VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Fachtagung OT Cybersecurity Sicherungsanlagen

Referate und gemeinsamer Erfahrungsaustausch

25. Juni 2025 in Bern

Willkommensgruss

Jörg Jungblut
Leiter Informationssicherheit SBB

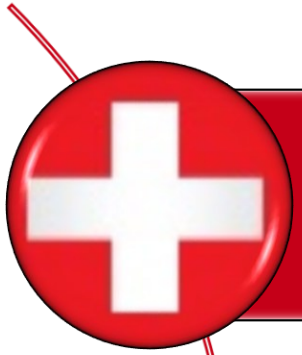
Informations- und Cybersicherheit

Weil **sichere & zuverlässige** Verbindungen die Schweiz ausmachen.

Cyber Security – Treiber und Gesetzeslage.

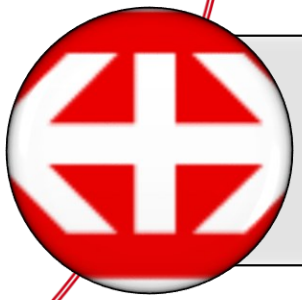
Nationale, internationale und eigene Vorgaben bilden den Rahmen.

Sicherheit



- **Schweizer Gesetzgebung**: Eisenbahngesetz (EBG)+ Verordnungen, Datenschutzgesetz (DSG) + Verordnungen, BAV Vorgaben + Richtlinie Cybersecurity Eisenbahn, Fahrdienstvorschriften, etc.
- **Europäische Gesetzgebung**: Cyber Resilience Act (CRA) incl. EU CE Conformity Requirements, Richtlinie Cybersicherheitsniveau (NIS2), EU-Datenschutzgesetzgebung (GDPR) und weitere

- **ISO/IEC 27001**: Informationssicherheit-Management System, NIST Cybersecurity Framework
- **IEC 62443**, **IEC 63452** (früher: TS50701): Sicherheit für OT
- EU-Rail: **System Pillar Cybersecurity Specifications** für Bahnbetreiber und Hersteller, inkl. TSI Spezifiikation und ERTMS.



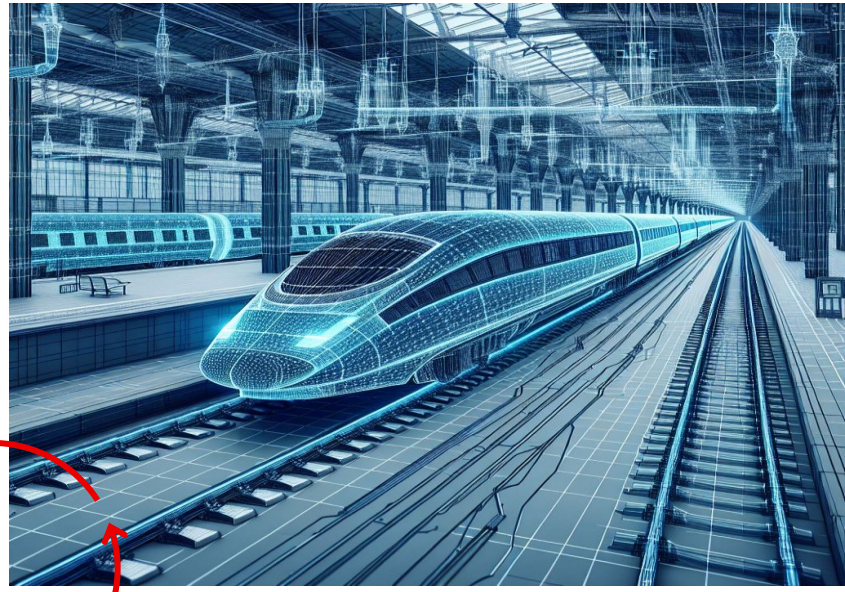
- Aufträge des **Verwaltungsrates**, des Eigners: Erwartungshaltung Sicherheit
- **Internes Recht**: etabliertes (Information) Security Policy Framework
- Etabliertes **Control Framework** zur Prüfung der Einhaltung
- **Messkriterien** und stufengerechtes **Berichtswesen**

Eine integrierte Bahn braucht eine integrierte Sicherheit

Viele zukünftige Herausforderungen können nur gemeinsam gemeistert werden.

Überall höherer Kapazitätsbedarf

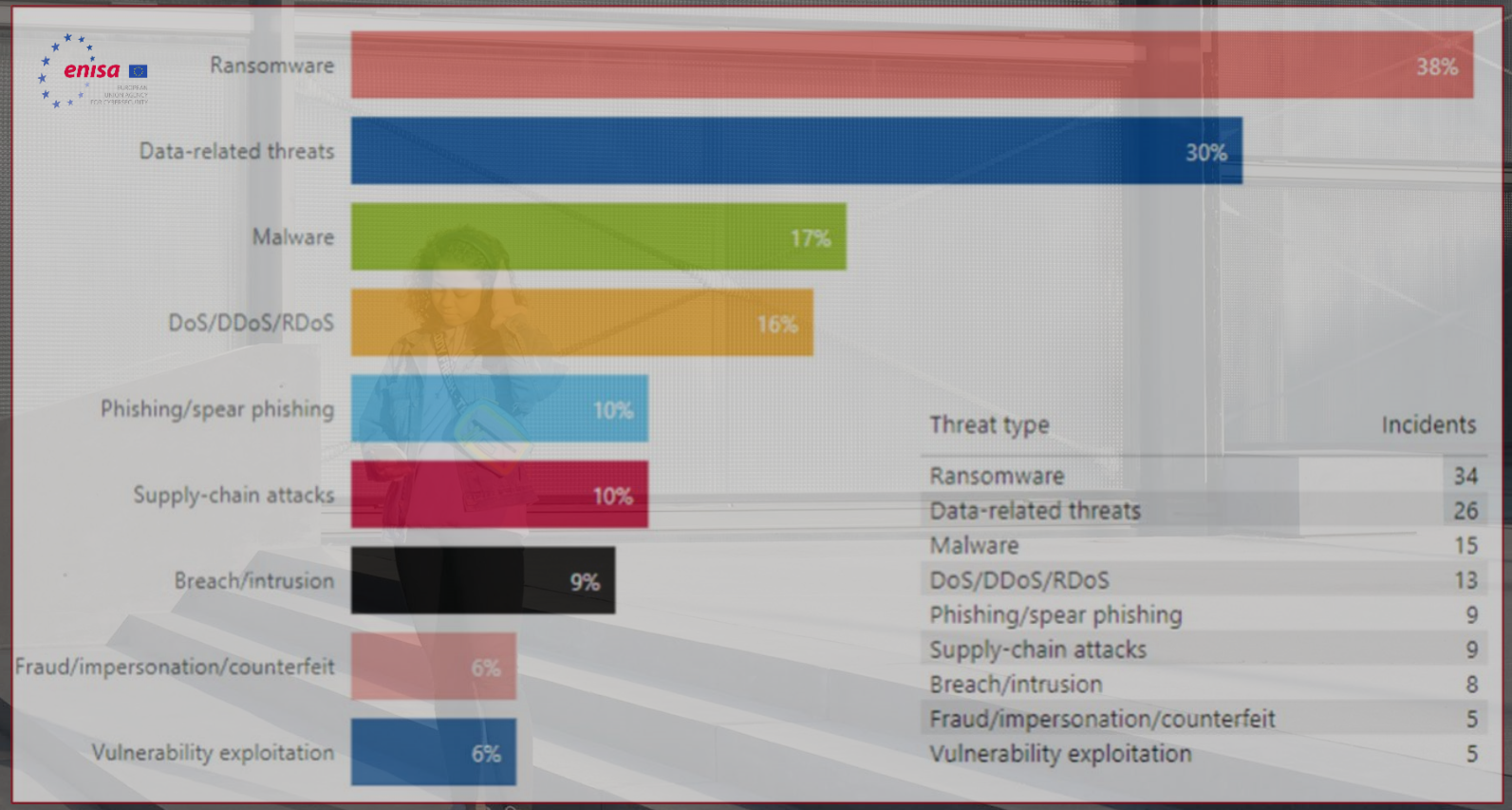
Mangelnde Aufmerksamkeit/Ablenkung/ Überforderung



Digitalisierung / Vernetzung nimmt weiter zu

Cyber-Bedrohungslage international / national für den Sektor Transport.

Cyberkriminelle sind für die meisten Angriffe auf den Verkehrssektor ver-antwortlich (54%). Sie zielen auf alle Teilsektoren (Flug, Strasse, Schiff-fahrt und Bahn) gleichermassen ab.



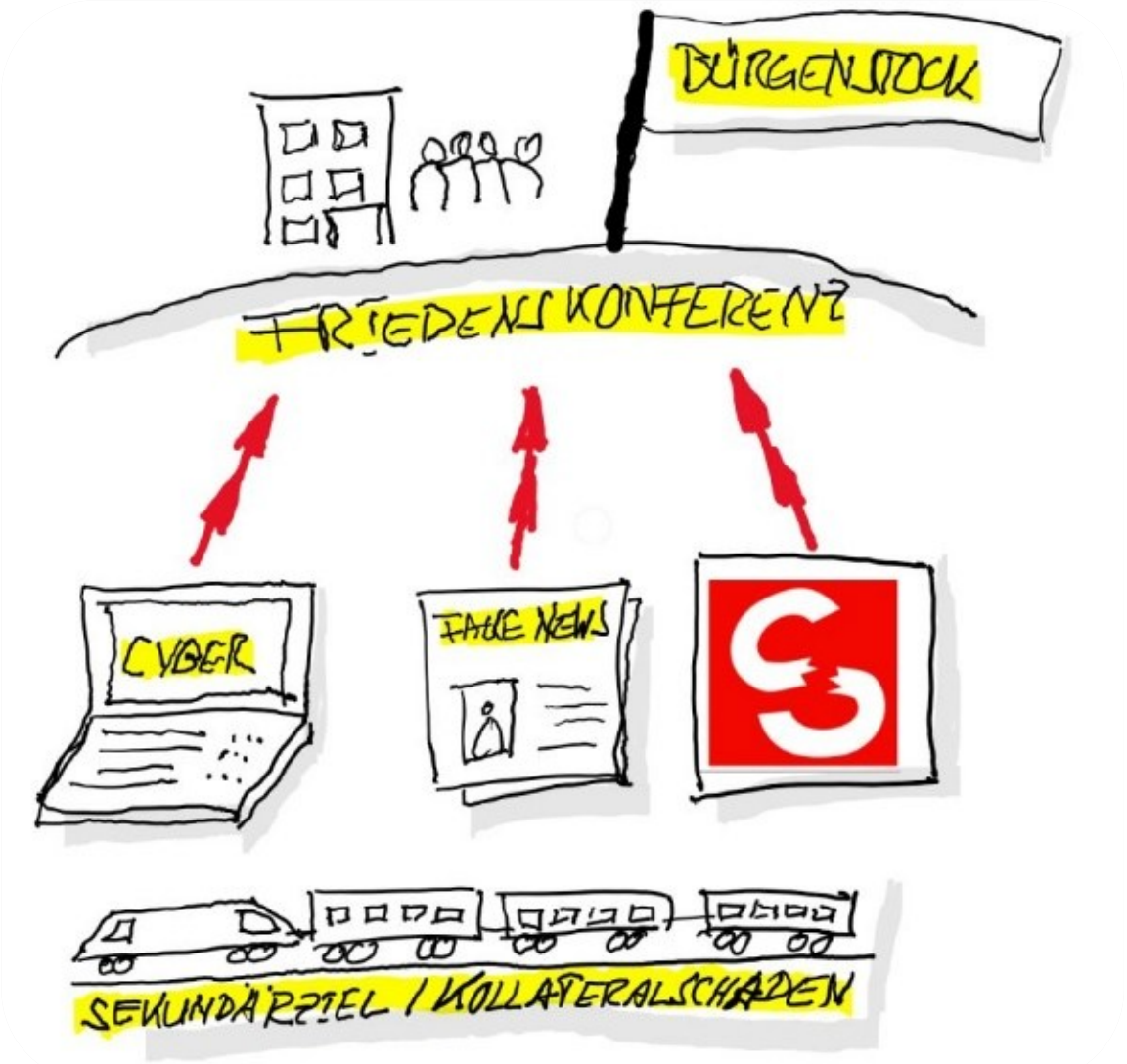
Threat type	Incidents
Ransomware	34
Data-related threats	26
Malware	15
DoS/DDoS/RDoS	13
Phishing/spear phishing	9
Supply-chain attacks	9
Breach/intrusion	8
Fraud/impersonation/counterfeit	5
Vulnerability exploitation	5

Aus dem ENISA-Bedrohungslagebericht des Verkehrssektor vom März 2023

Grosse Events lösen Unsicherheit aus

am Beispiel:

Friedenskonferenz von 15./16. Juni 2024 auf dem Bürgenstock



Unsere gemeinsame Mission: Stärkung System Bahn

Die zunehmende digitale Vernetzung, wachsende technologische Abhängigkeiten, komplexe Wertschöpfungsketten und sich wandelnde Bedrohungslage stellen uns vor neue Herausforderungen. Es fehlt noch immer an robusten Prozessen, Systemen und Anlagen.

Eine durchgängige Einbindung sicherheitsrelevanter Aspekte in zentrale Vorhaben (Projekte/ Programme) ist notwendig, um die **angestrebte Resilienz im System Bahn** zu erreichen.

Es braucht vor allem **gemeinsame Ansätze**, **gemeinsame Lösungen** und ein **bezahlbares, nachhaltiges Sicherheitsniveau** in der gesamten Branche in der Schweiz und an den Schnittstellen zum angrenzenden Ausland.

Spannende Einsichten und gute Gespräche heute!

Herzlich willkommen

Tagungsleitung und Organisation

- Tobias Hubschmid, BAV
- Daniela Nowak, SBB AG
- Marcel Schmid, VöV
- Andreas Studer, BAV

Übersetzung

- François Fellay

Referenten

- Stephan Berger, BLS AG
- Flavio Ferrari, SBB AG
- Andreas Haas, Swissrail Industry Association
- Björn Lenggenhager, SOB
- Reto Inversini, SBB AG
- Jörg Jungblut, SBB AG
- Mauro Montani, SBB AG
- Nicolas Murbach, MOB

Programm Vormittag

09:00 **Begrüssung und Tagungsablauf**
Daniela Nowak, SBB und Tobias Hubschmid, BAV

09:15 **Zwischen IT und OT: Cybersecurity bei der BLS**
Stefan Berger, BLS

09:40 **Cybersecurity aus Sicht Meterspurbahn / Westschweiz**
Nicolas Murbach, MOB

10:05 **Herausforderungen Vulnerability Management**
Björn Lenggenhager, SOB

10:30 **OT-Security SBB – Fokus Sicherungsanlagen**
Flavio Ferrari und Mauro Montani, SBB

11:00 Pause

11:25 **Rail ISAC**
Reto Inversini, SBB

11:50 **CyberSec, Verantwortung der Industrie, Positionspapier**
Andreas Haas, Swissrail

12:15 **Auftrag Workshops**
Daniela Nowak, SBB

12:30 Mittagessen

Programm Nachmittag für ordentliche VöV-Mitglieder

13:45 **Workshops**
Erfahrungsaustausch Cybersecurity
Sicherungsanlagen zu verschiedenen Themen

14:50 Pause

15:10 **Präsentation Workshop Ergebnisse**

15:40 **Info VöV und Abschluss**
Daniela Nowak, SBB
Marcel Schmid, VöV

16:00 **Ende der Tagung**

Fragen

Zwischen IT und OT: Cyber Security bei der BLS

Stephan Berger
CISO BLS AG

Über mich

- Stephan Berger
- Jahrgang 1973
- Seit Juli 2019: CISO BLS AG
- 25 Jahre als Security Officer und Security Consultant
- Background: System Engineer
- Hobby: Retro Computing (hilfreich für OT)

Über mich

- Stephan Berger
- Jahrgang 1973
- Seit Juli 2019: CISO BLS AG
- 25 Jahre als Security Officer und Security Consultant
- Vorher: System Engineer
- Hobby: Retro Computing (hilfreich für OT)

Home / News / Hardware

NEWS

Commodore Amiga steuert seit 30 Jahren die Klimaanlage in der Schule

Er läuft Tag und Nacht und steuert seit 30 Jahren die Heizung und Klimaanlage von 19 Schulen: dieser alter Commodore Amiga ist immer noch im (öffentlichen) Dienst.

Von Benjamin Schischka
Autor, PC-WELT | 15.6.2015 13:37 UHR

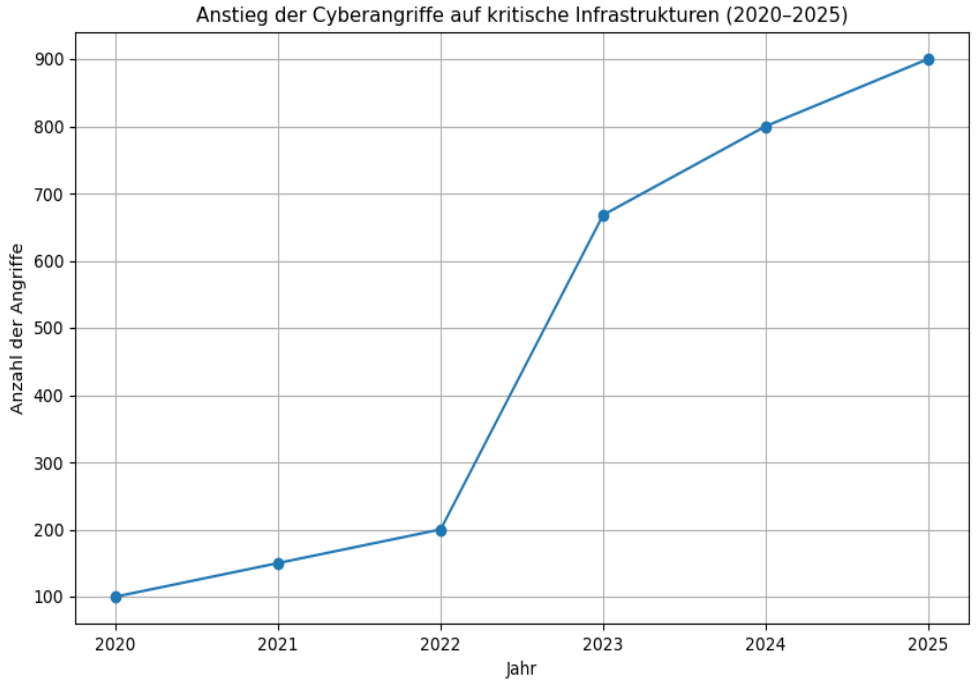
Image: IDG

Disclaimer

Einige Inhalte dieser Präsentation basieren auf meinen persönlichen Einschätzungen und Erfahrungen. Sie spiegeln nicht zwangsläufig die Meinung anderer Personen oder Organisationen wider.

Zunahme der Cyberangriffe auf kritische Infrastrukturen (2020–2025)

Die Anzahl der Cyberangriffe auf kritische Infrastrukturen ist zwischen 2022 und 2024 um 668% gestiegen.



Sources: Forescout Threat Roundup 2024, BSI Lagebericht 2023

Rückblick

Rückblick

2019 wurde in der BLS die Stelle des CISO neu geschaffen:

- *CISO: «Wenn wir nichts unternehmen, liegt die Wahrscheinlichkeit für einen betriebsverhindernden Cybervorfall in den nächsten 2 Jahren bei etwa 100%»*

  VR: «Sind wir denn nicht ISO27001-zerztifiziert?»

- *CFO: «Bevor wir viel Geld für Massnahmen ausgeben, sollten wir unseren Risikoappetit kennen, wir sind ja schliesslich keine Bank»*

  CISO: «Ohne die vorgeschlagenen Massnahmen können wir unsere Risiken gar nicht ermitteln und erst recht den Risikoappetit nicht bestimmen.»

Rückblick

- 2020: VR erlässt Informationssicherheitspolitik
- 2021: GL setzt Weisung über die Informationssicherheit in Kraft
- 2021-2023: Vulnerablity Scanner, Endpoint Protection, Server und Client Hardening, Active Directory Tiering, ISMS-Konzept
- 2023: Team für operative Cyber Security, Aufbau Sicherheitsorganisation in den Bereichen
- 2024 Beginn Onboarding OT Infrastruktur und Fahrzeuge zusammen mit ISB und EVUs der BLS AG

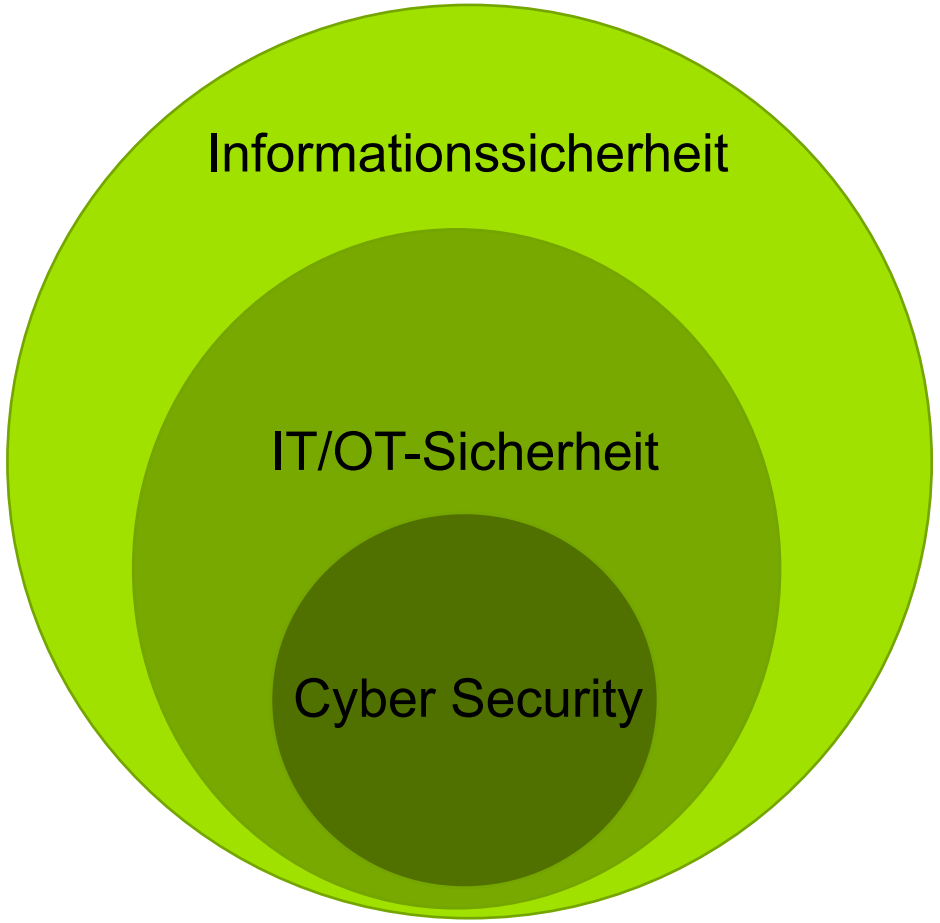
Wo stehen wir aktuell?

- Informationssicherheit und Cyber Security haben Top-Priorität bei VR und GL
- Die Resilienz der IT-Systeme gegen Cyberangriffe wurde signifikant verbessert (*CISO schläft inzwischen relativ ruhig*)
- Aufbau ISMS und OT-Security schreitet kontinuierlich voran, es gibt allerdings noch viel zu tun
- Aus Sicht des (ungeduldigen) CISO dürfte selbstverständlich alles deutlich schneller gehen!

Von IT und OT

Begrifflichkeiten

- **Cyber Security** ist inhaltlich praktisch identisch zur IT/OT-Security, tönt einfach besser
- Gibt's eigentlich schon seit Jahrzehnten, ähnlich wie die Digitalisierung
- Buzzword (#cyber, #blockchain #AI)
- Vorteil: Man muss nicht zwingend etwas von IT/OT-Security verstehen, um mitreden zu können
- Nachteil: Es reden viele mit, die wenig von IT/OT-Security verstehen



Begrifflichkeiten

IT: Die Kunst, eilig entwickelten und oft unzureichend getesteten Bastelkram so lange am Laufen zu halten, bis der Kunde ihn unfreiwillig in der Produktion getestet hat

OT: Der Bereich, in dem genau dieser Bastelkram plötzlich Steuerbefehle an Anlagen überträgt, von deren fehlerfreiem Betrieb Menschenleben, Umwelt und Produktionssicherheit abhängen und in dem „Trial and Error“ keine Option ist

OT-Spezialisten zu Cyber Security

OT-Spezialisten zum Thema Patch Management

«Ich bin mir nicht sicher, ob es sich noch lohnt, diese Security Patches einzuspielen, die betroffene Fahrzeugflotte ist ja nur noch 15 Jahre im Einsatz.»

Fünf häufige Fehlannahmen von Cyber Security-Spezialisten zum Thema OT Security

1. „OT ist wie IT – wir können dieselben Sicherheitslösungen anwenden.“
2. „Unsere Security-Tools verursachen keine Nebeneffekte“
3. „Man kann alles überwachen – man muss nur Sensoren und Logs aktivieren“
4. „Die Mitarbeitenden in der OT verstehen Security-Prozesse“
5. „Veraltete Software muss aktualisiert, veraltete Systeme müssen ersetzt werden“

Fünf häufige Fehlannahmen von OT-Spezialisten zum Thema Cyber Security

1. „Unsere Systeme sind sicher, weil sie alt oder proprietär sind“
2. «Wir brauchen Safety, nicht Security»
3. „Cyber Security ist Aufgabe der IT“
4. „Wir sind ja nicht am Internet und haben eine Firewall, also sind wir sicher“
5. „Unsere Systeme sind zertifiziert und daher sicher“

Risk Management

Cyber Security Risk Manager

Risk Manager bei der Eisenbahn

Risk Management

In der Cyber Security ist die Quantifizierung von Risiken problematisch, denn

- Es fehlen belastbare Wahrscheinlichkeiten und historische, verlässliche Eintrittsdaten (Im Gegensatz z.B. zu Safety-Risiken in der Bahnwelt)
- Angriffe sind dynamisch, zielgerichtet und verändern sich ständig. Anders als bei mechanischen Fehlern passen sich Angreifer aktiv an.
- Neue Schwachstellen entstehen täglich (Zero Days, Supply Chain, Social Engineering)
- Cyberrisiken sind daher nicht zufallsbasiert, sondern strategisch und böswillig.
- Schaden ist schwer quantifizierbar, da die Auswirkungen eines Cyberangriffs oft von vielen Faktoren abhängen: Reaktionszeit, Ausbreitung, Imageverlust, regulatorische Folgen usw.
- In vernetzten IT/OT-Systemen ist meist unklar, wie sich ein Angriff ausbreitet oder was betroffen sein wird. Ein kleiner Fehler kann massive Dominoeffekte auslösen. Die Unsicherheit ist so hoch, dass präzise Modelle wenig Aussagekraft haben

Geeignet sind häufig qualitative Methoden, das Denken in Szenarien und vor allem: Kenntnis der Schwachstellen und der Angriffsoberfläche

Denkanstösse

Standards

- ISO 27001, IEC 62443, TC 50701 und wie sie alle heissen, sagen alle mehr oder weniger das Gleiche: Kenne deine Systeme, ermittle ihren Schutzbedarf, versuche Schwachstellen und Risiken in Erfahrung zu bringen und treffe Massnahmen, um diese in den Griff zu kriegen.
- Gefahr bei allen Standards: Viele Controls, Prozesse, Dokumentation und Brimborium überfordern die Organisation und erzeugen nicht selten wirkungsfreien Overhead. Daher bei der Umsetzung unbedingt skalieren!
- Ich kann vortrefflich ISMS betreiben und Risiken managen, ohne jemals ein IT oder OT-System sicherer machen zu müssen. Vermutlich kriege ich sogar ein Zertifikat dafür.
- Ein ISO 27001-Zertifikat verhindert keinen Cyberangriff. Gut gepatchte Endgeräte allerdings schon!

Vulnerability- vor Risk Management

- Für die Detektion der Schwachstellen und Verwundbarkeiten in meinen Systemen brauch ich keine Glaskugel, es reichen geeignete Werkzeuge. Zudem ist das Common Vulnerability Scoring System (CVSS) ein guter Indikator für die Kritikalität
- CVSS-Score und eine Bewertung der Angriffsoberfläche geben ein viel präziseres Bild, als Eintretenswahrscheinlichkeit x Schadenhöhe
- Keine Schwachstelle, kein Risiko: Risk Management benötige ich dann, wenn ich die Schwachstelle nicht beseitigen kann (z.B. für IT-Systgeme, deren Lieferanten über keinerlei Patch Management-Prozsse verfügen, auch dann nicht, wenn die Systeme nicht Safety-kritisch sind)
- Es lassen sich viel mehr OT- und insbesondere OT-nahe IT-Systeme regelmässig patchen als man meint!

Security Monitoring

- Die meisten Cyber-Angriffe kann man mit passender Ausrüstung rechtzeitig detektieren und unterbinden
- Ein gut konfiguriertes EDR (Endpoint Detection and Response)-System ist Pflicht
- Ebenso ein zentrales Logging oder SIEM (Security Information and Event Management), für mindestens Entra ID und Active Directory, DNS, Proxy, Firewalls und andere Netzübergänge
- Sinnvolle Alerts definieren: Ein EDR oder SIEM-System, das bei jeder Regung einen Alarm auslöst, ist kontraproduktiv
- Prozesse für Standard-Incidents: In der BLS verlieren wir trotz 2FA immer wieder User Accounts durch Phishing, entsprechend lohnt es sich, einen passsenden Incident Response-Prozess zu definieren

Sichere Endgeräte

- Fast alle Cyberangriffe erfolgen über die Clients der Benutzer:innen. Es lohnt sich daher, diese angemessen zu schützen
- Hardening: Abschaltung unsicherer Uralt-Protokolle (z.B: NTLM, und SMBv1), Aktivierung der Sicherheitsfunktionen aus dem Lieferumfang der Betriebssysteme (bei Windows: AppLocker, BitLocker, Crendential Guard, usw.), Umsetzen der Empfehlungen aus dem EDR-Tool
- Always-On-VPN, resp. Policy Enforcement Point: Internetzugriff über einen zentralen Proxy mit der Fähigkeit, TLS zu unterbrechen. Nur so kann die Kommunikation mit bösartigen URLs erkannt und unterbunden werden
- Wenn immer möglich passwortlose Authentisierung (Windows Hello, Security Token, Passkey, etc.)
- Automatische Einbindung von IOC (Indicators of Compromise)-Feeds, z.B. von unseren Freunden vom Rail ISAC (unbedingte Empfehlung!)
- Patchen, patchen und nochmals patchen!

Von möglichst realistischen Szenarien ausgehen

Wir können unsere Umgebungen nicht gegen alle Eventualitäten schützen, es lohnt sich daher die realistischsten Szenarien zu priorisieren.

- Ransomware ist in erster Linie ein Windows- und Active Directory-Problem. Linux-Systeme sind dabei lediglich als «Target of Opportunity» betroffen, wenn sie schlecht gepatcht sind
- OT-Umgebungen (hoffentlich ohne Active Directory ☺) müssen daher eher vor gezieltem Hacking und Supply Chain Attacks geschützt werden, da sich in der OT viele «Targets of Opportunity» (resp. schlechte gepatchte Systeme) befinden
- Der Zugang zur OT-Welt muss unbedingt von vertrauenswürdigen Endgeräten aus erfolgen (kein BYOD und schon gar nicht der alte Windows XP-Laptop von daheim!)
- Augenmerk auf die Lieferantenzugänge: Lieferanten mit teilweise geringem Bewusstsein für die Cyber Security verbinden sich über nicht vertrauenswürdige Endgeräte und ungemanagte Zugänge direkt mit schlecht gepatchten OT-Systemen

Last but not least: Wir alle müssen zusammen reden!

Cyber Security geht nur als Teamwork:

Ein offener Austausch auf Augenhöhe zwischen uns allen, IT, OT, Lieferanten und Behörden ist zwingend!

Ohne Cyber Security keine Safety!

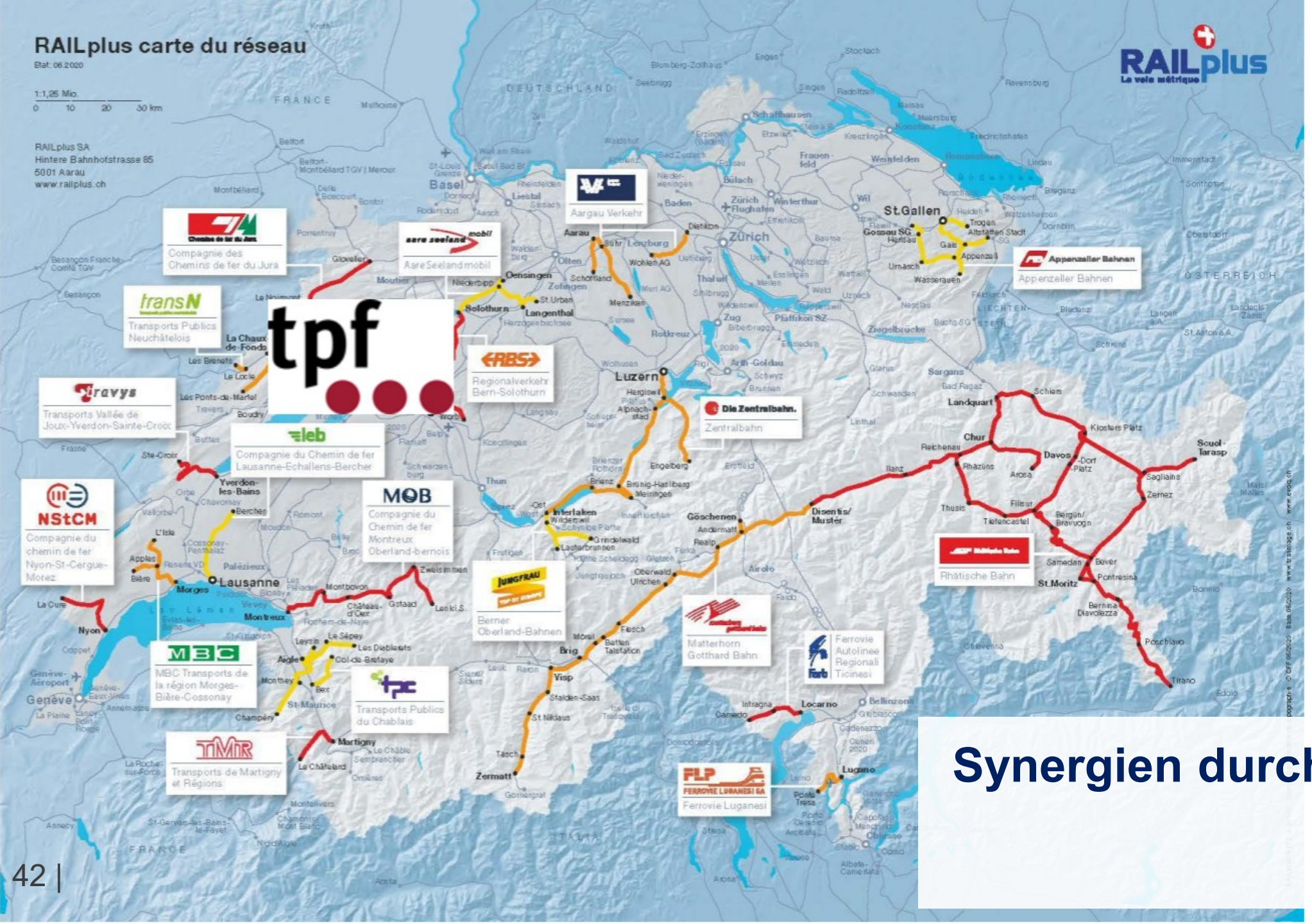
Fragen und Antworten?


bls
Vielen Dank!

Cybersecurity aus Sicht Meterspurbahn / Westschweiz

Fachtagung OT Cybersecurity für Sicherungsanlagen
25.06.2025

Nicolas Murbach / MOB



Synergien durch Railplus

Präsentation

- Die 21 Meterspurbahnen der Schweiz sind unter Railplus zusammengefasst.
- Ziel von Railplus ist es, für die beteiligten Bahnen über verschiedene Arbeitsgruppen Synergien zu schaffen.
- Die Grösse der beteiligten Unternehmen variiert stark (~100 bis 2000 Angestellte).
- Die einzelnen Bahnen bleiben selbstständig und verantwortlich.

Kompetenzzentrum Cybersicherheit

- Das Thema Cybersicherheit ist für Railplus nicht neu.
- 2020 wurde ein Kompetenzzentrum für Cybersicherheit gegründet. Wird werden dabei von einem auf Cybersecurity spezialisierten externen Partner begleitet.
- Ziel:
  - Förderung des Bewusstseins für Cybersicherheit und der sicheren Digitalisierung der Meterspurbahnen durch Beratung, Unterstützung und Austausch zu zentralen Themen der Cybersicherheit.
- Die Maturität und die verfügbaren Ressourcen (insbesondere finanzielle und personelle) sind sehr unterschiedlich.
- Jede Eisenbahn ist für die Umsetzung der Empfehlungen zuständig und bleibt für ihre Cybersicherheit verantwortlich.

Beispiele für von Railplus vorgeschlagene Massnahmen

- Fokus auf Sicherungsanlagen
  - Bewertung der Cyber-Maturität im Bereich OT
  - Empfehlung für eine bessere Verwaltung der Fernzugriffe
  - Vertragsklauseln für die Beziehung zu den Lieferanten
  - Die wichtigsten Schritte zur Erkennung von IT und OT
  - Sicherheitsempfehlungen für den Bereich OT
  - Organisation einer Cyber-Krisenübung für einen Vorfall, der die Sicherungsanlagen betrifft
  - Begleitung bei der Einführung eines ISMS
  - Stellungnahmen zu verschiedenen Themen
  - Dokument zur Beschreibung der Cybersicherheitsmassnahmen im Rahmen der PGV-Unterlagen
  - Lieferanten-Audit

- Die Cyber-Arbeitsgruppe von Railplus hat ausserdem gemeinsam mit Swissrail ein Dokument erstellt, um die Einhaltung von «Mindeststandards» in der Branche zu fördern, insbesondere im Bereich der Auditrechte.

Zusammenfassung

- Insgesamt lässt sich feststellen, dass auf technischer Seite bereits einiges vorhanden war, doch auf Ebene der Governance wurde nur wenig umgesetzt.
- Die Arbeit der vergangenen fünf Jahre hat den Bahnen und ihrem Management bewusst gemacht, dass Cybersicherheit nicht nur die IT betrifft.
- Jeder hat sein eigenes Tempo, und wir tauschen unsere Erfahrungen aus.
- Die Einführung der CySec Rail kam für die Eisenbahnen nicht überraschend, auch wenn noch viel zu tun ist, um unsere Cyber-Maturität zu verbessern.

MOB

Erfahrungsaustausch

MOB

Zu einer integrierten Cybersicherheit

- Das Thema war neu, und die internen Mitarbeiter mussten davon überzeugt werden, dass Cybersicherheit nicht nur die IT betrifft.

- Ab 2023 begann eine echte Verbindung zwischen IT und OT zum Thema Cybersicherheit.

- Da es sich um ein sehr umfangreiches Thema handelt, mussten personelle und finanzielle Ressourcen freigesetzt werden, um voranzukommen.

- Das Thema Cybersicherheit konnte erstmals auch in die RPV-Angebote (Kantone) sowie in die Infrastruktur-Leistungsvereinbarung 2025–2028 aufgenommen werden.

- Die Konzepte werden zunächst auf IT-Seite getestet, bevor sie im Bereich OT oder RM angewendet werden, um Erfahrungen zu sammeln.

Hauptmeilensteine

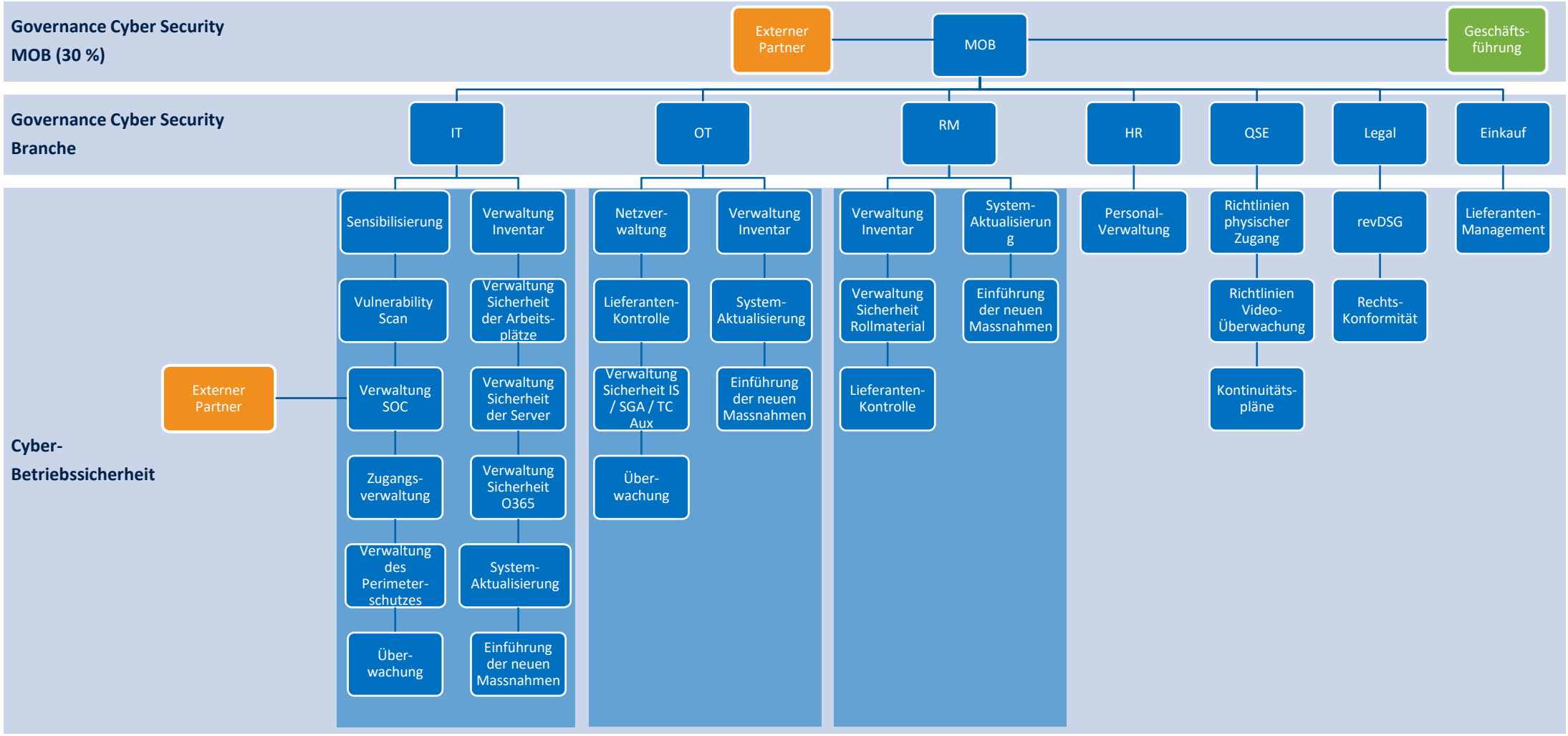
- 2023
  - Aktualisierung der Cyber-Maturität IT, OT
  - Analyse der Cyberrisiken für alle Unternehmensprozesse
  - Festlegung einer Roadmap mit Massnahmen für 2024–2027
  - Festlegung einer Organisation

- 2024
  - Gutheissung der Organisation und der Ressourcen
  - Arbeit an den ersten Massnahmen
    - Erstellung von Richtlinien
    - Einführung einer gemeinsamen Inventarstruktur für IT, OT und RM
  - Aufnahme von Cyberrisiken in das IMS des Unternehmens
  - Integration des Rollmaterials im Ansatz
  - Risikobewertung mit den Prozessverantwortlichen des Unternehmens
  - Sensibilisierung der Mitarbeitenden
  - Start eines Projekts zum besseren Schutz der physischen Zugänge (z. B. IS-Räume)

Hauptmeilensteine

- 2025
  - Fortsetzung der Arbeit am gemeinsamen Inventar
  - Lieferanten-Management
    - Bewertung der Kritikalität der Lieferanten
    - Vertragsklauseln für neue Lieferanten
  - Bewertung der Kritikalität der Assets
  - Risikoanalyse kritischer Assets
  - Aufnahme der Cybersicherheit in die Projekte
  - Verbesserung der Überwachung des OT-Netzes
  - Integration Human Ressources
  - Reaktion auf Vorfälle

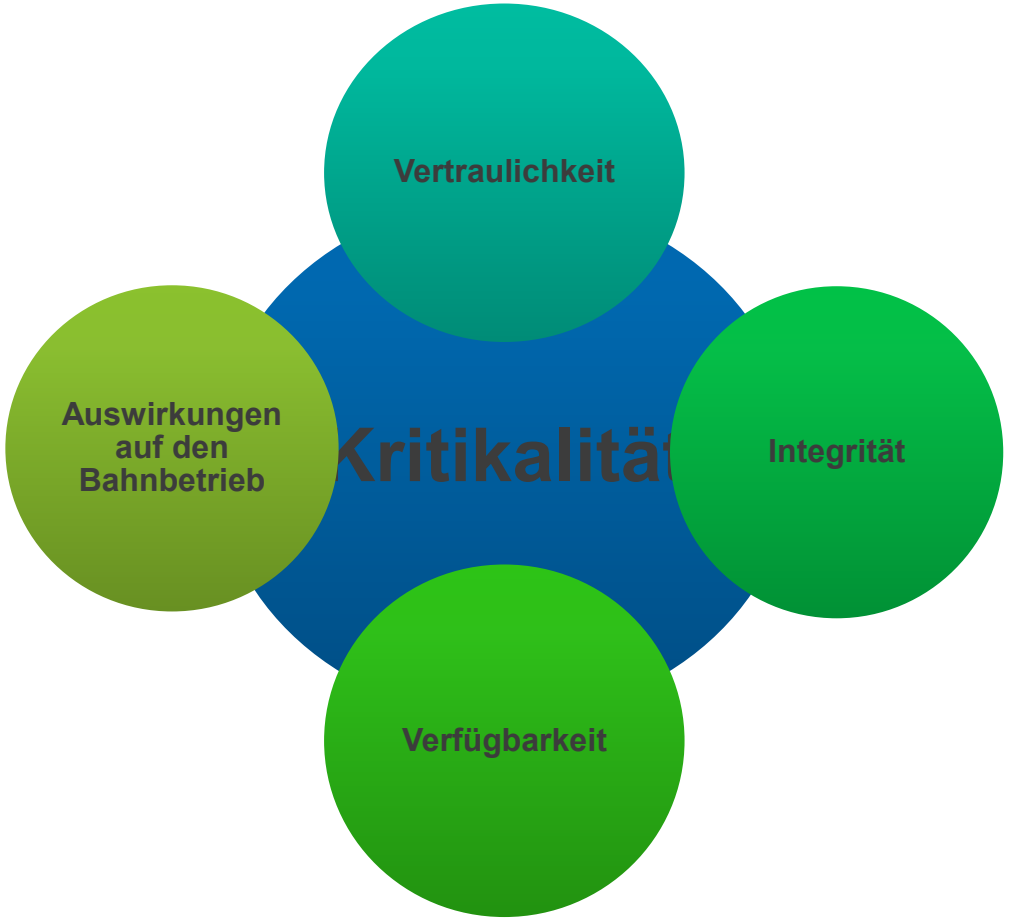
Cyber-Organisation



Herausforderung Inventar

- 3 verschiedene Tools → sofern möglich in einem einzigen Tool zusammenfassen
  - Keine Doppeleinträge → falsche Daten
- Geeignete Gliederungsebene festlegen
- Einführung eines neuen Tools für die Verwaltung der Infrastruktur-Wartung
  - OT-Geräte müssen in diesem Tool aufgeführt sein, da sie zu einer Kategorie von Anlagen gehören, die für den vom BAV angeforderten Netzzustandsbericht erforderlich sind.
- Die Tools, in denen sich das Inventar befindet, sind nicht für den Umgang mit Cyberrisiken konzipiert.

Kritikalität der Assets



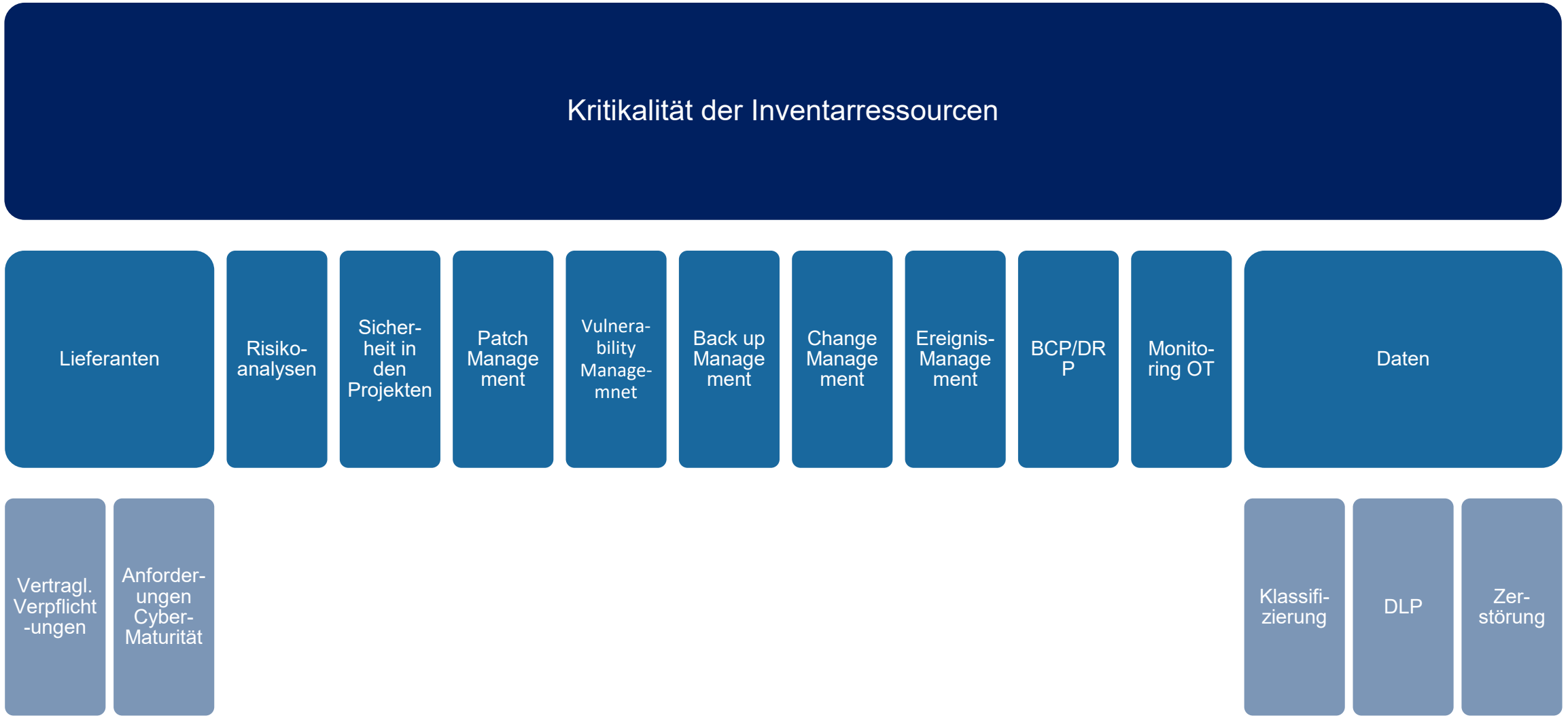
Kritikalität der Assets

		Bahnbetrieb
		Auswirkung des Systems auf den Bahnbetrieb bei einem Ausfall in den Bereichen Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit
sehr gering	**4**	Keine Auswirkung auf den Bahnbetrieb
gering	**3**	Indirekte Auswirkung auf den Bahnbetrieb, besonders bei anhaltenden Problemen
mittel	**2**	Direkter Einfluss auf den Bahnbetrieb
hoch	**1**	Unverzichtbar für den Bahnbetrieb

	Vertraulichkeit	Integrität	Verfügbarkeit	Kritikalität
IT-Asset	1 – hoch	1- hoch	2 – mittel	1 – hoch
OT-Asset	3 – gering	1 – hoch	1 – hoch	**2 - mittel**

	Vertraulichkeit	Integrität	Verfügbarkeit	Auswirkung Bahnbetrieb	Kritikalität
IT-Asset	1 – hoch	1- hoch	2 – mittel	3 – gering	**2 - mittel**
OT-Asset	3 – gering	1 – hoch	1 – hoch	1 – hoch	**1 – hoch**

Abhängigkeit der Kritikalität im SMSI



MOB

Cyber-Massnahmen für PGV-Unterlagen

- Beschreibung Cybersicherheit im Rahmen von PGV-Unterlagen
- Verwendung des von Railplus eingeführten Dossiers
- Mit dem Erscheinen des D RTE 28‘100 (insbesondere Kapitel 5 und 6) und durch verschiedene Gespräche mit dem BAV konnte das Ausfüllen des Dokuments vereinfacht werden.

Schlusswort

Die Cybersecurity-Bedürfnisse in Eisenbahnunternehmen werden weiter steigen.

- Man darf nicht aus den Augen verlieren, dass man nur das schützt, was man kennt
- Um Ressourcen und Massnahmen priorisieren zu können, muss man die Kritikalität der eigenen Assets kennen.
- Die Synergien und der Austausch zwischen Eisenbahnunternehmen müssen weiter gefördert werden, damit die ganze Branche Fortschritte erzielen kann.

SÜDOSTBAHN
gerade unterwegs

Herausforderungen Vulnerability Management

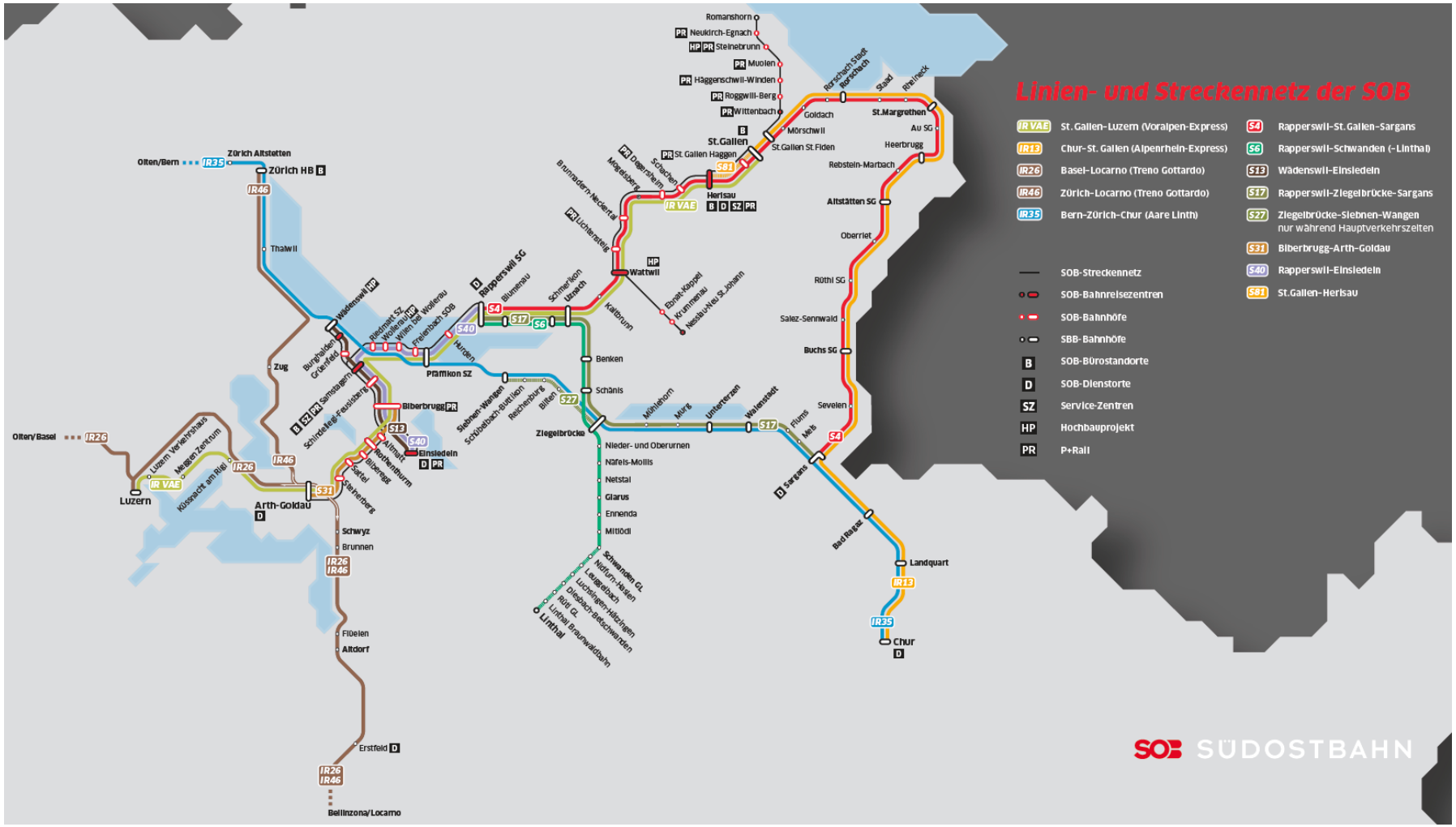
Fachtagung OT Cybersecurity SA
25. Juni 2025

Björn Lenggenhager
Technologie Manager Telecom

Agenda

- Vorstellung SOB
- Rückblick auf bisherige IT-Infrastruktur
- Entwicklung
- Massnahmen
- Menschliche Herausforderungen
- Technische Herausforderungen
- Learnings

Vorstellung SOB



SÜDOSTBAHN
gerade unterwegs

Rückblick auf bisherige IT-Infrastruktur

Rückblick auf bisherige IT-Infrastruktur

- Flaches Netzwerk
- Standorte lediglich durch Router vernetzt
- Keine Firewalls an den einzelnen Standorten
- Assets nicht zentral erfasst
- Keine Verantwortlichkeiten geregelt

SÜDOSTBAHN
gerade unterwegs

Entwicklung

Entwicklung

- Mikrosegmentierung (Client, OT1, OT2, IoT,…)
- Firewalls an den einzelnen Standorten
- Massnahmen zur weiteren Erhöhung der Sicherheit (Cyber-Security Projekt)

SÜDOSTBAHN
gerade unterwegs

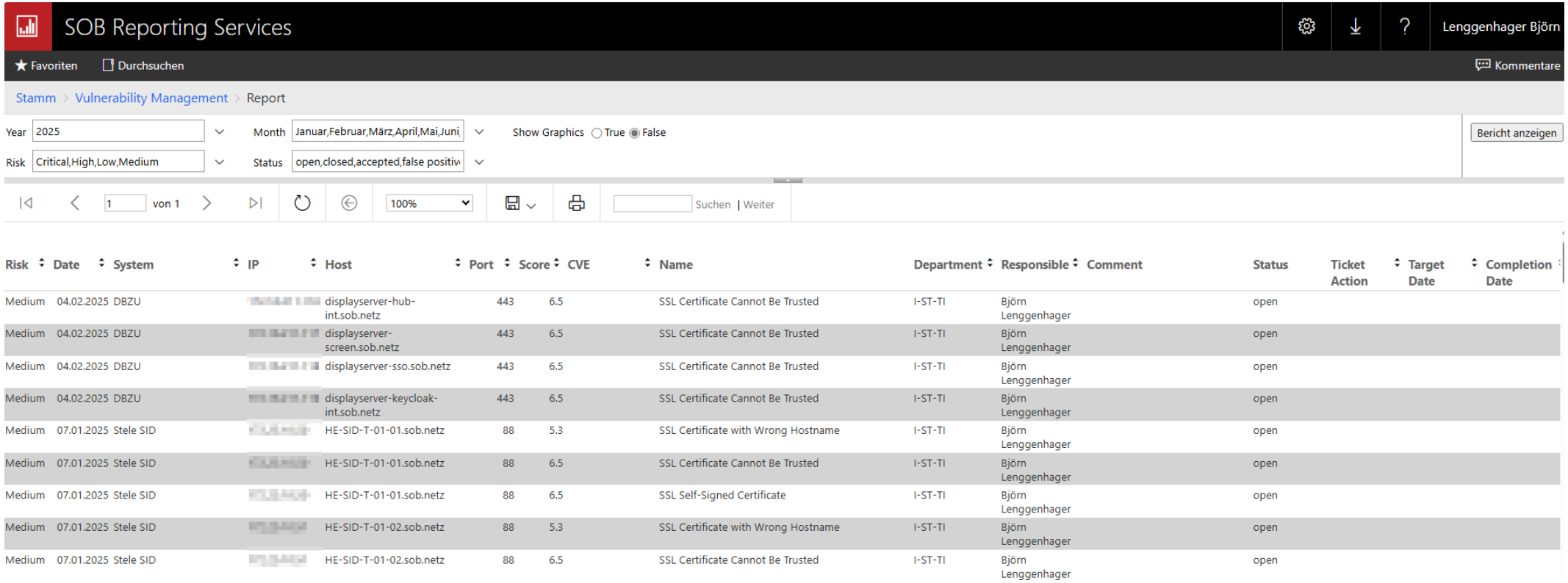
Massnahmen

Massnahmen

- ICT-Sicherheitsexperte als Schnittstelle
- Vulnerability Management
- Asset Management
- Risiko Management

Massnahmen – Vulnerability Management

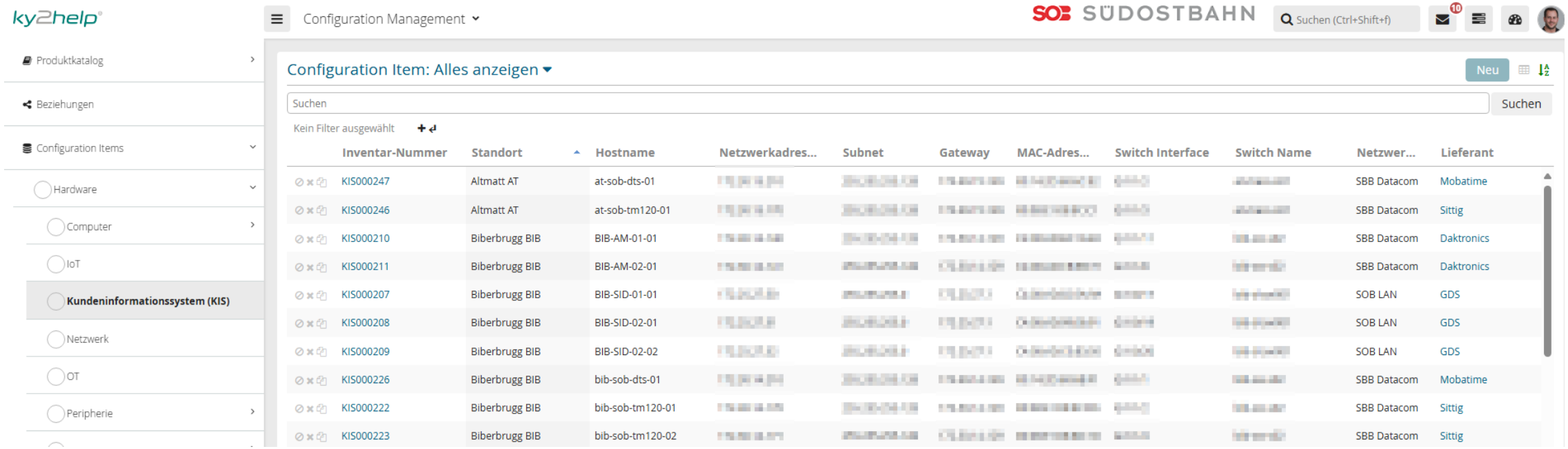
- Regelmässige Scans auf Schwachstellen der Assets
- Erfassung & Auswertung der Schwachstellen in Datenbank



Risk	Date	System	IP	Host	Port	Score	CVE	Name	Department	Responsible	Comment	Status	Ticket Action	Target Date	Completion Date
Medium	04.02.2025	DBZU		displayserver-hub-int.sob.netz	443	6.5		SSL Certificate Cannot Be Trusted	I-ST-TI	Björn Lenggenhager		open			
Medium	04.02.2025	DBZU		displayserver-screen.sob.netz	443	6.5		SSL Certificate Cannot Be Trusted	I-ST-TI	Björn Lenggenhager		open			
Medium	04.02.2025	DBZU		displayserver-sso.sob.netz	443	6.5		SSL Certificate Cannot Be Trusted	I-ST-TI	Björn Lenggenhager		open			
Medium	04.02.2025	DBZU		displayserver-keycloak-int.sob.netz	443	6.5		SSL Certificate Cannot Be Trusted	I-ST-TI	Björn Lenggenhager		open			
Medium	07.01.2025	Stele SID		HE-SID-T-01-01.sob.netz	88	5.3		SSL Certificate with Wrong Hostname	I-ST-TI	Björn Lenggenhager		open			
Medium	07.01.2025	Stele SID		HE-SID-T-01-01.sob.netz	88	6.5		SSL Certificate Cannot Be Trusted	I-ST-TI	Björn Lenggenhager		open			
Medium	07.01.2025	Stele SID		HE-SID-T-01-01.sob.netz	88	6.5		SSL Self-Signed Certificate	I-ST-TI	Björn Lenggenhager		open			
Medium	07.01.2025	Stele SID		HE-SID-T-01-02.sob.netz	88	5.3		SSL Certificate with Wrong Hostname	I-ST-TI	Björn Lenggenhager		open			
Medium	07.01.2025	Stele SID		HE-SID-T-01-02.sob.netz	88	6.5		SSL Certificate Cannot Be Trusted	I-ST-TI	Björn Lenggenhager		open			

Massnahmen – Asset Management

- Erfassung der Assets
- Zentralisierung in Datenbank
- Systemverantwortliche identifizieren und bestimmen



Massnahmen – Risiko Management

- Risikobewertung / Schutzbedarfsanalyse

Schutzbedarfsanalyse SOB Asset	
Projektname / Schutzobjektname	USV Anlagen bei der SOB
Abteilung/Ressort	I-TI-ST
Verantwortlicher	
Projekt Nr. / Projekt ID	
Unterstützte Geschäftsprozesse	Unterhalt, Störung, ICT Informationssicherheit

Ergebnis der Einstufung - die Einstufung wird aus der untenstehenden Tabelle übernommen, Auswahl aus DropDown "Antworten"	
Vertraulichkeit:	Keine Personendaten
	Klassifizierung: ÖFFENTLICH
	Keine erhöhten Anforderungen an die Vertraulichkeit
Verfügbarkeit:	Ausfalldauer max. 2 Std.
	Servicezeiten 24/7 mit Pikett
	ITSCM / BCM notwendig
Integrität:	Keine speziellen Anforderungen
Nachvollziehbarkeit:	Keine speziellen Anforderungen
Kommunikationspartner	nur SOB LAN
Datenhaltung	auf den Systemen der SOB inhouse

Kriterien	Fragen	Antworten (Drop Down Felder)	Kommentare, Begründungen für alle Zeilen ausfüllen
Vertraulichkeit	Sollen [mit diesem Schutzobjekt] Personendaten nach der Datenschutzgesetzgebung bearbeitet werden? Wenn ja, ergibt sich daraus ein hohes Risiko für die Grundrechte der betroffenen	Keine Personendaten	
	Sollen [mit diesem Schutzobjekt] klassifizierte Informationen nach der Informationsschutzverordnung (ISchV) bearbeitet werden? Wenn ja, Informationen aus welchen Klassifizierungsstufen (vgl. Art. 5 bis 7 ISchV) sind	Klassifizierung: ÖFFENTLICH	
Brauchen wir so was - oder so ähnlich?	Sollen [mit diesem Schutzobjekt] Informationen oder Daten bearbeitet werden, die aus einem sonstigen Grund (spezielle Gesetzgebungen) besonders geschützt werden müssen? Wenn ja, wie hoch sind die Schutzanforderungen?	Keine erhöhten Anforderungen an die Vertraulichkeit	
Verfügbarkeit	Max. zulässige Ausfalldauer?	Ausfalldauer max. 2 Std.	ST-Pikette wird sofort aufgeboten und kann die Anlage Bypass-Schalten. IT-Verbindung ist ein reines Monitoring. Zugriff auf die Anlage nicht möglich
	Servicezeiten?	Servicezeiten 24/7 mit Pikett	27/365 ST-Pikette wird sofort aufgeboten und kann die Anlage Bypass-Schalten.

Wann gilt ein erhöhter Schutzbedarf als Vorgabe zur Risikoanalyse?

Erhöhter Schutzbedarf liegt vor, sobald eines der Felder aus der Einstufung im Bereich der Vertraulichkeit als rot gekennzeichnet wird oder wenn mehr als zwei Kriterien in den Bereichen Verfügbarkeit, Integrität, Nachvollziehbarkeit, Kommunikationspartner oder Datenhaltung als rot gekennzeichnet werden.

Bei ausgewiesenem, erhöhtem Schutzbedarf ist eine Risikoanalyse mit dem iRisk RISIKOMANAGMENTTOOL zu erstellen. Neben der Umsetzung der Sicherheitsvorgaben für den Grundschutz und basierend auf der Risikoanalyse, sind weitere Sicherheitsmassnahmen spezifisch für das Projekt oder das Informatikschutzobjekt (Asset) zu definieren, dokumentieren und umzusetzen. Dies erfolgt vorzugsweise in diesem Dokument mittels Excel-Menu RISIKOMANAGMENTTOOL (Bereich Input).

Falls angezeigt muss anschliessend ein Informationssicherheits- und Datenschutz-konzept (ISDS-Konzept) für den Betrieb dieses Asset erstellt werden. Sind Datenschutzrelevante Informationen betroffen ist jeweils eine Datenschutzfolgen-Abschätzung (DSFA) zu erstellen.

SÜDOSTBAHN
gerade unterwegs

Menschliche Herausforderungen

Menschliche Herausforderungen

- Ressourcen
- Der Wille mitzumachen (Mindset)
- Know-how
- Alles auf «einmal»
- Unklar, was genau gemacht werden muss (Prozesse, Dokumente)
- Auftragsflut
- Sprache «IT vs. Systemverantwortliche»

SÜDOSTBAHN
gerade unterwegs

Technische Herausforderungen

Technische Herausforderungen

- Vulnerability Scans können zu Systemausfällen führen
- Erstellte Auswertungen verständlich darstellen (Sprache)
- Schliessen der Sicherheitslücken
- Einbezug Lieferanten (nicht fit in Security, nicht willens, Business nicht erkannt)
- Hardware (Industrielle Netzwerkkomponenten oftmals veraltet)
- Funktionalität der Assets bei z.B. Schliessung der Ports

SÜDOSTBAHN
gerade unterwegs

Learnings

Learnings

- Kommunikation top down
- Prozesse und Verantwortlichkeiten klar definieren
- Einbezug Systemverantwortliche
- Genügend personelle Ressourcen zur Verfügung stellen
- Know-how aufbauen
- Lieferanten mit ins Boot holen (bereits in der Ausschreibung CySec definieren)
- «Bindeglied» zwischen IT und OT
- Zeitliche Komponenten berücksichtigen


Danke für Ihre Aufmerksamkeit

SÜDOSTBAHN
gerade unterwegs

Fragen ?

OT-Security SBB

Fokus Sicherungsanlagen

Mauro Montani, Flavio Ferrari

Fachtagung VöV, 25.06.2025

Foto: Flavio Ferrari

Agenda.

Organisation OT-Security SBB

Überblick der Linien- sowie Fach-Organisation im Beriech der OT-Security innerhalb der SBB bzw. Infrastruktur

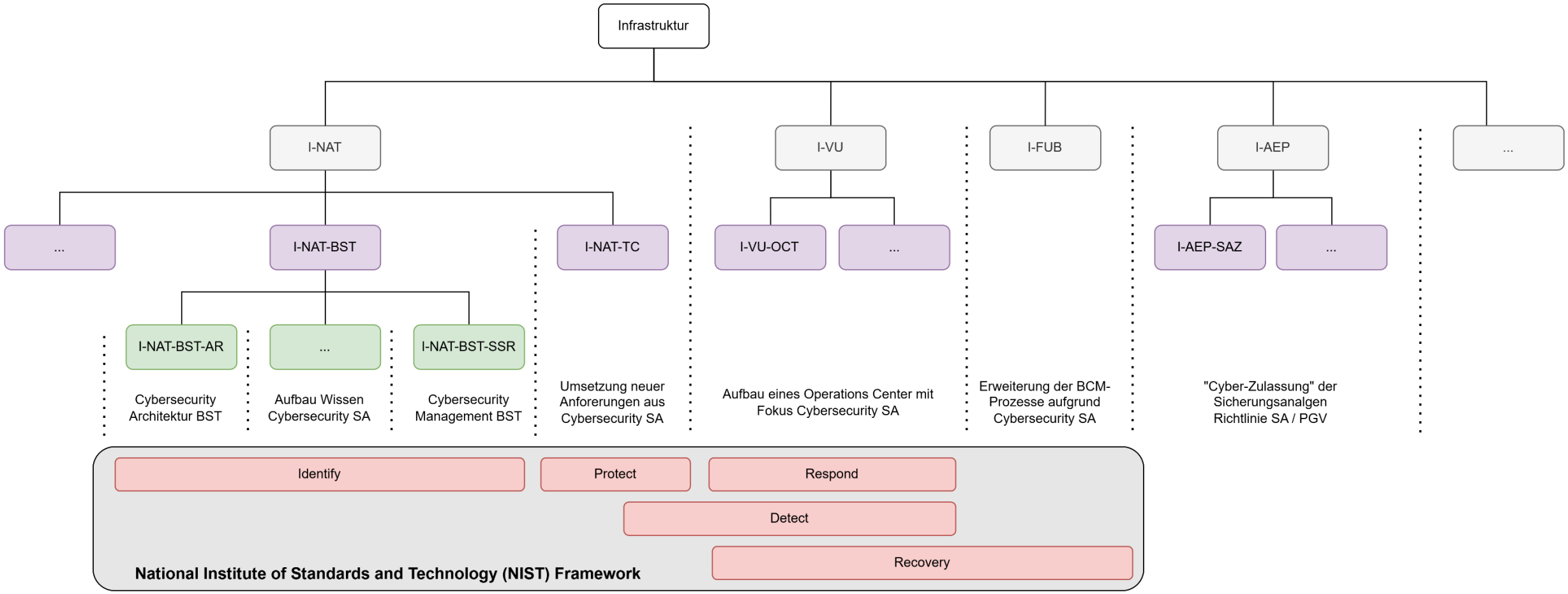
Ausgangslage OT-Security SA

Kurzbeschrieb oder Aufzählung mit mehreren Zeilen

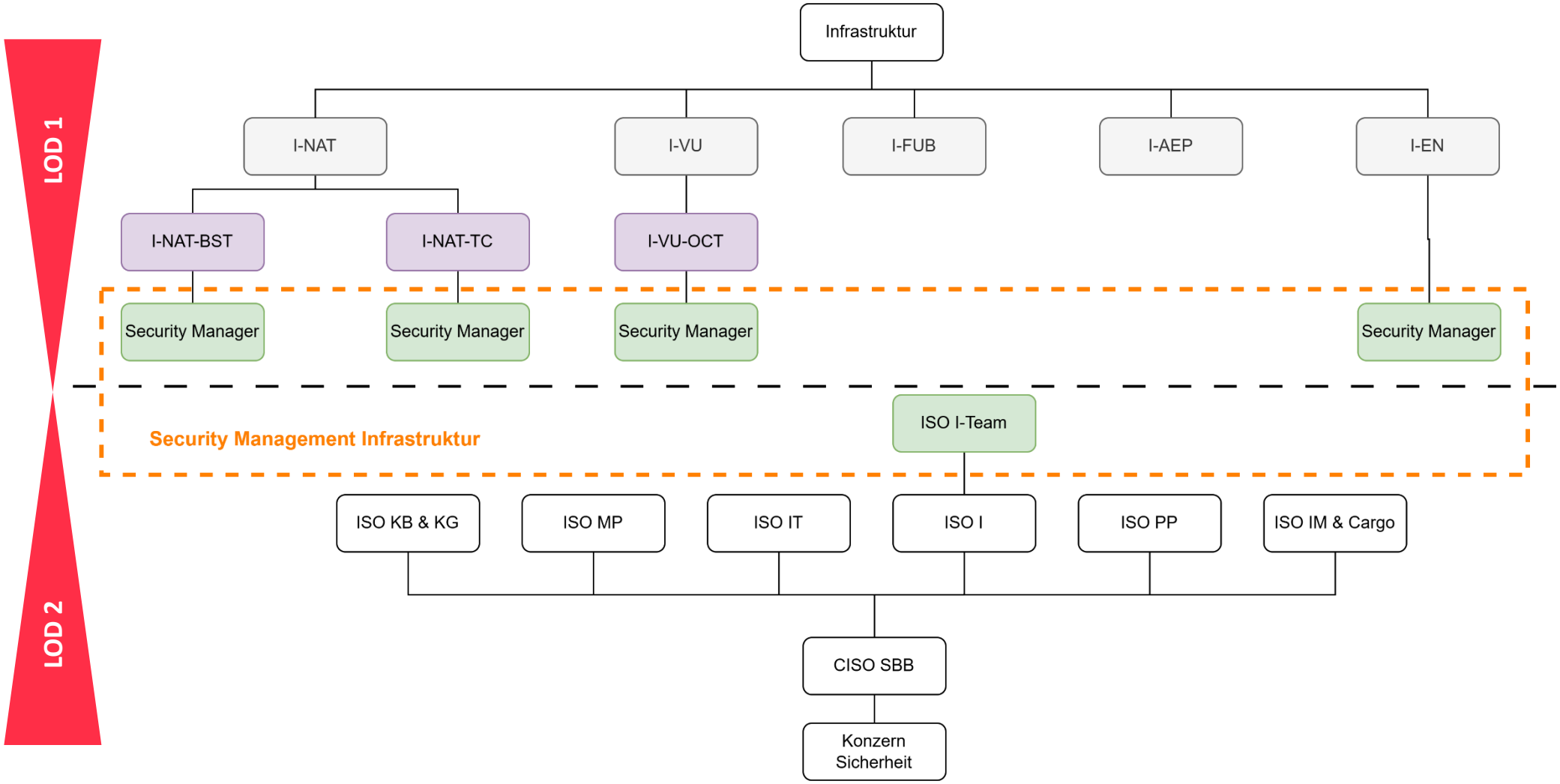
Herangehensweise OT-Security SA

Kurzbeschrieb oder Aufzählung mit mehreren Zeilen

Organisation «OT-Security@Infrastruktur».



Organisation «OT-Security@SBB».



Agenda.

Organisation OT-Security SBB

Ausgangslage OT-Security SA

Übersicht der einzelnen Kategorien innerhalb der Sicherungsanlagen – Baukasten SA und vereinfachte Übersicht der Architektur SA.

Herangehensweise OT-Security SA

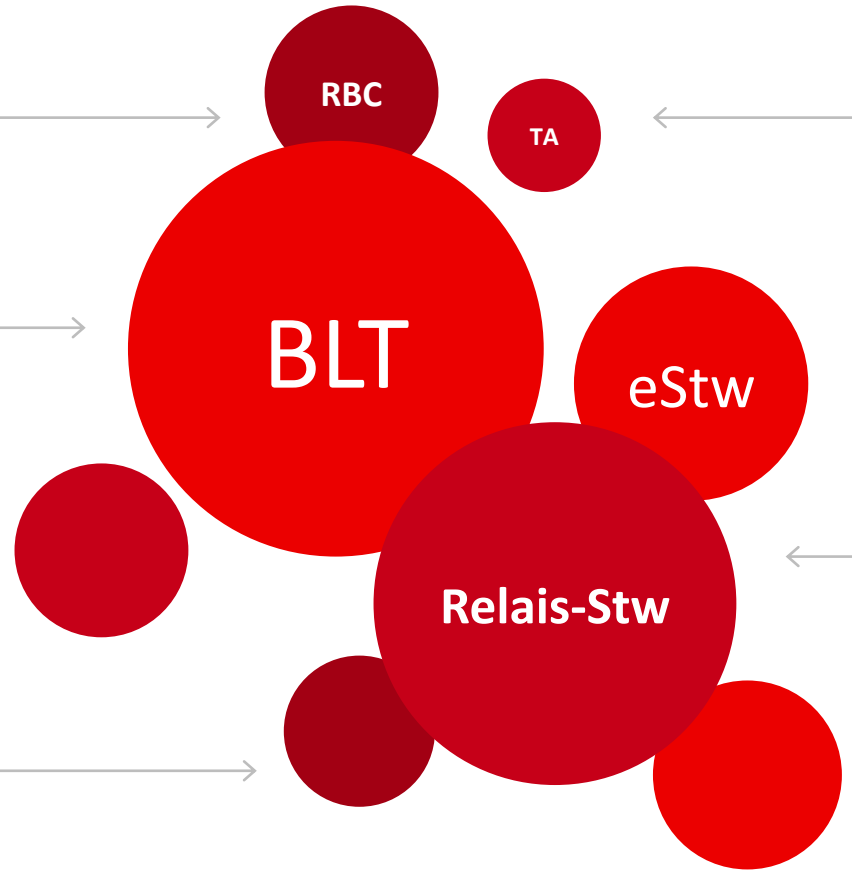
Ausgangsalge «Baukastenelemente Sicherungsanlagen».

Radio Blockl Center (RBC)
- RBC Hitachi
- RBC SMO
- RBC Alstom.

Bahnleittechnik
- Iltis N und Iltis N-R
- Schnittstelen zu Umsystemen (Stellwerk, Partnerbahn, Zugbeeinflussung)

Weichenheizung

Rangiertechnik



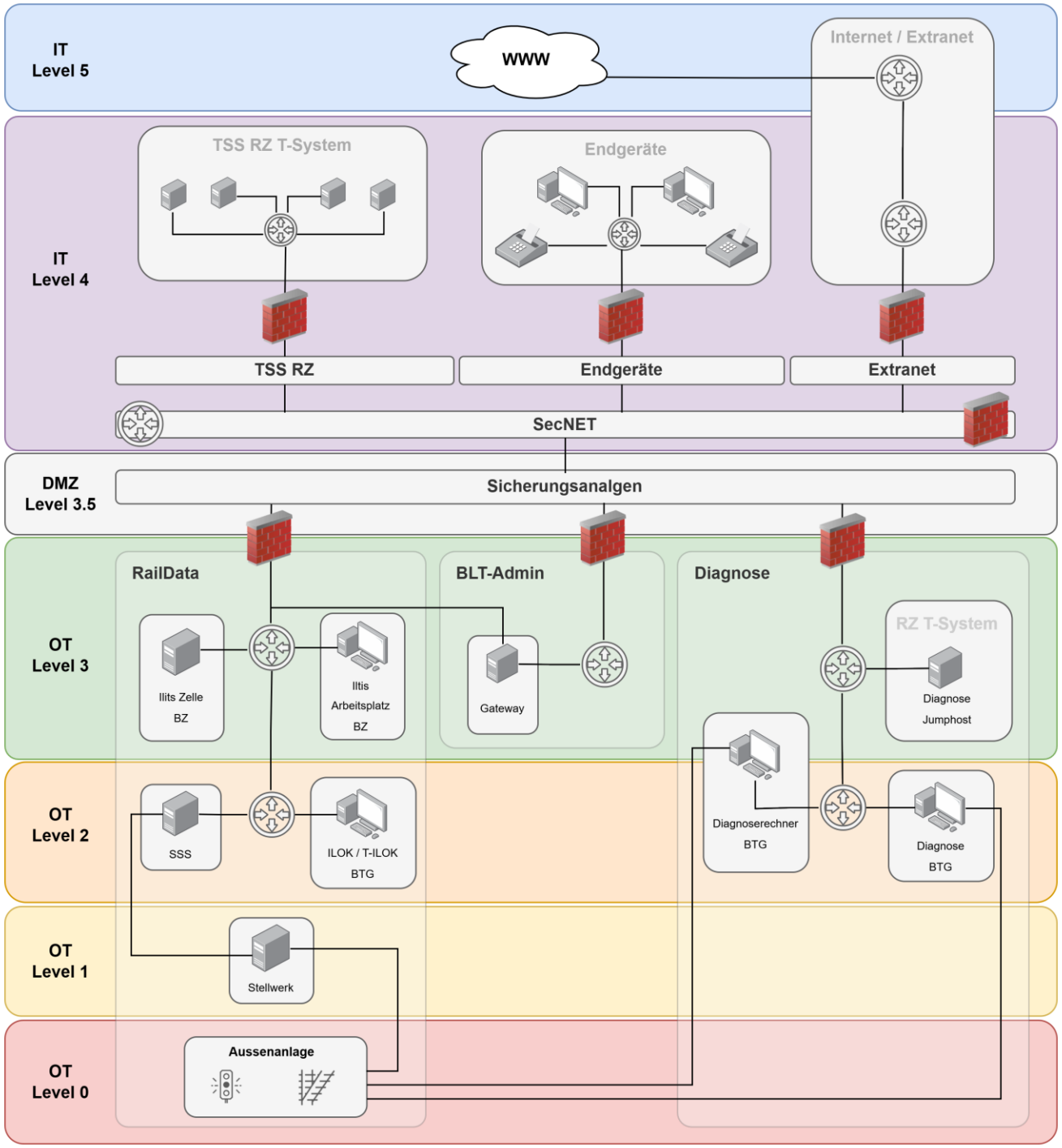
Tunnelautomatik
- CBT und GBT

Elektronische Stellwerke
- SMO – Simis-C / Simis-C Plus / Smis W
- Hitachi – ELEKTRA 1 / ELEKTRA 2
- „neue Generation“

Relaisstellwerke
- Domino
- ISAG (elektromechanisch)
- SpDrS-SBB

Warnsysteme (Bahnübergänge)

Ausgangsalge «Architektur SA – Perdue Modell».



Agenda.

Organisation OT-Security SBB

Ausgangslage OT-Security SA

Herangehensweise OT-Security SA

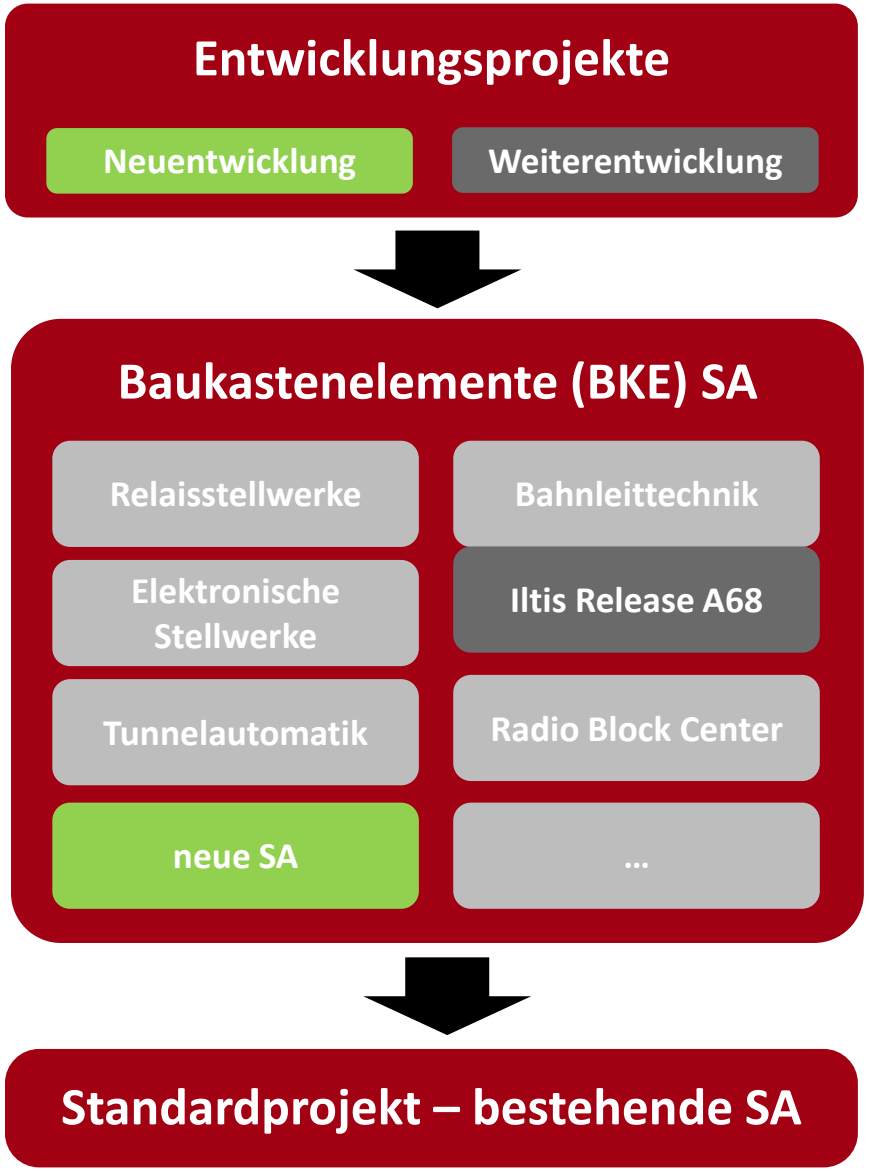
Umsetzung von Cybersecurity Massnahmen innerhalb der Projekte.
Zulassungsprozess von Standard- und Entwicklungsprojekten

Herangehensweise «Anwendungsfälle».

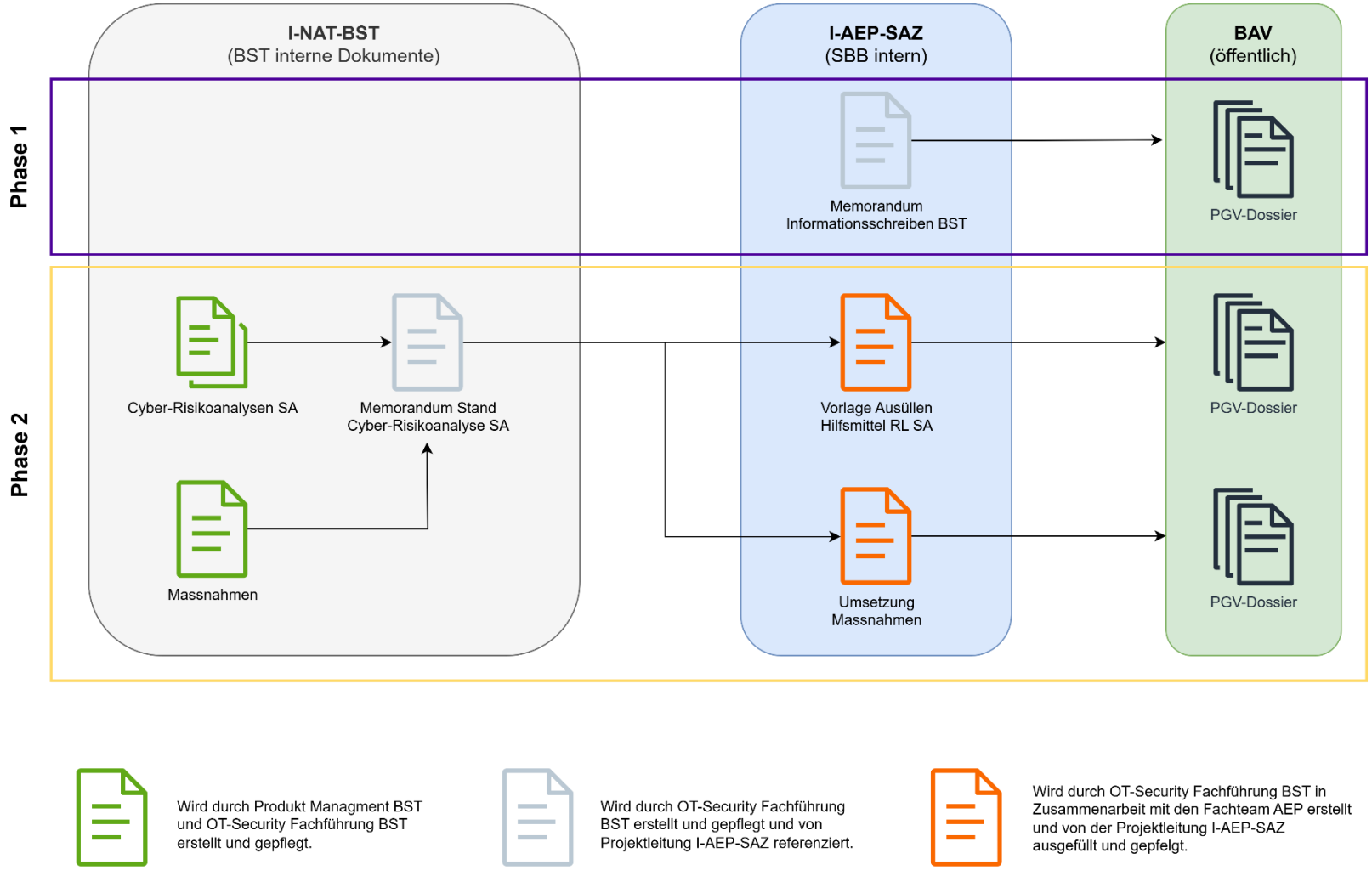
Grundlagen
OT-Security Management

- 3 Anwendungsfälle:
  - Neuentwicklungen SA
  - Weiterentwicklung SA
  - bestehende SA

- Unterschiedlicher Stand und Bedarf der OT-Security Risikobewertung



Herangehensweise «Prozess bzw. Vorgehen PGV».



Herangehensweise «Ausblick».

1. **Integration neuer SA mit bestehenden Systemen**
   Unterschiedliche Security-Fähigkeiten

2. **Bald geschafft!**
   Aber was ist mit der nächsten Generation SA, wenn die aktuell neue securitytechnisch veraltet ist?

3. **Ansteigende Vernetzung**
   Wie gehen wir damit um?

4. **Security-Kultur**
   Bereitschaft für Mitarbeit, Sensibilität, Security zum Selbstzweck, Compliant = Secure?, «das macht man halt so / haben wir halt immer schon so gemacht»

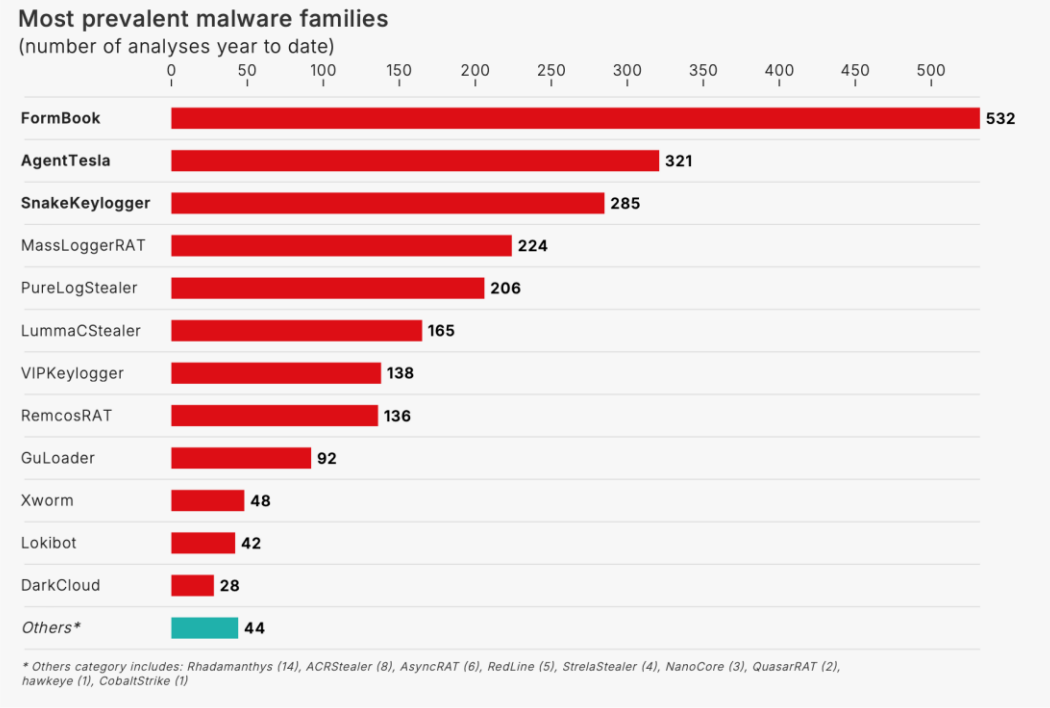

SBB CFF FFS
Danke, merci
& grazie.

Getränke und Zwischenverpflegung im Foyer
Bitte um 11:20 wieder Platz nehmen, das nächste Referat beginnt um 11:25

Threat Landscape & Rail ISAC

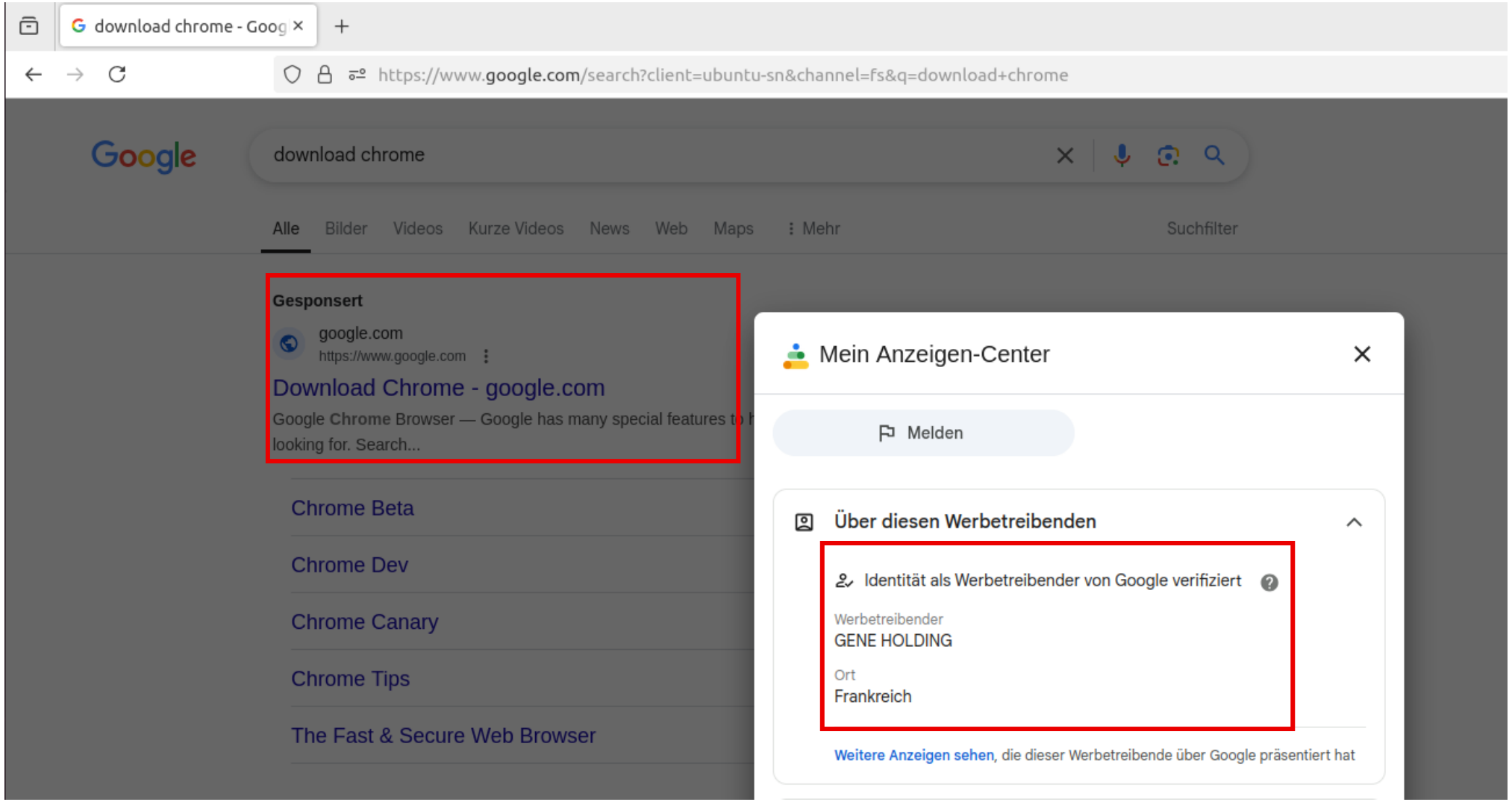
Reto Inversini
Rail ISAC
25.06.2025

Kriminelle Akteure.

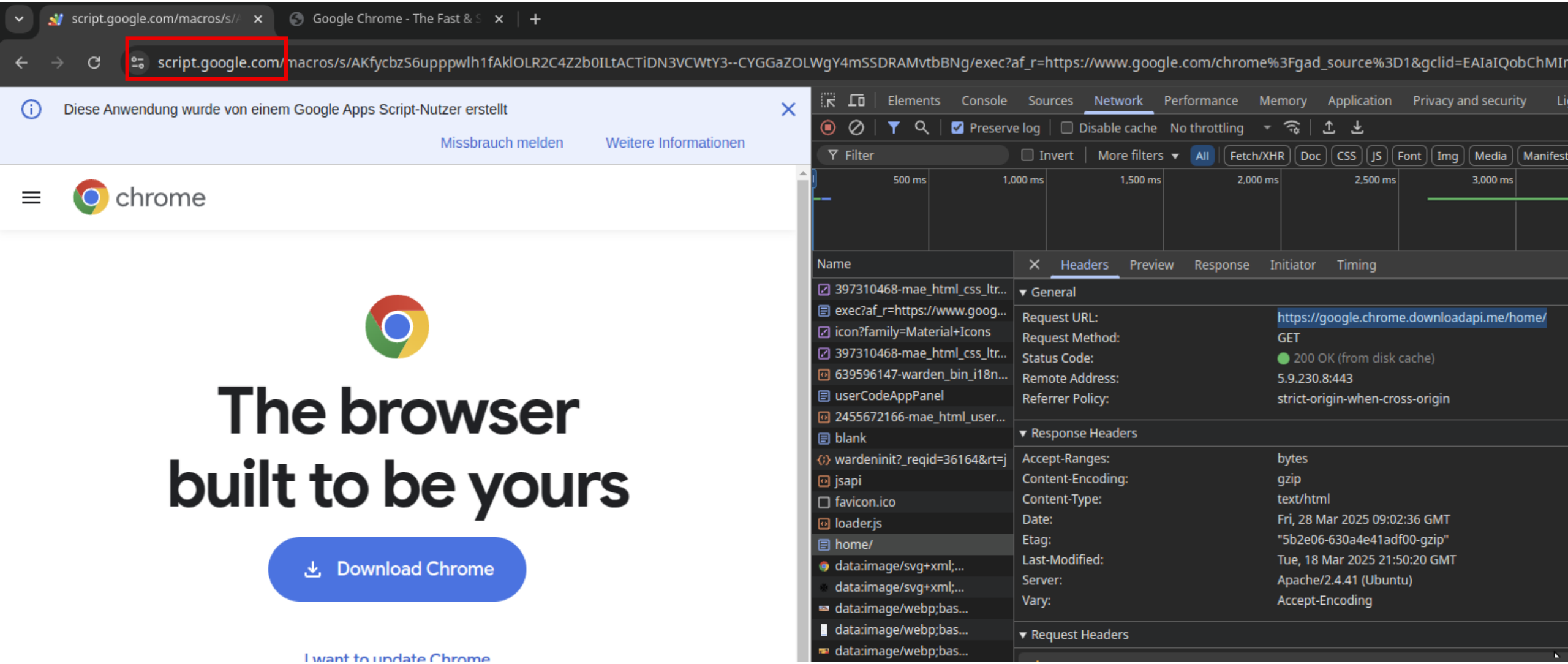


- Opportunistische Angreifer
  - Sind täglich sichtbar.
  - Modus Operandi: (Realtime) Phishing, Information Stealer, Übernahme von exponierten Systemen, Ransomware, Supply Chain Attacks, Fraudulent Advertisements.
  - Letzten Freitag gab es eine Infektion von drei Geräten aufgrund eines Fraudulent Ads für Chrome.

Malvertising – Stage 1.



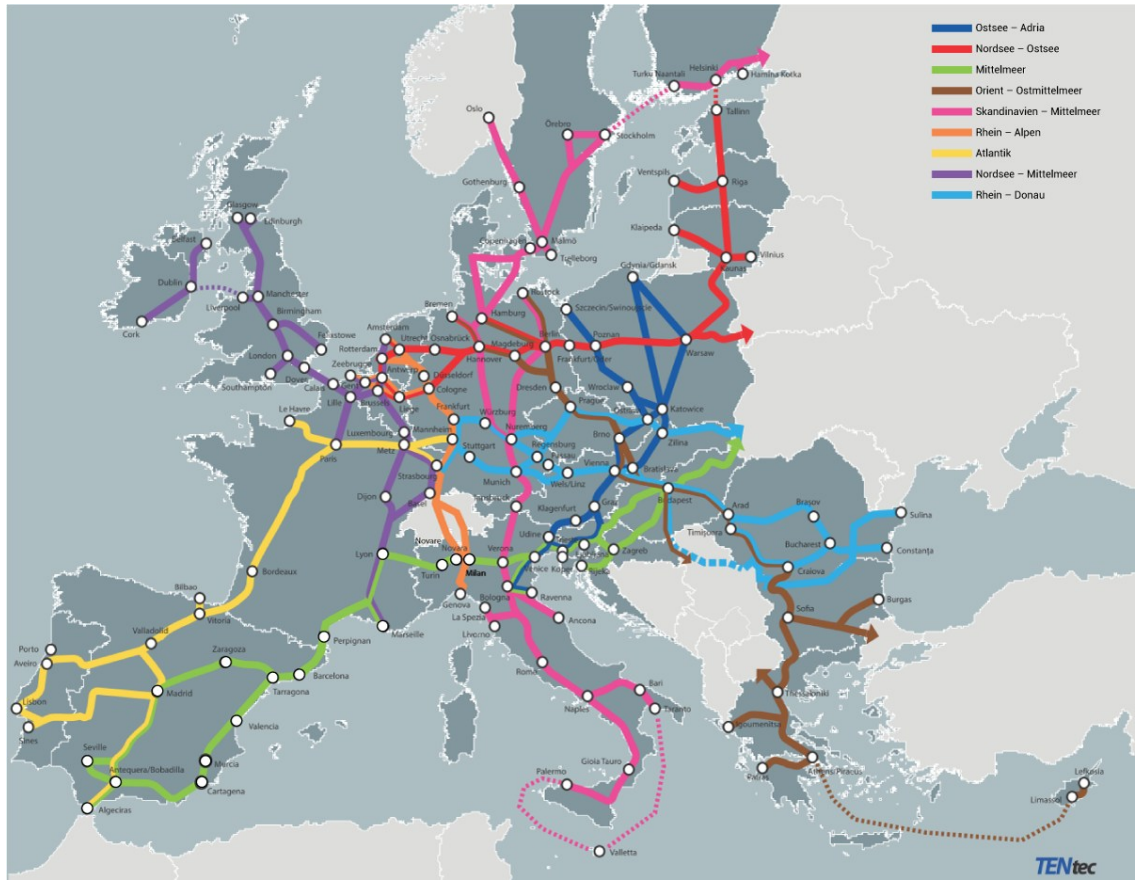
Malvertising – Stage 2.



Kriminelle Akteure.

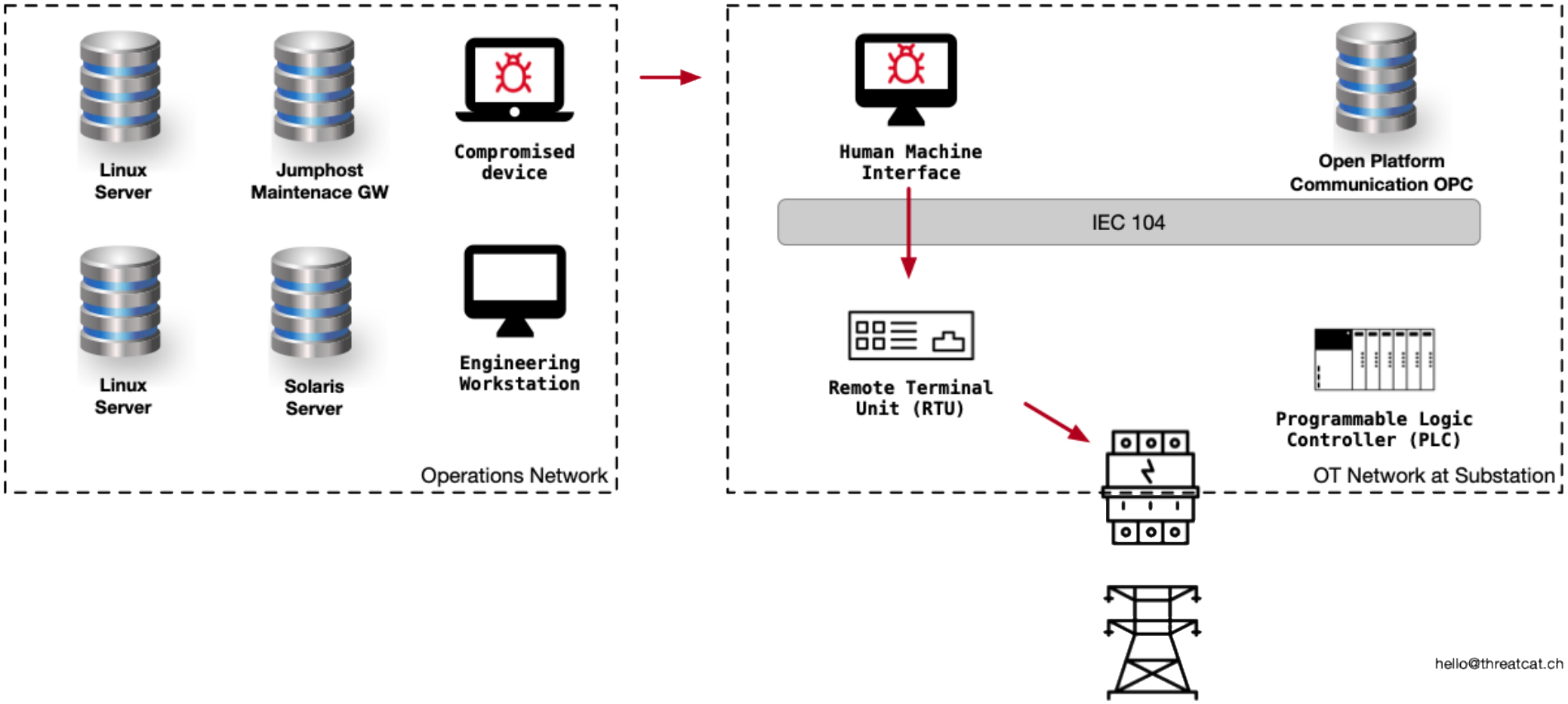
- Gezielte Angriffe («Big Game Hunting»)
  - Modus Operandi: Meist mehrstufiger Angriff mit lateraler Bewegung Erpressung.
  - Der Angreifer sieht ein Erpressungspotential durch das Ausspielen des Safety Elements im Bahnsektor.
  - Der Angreifer muss nur glaubhaft machen können, dass er das System manipuliert hat.
  - Es kann remote oder hybrid passieren. Als Beweismittel schickt er uns Screenshots, wie er mit einem Laptop auf ein Steuerungssystem zugreift.

Staatliche Akteure.

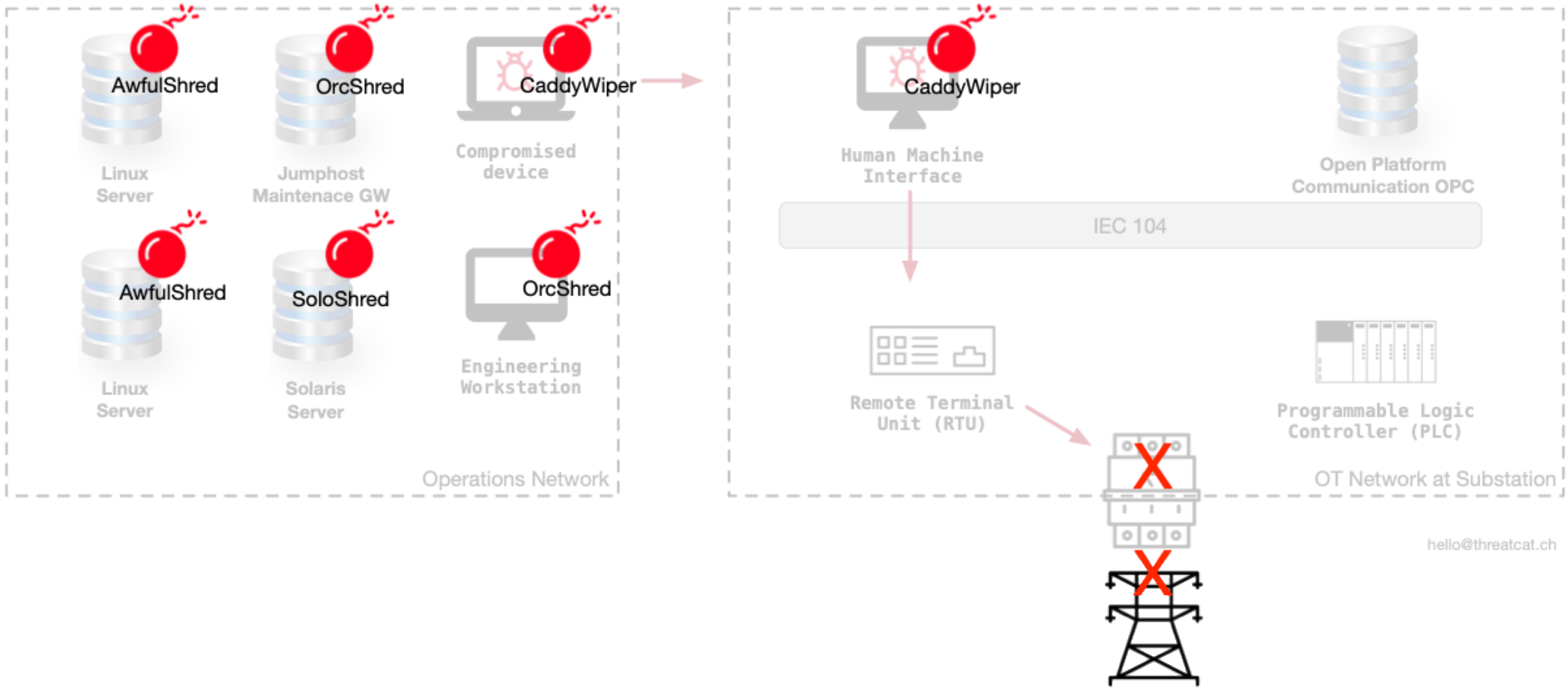


- Der Angreifer hat das Ziel den Bahnverkehr zu stören oder lahmzulegen.
- Der Angreifer benötigt dazu einen möglichst tiefen Zugang.
- Diese Angriffe sind gezielt und werden vorbereitet
  - Wir sind heute in der Phase einer Reconnaissance.
  - Ein Angreifer hat auch ein Interesse, unsere Detektions- und Reaktionsfähigkeiten zu testen.

Beispiel aus der Ukraine.



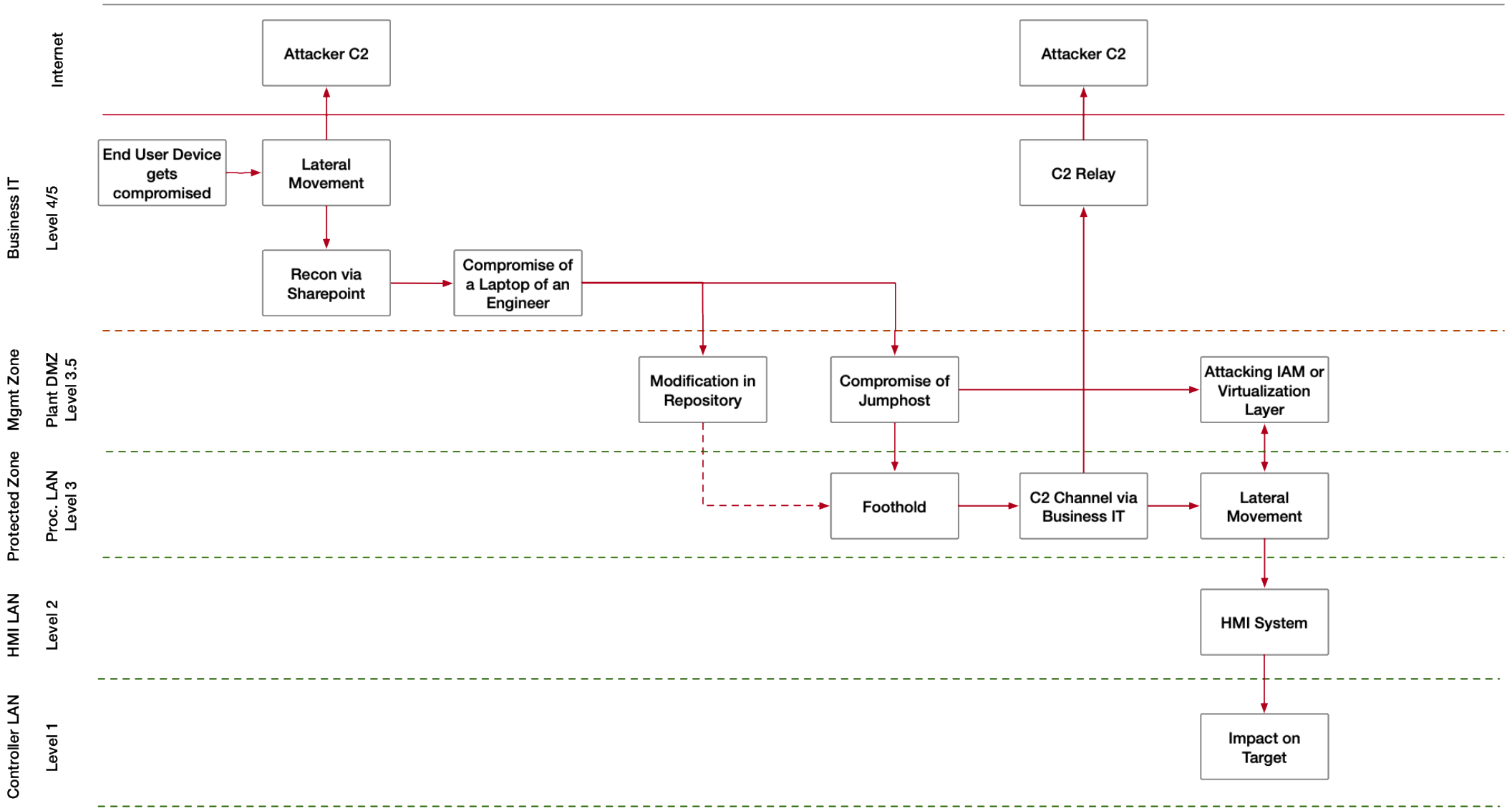
Beispiel aus der Ukraine.



Was bedeutet das für Sicherungsanlagen?

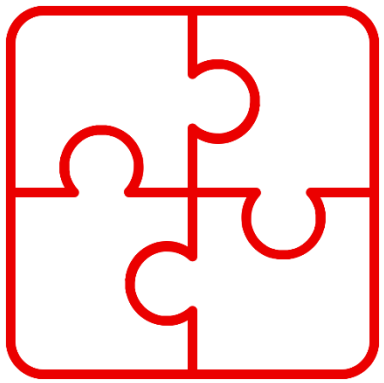
- Auch bei abgeschotteten Netzen gibt es Angriffsvektoren
  - Gestohlene Credentials von Engineers können zu Sharepoint Zugriffen mit interessanten Daten führen.
  - Kontrolliert der Angreifer das Büroautomationsgerät eines Engineers, gibt es oft den Vektor via Jumphost/Wartungsgateway.
  - Repositories mit Software Paketen / Firmware sind ebenfalls ein Ziel, das so in Reichweite des Angreifers kommt.
  - Der Angreifer muss nicht zwingend, Malware verwenden, um den Angriff durchzuführen. Er kann direkt über die normale HMI Software (z.B. WinCC bei Siemens Steuerungen) Befehle absetzen.

Angriffspfade finden über Systemgrenzen hinweg statt.



rail.isac@sbb.ch

Was ist ein ISAC?

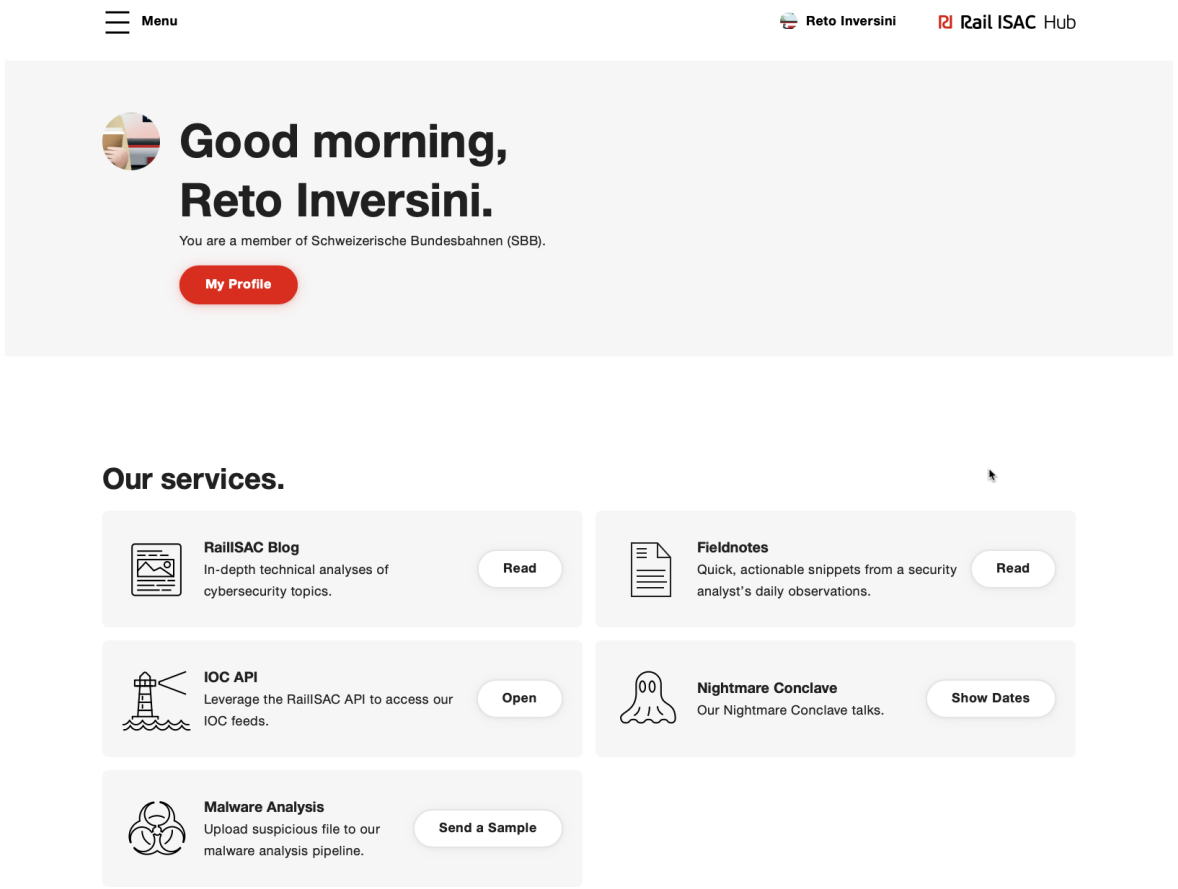


- ISAC steht für Information Sharing and Analysis Center und bezieht sich meist auf einen Sektor.
- Es ist eine Antwort auf die steigende Bedrohungslage und soll den Sektor als Gesamtes resilienter machen.
- Das Ziel ist es, Sektor spezifisches Wissen zu bündeln und diese Fähigkeiten dem gesamten Sektor zur Verfügung zu stellen.
- Das Konzept wird national und international gefördert, um Cyberbedrohungen sektorweit erkennen und bekämpfen zu können.

Status Rail ISAC.

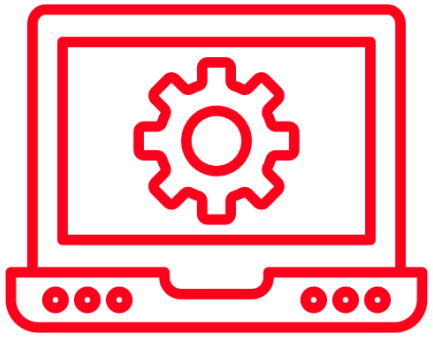
- Rail ISAC ist seit dem 30.4. vollständig operativ
  - Die Gründungsversammlung hat stattgefunden und die Charta wurde formell genehmigt.
  - Das Governance Board wurde konstituiert.
  - Es sind 20 Bahnen aufgenommen worden.
  - Die Core Services sind alle operativ.
  - Eine 24/7 Pikettorganisation ist seit dem 1.5.2025 aktiv.

Die Plattform & die Services.



- Die Services umfassen aktuell:
  - Zugang zu der Plattform und zu sektorspezifischer Threat Intelligence.
  - Analyse von Schadsoftware (Dynamische Analyse und Reverse Engineering).
  - Bedrohungsanalyse im Bereich der Operational Technology.
  - Erstellen von Detektions Regeln.
  - Incident Response bei Cybersicherheits-vorfällen.

CTI im OT Bereich.



- Analyse von Schadsoftware wie Industroyer / Industroyer2.
- Ausbau des Trackings mit Hilfe von Google GTI / Virustotal.
- Entwickeln von Detection Rules basierend auf diesen Erkenntnissen.
- Ableiten von Angriffsmustern und Entwerfen von möglichen Schutzmassnahmen.
- Unterstützung der OT Teams mit Wissen über Angriffsmuster und mögliche Detektionsmassnahmen.

ISAC und Krisenbewältigung.

- Ein ISAC ist ein wichtiges Instrument für die Krisenbewältigung bei digitalen und hybriden Bedrohungen
  - Es reduziert durch bessere Präventions- und Detektionsmechanismen die Eintretenswahrscheinlichkeit.
  - Es reduziert durch schnellere Reaktion das Schadensausmass.
  - Es berät die Organe der Krisenbewältigung und versorgt sie mit aktuellen Informationen über die aktuelle Bedrohungslage.
  - Es unterstützt den Sektor bei einem Cyberangriff und dient als strategische Reserve, welche die Durchhaltefähigkeit stark erhöht.

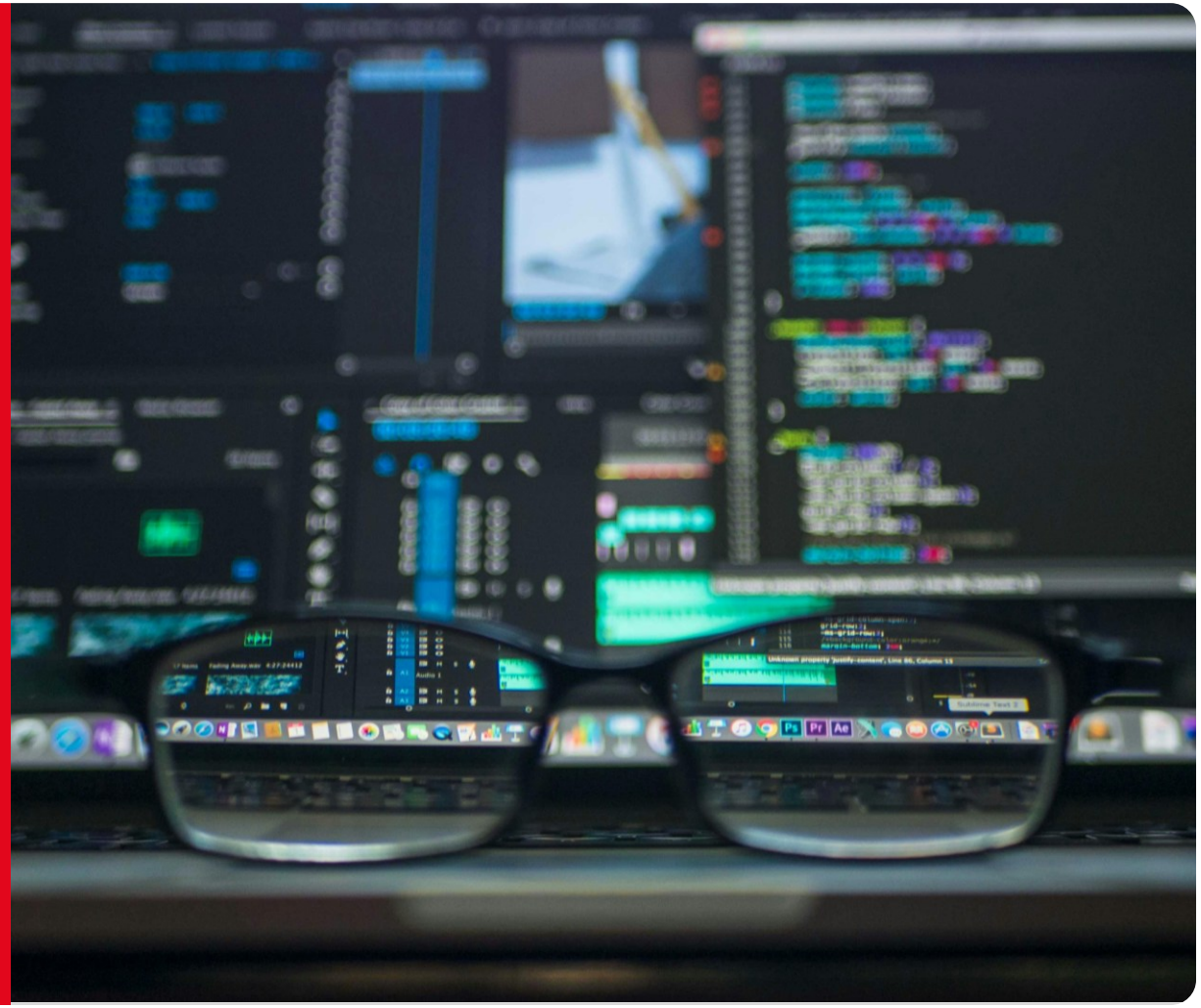

SBB CFF FFS
Danke, merci
& grazie.

SWISSRAIL

TOGETHER FOR THE SWISS RAIL AND MOBILITY INDUSTRY.
NATIONAL. GLOBAL

Fachtagung OT Cybersecurity, 25. Juni 2025

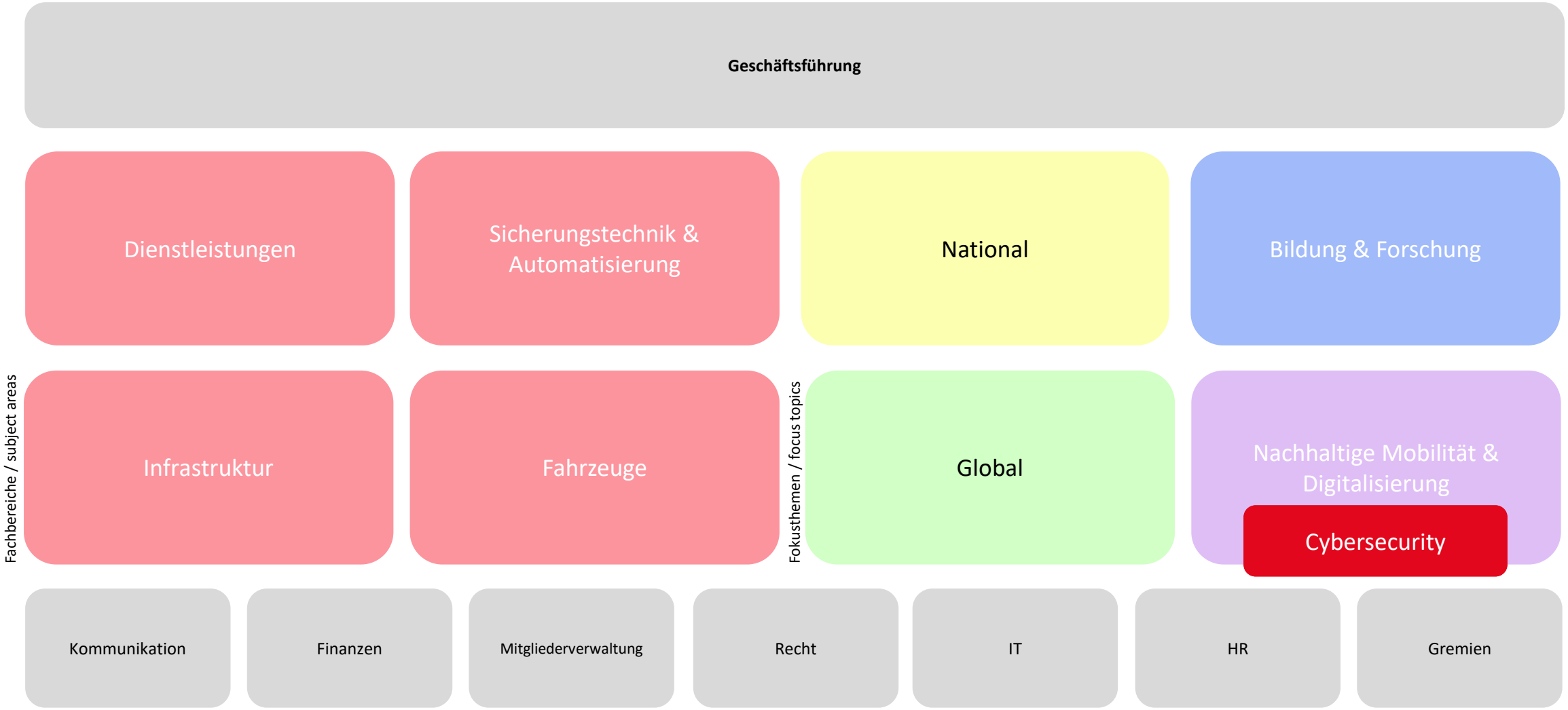
Cybersecurity aus Sicht der Industrie



Unsere Vision und Mission

Together for the Swiss Rail and Mobility Industry.
National. Global.

Struktur


Geschäftsführung
Dienstleistungen
Sicherungstechnik & Automatisierung
National
Bildung & Forschung
Fachbereiche / subject areas
Infrastruktur
Fahrzeuge
Fokusthemen / focus topics
Global
Nachhaltige Mobilität & Digitalisierung
Cybersecurity
Kommunikation
Finanzen
Mitgliederverwaltung
Recht
IT
HR
Gremien

Gemeinsam stärker

160 Mitglieder

Übersicht Mitglieder auf www.swissrail.com/mitglieder

Cybersecurity bei Swissrail

Cybersecurity bei Swissrail

Warum haben wir eine Arbeitsgruppe Cybersecurity gegründet?

Bedeutung von Cybersecurity im Bahnbereich vs. Unsicherheiten
- IT- und OT- Kompetenzen bündeln
- Regelmässiger Dialog und Erfahrungsaustausch hilft allen
- Swissrail will seine Mitglieder sensibilisieren und bei Umsetzung von Cybersecurity unterstützen
  → BAV Richtlinie CySec-Rail: Swissrail Umsetzungsempfehlungen

Zusammenarbeit von Behörden – Betreibern – Industrie
- Verantwortung bei Betreibern, Lieferanten sind von Pflichten der Richtlinie CySec-Rail aber nicht ausgenommen
- Swissrail will den Dialog zwischen den Stakeholdern fördern
  → Umsetzungsempfehlungen als Grundlage für Dialog

Roundtable Cybersecurity am Swissrail Mobility Day 2025

Awareness ist da – Zusammenarbeit stärken

— Transparenz
— Kommunikation
— Gemeinsames Verständnis

Fazit: Bei der Umsetzung von Cybersecurity müssen alle Stakeholder miteinbezogen werden

Umsetzungsempfehlungen zu der BAV CySec-Rail Richtlinie

V1.0, noch nicht publiziert

SWISSRAIL

Umsetzungsempfehlungen zu der BAV CySec-Rail Richtlinie

Inhalt

Fokus auf Basismassnahmen (Kapitel 8), B01 - B29

— Welche Aufgaben müssen von den EVU und ISB übernommen werden, welche von den Lieferanten
— Aufbau der Empfehlungen: Control – Empfehlung – Verantwortlichkeiten (Betreiber, Lieferant und beide)

Wir haben Empfehlungen erarbeitet – keine Checkliste zum Abhaken

— Awareness für risikobasierter Absatz schaffen

In Zusammenarbeit mit Railplus verfasst, abgestimmt mit dem Bundesamt für Verkehr BAV

Beispiel: B01 – Rollen und Verantwortlichkeiten

In der BAV-Richtlinie CySec-Rail (V1.1, 24.06.2024)

Nr.	Control	Verweis	Synergie zu VO 2018/762 [3]
B-01	**Festlegung von Rollen und Verantwortlichkeiten** Es müssen Rollen und Verantwortlichkeiten für den Bereich der Informationssicherheit definiert werden. Die einzelnen Aufgabenbereiche müssen Personen mit den entsprechenden Fachkenntnissen zugewiesen werden.	ISO/IEC 27002:2022 Kapitel 5.2 NIST CSF 2.0 GV.RR-02	Kapitel 2.3 Kapitel 4.1 Kapitel 4.2

Beispiel: B01 – Rollen und Verantwortlichkeiten

In den Swissrail Umsetzungsempfehlungen

Control:

B-01: Festlegung von Rollen und Verantwortlichkeiten

Es müssen Rollen und Verantwortlichkeiten für den Bereich der Informationssicherheit definiert werden.

Beispiel: B01 – Rollen und Verantwortlichkeiten

Empfehlung:

— «Es ist eine Liste aller notwendigen Rollen im Bereich der Informationssicherheit zu erstellen, wie z.B. CISO. Die Aufgaben sind klar zu definiert und ohne Interessenkonflikte zu gestalten (…) Das Anforderungsprofil für Fachkenntnisse ist ein weiterer wichtiger Punkt. Alle Beteiligten sollten über die erforderlichen Kenntnisse verfügen oder diese – wie etwa beim Datenschutzbeauftragten im Datenschutzrecht – durch geeignete Schulungen erwerben. Abschliessend werden die definierten Rollen und Verantwortlichkeiten in einem formellen Dokument festgehalten und an alle relevanten Mitarbeiter und Parteien kommuniziert, z.B. als "Rollen- und Verantwortlichkeitsmatrix".»

Rolle	Hauptverantwortung	Berichtsweg
IT-Sicherheitsbeauftragter / CISO	Gesamtverantwortung für die Informationssicherheit	Berichtet direkt an den Vorstand oder CIO (Chief Information Officer)
Datenschutzbeauftragter (DSB) - **Schweizerisches DSG** **Data Protection Officer (DSO)** - **EU DSGVO**	Sicherstellung der Einhaltung der Datenschutzvorschriften (in spezifischen Abteilungen)	Berichtet an den Abteilungsleiter Es kann auch ein externer Berater sein
Risikomanager Informationssicherheit	Identifizierung, Bewertung und Management von Sicherheitsrisiken	Berichtet an den IT-Sicherheitsbeauftragter

Beispiel einer Rollen- und Verantwortlichkeitsmatrix

Beispiel: B01 – Rollen und Verantwortlichkeiten

Verantwortlichkeiten:

Betreiber:

— „Betreiber müssen Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit klar definieren. Zentrale Funktionen wie CISO, Datenschutz- und Risikobeauftragte sind verbindlich festzulegen, ihre Aufgaben eindeutig zuzuweisen und regelmässig zu überprüfen.“

Lieferanten:

— „Lieferanten mit sicherheitsrelevanten Leistungen müssen geeignete Rollenmodelle vorweisen. Verantwortliche Personen müssen qualifiziert sein oder entsprechend geschult werden. Zuständigkeiten sind nachvollziehbar zu dokumentieren.“

Beide:

— „Bei geteilter Verantwortung sind Rollen und Schnittstellen gemeinsam festzulegen. Die Aufgabenverteilung muss klar, widerspruchsfrei und dokumentiert sein, um eine wirksame Zusammenarbeit sicherzustellen.“

Wie geht es weiter?

Umsetzungsempfehlungen
- ASAP: Publikation auf www.swissrail.com und senden an Betreiber für Feedback und Dialog
- Regelmässige Überarbeitung im Dialog mit Stakeholdern

Swissrail als Plattform für Austausch
- Regelmässige Veranstaltungen und Austausche für Swissrail-Mitglieder
- Transparenter Dialog aufbauen und pflegen mit allen Stakeholdern

Ziel
- Das notwendige Vertrauensverhältnis zwischen der Industrie und den verschiedenen Stakeholdern stärken und gewährleisten, dass alle Beteiligten eine gemeinsame Sprache sprechen und so die Cybersicherheit effektiv umgesetzt wird.

Swissrail: Your Contact to the Swiss Rail and Mobility Industry

Swissrail Industry Association
Taubenstrasse 32
CH-3011 Bern

swissrail@swissrail.com
+41 31 398 50 50