SCAUT

Swiss Center of Applied Underground Technologies

Partner Event

«Digitalisierung für Sicherheit»

Dätwyler IT Infra AG, Dietlikon, 23. März 2022

SCAUT
Swiss Center of Applied Underground Technologies

Veronika Petschen

- Master in Bauingenieurwesen der Technischen Universität Budapest
- 12 Jahren Erfahrung als Projektleiterin im Tunnel- und Infrastrukturbau
- digitale Technologien (BIM, point clouds, KI etc), Digitalisierungs- und Entwicklungsprojekten engagiert (z.B Tunnel Digitalization Center)

vpetschen@scaut-association.com

SCAUT
Swiss Center of Applied Underground Technologies

Programm (1/2)

13:00 – 13:15 Uhr	**Eintreffen und Registrierung**
13:15 – 13:30 Uhr	**Begrüssung & Tagesablauf** Veronika Petschen, Geschäftsführerin SCAUT Johannes Müller, CEO Dätwyler IT Infra AG
13:30 – 14:15 Uhr	**Vortrag 1 inkl Q&A – Cybersecurity** Raphael Reischuk, Head of Cyber Security, Zühlke Engineering AG Vice-President of the Cyber Security Commitee of Digital Switzerland Member of the Advisory Board**,** Cyber Security Advisory Board of the Swiss Academy of Engineering Sciences (SATW)
14:15 – 14:40 Uhr	**Vortrag 2 – Erfahrungen eines Cyberangriffs** Thomas Freuler, CEO Später Gruppe
14:40 – 15:05 Uhr	**Vortrag 3 – Edge Datacenter zur Erhöhung der Datensicherheit** Adrian Bolliger, Geschäftsführer Europa, Dätwyler IT Infra AG
15:05 – 15:25 Uhr	**Pause**

SCAUT
Swiss Center of Applied Underground Technologies

Programm (2/2)

15:25 – 15:50 Uhr	**Vortrag 4: Sicherheit und IOT** Rainer Stocker, Geschäftsführer, Swiss1mobile AG Reto Amstad, Senior Security Consultant, CyOne AG
15:50 – 16:15 Uhr	**Vortrag 5: Digitale Sicherheit am Bau** Yvette Körber, CEO, Amberg Loglay AG
16:15 – 16:25 Uhr	**Zusammenfassung & Ausblick** Veronika Petschen, Geschäftsführerin, SCAUT
ab 16:30 Uhr	**Rundgang durch die Dätwyler Werke**

SCAUT
Swiss Center of Applied Underground Technologies

Cybersecurity

Raphael Reischuk

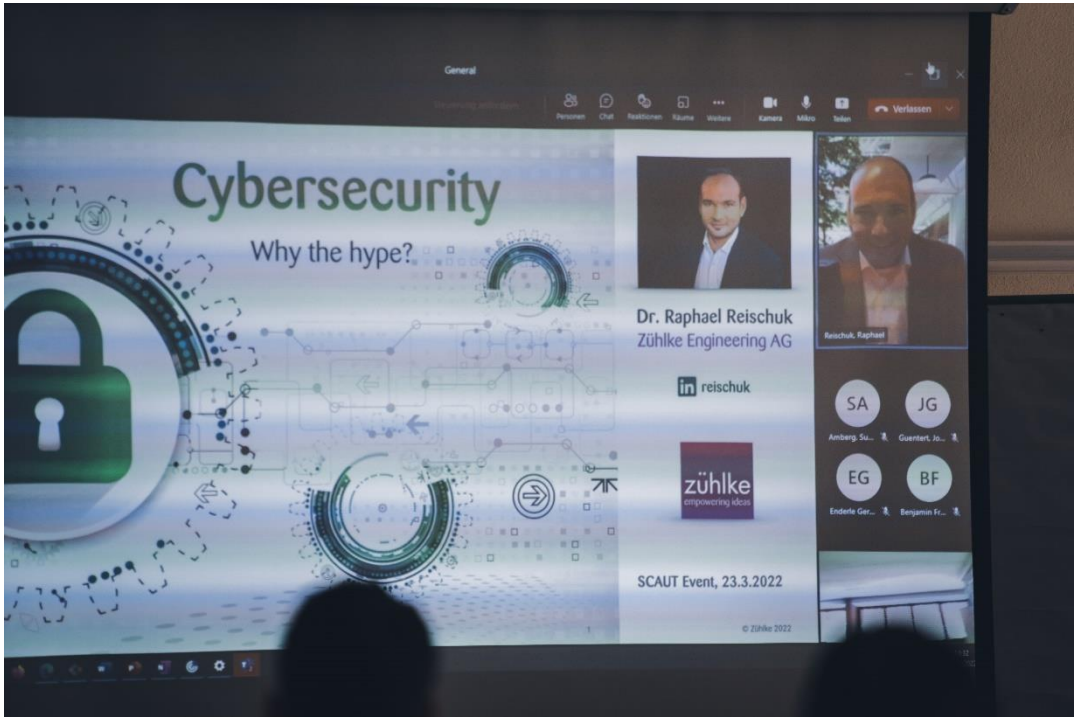
Head of Cyber Security, Zühlke Engineering AG

Vice-President of the Cyber Security Commitee of Digital Switzerland

Member of the Advisory Board, Cyber Security Advisory Board of the Swiss Academy of Engineering Sciences (SATW)

SCAUT
Swiss Center of Applied Underground Technologies

Vortrag nicht öffentlich



SCAUT
Swiss Center of Applied Underground Technologies

Erfahrungen eines Cyberangriffs

Thomas Freuler

CEO Später Gruppe

SCAUT
Swiss Center of Applied Underground Technologies

Erfahrungen eines Cyber-Angriffs beim Spaeter

Cyber-Angriff – Risiken werden unterschätzt

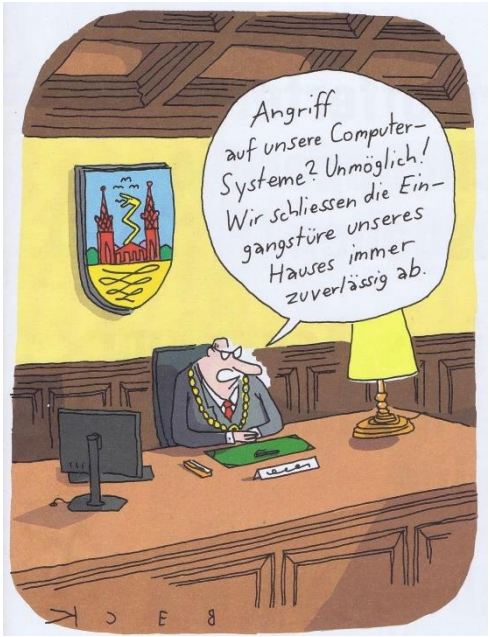
GFS Schweiz hat 503 Geschäftsführende kleiner Unternehmen zu den Auswirkungen der Corona-Krise auf Digitalisierung und Cybersicherheit in Schweizer KMU befragt.

- Homeoffice + 60%
- 25% der KMU's waren Opfer eines Cyberangriffs
- 13'000 KMU's mit finanziellem Schaden
- Präventive Massnahmen werden selten ergriffen
- Cyberrisiken werden durch CEO's unterschätzt (Quelle: GFS Schweiz)

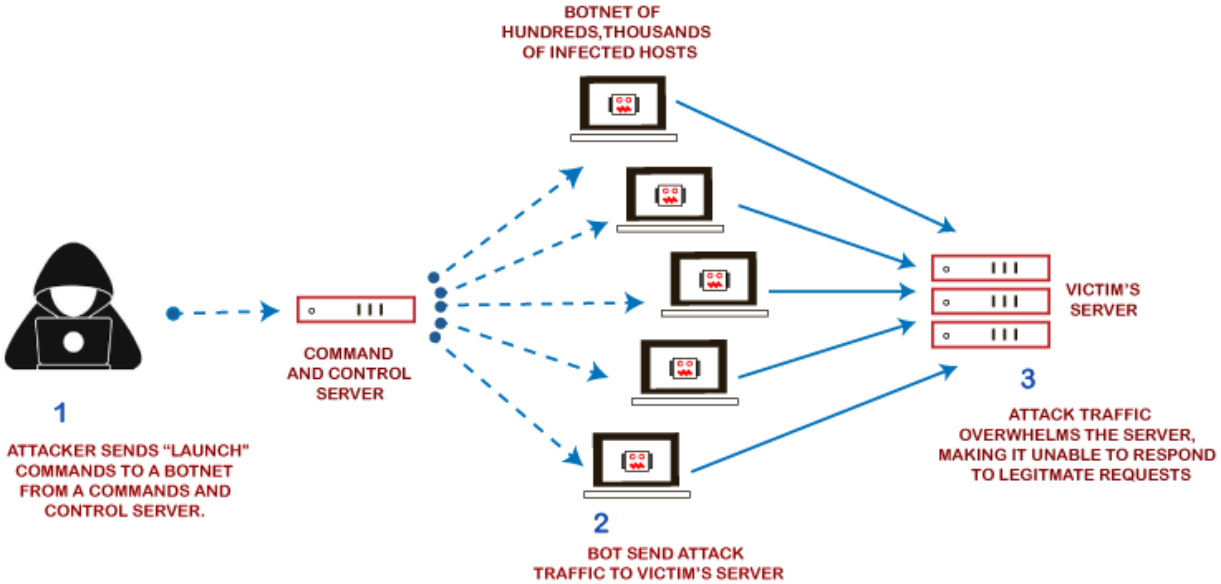
Cyber-Angriff – Übliche Irrtümer

- «Wir sind kein lohnendes Angriffsziel.»
- «Die haben halt nicht aufgepasst, sonst hätte es sie nicht erwischt!»
- «Um Cyber-Security muss ich mir als Chef keine Sorgen machen. Meine Spezialisten kümmern sich darum!»
- «Auf sowas kann man sich nicht vorbereiten.»
- «Uns kann das nicht passieren, wir sind umfassend geschützt.»

Die Frage ist nicht ob es passiert, sondern wann!



Cyber-Angriff beim Spaeter – DDoS Attacke (*Distributed-Denial-of-Service)*



Cyber-Angriff bei Spaeter – Wie alles begann: Ruhe vor dem Sturm

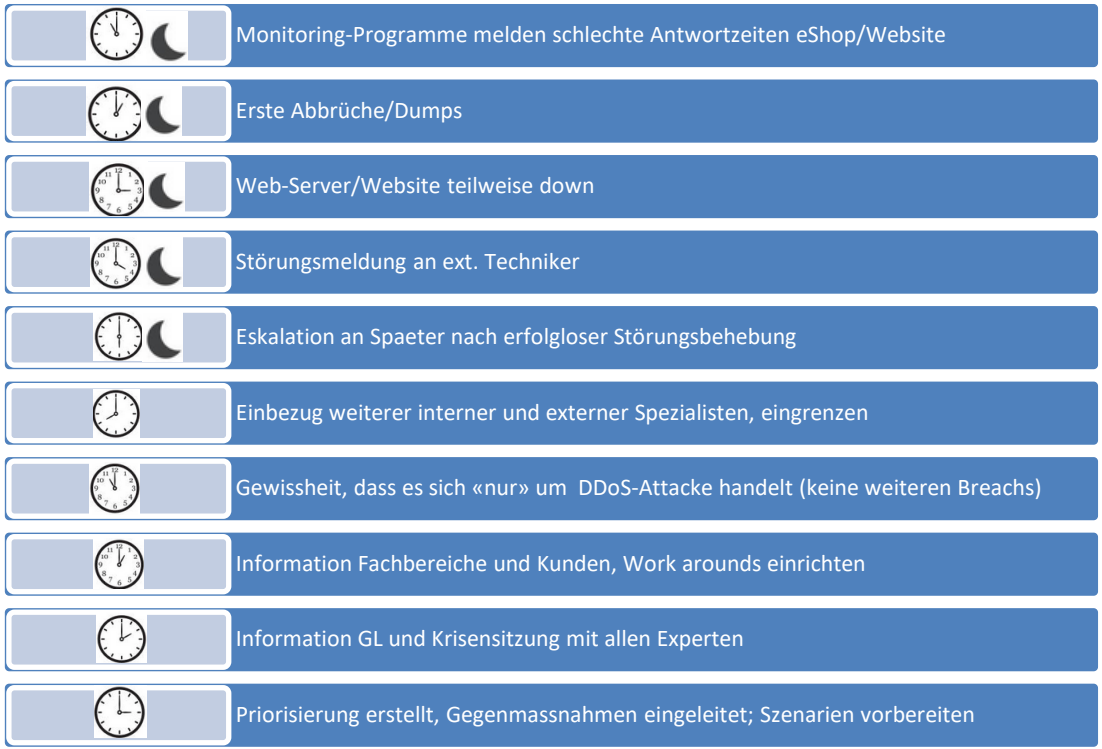
- **Es begann mit einer trivialen, unscheinbaren Fehlermeldung ….**
- … ungewöhnlichem Verhalten von technischen Komponenten
- … zur Unzeit (Nacht, Wochenende, Urlaub)
- … bei unübersichtlicher Gesamtlage …
- … widersprüchlichen Angaben …
- … Eskalation … Verdacht … Gewissheit …
- … Krisenmodus … Angst … Schuld … Wut … (gefährlicher Aktionismus …)

Probleme mit Webshop / Hintergrundinformationen

Guten Abend,

Wir kämpfen seit gestern Abend mit unserem Webserver/Webshop. Sämtliche Spezialisten sind aufgeboten und arbeiten am Problem.

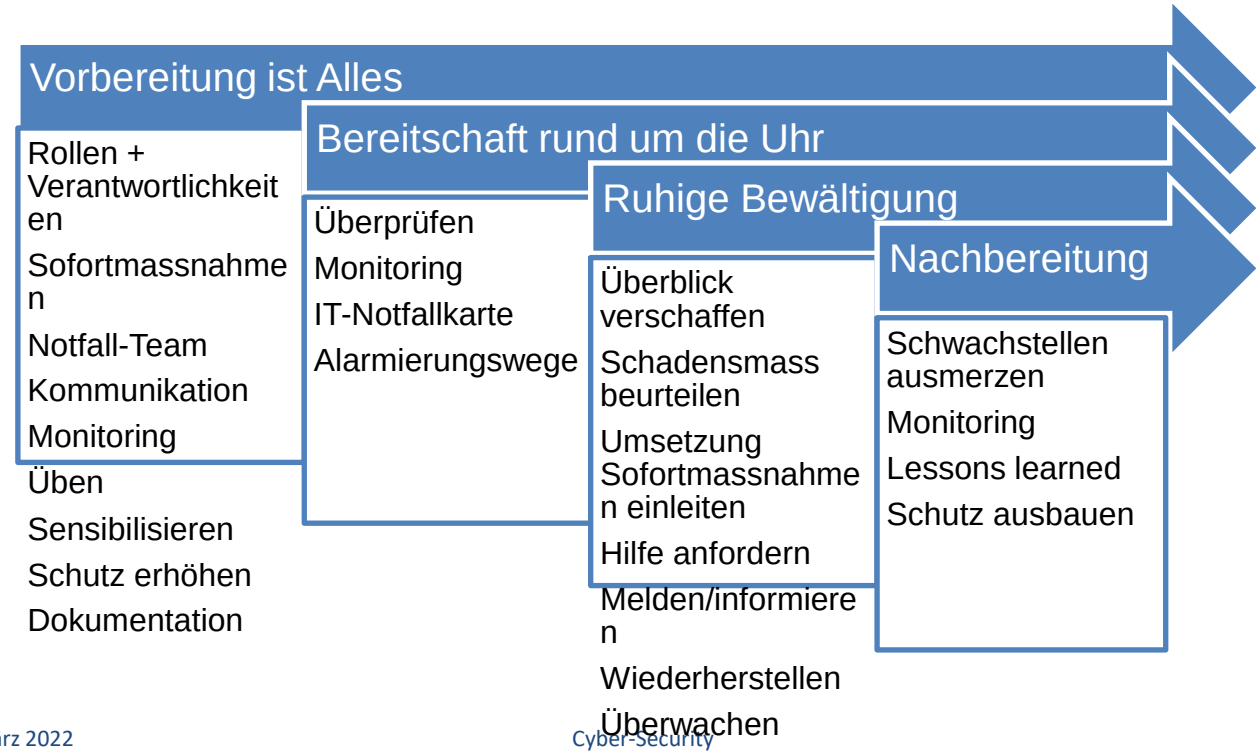
Cyber-Angriff beim Spaeter – Chronologischer Ablauf in den ersten 24h



Cyber-Angriff beim Spaeter – Abwehrmassnahmen

- Kein Sprint – sondern ein Marathon
- Angriffswellen überstehen und trotzdem «online» bleiben (Betrieb aufrechterhalten!)
- Logs auswerten und Firewall-Regeln anpassen
- Proxy-Server ausbauen
- Geoblocking für gewisse Regionen/Länder aktivieren
- Monitoring erweitern
- Geoblocking für gewisse Länder wieder deaktivieren (Druck Kunden)
- Melden … überwachen … analysieren … justieren: In hoher Kadenz
- «Normale» Spezialisten beigezogen
- (kein Einsatz ext. Forensic Spezialisten; kein Einsatz ext. Cyber Defense Team)
- Meldung an NCSC (Nationales Cyber Security Center) und der Versicherung

Cyber-Angriff: Learnings – Notfallplan erstellen



Cyber-Angriff –
If you remember 1 Slide

Cyberbedrohung ernst nehmen.
Aufrüsten! (KCHF 200-800)

Üben, üben, üben

Men in Black bereithalten

Notfallplan bereithalten

Edge Datacenter zur Erhöhung der Datensicherheit

Adrian Bolliger

Geschäftsführer Europa, Dätwyler IT Infra AG

SCAUT
Swiss Center of Applied Underground Technologies

Edge Computing

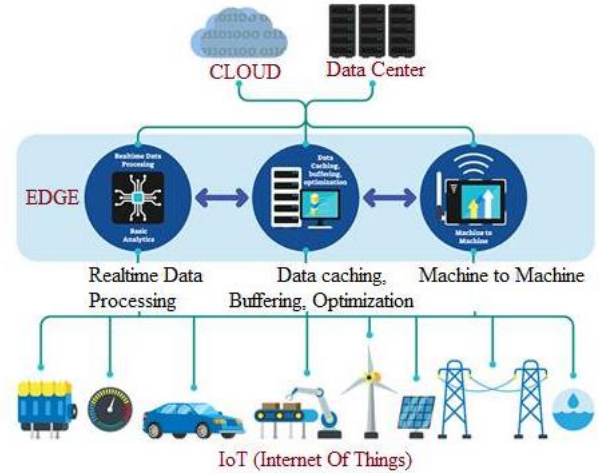


Image Courtesy : IEEE

“ Around 10% of enterprise-generated data is created and processed outside a traditional centralized data center or cloud. By 2025, Gartner predicts this figure will reach 75%”

Source: Gartner

DATWYLER

Verschiedene Schutzstufen mit Edge Computing

Elementarereignisse

Ich kann selbst steuern was auf meinem Gelände passiert - public nicht, z.B. bei Elementarereignisse, Stromverfügbarkeit – wer hat die Kontrolle?

Physisches Sicherheitskonzept

Auf dem Gelände greift das physische Sicherheitskonzept, schwieriger auffindbar als ein Rechenzenter

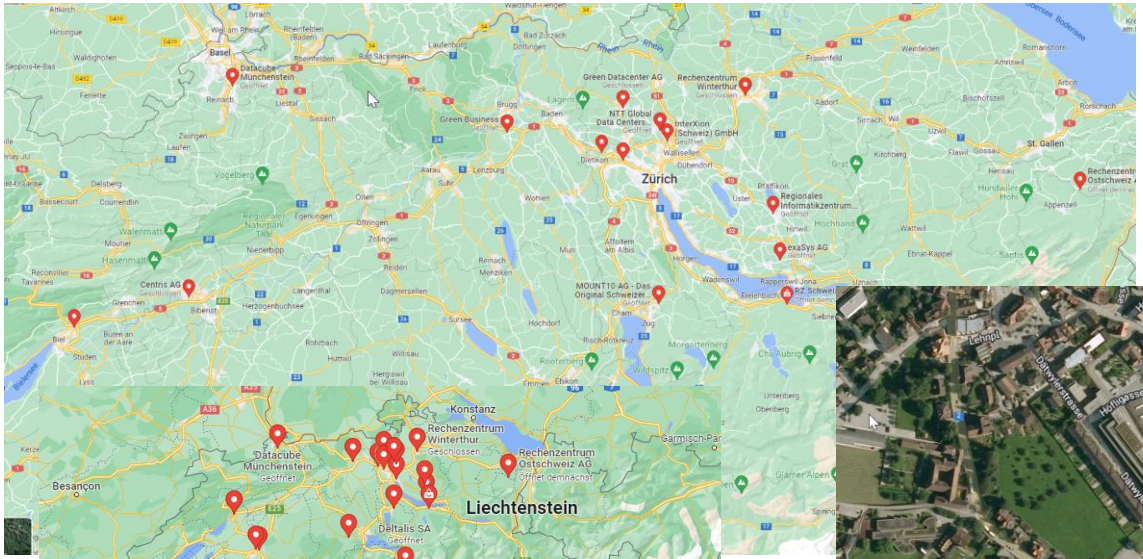
Netzanbindung vorhanden

Sichere Umgebung zwischen Geräte und Edge Computing / Cloud durch Zertifikate, läuft autark ohne Netzanbindung weiter

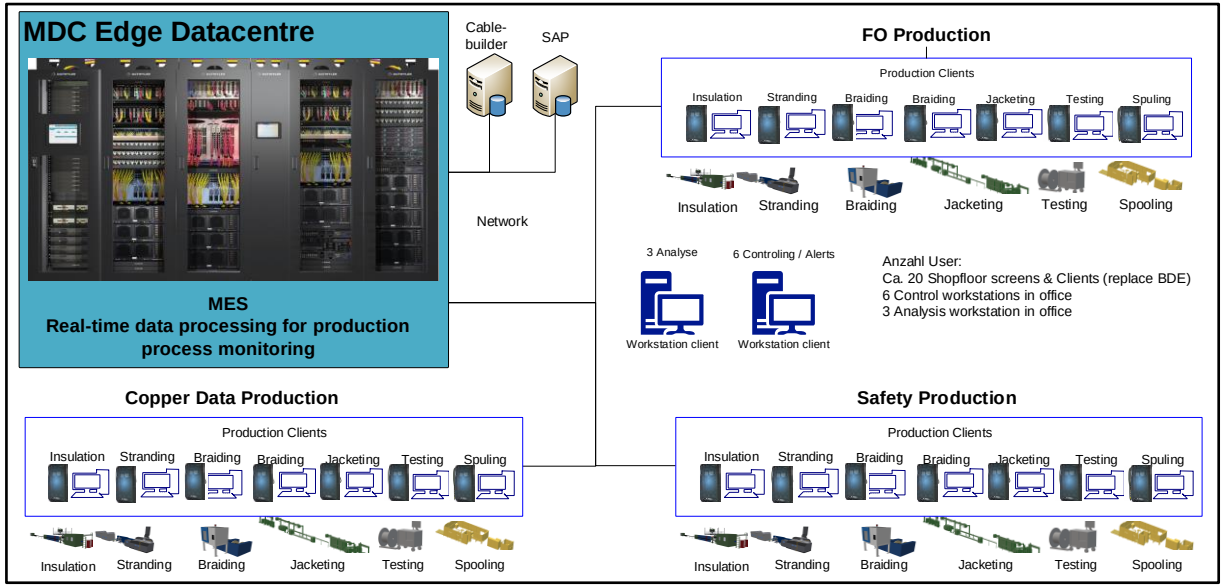
Keine Netzanbindung

Völlige Isolation – update nur über USB, trotzdem economy of scale in Bezug auf SW Nutzung

Sichtbarkeit der Rechenzenter



Beispiel Dätwyler IT Infra



- Schnelle Datenauswertung vor Ort
- Analyse und Visualisierung der Daten
- Hohe Bandbreiten vor Ort
- Lernen wie Industrie 4.0 geht
- TCO - Kosteneinsparung

DÄTWYLER

Fazit

1) Je intelligenter die Maschinen werden desto besser müssen wir sie schützen
2) Nebst vielen anderen Vorteilen bietet Edge Computing auch einen guten Schutz ihrer Daten / Geräte

Die Technologie ist ready und die Zeit somit reif in die richtige Technologie zu investieren. Gerne teilen wir unsere Erfahrungen mit ihnen.

Vielen Dank für eure Aufmerksamkeit!

DATWYLER

Pause

SCAUT
Swiss Center of Applied Underground Technologies

Sicherheit im Zeitalter von Software-Entwicklungen & IoT

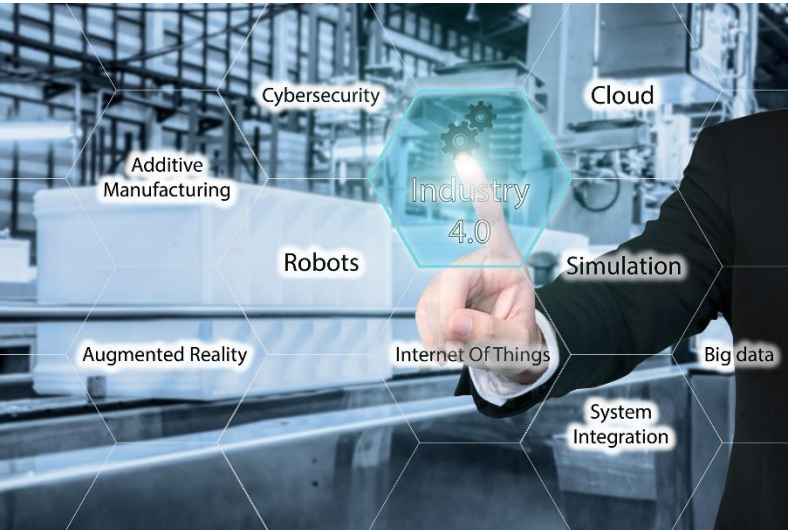
Rainer Stocker

Geschäftsführer, Swiss1mobile AG

Reto Amstad

Senior Security Consultant, CyOne AG

SCAUT
Swiss Center of Applied Underground Technologies



Sicherheit im Zeitalter von Software-Entwicklungen & IoT

Rainer Albert Stocker,
Gründer & Partner
Swiss1mobile & Collana Group
rainer.stocker@swiss1mobile.com

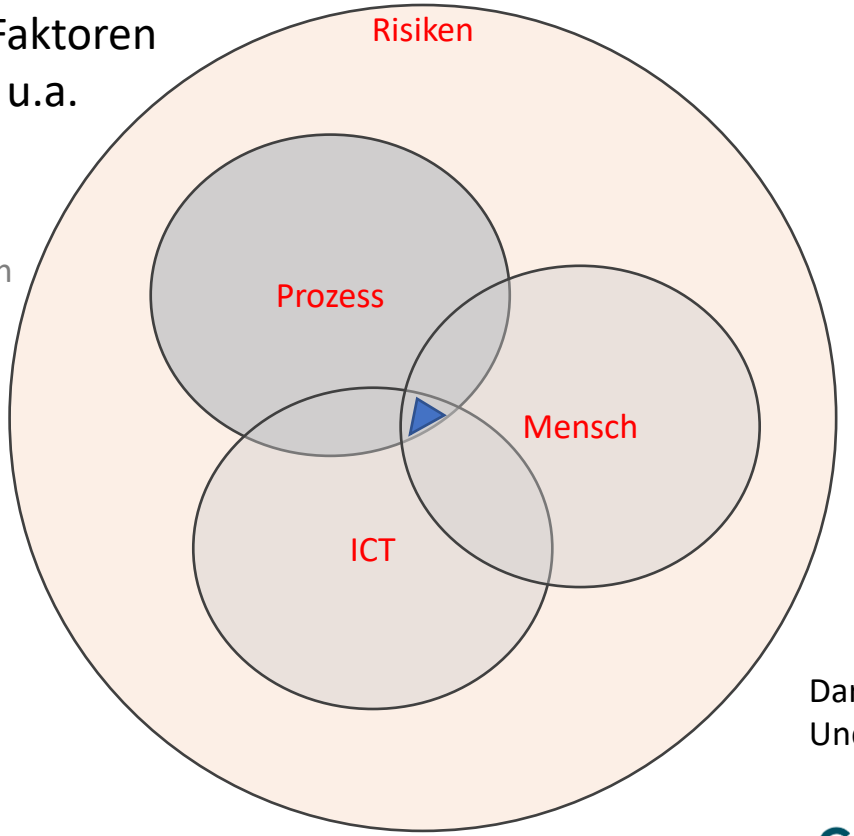
SCAUT Partner

Event «Digitalisierung und Sicherheit»

Critical Factor

Globale Faktoren
im Chain u.a.

Kenntnisse
Definition
Beziehungen
Folgen
Strategie
Gewichtung



Darum arbeiten wir mit Cyper Security Spezialisten
Und zertifizierten Partnern zusammen

CyOne SECURITY

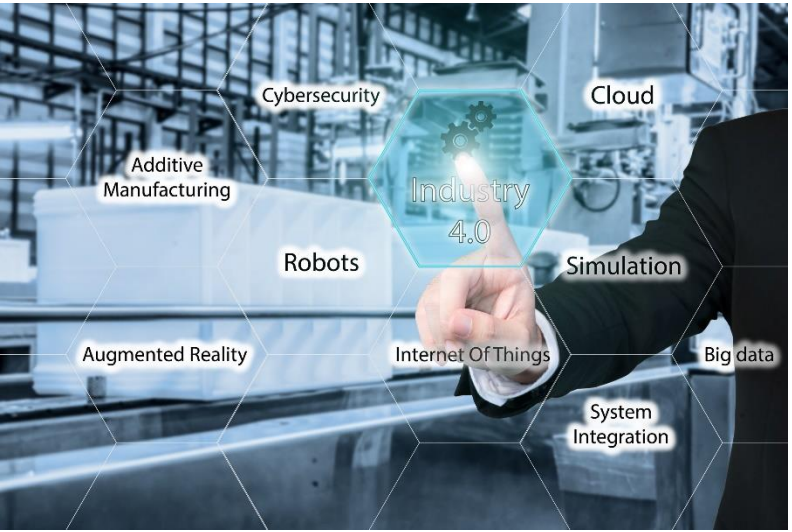
swissmobile Lösungen die bewegen

Ref’s IoT-Projects

FGG-Carlsberg, Tank Fullfillment System for Beer
- Innovation Workshop Process & Technology, Concept
- Select Sensortechnologies, Transmitter—Electr., Communication, Radio-Antenna Booster, Elektronik-Board, MVP, Pilot
- SW-Devops Platform & Business BI Apps
- Industialization 350 Pc’s

BAK, Tank Overheating System for plastic-welding machines
- Innovation - Workshop, Concept, Select Sensortechnologies, Transmitter, Communication, Elektronik-Board
- SW-Devops Platform & Business Apps, BI
- Industrialization

Syngenta, Counting System for pest (insect&fungal)
-Innovation Workshop, Concept F&E
- Select Sensortechnologies, Machines (Thermal Image)
- Plant recognize



23. März 2022

Merci und nun weiter zu CyOne Security

Rainer Albert Stocker,
rainer.stocker@swiss1mobile.com

Gründer & Partner
Swiss1mobile & Collana Group

SCAUT Partner

Event «Digitalisierung und Sicherheit»

23. März 2022

Sicherheitsstrategie im Zeitalter von IoT

Öffentliche Präsentation

Reto Amstad, Senior Security Consultant

SCAUT Partner Event «Digitalisierung und Sicherheit»

Inhaltsverzeichnis

Die CyOne Security AG

- Innovative, State-of-the-Art-Lösungen für sämtliche Sicherheitsherausforderungen
- Höchste Kompetenz in Kryptographie und Security Engineering
- 100% Schweizer Management
- 60 sicherheitsüberprüfte und hochqualifizierte Expertinnen und Experten

Sichere Schweiz. Bit für Bit.

CyOne Security AG
Hinterbergstrasse 18 • 6312 Steinhausen
Telefon +41 41 748 85 00 • cyone.ch

BLOG Cyber Security BLOG IoT Security

Cyber-Risiken durch IoT

Kritische Infrastrukturen: Cyber-Angriffe nehmen zu!

Foto: Raisa Milova / Unsplash

Cyber-Angriffe auf kritische Infrastrukturen nehmen zu, diese Woche wurden in Portugal Teile des Notrufsystems lahmgelegt. Eine Studie zeigt Ausmass und Entwicklung.

AVENIQ

Diesen Montag traf eine verheerende

Source: https://www.inside-it.ch/

Ungenügender Cyberschutz bei Bahnunternehmen

Aus HeuteMorgen vom 03.06.2021.

News > Schweiz >

Bericht der Finanzkontrolle

Hacker haben bei Regionalbahnen zu leichtes Spiel

Source: https://www.srf.ch/

Sicherheitsanforderungen: Schutzziele für IACS-Netzwerke

Vertraulichkeit

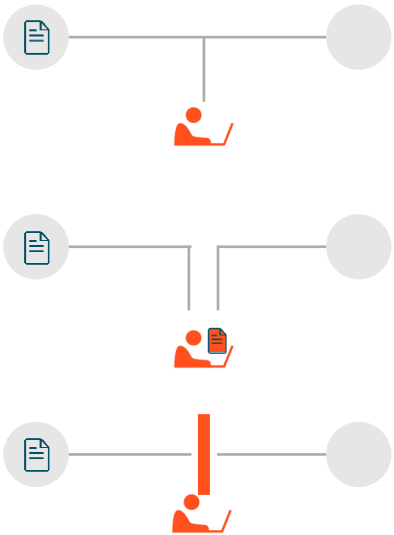
- Schutz vor unerlaubtem Abhören durch Verschlüsselung und physischen Schutz

Integrität

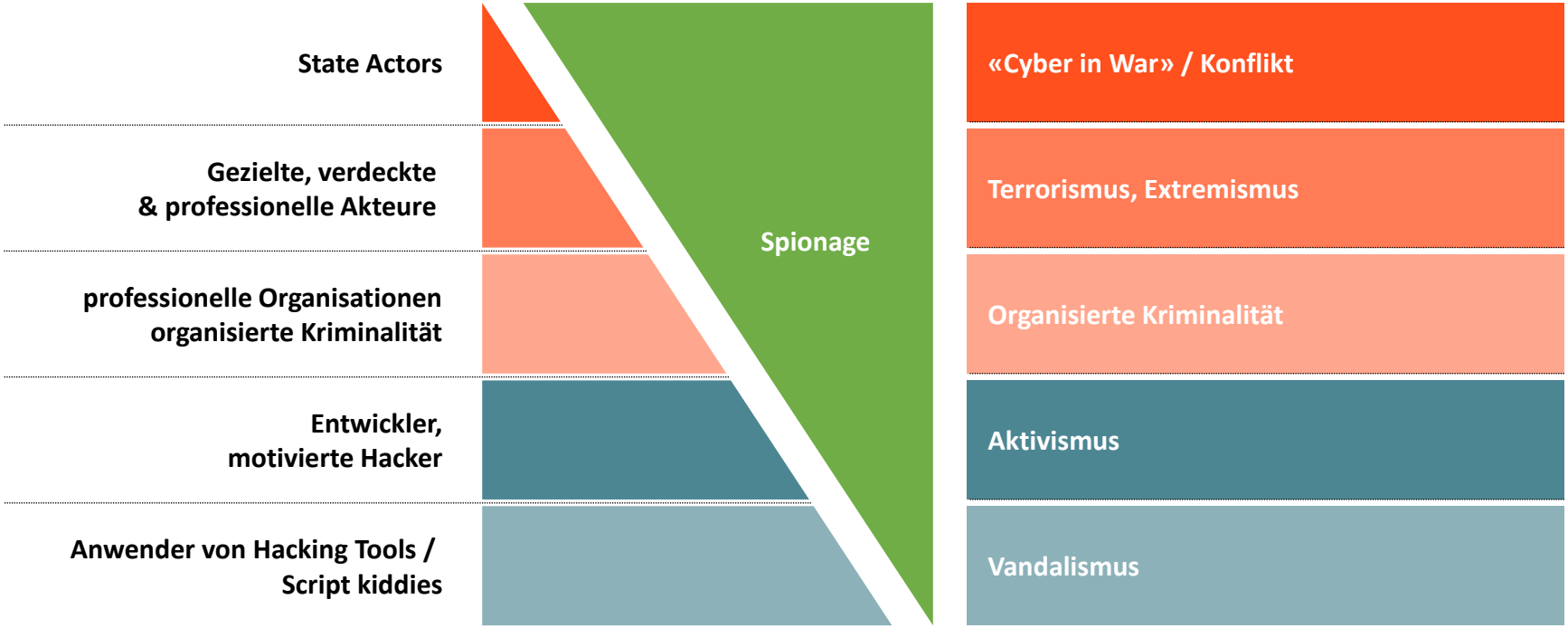
- Schutz vor Verfälschung durch Sicherstellung der Authentizität

Verfügbarkeit

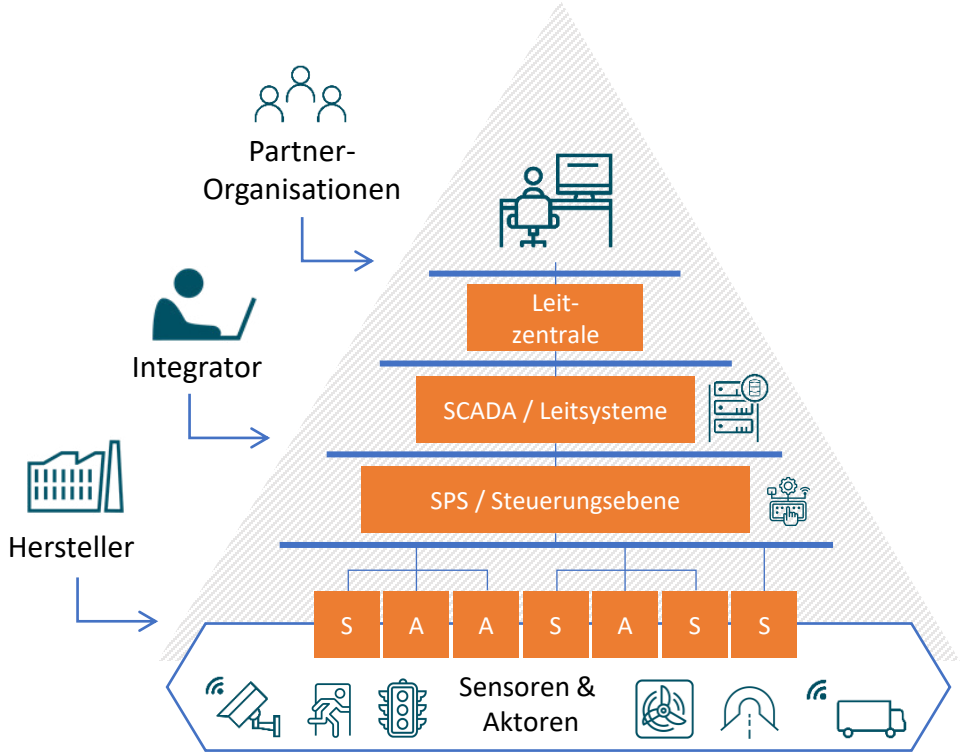
- Ausfallsicherheit durch redundante oder ringförmige Netztopologien



Akteure und Kategorien bei Cyber-Attacken

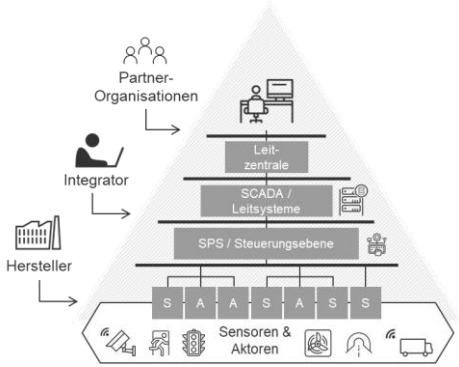


Heutiger klassischer Systemaufbau

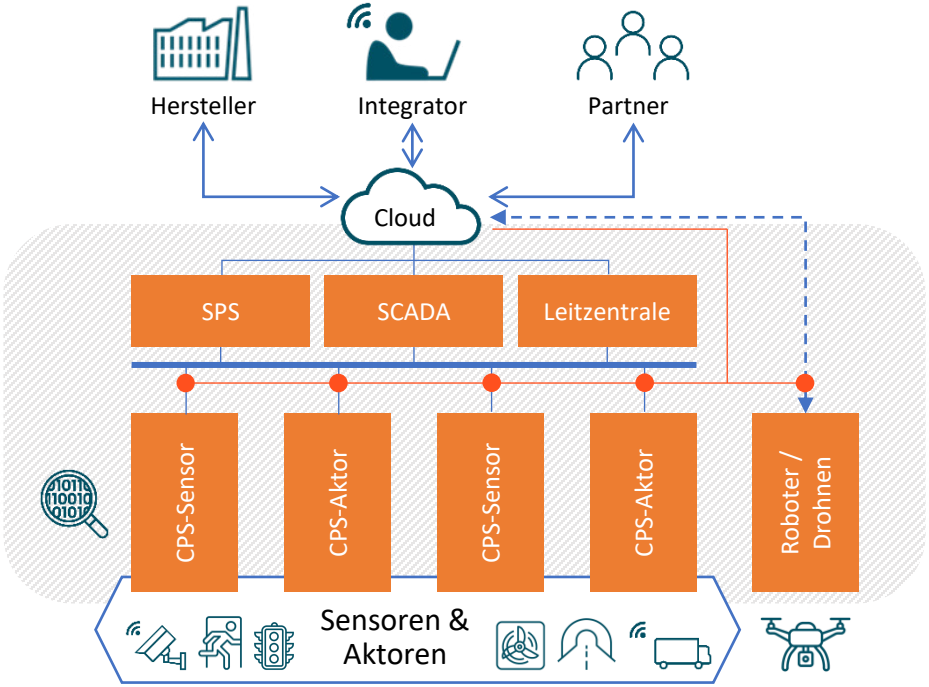


- **Situation heute (oder zumindest «Soll»):**
- Hierarchische Netzwerke
- Vorwiegend OT-Komponenten
- Kontrollierte und terminierte Verbindungen nach extern
- Segmentierte Netze
- Klare Trennung IT / OT
- Klare Perimeter

Industrie 4.0 verändert die Systemlandschaft



Auflösung der
(Automatisierungs)-Pyramide



Modulare
IT-Systeme

Smarte
Feldgeräte

Smarte
Produkte

CPS: Cyber Physische Systeme

IoT-Geräte sind attraktive Angriffsziele

Weil IoT-Geräte sind …

… immer on

… immer online

… Produkte mit geringen Security Standards

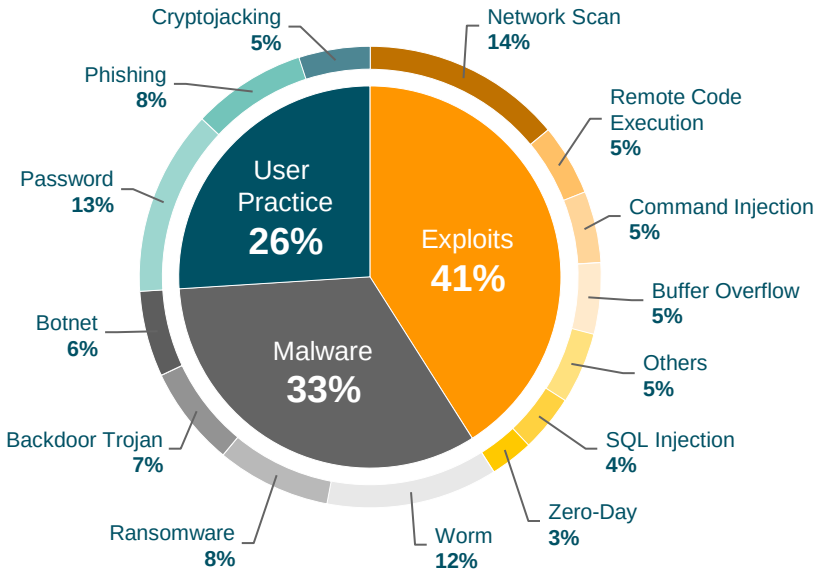
… leicht ausnutzbar

… schlecht gewartet / ungepatched

… selten überwacht und schlecht gehärtet

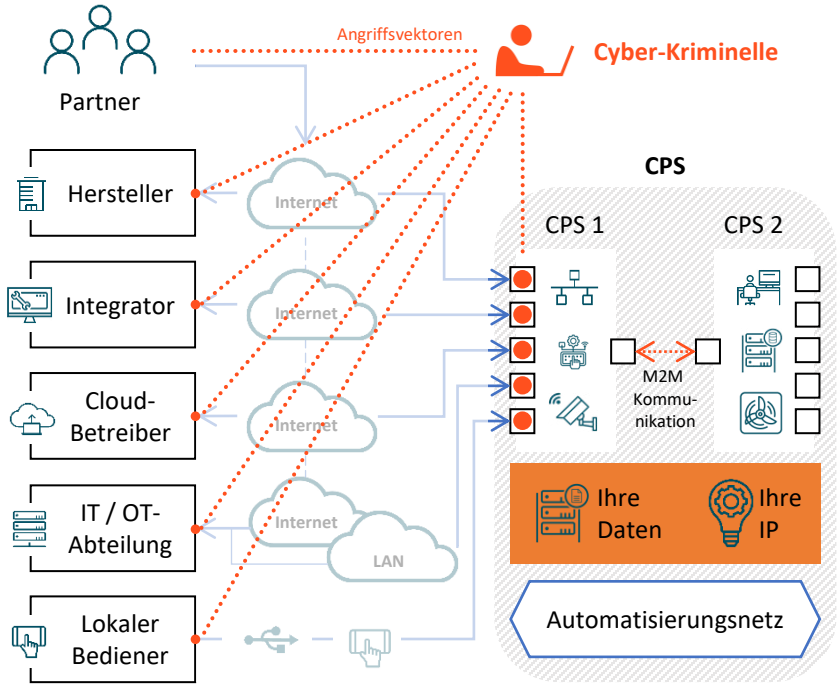
… ermöglichen laterale und horizontale Infiltration

Die drei Cyber-Attacken-Methoden



Source: 2020 Unit 42 IoT Threat Report, Palo Alto Networks, 2020

IIoT-Ökosystem: komplexere Sicherheit



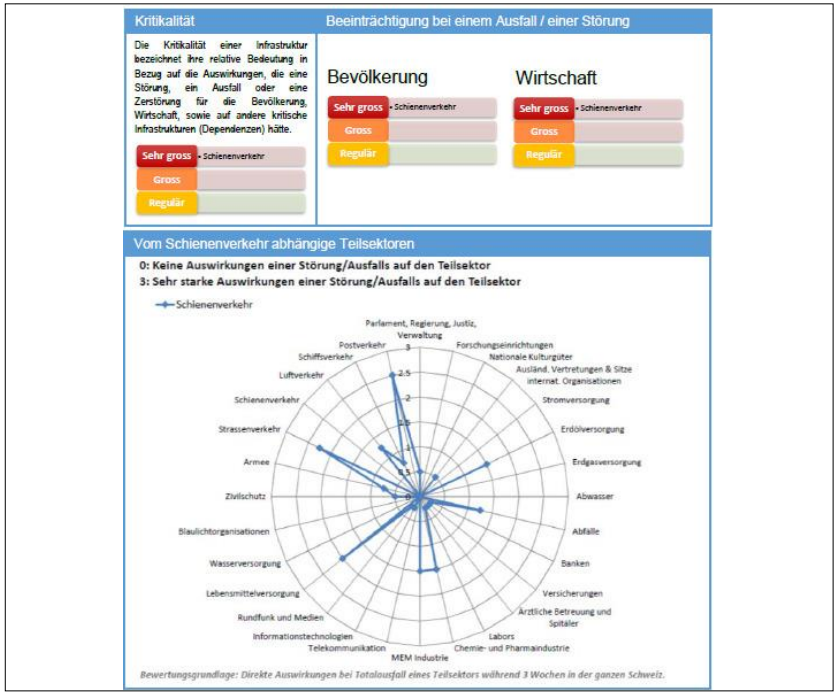
Komplexes Sicherheitsumfeld

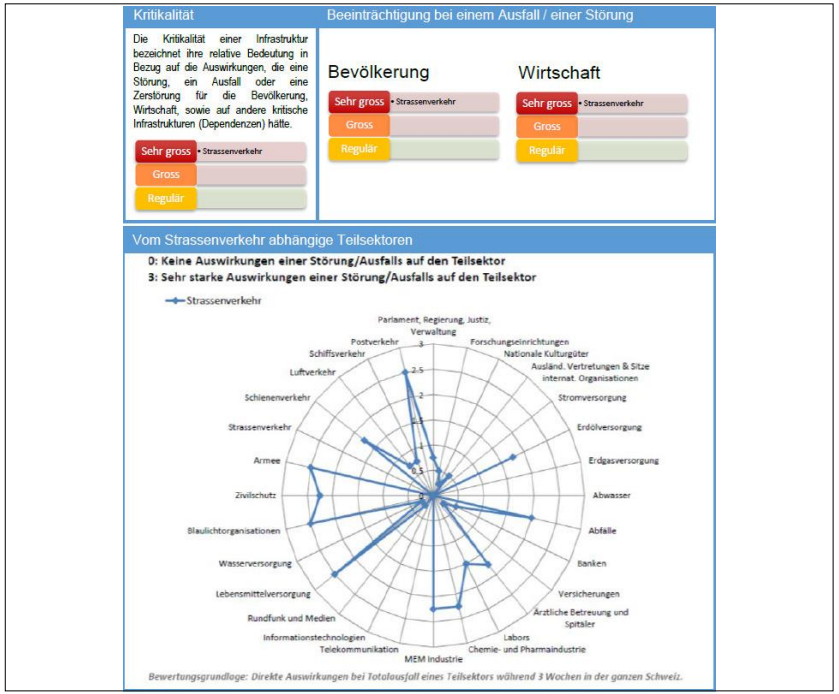
- Mehrere unterschiedliche Stakeholder
- Datenhoheit der Stakeholder
- Externe Anbindungen und Inter-Device-Verbindungen
- Cyber-Bedrohungen für Geräte und Umfeld
- Gefahren für **Verfügbarkeit** und **Integrität** (Vertraulichkeit)

Cyber-Kriminelle suchen den einfachsten Zugang, um an «Ihre Daten» oder «Ihren Prozess» zu kommen.

Sicherheitsstrategie im Zeitalter von IoT

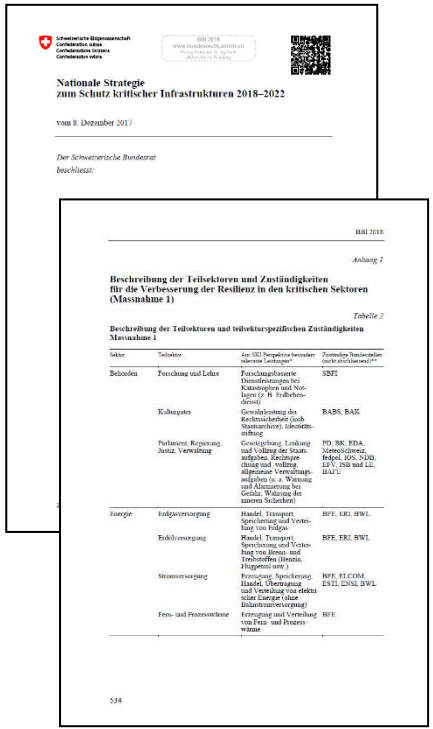
Kritikalität von Schiene und Strasse





Source: BASP Bundesamt für Bevölkerungsschutz

IoT Security im Tunnel – gibt es Vorgaben?



IEC 62443:
Nützlicher Leitfaden für (I)OT-Security

General	**IEC 62443-1-1** Terminology, concepts and models	**IEC 62443-1-2** Master glossary of terms and abbreviations	**IEC 62443-1-3** System security compliance metrics	**IEC 62443-1-4** IACS security lifecycle and use-case
Policies & procedures	**IEC 62443-2-1** Requirements for an IACS security mgmt. system	**IEC 62443-2-2** Implementation guidance for an IACS security mgmt. system	**IEC 62443-2-3** Patch mgmt. in the IACS environment	**IEC 62443-2-4** Installation and maintenance requirem. for IACS suppliers
System	**IEC 62443-3-1** Security technologies for IACS	**IEC 62443-3-2** Security levels for zones and conduits	**IEC 62443-3-3** System security requirements and security levels	
Component	**IEC 62443-4-1** Product development requirements	**IEC 62443-1-2** Technical security requirements for IACS components		

IEC 62443 ermöglicht langfristige Orientierung und Planung

Based on IEC 62443-3-3

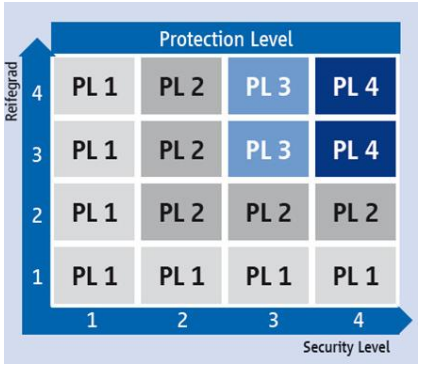
Assessment of security functionalities

SL 1	Capability to protect against casual or coincidental violation
SL 2	Capability to protect against intentional violation using simple means with low resources, generic skills and low motivation
SL 3	Capability to protect against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 4	Capability to protect against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Based on IEC 62443-2-1 and -2-4

Assessment of security processes

ML 1	**Initial** – Process unpredictable, poorly controlled and reactive
ML 2	**Managed** – Process characterized, reactive
ML 3	**Defined** – Process characterized, proactive deployment
ML 4	**Optimized** – Process measured, controlled and continuously improved



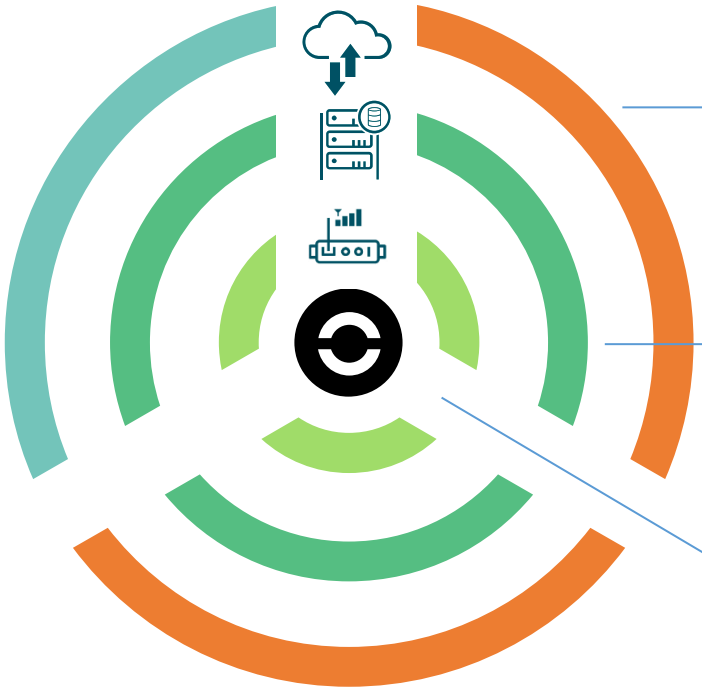
Source: ZVEI

IEC 62443 als Grundlage für die Security-Strategie

SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)					
SR 1.1 – Human user identification and authentication	5.3	✓	✓	✓	✓
SR 1.1 RE 1 – Unique identification and authentication	5.3.3.1		✓	✓	✓
SR 1.1 RE 2 – Multifactor authentication for untrusted networks	5.3.3.2			✓	✓
SR 1.1 RE 3 – Multifactor authentication for all networks	5.3.3.3				✓
SR 1.2 – Software process and device identification and authentication	5.4		✓	✓	✓
SR 1.2 RE 1 – Unique identification and authentication	5.4.3.1			✓	✓
SR 1.3 – Account management	5.5	✓	✓	✓	✓
SR 1.3 RE 1 – Unified account management	5.5.3.1			✓	✓
SR 1.4 – Identifier management	5.6	✓	✓	✓	✓
SR 1.5 – Authenticator management	5.7	✓	✓	✓	✓
SR 1.5 RE 1 – Hardware security for software process identity credentials	5.7.3.1			✓	✓
SR 1.6 – Wireless access management	5.8	✓	✓	✓	✓
SR 1.6 RE 1 – Unique identification and authentication	5.8.3.1		✓	✓	✓
SR 1.7 – Strength of password-based authentication	5.9	✓	✓	✓	✓
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users	5.9.3.1			✓	✓

Beispielmassnahmen zur IoT-Systemhärtung

Holistic Security with Defence in Depth



Sicherer Betrieb

Sichere Integration

Sichere Produkte

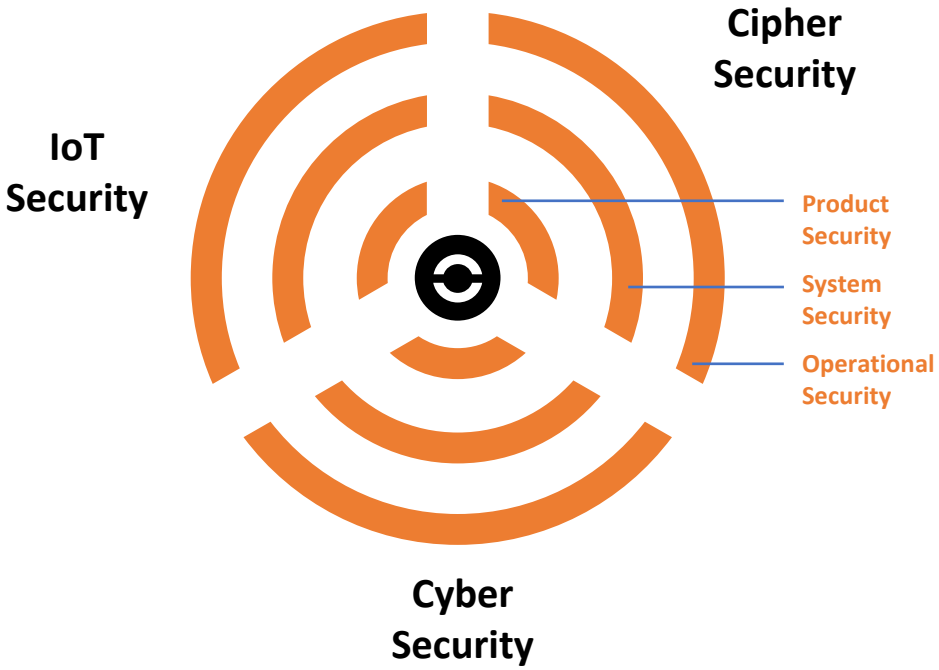
Policies & procedures	**IEC 62443-2-1 & 2-4**	Requirements for an IACS security mgmt. system
System	**IEC 62443-3-3**	System security requirements and security levels
Component	**IEC 62443-4-1**	Product development requirements

Product Security by Design

Sichere Produkte / Product Security by Design

- Integration von hardwarebasierten Sicherheitsfunktionen
- Software-Integrität / Secure Boot-Mechanismen
- Resistente Kryptografie inkl. Key-Management
- Tamper Protection
- Trusted Plattform & Sichere Supply Chain
- Datentrennung und Verschlüsselung
- Sichere Schnittstellen
- Monitoring und Updatefähigkeit
- Validierungsmöglichkeiten von Software Features und Updates

Smarte 360°-Sicherheitskonzepte und -lösungen von CyOne Security



•Sichere Schweiz.
Bit für Bit.

Vielen Dank für Ihre Aufmerksamkeit!

Reto Amstad
Senior Security Consultant
reto.amstad@cyone.ch

Telefon +41 79 723 18 41

Mehr zu unseren
IoT Security Solutions

cyone.ch

BLOG Cyber Security

BLOG IoT Security

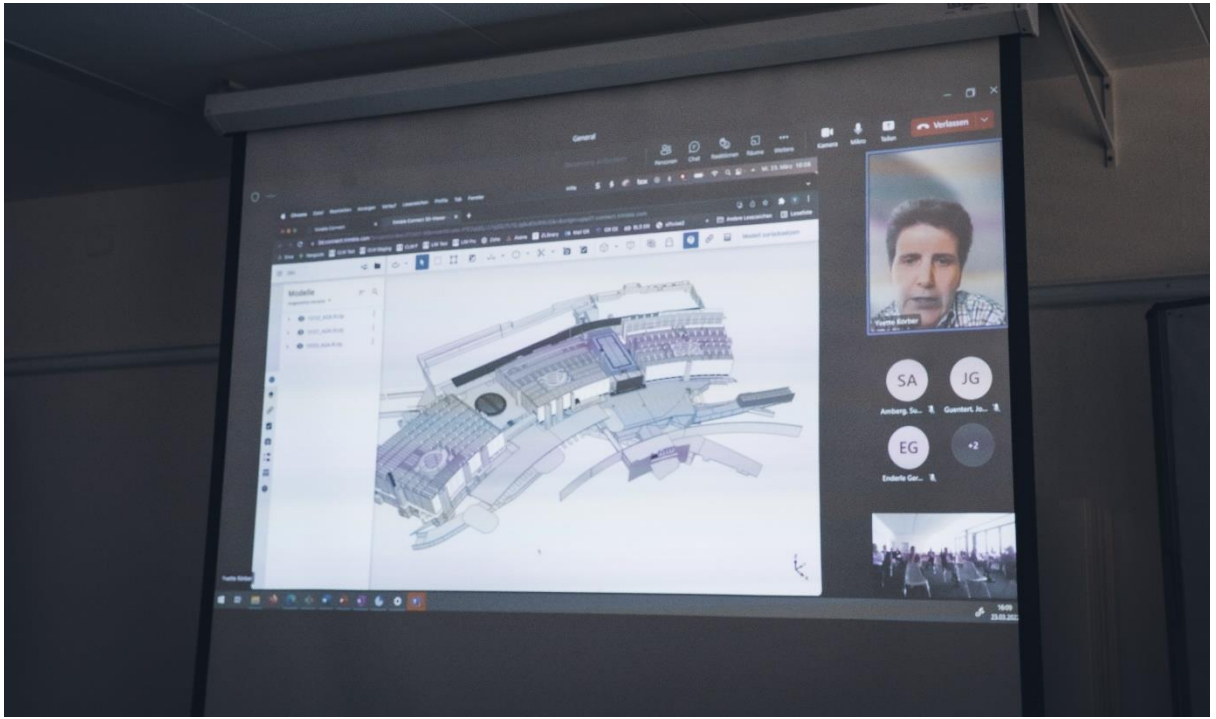
Digitale Sicherheit am Bau

Yvette Körber

CEO, Amberg Loglay AG

SCAUT
Swiss Center of Applied Underground Technologies

Vortrag war nicht in PPT Format



SCAUT
Swiss Center of Applied Underground Technologies

Zusammenfassung & Ausblick

Veronika Petschen

Geschäftsführerin, SCAUT Förderverein

SCAUT
Swiss Center of Applied Underground Technologies

SCAUT Technology projects

Tunnel Digitalization Center

Project ideas

Underground Energy Solutions – 2. Roundtable 19.Mai 2022, ETH Zürich

- Potentials of underground energy generation & storage (UES)? Which are the possibilities of CO_2 capture and storage in combination of hydrogen?
- What are the key factors to be considered?
- Which are the low hanging fruits?
- How could we collaborate?

SCAUT
Swiss Center of Applied Underground Technologies

Rundgang durch die Dätwylerwerke und Apéro

www.scaut-association.com
vpetschen@scaut-association.com

SCAUT
Swiss Center of Applied Underground Technologies