
☠	Pallas Kliniken	Klinik	August	2021
☠	Neuenburger Kantonalbank	Bank	August	2021
☠	Saurer	Textilmaschinenbauern	August	2021
☠	Comparis	Vergleichsportal	Juli	2021
☠	Gemeinde Rolle (Waadtland)	Gemeindeverwaltung	Mai	2021
☠	Stadt & Kanton St. Gallen	Verwaltung	April/Juli/Oktober	2021

Definition von Informations-Sicherheit



Mythen, Missverständnisse und Fehleinschätzungen

Gerade KMU haben oft Schwierigkeiten, die Bedrohungslage realistisch einzuschätzen...

I.

„Wir sind doch viel zu klein und unbekannt, um Hacker anzulocken.“

Aber:

- Kleine Unternehmen stellen oftmals ein viel interessanteres Ziel dar
- Nicht-zielgerichtete Angriffe betreffen sämtliche Unternehmen

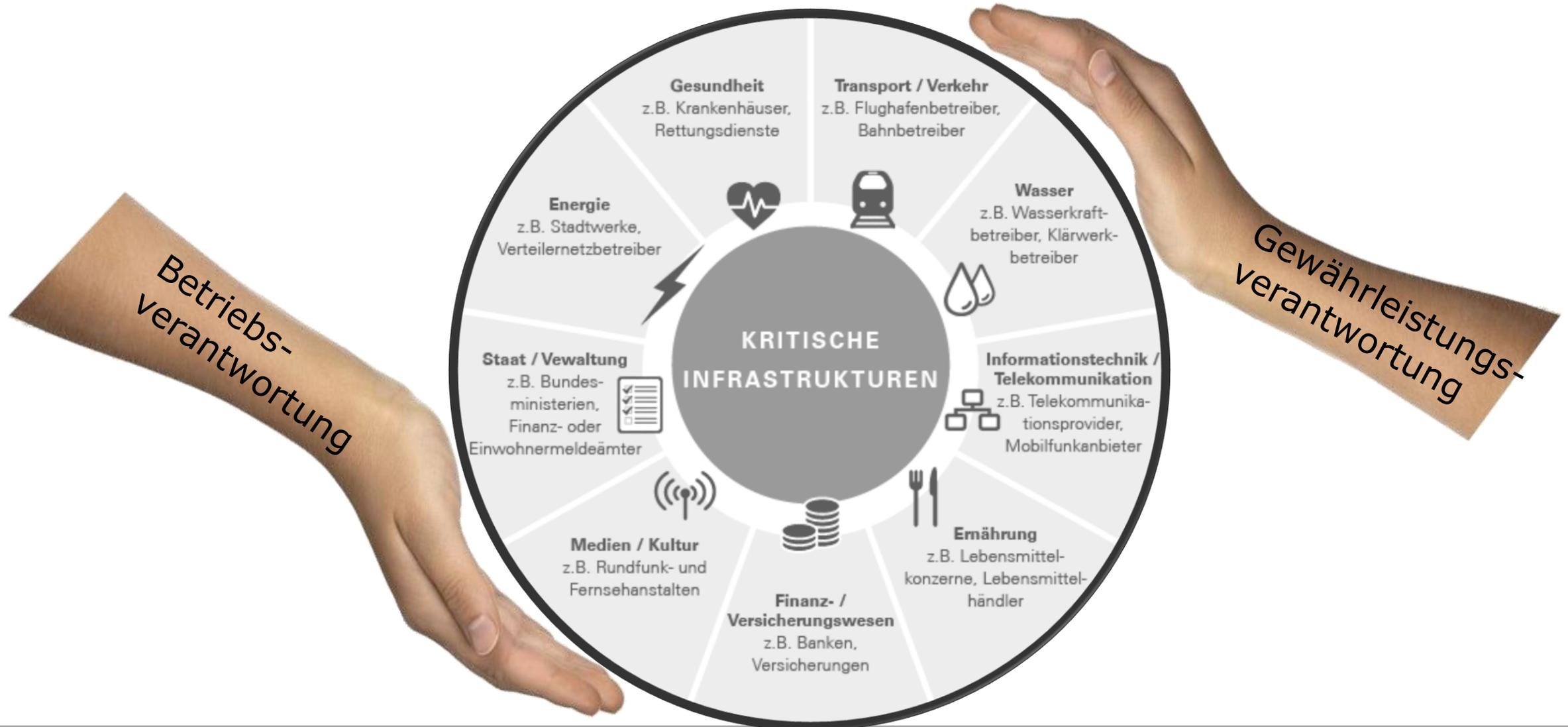
II.

„Wir sind eine verschworene Gemeinschaft, auf jeden unserer Mitarbeiter können wir uns voll verlassen.“

Aber:

- Bis zu 80%* aller Datenverlust-Vorfälle werden durch „Unachtsamkeit“ von Mitarbeitern zumindest begünstigt

Kritische Infrastrukturen



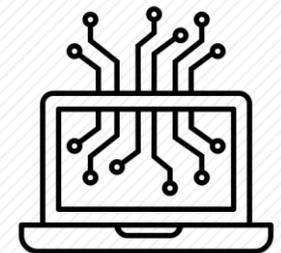
Ein Hacker-Angriff auf kritische Infrastruktursysteme hat das Potenzial Regionen oder ganze Länder ins Chaos zu stürzen

Grundlagen - Die fünf Dimensionen von Krieg

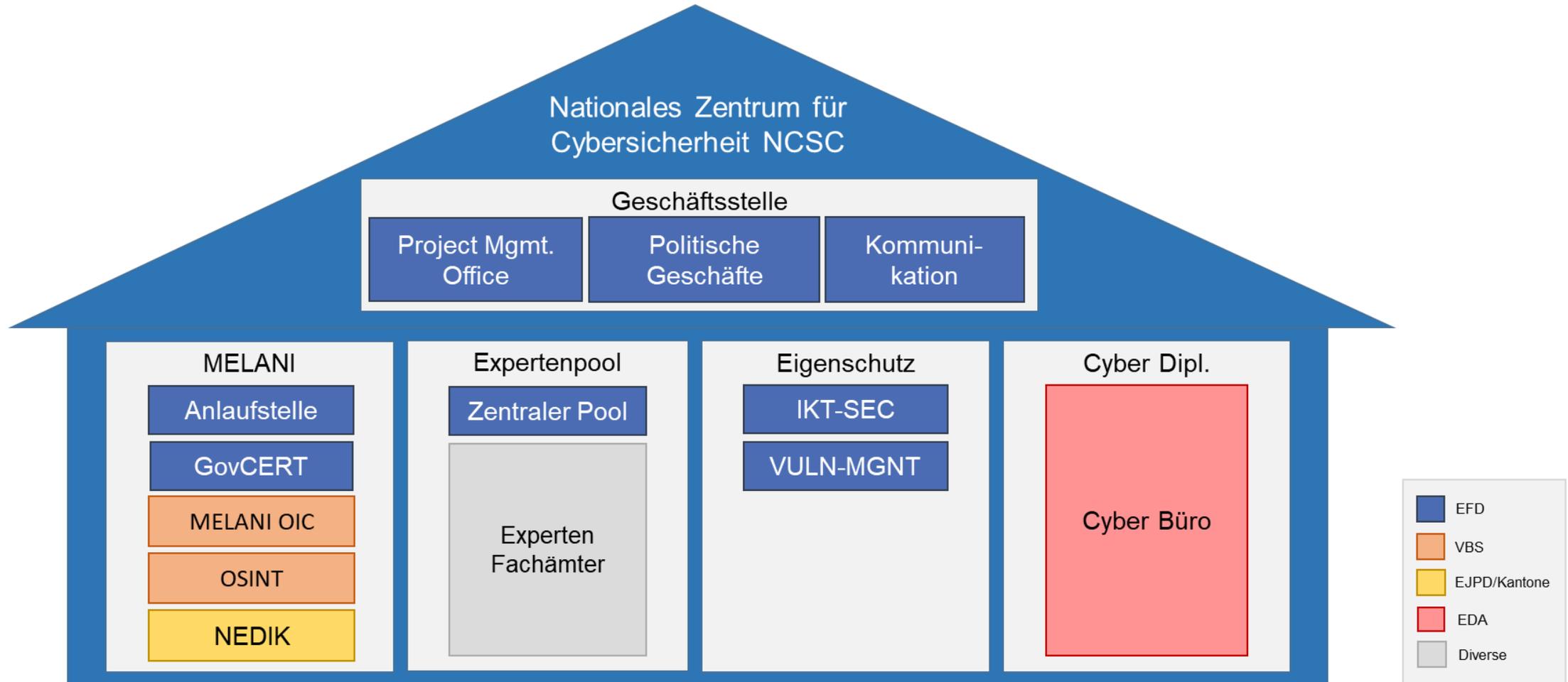
Land, Wasser, Luft und **Weltraum** sind die bekannten Dimensionen der Kriegführung.

Die fünfte Dimension **Cyberattacken** ist von grosser Wichtigkeit für die Sicherheit eines Landes. Die Gefahr besteht vor allem in möglichen Angriffen auf strategisch wichtige infrastrukturelle Knotenpunkte von Kritischen Infrastrukturen, wie die Energieversorgung.

Bei Cyberattacken stehen Ethik und Völkerrecht vor neuen Herausforderungen. Gibt es eine legitime, verhältnismässige, militärische Reaktion auf einen Cyberangriff? Wann ist die Schwelle zu einem bewaffneten Konflikt überschritten? Wie viel menschliches Leid kann ein Hacker-Angriff verursachen oder gar verhindern?



Nationales Zentrum für Cybersicherheit (NCSC) vormals MELANI



Grundlagen - Gesetze und Vorlagen Schweiz

Schweizerisches Datenschutzgesetz (DSG), welches den Schutz der Personendaten und der Persönlichkeitsrechte regelt. Das Gesetz geht auf **1992** zurück und befindet sich seit **2015** in Revision. Im September **2020** hat das Parlament das totalrevidierte Gesetz angenommen und die Einführung wurde auf **Juli 2022** geplant. Das neueste Umsetzungsdatum wurde auf den **1. September 2023** verschoben.

Empfehlungen für Cybersicherheit durch BWL 2018 (Bundesamt für wirtschaftliche Landesversorgung)



IKT-Minimalstandard - Branchenstandards

Schweizerischer Verein des Gas- und Wasserfaches
Société Suisse de l'Industrie du Gaz et des Eaux
Società Svizzera dell'Industria del Gas e delle Acque
Swiss Gas and Water Industry Association

SVGW
SSIGE
SSIGA
SGWA



W1018 d Ausgabe März 2019

REGELWERK

Empfehlung

Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Wasserversorgung

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Bundesamt für wirtschaftliche Landesversorgung BWL
Gesetzgebende IKT

SVGW, Grütlistrasse 44, Postfach 2110, 8027 Zürich
Telefon 044 288 33 33, Fax 044 202 16 33, www.svgw.ch

Schweizerischer Verein des Gas- und Wasserfaches
Société Suisse de l'Industrie du Gaz et des Eaux
Società Svizzera dell'Industria del Gas e delle Acque
Swiss Gas and Water Industry Association

SVGW
SSIGE
SSIGA
SGWA



G1008 c Ausgabe Dezember 2020

REGELWERK

Empfehlung

Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Gasversorgung

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Bundesamt für wirtschaftliche Landesversorgung BWL
Gesetzgebende IKT

SVGW, Grütlistrasse 44, Postfach, 8027 Zürich
Telefon 044 288 33 33, Fax 044 202 16 33, www.svgw.ch



Minimalstandard für die Sicherheit
der Informations- und Kommunika-
tionstechnologie in Abwasserbetrieben



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF
Bundesamt für wirtschaftliche Landesversorgung BWL

step by STEP

Bedrohung

+

Schwachstelle

=

Gefahr (Auswirkung)



Manipulation

Diebstahl

Erpressung

Ausfall

Zerstörung

Verlust

Bedrohung - Angreifer-Typologie

Cybermächte

+ können es

Nachrichten- Geheimdienste

- Spionage
- Wirtschaftsspionage

+ haben geheime Infos

Cyber-Kriminelle

- Organisationen

+ haben Netzwerk, Geld, Personal – verdienen Geld!

Geübte Händer

- Clubs / Verbindungen

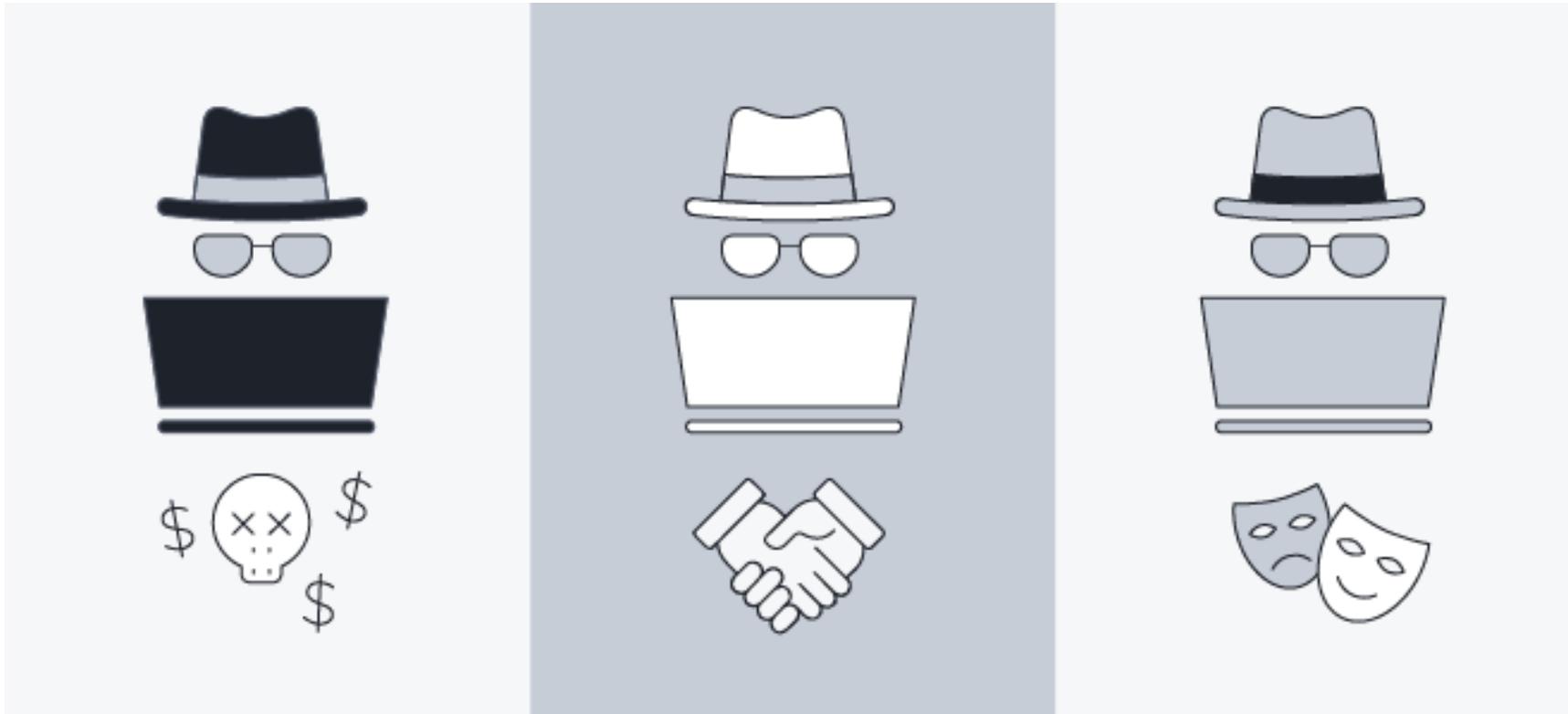
+ haben Motivation, Wissen und Erfahrung
aus Protest, Politisch motiviert, Sabotage

Hobby Händer

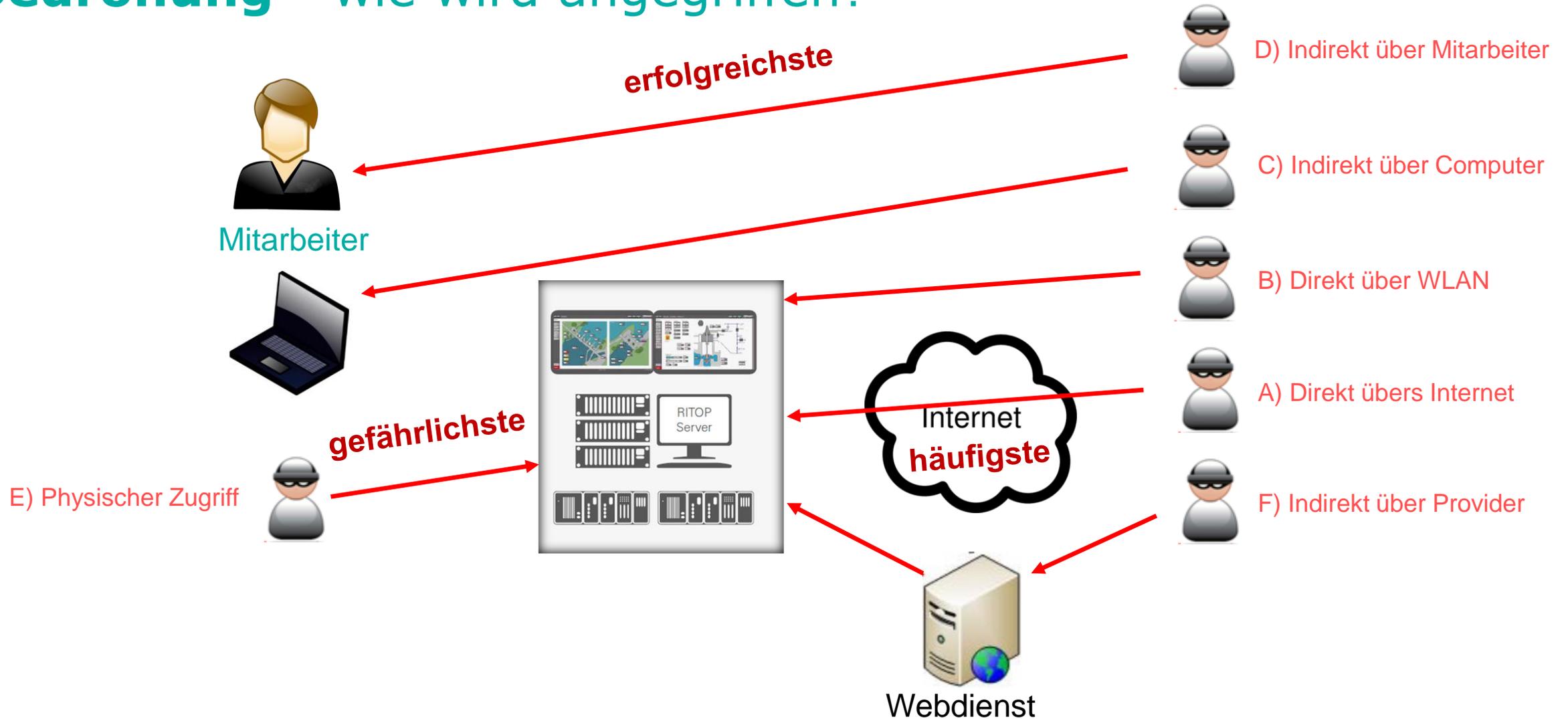
- Studenten
- Innentäter
- Kids

Besorgen sich Werkzeuge und haben Spass oder Frust

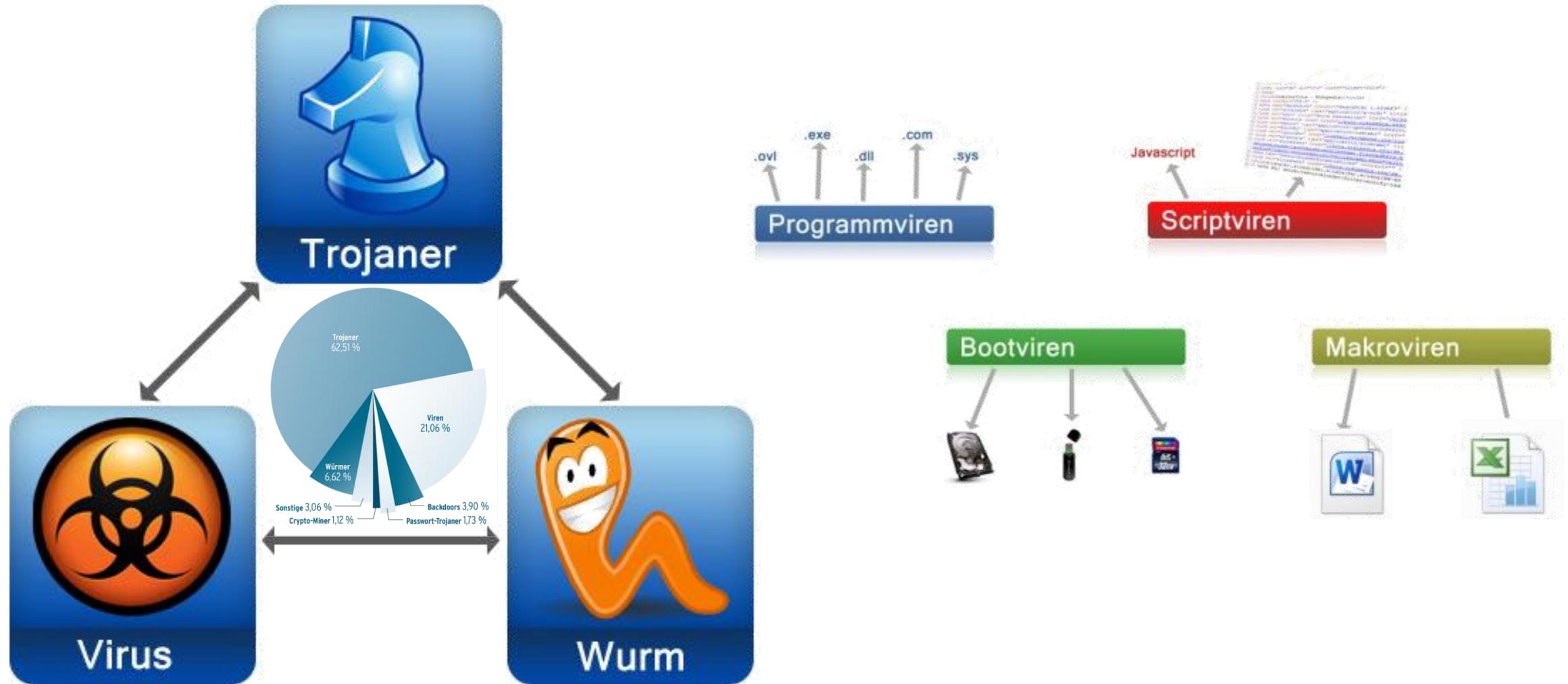
Bedrohung - Hacker – der Unterschied



Bedrohung - wie wird angegriffen?



Bedrohung - Malware



Bedrohung - Ransomware



The screenshot shows a ransomware message window with a red background and a white padlock icon. The title bar reads "Oops, your files have been encrypted!". The main text explains that files are encrypted and provides instructions on how to recover them. It includes two countdown timers: "Payment will be raised on 5/15/2017 16:50:06" with a time left of "02:23:34:22", and "Your files will be lost on 5/19/2017 16:50:06" with a time left of "06:23:34:22". The text is divided into sections: "What Happened to My Computer?", "Can I Recover My Files?", and "How Do I Pay?". The "How Do I Pay?" section includes a Bitcoin logo and the text "Send \$300 worth of bitcoin to this address:" followed by the address "115p7UMMngo1pMvvpHijcRdfJNXj6LrLn" and a "Copy" button. At the bottom, there are two buttons: "Check Payment" and "Decrypt".

Oops, your files have been encrypted! English

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.

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

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
115p7UMMngo1pMvvpHijcRdfJNXj6LrLn Copy

Check Payment Decrypt

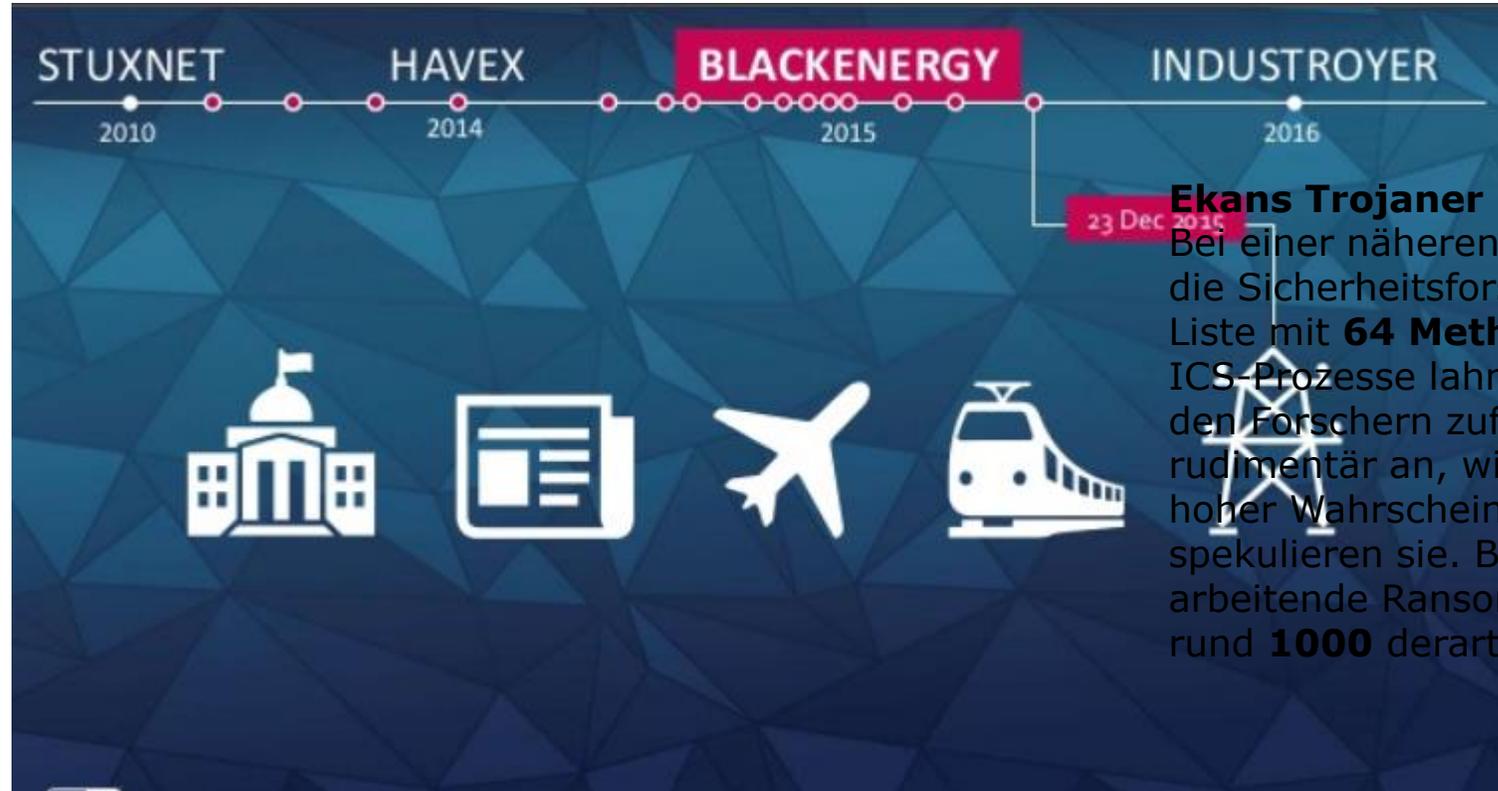
- Blockade des Systems
- Verschlüsselung von Dokumenten
- Löschung von Dokumenten
- Veröffentlichung von Dokumenten
- Angriff auf Lieferketten / Partner

→ **Alle Laufwerke**

→ **Alle Netzfreigaben**

→ **Alle aktiven Cloudkonten**

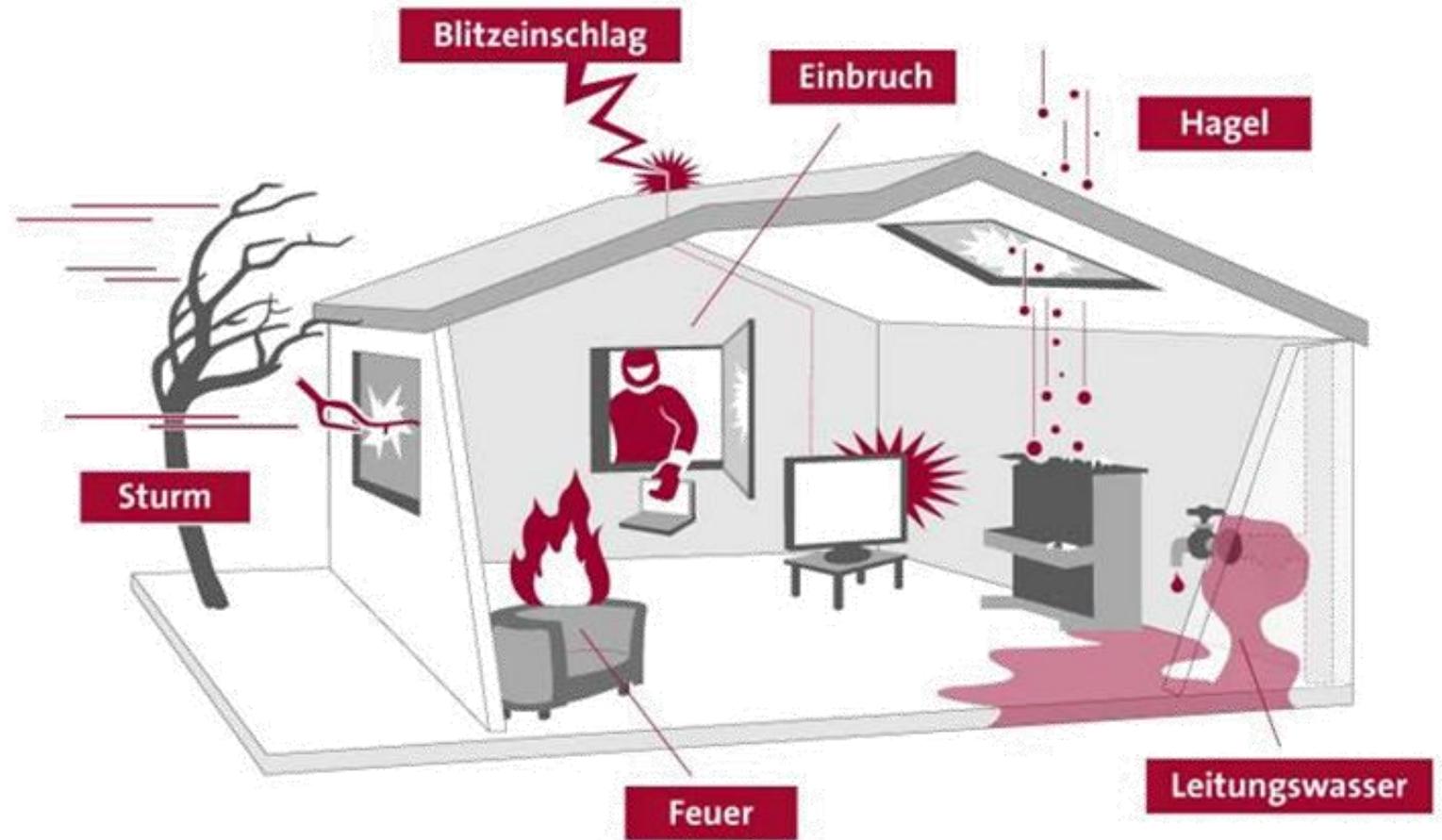
Bedrohung – Industrie-Malware



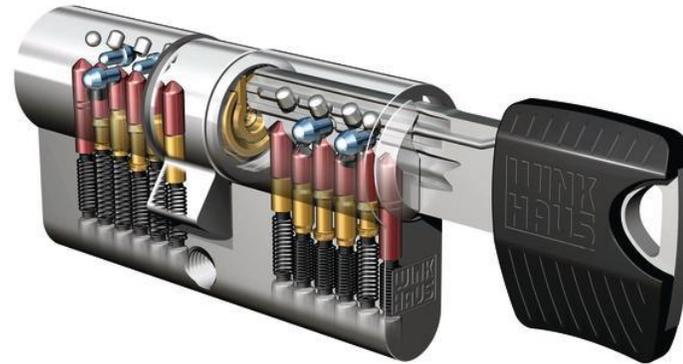
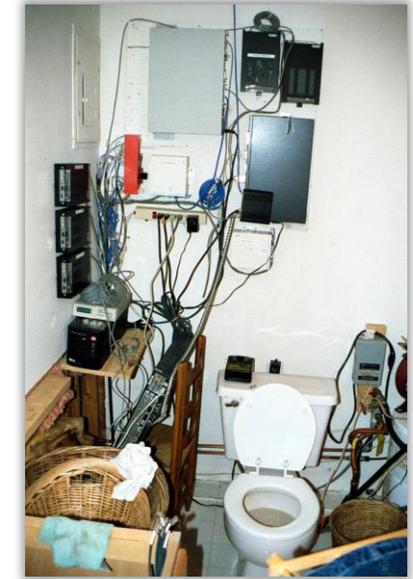
Der Schadcode beherrscht mehrere **Kommunikationsprotokolle**, die von SCADA-Anlagen verwendet werden (IEC 60870-5-101 / 103 / 104, IEC 61850, IEC 60870-6-503 (TASE.2), TG80x, Sinaut, OPC etc.)

Bedrohung – Traditionelle

- kein Strom
- Hardware defekt
- keine Mitarbeiter
- Diebstahl
- physischer Angriff
- Terror Anschlag



Schwachstelle - physischer Schutz



Schwachstelle - Internet

JAN
2019

DIGITAL AROUND THE WORLD IN 2019

THE ESSENTIAL HEADLINE DATA YOU NEED TO UNDERSTAND GLOBAL MOBILE, INTERNET, AND SOCIAL MEDIA USE

TOTAL
POPULATION



7.676

BILLION

URBANISATION:

56%

UNIQUE
MOBILE USERS



5.112

BILLION

PENETRATION:

67%

INTERNET
USERS



4.388

BILLION

PENETRATION:

57%

ACTIVE SOCIAL
MEDIA USERS



3.484

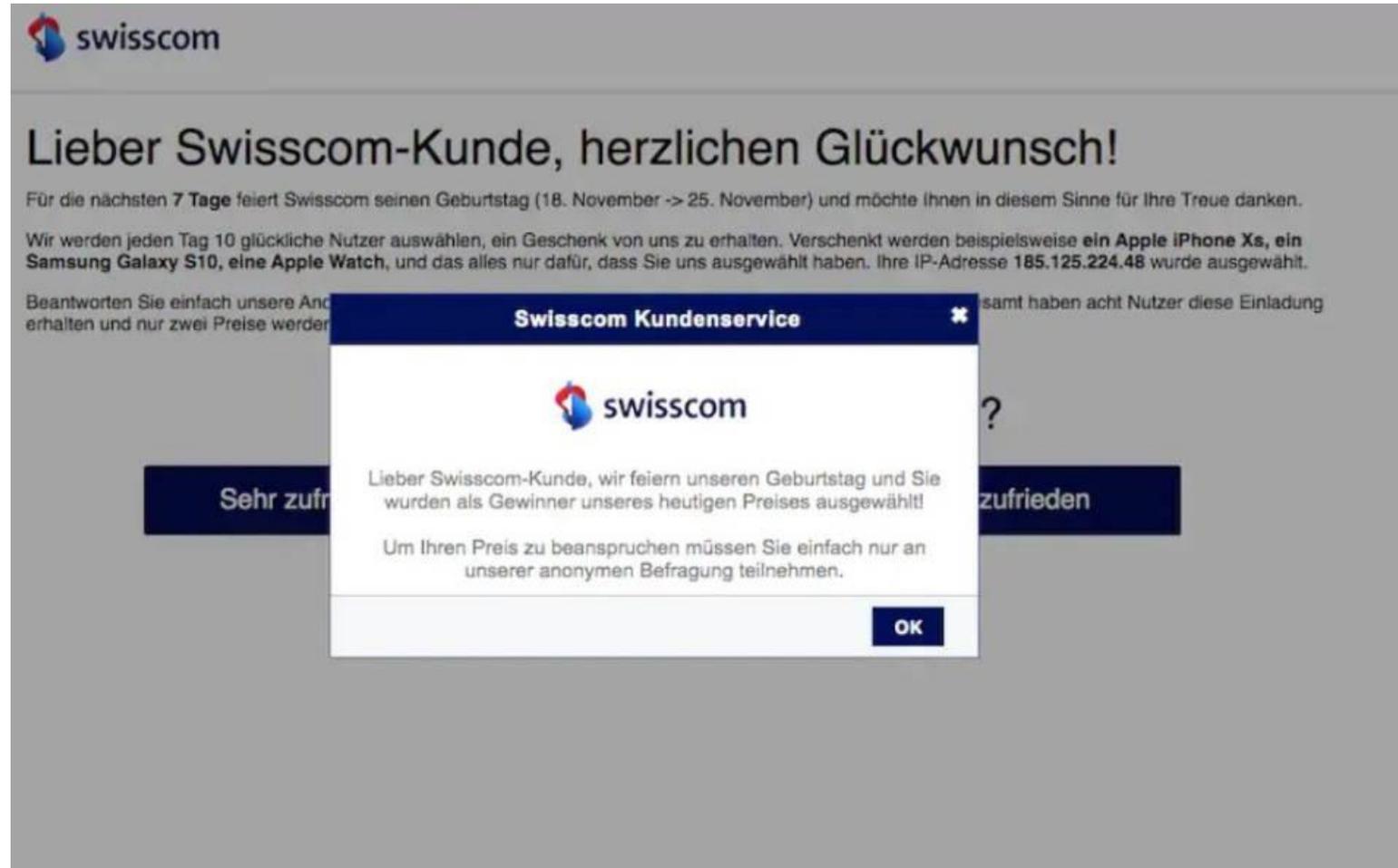
BILLION

PENETRATION:

45%



Schwachstelle - Internet



The screenshot shows an email from Swisscom. The main text of the email is partially obscured by a pop-up window. The pop-up window has a dark blue header with the text "Swisscom Kundenservice" and a close button. The main content of the pop-up features the Swisscom logo, followed by the text: "Lieber Swisscom-Kunde, wir feiern unseren Geburtstag und Sie wurden als Gewinner unseres heutigen Preises ausgewählt! Um Ihren Preis zu beanspruchen müssen Sie einfach nur an unserer anonymen Befragung teilnehmen." At the bottom right of the pop-up is an "OK" button. In the background, the email text includes the Swisscom logo, a greeting "Lieber Swisscom-Kunde, herzlichen Glückwunsch!", and a paragraph about a birthday promotion: "Für die nächsten 7 Tage feiert Swisscom seinen Geburtstag (18. November -> 25. November) und möchte Ihnen in diesem Sinne für Ihre Treue danken. Wir werden jeden Tag 10 glückliche Nutzer auswählen, ein Geschenk von uns zu erhalten. Verschenkt werden beispielsweise ein Apple iPhone Xs, ein Samsung Galaxy S10, eine Apple Watch, und das alles nur dafür, dass Sie uns ausgewählt haben. Ihre IP-Adresse 185.125.224.48 wurde ausgewählt. Beantworten Sie einfach unsere An... erhalten und nur zwei Preise werden...". To the right of the pop-up, the text "samt haben acht Nutzer diese Einladung" and a question mark are visible. Below the pop-up, there are two dark blue buttons with white text: "Sehr zufried" on the left and "zufrieden" on the right.

Schwachstelle - Social Engineering



Social Engineering ist ein Verfahren, um sicherheitstechnisch relevante Daten Computer- oder Human Based durch Ausnutzung menschlicher Komponenten in Erfahrung zu bringen. **Menschen** sind manipulierbar und generell das schwächste Glied in einer Kette.

Die Informationen werden gesammelt aus:

- Persönliche Gespräche
- Telefongespräche
- Chat
- Briefpost
- Internet / Homepage
- Physischer Besuch (Swisscom, Microsoft, Elektriker..)
- Social Medien (Facebook, Xing, LinkedIn, Search, usw.)
- Darknet



Schwachstelle - E-Mail

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!](#)



Schwachstelle - USB-Schnittstelle



KeyGrabber Wi-Fi Premium

The world's first hardware keylogger with built-in Wireless LAN support! This keylogger connects to the Internet through an Access Point, and sends captured keyboard data as E-mails. With this Wi-Fi hardware keylogger, you can silently monitor a computer from anywhere in the world, just by checking your mailbox! Ultra stealthy, undetectable for software. [\[more...\]](#)



er ver. USB 4 GB - \$149.99 | €139.99
ver. PS/2 4 GB - \$139.99 | €130.99

Schwachstelle - Mensch – Social Engineering - USB



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

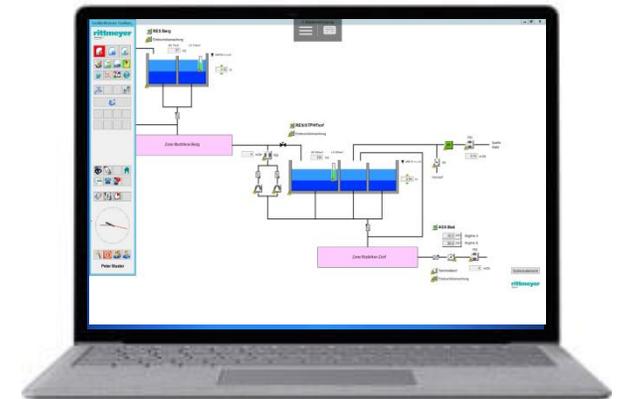
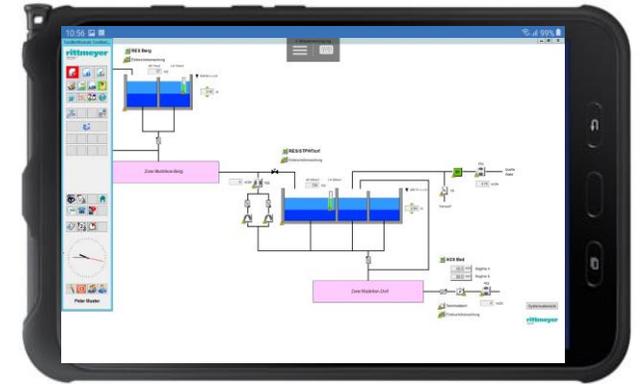
Zugleich enthält es aber eine **Mini-Platine** mit **WLAN-Chip**, über die es sich beim Einstecken am Computer als Eingabegerät ausgibt.

Schwachstelle - Mensch & Computer - Fernwartungszugang

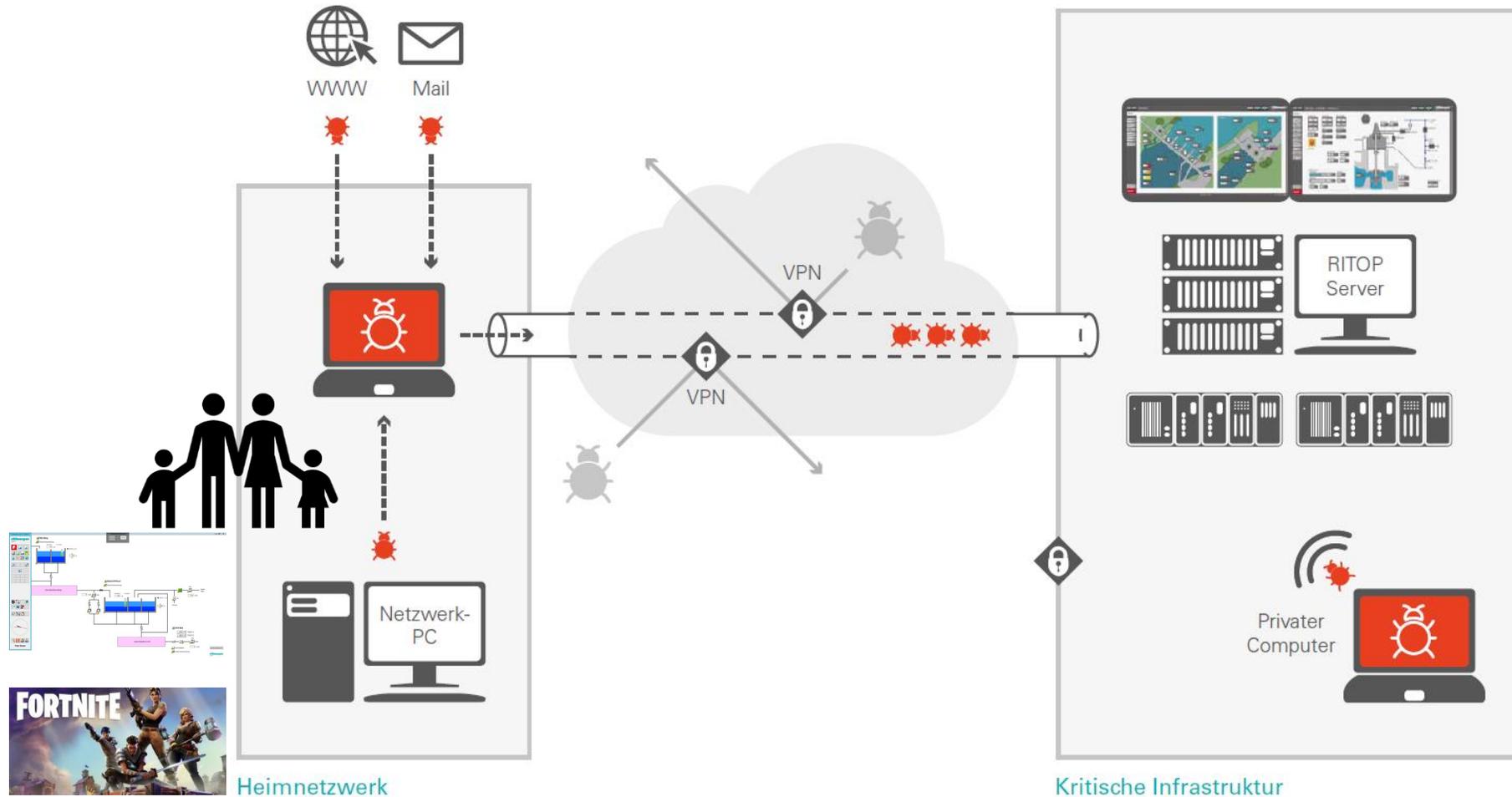
Sonntag Morgen 03:15 Uhr Alarm an Piket-Dienst

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

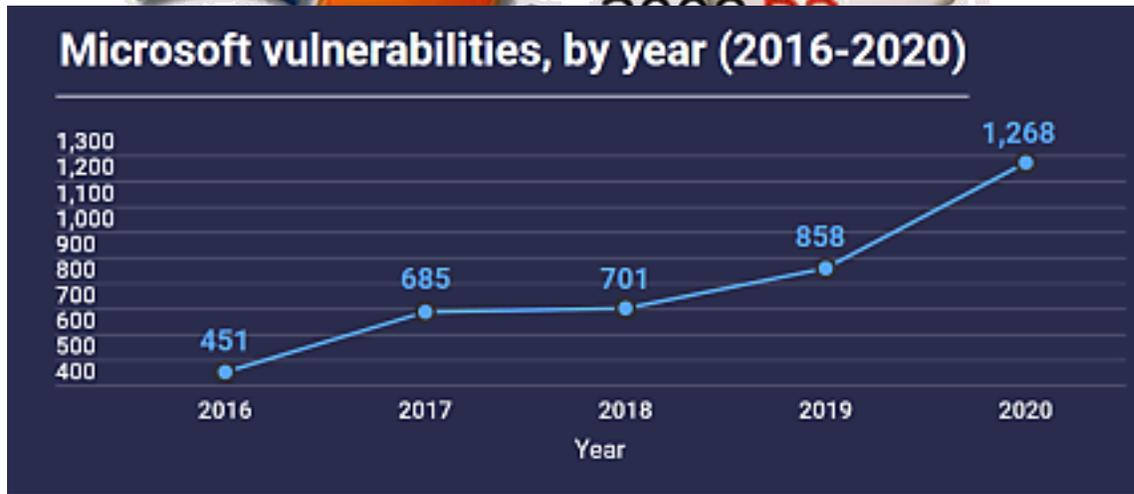
Die Liste mit allen möglichen PW ist in der Piket-Tasche...



Schwachstelle - Mensch & Computer - Fernwartungszugang



Schwachstelle - Software (Update)



Windows 7	9 Prozent
Windows 8 / 8.1	3 Prozent
Server 2003	2 Prozent
Server 2008	2 Prozent
Server 2008 R2	11 Prozent

Windows 10	84 Prozent
Windows 11	4 Prozent

Server 2012 / R2	29 Prozent
Server 2016 / R2	30 Prozent
Server 2019 / R1	25 Prozent
Server 2022	1 Prozent

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?



Gefahr - Auswirkung bei einem erfolgreichen Angriff

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

Datenmanipulation

- Falsche Berechnungen
- Falscher Inhalt von Webseiten
- Aufzeichnungen
- Abrechnungen

Fernsteuerung

- Software
- Hardware

Verfügbarkeit

Notwendige Informationen müssen abrufbar sein.

Availability

Vertraulichkeit

Informationen dürfen nicht in falsche Hände gelangen.

Confidentiality

Integrität

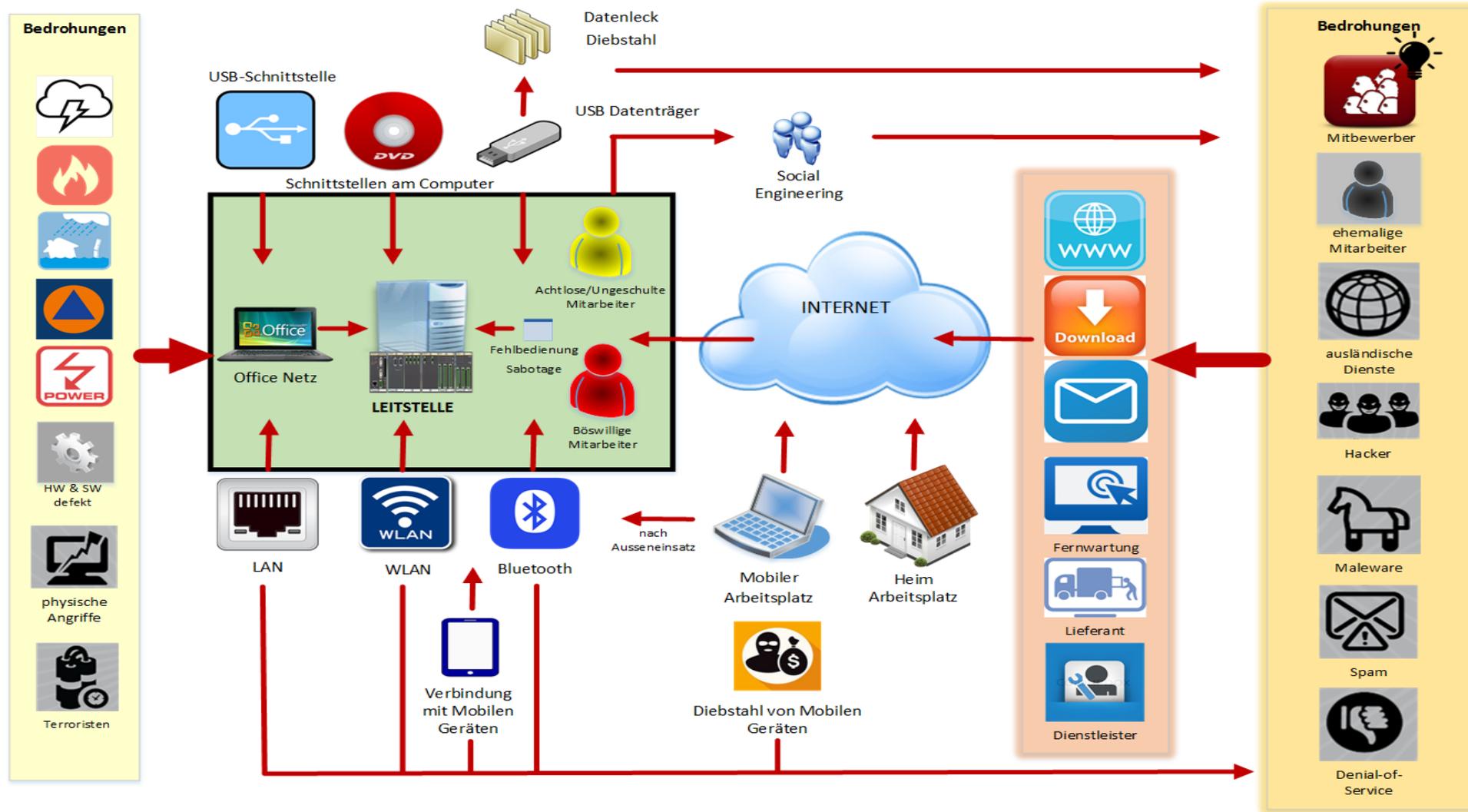
Sensible Informationen dürfen nicht verfälscht werden.

Integrity

Schutzmassnahmen - Wie müssen wir uns Schützen?



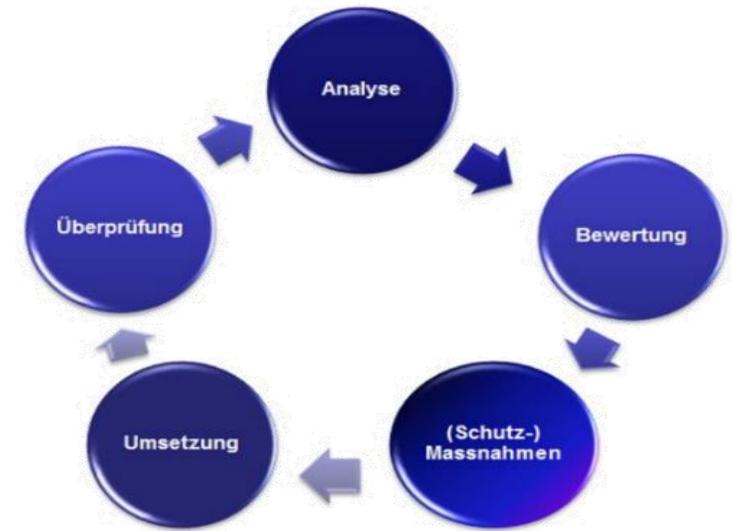
Identifizieren - Schwachstellen-Analyse



Massnahme - IKT-Assessment (Schwachstellen-Analyse)

Zertifizierte Sicherheits-Experten unterstützen Sie dabei, potenzielle Schwachstellen und Bedrohungen frühzeitig zu erkennen. Wir erfassen durch eine IST-Analyse den bestehenden IT-Schutz und können danach einen individuellen und strukturierten IT-Grundschutz mit entsprechenden Schutzmassnahmen erstellen.

- **Erfassen** und überprüfen der kritischen Infrastruktur
- **Analysieren** von Bedrohungen / Schwachstellen
- **Bewertung** von Bedrohungen / Schwachstellen
- **Massnahmen** und Sofortmassnahmen
- **(Umsetzen** der Massnahmen)



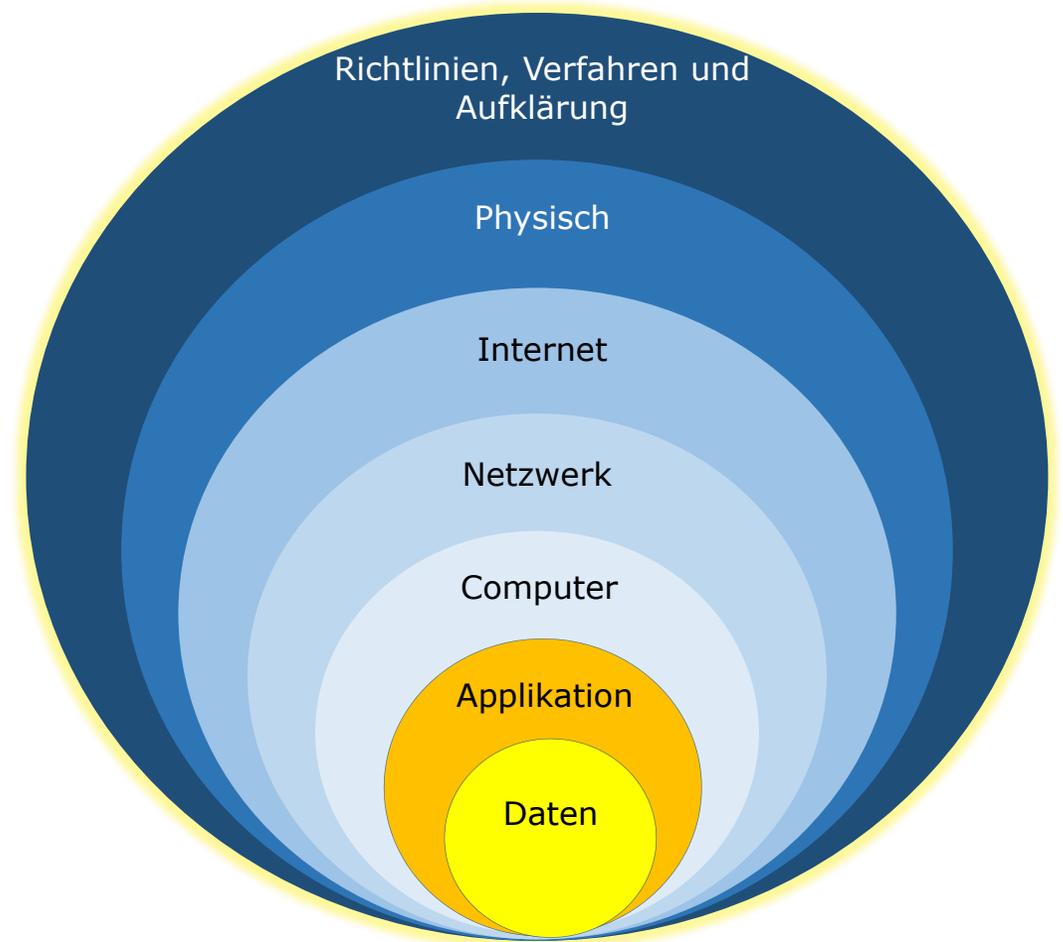
Massnahmen = Hindernisse einbauen

mit defence in depth (mehrschichtiger Ansatz)

ZERO TRUST

Damit es für einen Angreifer schwieriger wird, ein komplexes und mehrschichtiges Abwehrsystem zu überwinden als eine einzige Barriere.

Es muss vor bekannten Risiken schützen und mit einer umfassenden Überwachung auch vor zukünftiger Risiken.



Schutzmassnahmen - 2 Faktor Auth / Passwort-Richtlinie

WISSEN:

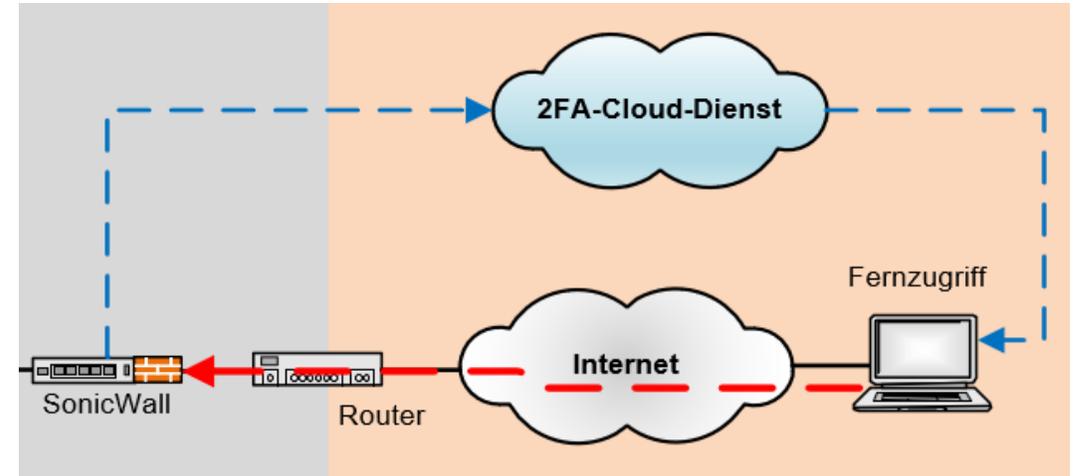
Username
Passwort
Pin
Verbindung
Nummer

HABEN:

Schlüssel
SMS auf Smartphone
E-Mail
Programm
Smart Card
NFC
Hard-/Software Token

SEIN:

Fingerabdruck
Gesichtserkennung
Stimme



Multi factor authentication



Something
you have

Something
you are

Something
you know

Schutzmassnahme – Update

Schluss mit „never change a running system!“

Um höchste Versorgungssicherheit zu gewährleisten und zu erhalten, müssen auftretende Sicherheitslücken in der Softwareinstallation umgehend behoben werden. Dafür ist es notwendig, dass verfügbare Aktualisierungen regelmässig getestet und installiert werden.



Schutzmassnahme - Backup

Kein Backup? – kein Mitleid!

Die Notwendigkeit für Backups ist vorhanden. Es wird jedoch unterschätzt, oft vernachlässigt und nicht seriös gehandhabt. Mit der vollautomatischen Daten-Backup Lösung übernimmt Rittmeyer die Verantwortung für die regelmässige und effiziente Sicherung der wertvollen Anlagendaten.



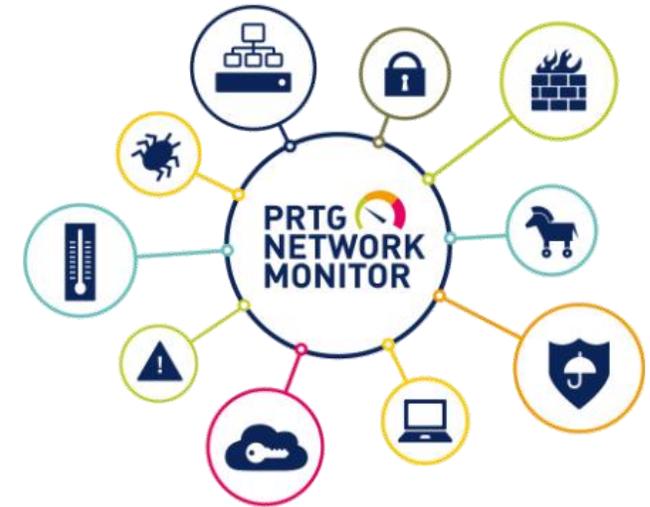
Schutzmassnahme – Monitoring

Wollen Sie wissen, ob auf Ihrer Anlage alles in Ordnung ist?

Sicherheitszustand des Netzwerkes & ICT-Komponenten

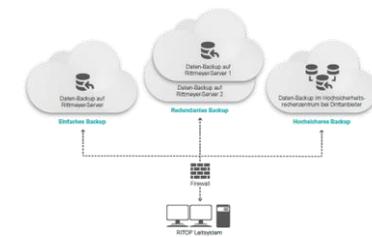
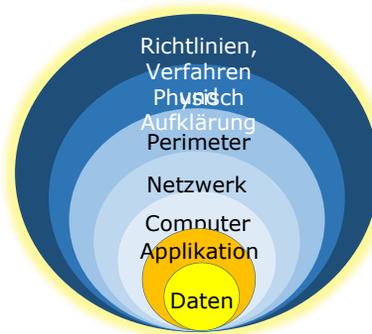
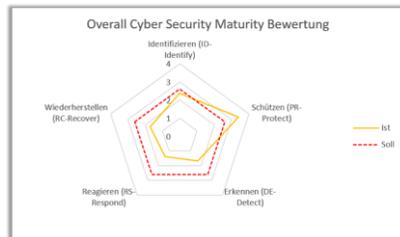
24x7 Überwachung mit Alarmierung an Helpdesk

- Überwachung Aktivitäten & Datenfluss Internet / Firewall
- Überwachung der Internet-Bandbreite
- Überwachung der Programme / Dienste / Hardware
- Software-Update Überwachung
- Überwachung Antivirus-Signaturen
- Erkennen von Anomalien auf Netzwerk & Computer
- Schliessen von Sicherheitslücken
- Stabile Datenübertragung
- Erhöhen der Netzwerk Geschwindigkeit

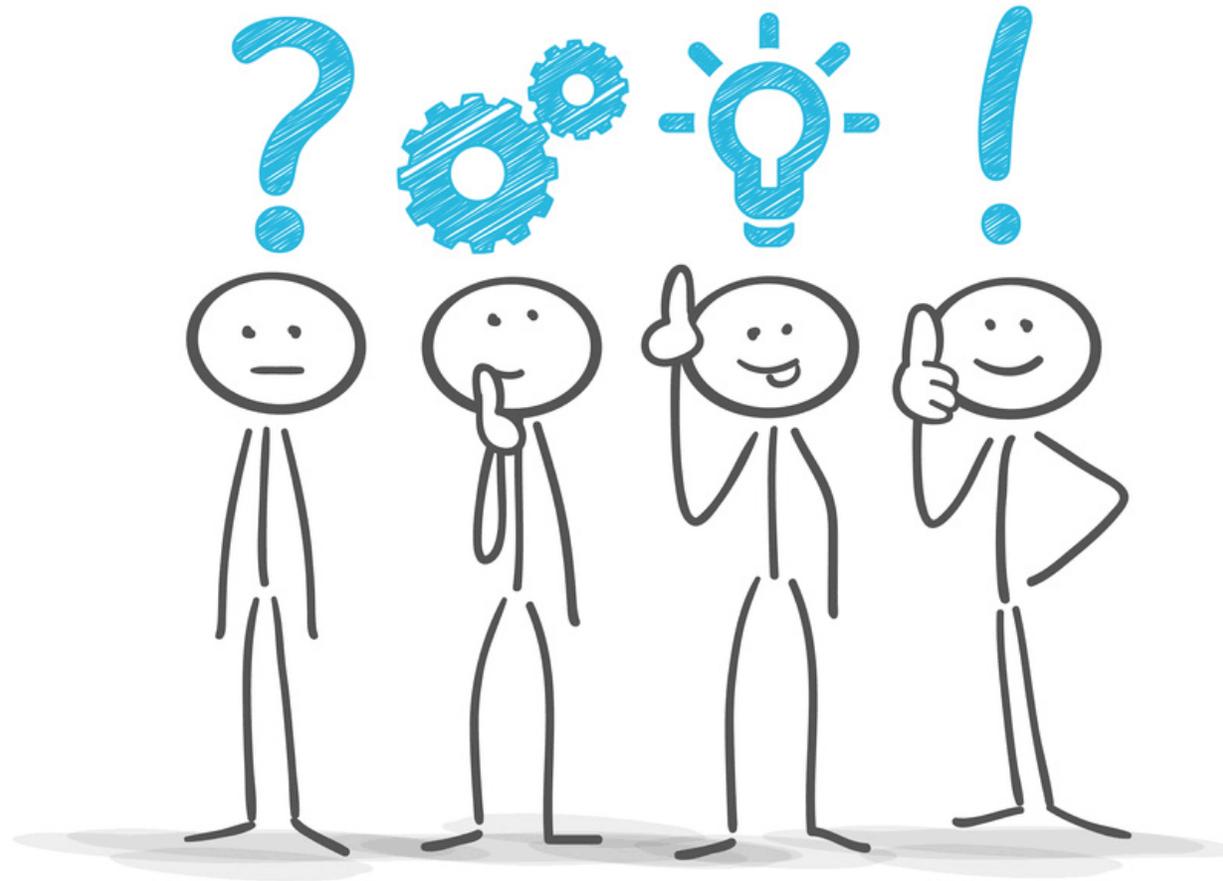


Zusammenfassung

Ja - kritische Infrastrukturen werden angegriffen – ich kann mich jedoch schützen
Ich bin an Gesetze und Empfehlungen gebunden und muss aktiv werden



Vielen Dank für Ihre Aufmerksamkeit



© Matthias Enter - Fotolia.com



patrick.erni@rittmeyer.ch

rittmeyer
BRUGG