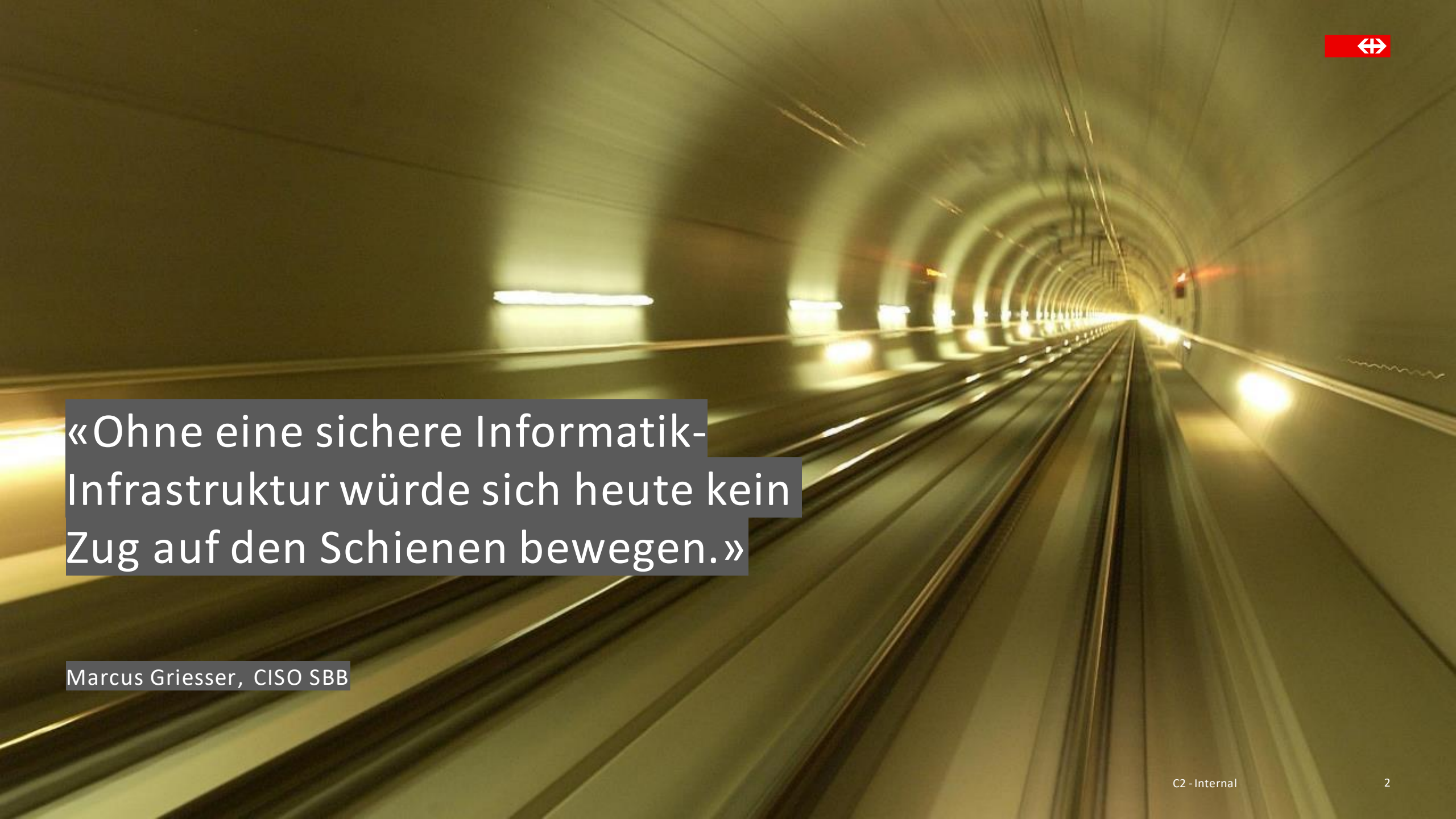
Die SBB – eine kritische Infrastruktur für die Schweiz

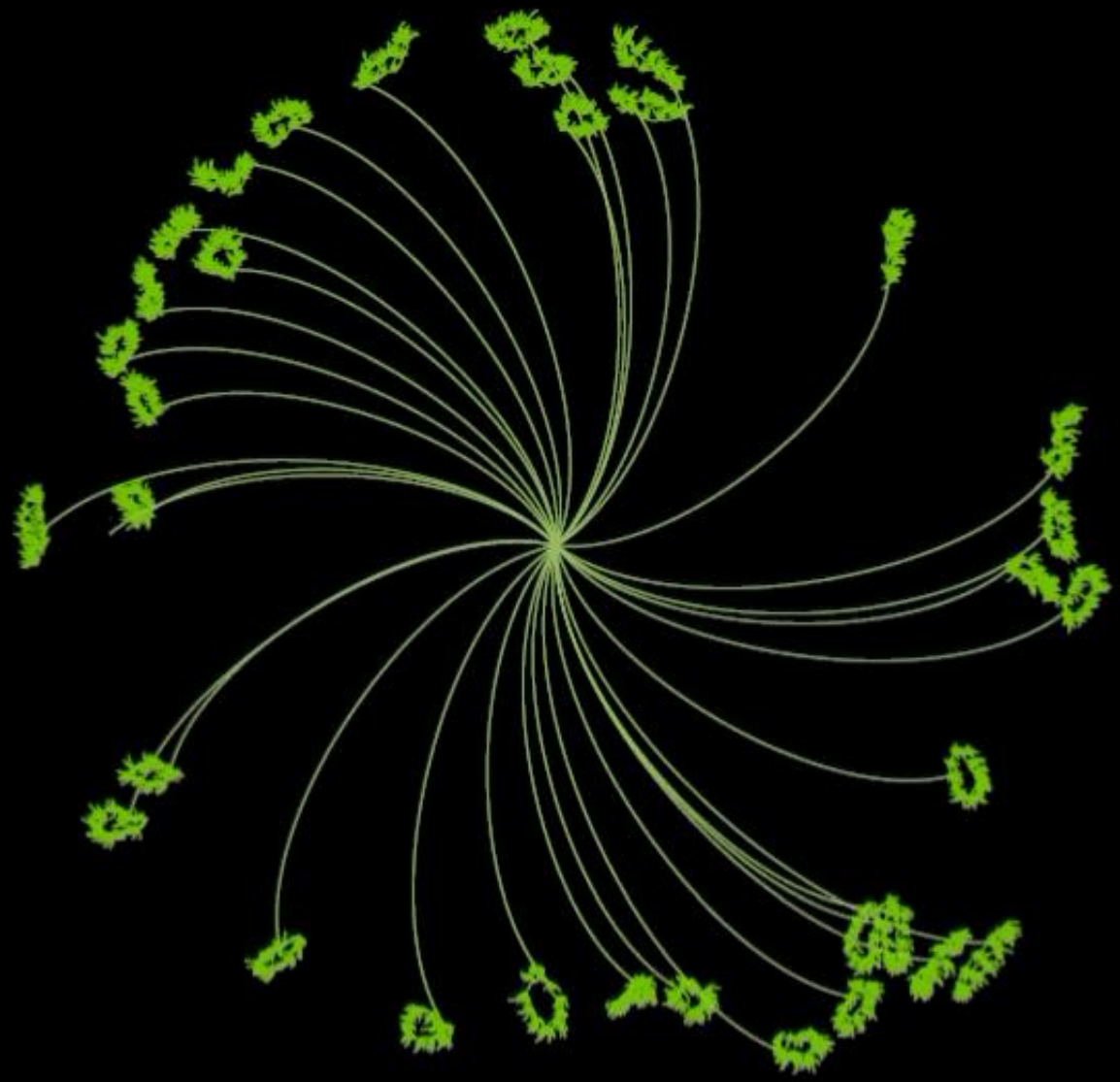
ISSS Berner Tagung | 11. Januar 2023

Jan Hohenauer



«Ohne eine sichere Informatik-Infrastruktur würde sich heute kein Zug auf den Schienen bewegen.»

Marcus Griesser, CISO SBB



Agenda.

Kritische Infrastrukturen

Die SBB

Resilienz

Was tun?

Q&A

Kritische Infrastrukturen.

Prozesse, Systeme und Einrichtungen, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind.

- 9 Sektoren, unterteilt in 27 Teilsektoren und zu deren Betrieb notwendige Elemente.
- Der Sektor Verkehr beinhaltet u.a. den Teilsektor Schienenverkehr und darunter fallen Elemente wie z.B. eine Betriebsleitzentrale

«Ein funktionsfähiges, zuverlässiges und leistungsfähiges Transport- und Verkehrssystem ist heutzutage eine Grund-voraussetzung für eine moderne Wirtschaft, die auf die Mobilität von Gütern und Personen angewiesen ist.» (BABS)

https://www.babs.admin.ch/de/aufgabenbabs/ski.html

Die letzten paar Monate.

Überlegungen

- Abhängigkeiten in komplexen Systemen
- Fokus auf physischem Schutz
- Cyberangriffe zwischen Bedrohung und Propaganda
- Grundschutz
- Melde & Nachweispflichten
- Verbundsübungen
- Zuständigkeiten
- Globale Lieferketten

https://ccdcoe.org/exercises/locked-shields/

Agenda.

Kritische Infrastrukturen

Die SBB

Resilienz

Was tun?

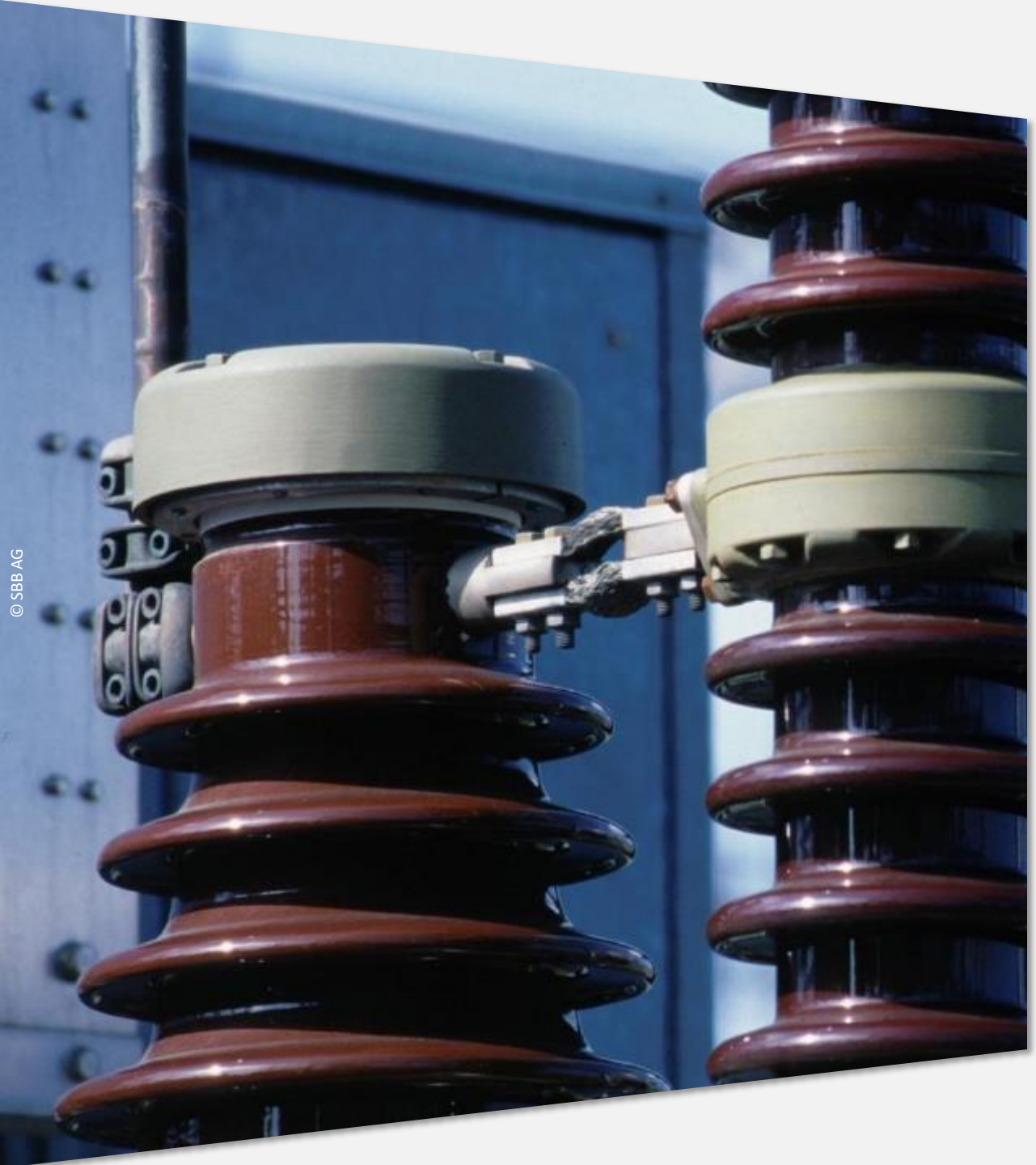
Q&A

Die 3 kritischen Netze der Bahn.

Ein Ziel: Bereitstellung Trassenkapazität*

- Stromnetz
- Telecomnetz
- Schienennetz

*die 11 260 Züge, welche sich täglich mit einer Pünktlichkeit von 91.9% auf den Gleisen sicher bewegen.



Die 3 kritischen Netze der Bahn.

Stromnetz

1872 km Übertragungsleitungen bringen 1635 GWh Leistung an den richtigen Ort.

8 Wasserkraftwerke und 372 Mitarbeiter:innen produzieren den benötigten Strom.

Die 3 kritischen Netze der Bahn.

Telekommunikationsnetz(e)

Schweizweites Telecomnetz sorgt dafür, dass Informationen an über 1000 Standorten verfügbar sind.

Mit GSM-R erreichen wir jeden Zug auf dem Normalspurnetz und steuern via ETCS die Züge auf Hochgeschwindig-keitsstrecken.

Jede:r Mitarbeiter:in verfügt über ein Gerät mit dem Informationen elektronisch abgerufen werden können.

Die 3 kritischen Netze der Bahn.

Schienennetz

3265 km Schienennetz mit 35 000 Signalen ermöglichen deine Reise.

503 Stellwerke steuern 656 Treibzüge und 1982 Personen-wagen ans Ziel.

Agenda.

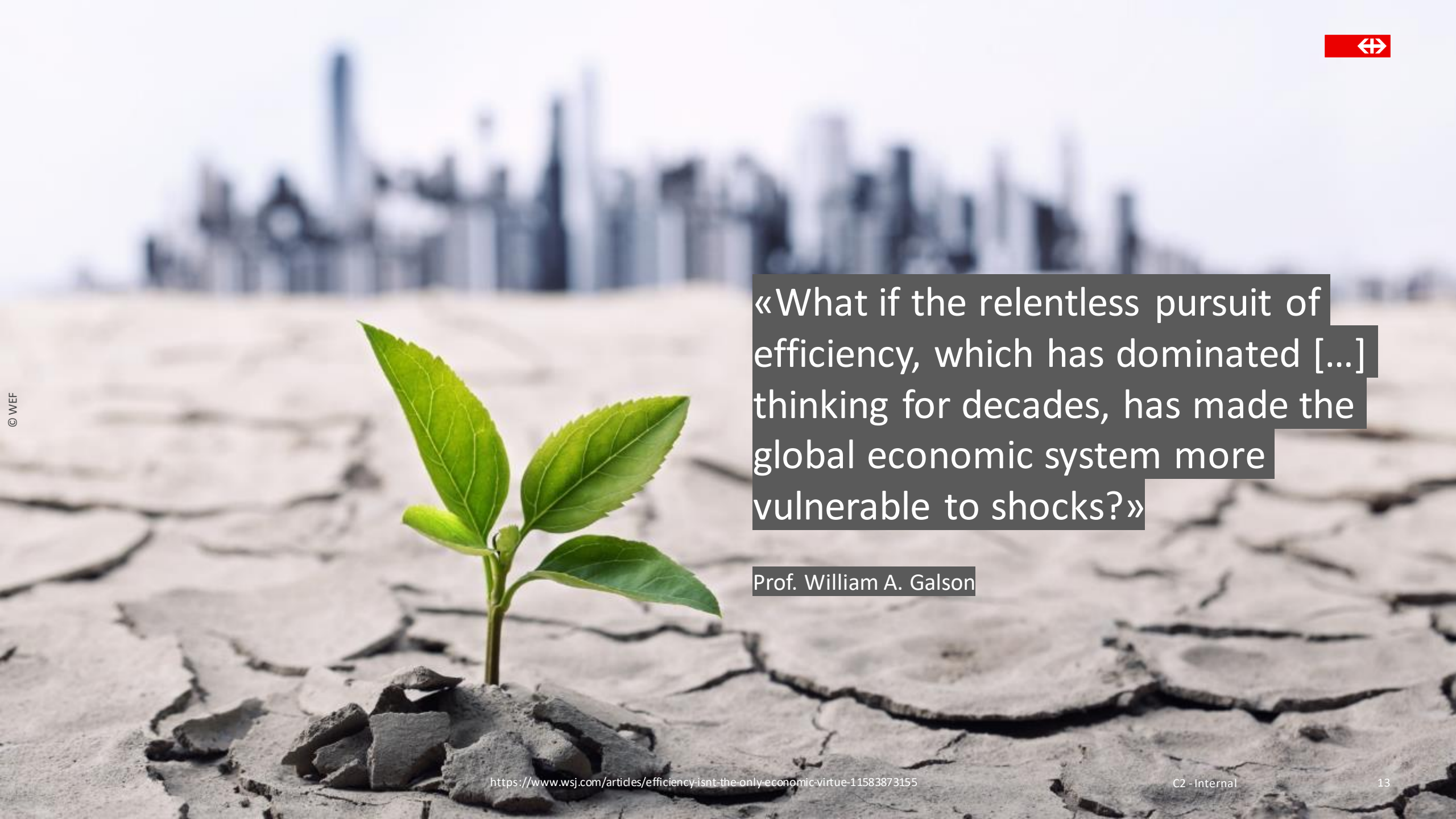
Kritische Infrastrukturen

Die SBB

Resilienz

Was tun?

Q&A



«What if the relentless pursuit of efficiency, which has dominated […] thinking for decades, has made the global economic system more vulnerable to shocks?»

Prof. William A. Galson

© WEF

https://www.wsj.com/articles/efficiency-isnt-the-only-economic-virtue-11583873155

Elektronik vor Beton.

1980: Mensch als Brücke zwischen den Ebenen

- Mensch als Vermittler zwischen den Ebenen
- Geprägt von System- und Medienbrüchen
- Örtlich begrenzte und autarke Produktionsinseln
- 50 Züge pro Strecke und Tag mit 16‘000 Mitarbeitenden

Elektronik vor Beton.

2015: Automatisierte Bahnproduktion

- Zentrale und automatisierte Betriebsführung
- Überregionale Rückfallebenen
- Computer bedient Stellwerk aufgrund von Daten (Fahrplan, Gleisbelegung, Dispo)
- Mehr als doppelt so viele Züge pro Strecke und Tag mit knapp der Hälfte der Mitarbeitenden

Heute: 7653 Züge pro Tag und 12.5 Mrd. Personenkilometer

Effiziente Resilienz?

Effizienz: Verhältnis der eingesetzten Mittel zum Erfolg. Die optimale Anpassung an die Umgebung.

Resilienz: Die Fähigkeit auf disruptive Veränderungen der Umgebung zu reagieren

…und wer sagt es dem CEO?

Resilience-by-Design

Agenda.

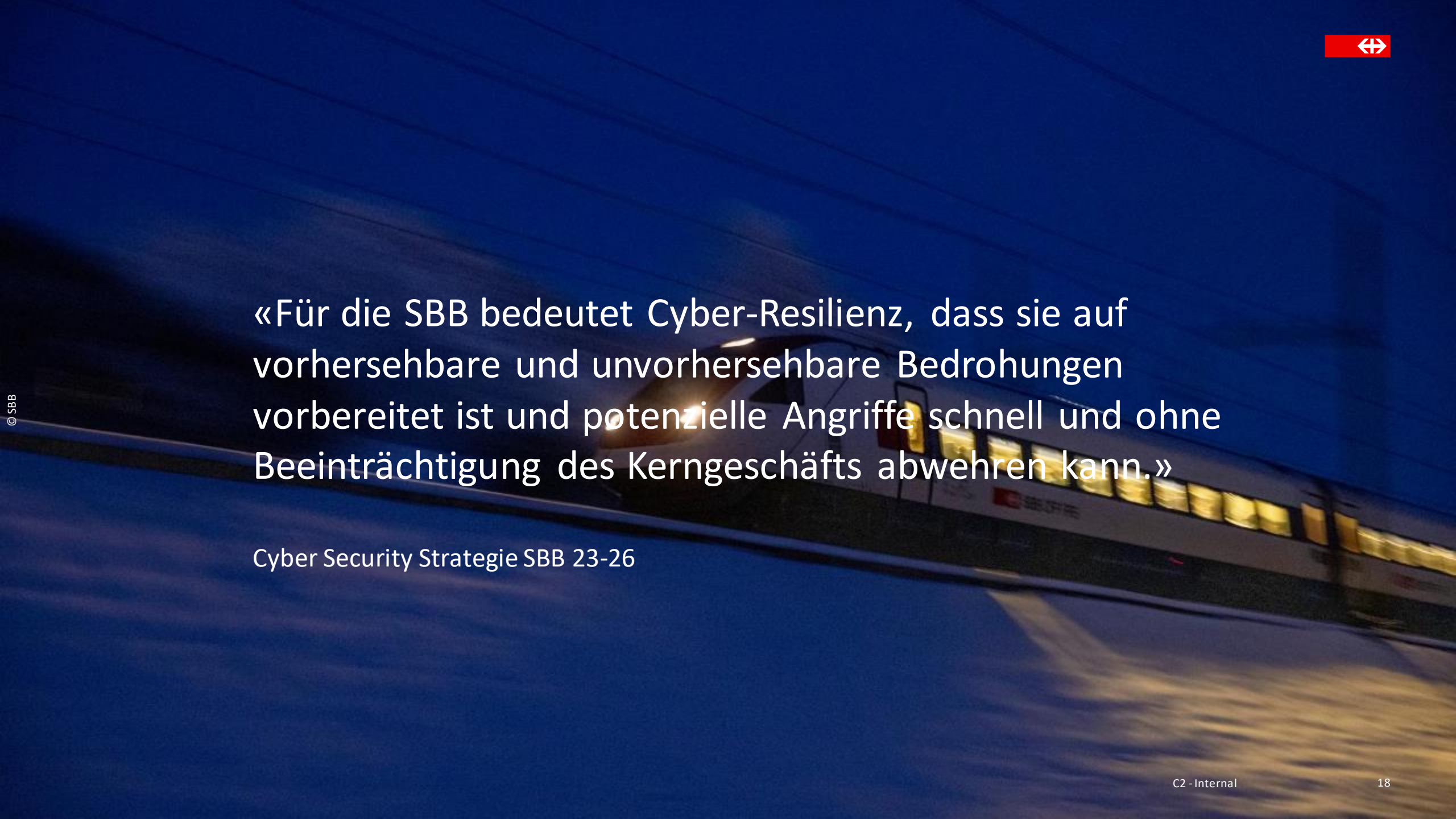
Kritische Infrastrukturen

Die SBB

Resilienz

Was tun?

Q&A



«Für die SBB bedeutet Cyber-Resilienz, dass sie auf vorhersehbare und unvorhersehbare Bedrohungen vorbereitet ist und potenzielle Angriffe schnell und ohne Beeinträchtigung des Kerngeschäfts abwehren kann.»

Cyber Security Strategie SBB 23-26

Cyber Risiken und Nebenwirkungen.

Herausforderungen einer integrierten Bahn

- Digitalisierung & Automatisierung vergrössern die Angriffsfläche
- Komplexität nimmt zu, das System reagiert empfindlich auf Störungen
- Veränderung der Bedrohungslage – Unsicherheit bezüglich der Securitylage
- LifeCycle-Management im Bereich der Operational-IT (OT) ist herausfordernd
- Kulturelle Aspekte insbesondere bei OT
- Zulassungen basieren auf veralteten Vorstellungen
- Geschäftsprozesse verändern die OT
- (Neue) Gesetze & Regulationen (CH + EU)
- Ungenügende Security bei Herstellern

Cyber Security für resilientere Infrastrukturen.

Menschen

- Awareness schaffen – Mitarbeitende schulen
- Kulturwandel initiieren
- Gemeinsamkeiten und nicht Unterschiede finden
- Umgang mit Unsicherheit lernen
- Superhelden gibt es nicht ☺

Cyber Security für resilientere Infrastrukturen.

Maschinen

- Cyber Hygiene
- Best of Suite oder Breed
- Chaos Monkey
- Cloud
- Zero Trust 

Cyber Security für resilientere Infrastrukturen.

Umfeld

- Lieferanten unterstützen – beide Parteien lernen
- Zusammenarbeit mit Regulator intensivieren
- Koordinierte (Verbunds-) Übungen
- Risiken managen, nicht die Methode

«Sind zwei Wanderer in der Wüste…»

Jan Hohenauer
Stv. CISO | cyberART Servant Leader

SBB AG
Cyber Security
Digital Governance
Trüsselstrasse 2, 3000 Bern 65
Mobile +41 79 301 60 55
Direkt +41 51 285 10 80
jan.hohenauer@sbb.ch | www.sbb.ch

Information Security SBB: cyber@sbb.ch | https://cyber.sbb.ch