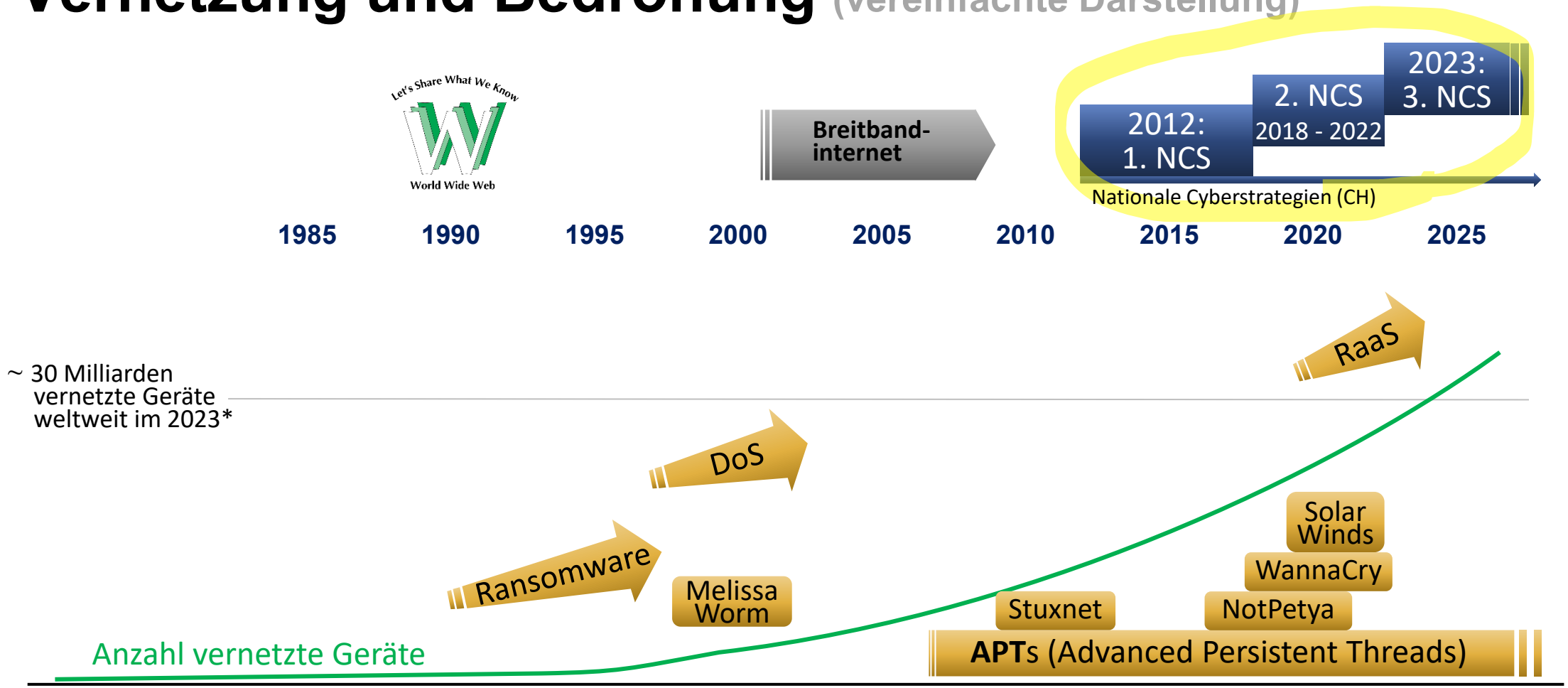
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK
Bundesamt für Verkehr BAV
Abteilung Sicherheit

Technischer Ausblick auf Richtlinien in Bezug auf Cybersicherheits-massnahmen im öffentlichen Verkehr

25. Oktober 2023 - Tobias Hubschmid

Geschichtlicher Überblick der zunehmenden Vernetzung und Bedrohung (vereinfachte Darstellung)



«Aktuelle» Bedrohungslandschaft siehe https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

*) Quelle: https://www.rcrwireless.com/20200218/internet-of-things/connected-devices-will-be-3x-the-global-population-by-2023-cisco-says

Die 5 strategischen Ziele der Nationalen Cyberstrategie NCS

Selbstbefähigung mit den Massnahmen M1-M4

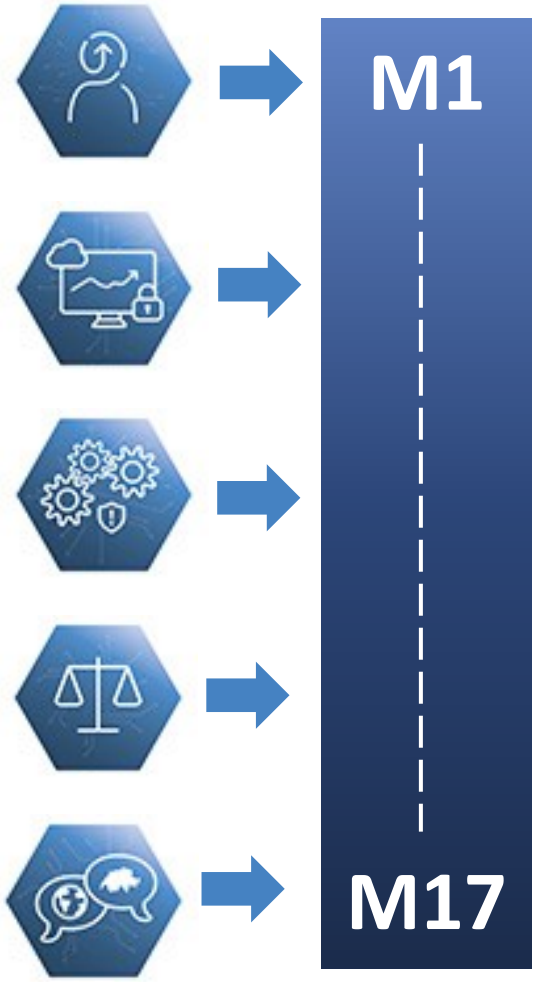
Sichere und verfügbare digitale Dienstleistungen und Infrastruktur mit den Massnahmen M5, M6, M7

Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen mit den Massnahmen M8-M11

Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität mit den Massnahmen M12-M14

Führende Rolle in der internationalen Zusammenarbeit mit den Massnahmen M15-M17

Massnahmen der neuen NCS



Die Massnahmen **bauen auf den bisherigen Aktivitäten auf** und spezifizieren, wie diese ausgebaut, weiterentwickelt und ergänzt werden müssen, um die strategischen Ziele zu erreichen. Es wird zudem aufgezeigt, welche Schwerpunkte bei der Umsetzung der Massnahmen gesetzt werden und welche Akteure dabei involviert sind. Die Auflistung der Schwerpunkte widerspiegelt dabei den Stand bei Erstellung der Strategie und wird durch den Steuerungsausschuss NCS geprüft und bei Bedarf ergänzt.

Sichere und verfügbare dig. Dienstleistungen u. Infrastruktur

Ziel 2:

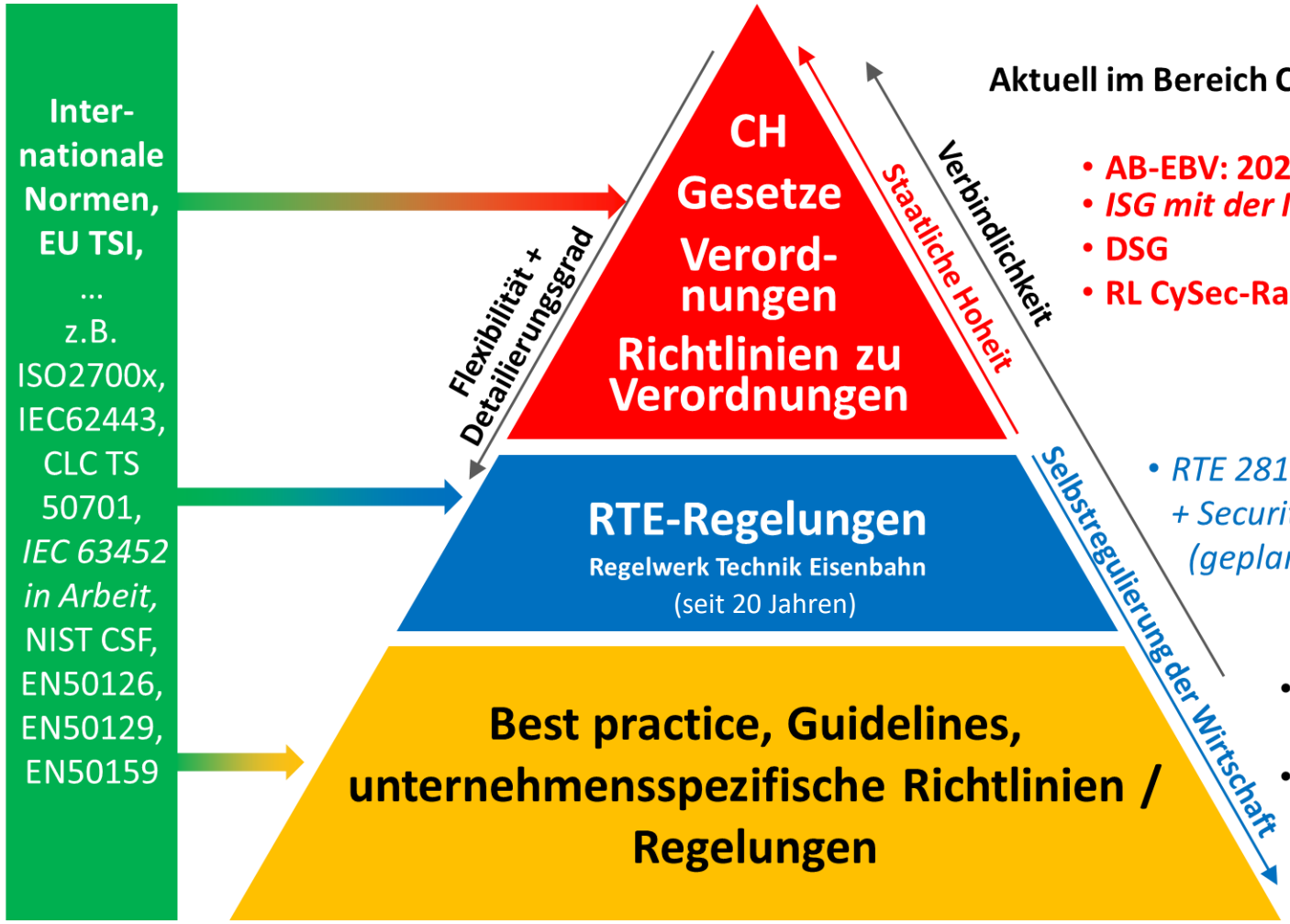
Die Schweiz setzt flächendeckend Massnahmen zur **Stärkung der Cyberresilienz** um. Bund und Kantone schaffen die **nötigen Rahmenbedingungen** dafür, dass ein hohes Schutzniveau gewährleistet ist, sichere digitale Infrastrukturen, Produkte und Dienstleistungen eingesetzt werden und die **Risikobereitschaft bewusst gesteuert** wird.

Massnahme **M5**:
Schwachstellen erkennen und verhindern

Massnahme **M6**:
Resilienz, Standardisierung und Regulierung

Massnahme **M7**:
Ausbau der Zusammenarbeit zwischen den Behörden

Regelungspyramide am Beispiel Eisenbahnsektor



Aktuell im Bereich Cybersicherheit und Datenschutz:

- **AB-EBV: 2020** Art. 5c
- ***ISG mit der Meldepflicht*** *(geplant)*
- **DSG**
- **RL CySec-Rail**

- *RTE 28100 Datennetze - Safety + Security (geplant - aktuell in der Lesung)*

- **Handbuch Cybersecurity für Betriebe des öV,**
- Diverse, weitere Guidelines

Abkürzungen

AB-EBV	Ausführungs-bestimmungen zur Eisenbahnverordnung
DSG	Datenschutzgesetz
ISG	Informationssicher-heitsgesetz
EU TSI	Europäische technische Spezi-fikationen für die Interoperabilität
RL	Richtlinie
CySec-Rail	Cybersicherheit Eisen-bahn

Aktueller Stand der CySec-Massnahmen im öV*

Im Bereich Standardisierung und Regulierung:

Allgemein im öV

Das Handbuch Cyber Security für Betriebe des öV ist seit Dezember 2020 publiziert.

Eisenbahnsektor

- Der «Cyberartikel» Art. 5c.1 in den AB-EBV ist seit November 2020 in Kraft
- Die neue RL CySec-Rail mit den Mindestanforderungen an ein ISMS tritt per 1.07.2024 zusammen mit der revidierten EBV und der revidierten AB-EBV in Kraft. In der Richtlinie werden die für den Eisenbahnsektor gängigen Standards aufgeführt (siehe auch folgende Folie).

Strasse

UNECE WP.29-Regelung R155 ➔ neue Vorgaben seit 2022 für neue Fahrzeuge und für alle Fahrzeuge ab dem 07.2024 (siehe https://www.astra.admin.ch/astra/de/home/themen/verkehrssicherheit/fahrassistenzsysteme/alle-fahrzeuge.html#accordion_581869727168007514230 3 und https://certx.com/de/automotive/unece-wp-29-r155-how-cyber-security-will-impact-the-automotiva-market-as-of-june-2022/)

Schifffahrt

Good-Practice-Leitfaden Cybersicherheit für die Binnenschifffahrt der CESNI

(siehe https://www.cesni.eu/wp-content/uploads/2023/05/Guide_cybersecurite_de.pdf)

Seilbahnen

Aktuell keine seilbahnspezifischen Cybersicherheitsvorgaben / Richtlinien oder Leitfäden vorhanden

*in Bezug zur Massnahme 6 der neuen NCS (resp. M5 der NCS 2018-2022)

Richtlinie Cybersicherheit Eisenbahn (RL CySec-Rail)

Die Richtlinie Cybersicherheit Eisenbahn hat das Ziel,

1. den «Cyberartikel» AB 5c.1 in den AB-EBV zu konkretisieren,
2. die minimalen Anforderungen an das geforderte Informationssicherheitsmanagementsystem (ISMS) zu definieren und den Bezug zum Sicherheitsmanagementsystem (SMS) resp. zum Integrierten Managementsystem (IMS) herzustellen,
3. die Hilfsmittel zum Aufbau eines ISMS und im Umgang mit Cybersicherheit bereit zu stellen und auf bestehende Hilfsmittel hinzuweisen.

Die RL CySec-Rail orientiert sich am risikobasierten, umfassenden Ansatz, wie er in der neuen NCS beschrieben ist.
Die Grundlage bilden insbesondere die internationalen ISO 2700x Normen, sowie das IEC 62443 wie auch das NIST CSF Framework und die neue CLC TS 50701:2023.

Internationale CySec-Massnahmen (Gesetze, Verordnungen) für KRITIS-Infrastrukturen/Produkte:

NIS2 Directive der EU

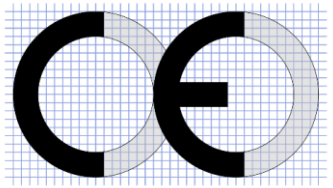
Am 16. Januar 2023 verabschiedeten das EU-Parlament und der Rat die Richtlinie 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Massnahmen für ein hohes gemeinsames Mass an Cybersicherheit in der Union. Die NIS2 erweiterte den Geltungsbereich. Die NIS2 zielt auch darauf ab, den EU-Ansatz für die Meldung von Vorfällen, Sicherheits-anforderungen, Aufsichtsmassnahmen und den Informationsaustausch zu harmonisieren.

Siehe https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Cyber Resilience Act (CRA) der EU

Der CRA ist eine Cybersicherheitsregulierung der EU, die am 15.09.2022 von der Europäischen Kommission vorgeschlagen wurde, um die Cybersicherheit und Cyberresilienz in der EU durch gemeinsame Cybersicherheitsstandards für Produkte mit digitalen Elementen in der EU zu verbessern.
Der Entwurf des CRA ist verfügbar.

Siehe https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act



KRITIS: Kritische Infrastrukturen
NIS: Network and Information Security

Eisenbahnspezifische, internationale CySec-Massnahmen (Gesetze, Verordnungen):

Aktuell sind **keine eisenbahnspezifische** Gesetze, Verordnungen resp. Richtlinien im Bereich der Cybersicherheit in der EU in Kraft.

Aktueller **Guideline im Bereich ERTMS**
(European **R**ail **T**raffic **M**anagement **S**ystem**)**

- Presseartikel siehe SIGNAL + DRAHT 9 / 2023
  https://incyde.com/topic/cyber-security-measures-for-ertms-from-the-rail-operators-perspective

- Guideline und Tool siehe
  https://ertms.be/activities/ertms-security-core-group

Cyber-Security-Maßnahmen für ERTMS aus Sicht der Bahnbetreiber

Cyber security measures for ERTMS from the rail operators' perspective

Richard Poschinger | Christof Jungo | Ernst Kleine | Martin Espenschied

Durch eine steigende digitale Gefährdungslage rückt die Cyber Security im Bahnbereich verstärkt in den Vordergrund. Die Anzahl der mit dem europäischen digitalen Zugbeeinflussungssystem ETCS betriebenen Strecken steigt. Der damit einhergehende Bedarf zur securityspezifischen Absicherung von ETCS resultierte innerhalb der ERTMS Users Group (EUG) in der Gründung der ERTMS Security Core Group (ESCG). Die Arbeit der ESCG resultierte in umfangreichen, praktisch anwendbaren Security-Maßnahmen und Vorschlägen für die zukünftige Entwicklung von ETCS.

1 Einleitung

Bei der Etablierung der verbindlichen europäischen Interoperabilitätsspezifikationen (TSI CCS) für ERTMS (European Railway Traffic Management System) wurde das Thema Security bisher nicht adressiert. Erst in der erst kürzlich vereinbarten TSI CCS 2023 wurde dieses Thema aufgenommen, allerdings nur auf generischer Ebene.

1.1 Gründung und Aufbau der ESCG

Die Entwicklung und Umsetzung des ERTMS ist eine der Maßnahmen zur Schaffung eines transeuropäischen Eisenbahnnetzes. Die EUG (www.ertms.be) bündelt das Wissen und die Erfahrung ihrer Mitglieder, um die Einführung des ERTMS zu unterstützen und sicherzustellen, dass es sich um ein sicheres, zuverlässiges und in-

The growing digital threat means that cyber security is assuming an increasingly prominent role in the railway sector. More lines are being operated with ETCS, the European digital train control system. The consequent need to provide ETCS with specific security protection was the impetus for establishing the ERTMS Security Core Group (ESCG) within the ERTMS Users Group (EUG). The work undertaken by the ESCG has resulted in comprehensive security measures with practical applications and proposals for the future development of ETCS.

1 Introduction

Security was not specifically addressed when the mandatory European interoperability specifications (TSI CCS) for ERTMS (the European Railway Traffic Management System) were drawn up. This subject has only been taken up in the recently agreed TSI CCS 2023 and even then only at a generic level.

1.1 The establishment and structure of the ESCG

The development and implementation of ERTMS are some of the measures behind the creation of a trans-European rail network. The EUG (www.ertms.be) pools the knowledge and experience of its members in order to support the introduction of ERTMS and ensure that it is a safe, reliable and interoper-

SIGNALLING + DATACOMMUNICATION (115) 9 / 2023 63

Fazit

Im Bereich der Cybersicherheit gibt es für kritische Infrastrukturen des öV* mittlerweile viele Guidelines und Regelwerke. Im Bereich der Normen laufen diverse Aktivitäten.
Bei der Harmonisierung/Konsolidierung der Regelwerke (inkl. Normen) ist noch Potential vorhanden.
Das Thema Cybersicherheit ist in der Branche angekommen und wird ernst genommen. Auf verschiedenen Ebenen laufen Aktivitäten, um die Resilienz der öV-Infrastruktur zu erhöhen.
Die nationale und internationale Koordination zwischen den Akteuren ist ein entscheidender Erfolgsfaktor.

picture: flaticom.com

Wir befinden uns nicht in einem Sprint, sondern in einem Bergmarathon!

*) inkl. deren Energieversorgung (Bahnstrom, etc.) und deren Telekommunikationsinfrastruktur

Vielen Dank für Ihre Aufmerksamkeit!

25.10.2023

Tobias Hubschmid
tobias.hubschmid@bav.admin.ch
cybersecurity@bav.admin.ch