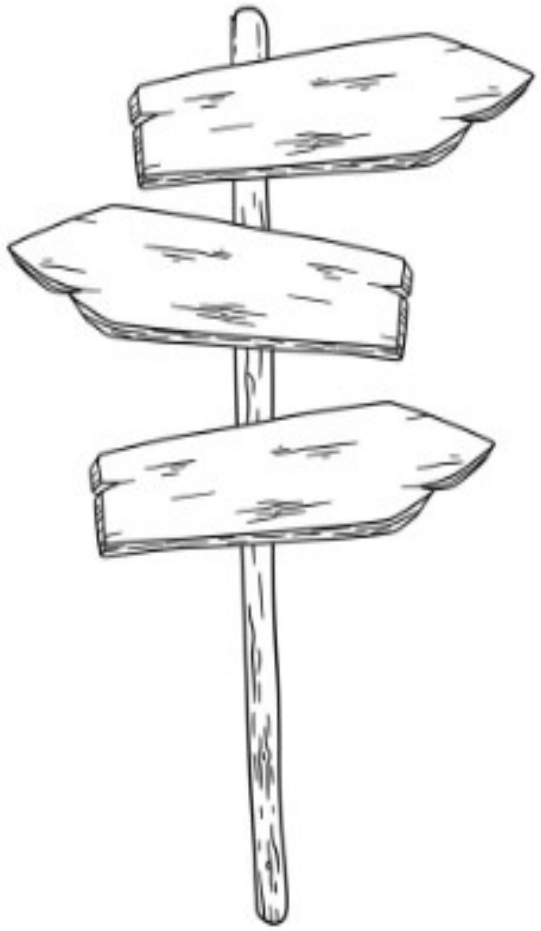
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Erwartungen an die Bahnen aus Sicht des Regulators und was darf die Branche vom Bund erwarten?

10.Juni 2024, Tobias Hubschmid, Andreas Studer, BAV

Agenda



- Vorstellung
- Aufgaben
- Hoheitliche Vorgaben
- Richtlinie CySec-Rail
- Safety vs. Security
- Erwartungen
- Grundsätze
- Dienstleistungen und Angebote

Warum das Ganze?

Viele Schweizer Firmen-Chefs unterschätzen das Risiko von Cyberattacken

Kleine und mittlere Unternehmen (KMU) in der Schweiz verlieren laut einer aktuellen Studie beim Thema Cybersicherheit den Anschluss.

News folgen

20.09.2023, 06:31 20.09.2023, 08:00

Das Thema Cybersicherheit wird von vielen
Firmen-Chefs gemäss einer Erhebung imm
unterschätzt. Vor allem bei der Umsetzung
Massnahmen zum Schutz vor Hackerangrif
kaum Fortschritte.

So wenig braucht es, um sich vor Hackern zu schützen

100 Ideen für ein besseres Leben: Eine Cyberattacke kann jeden treffen. Mit diesen drei einfachen Tipps wird das digitale Leben sicherer.

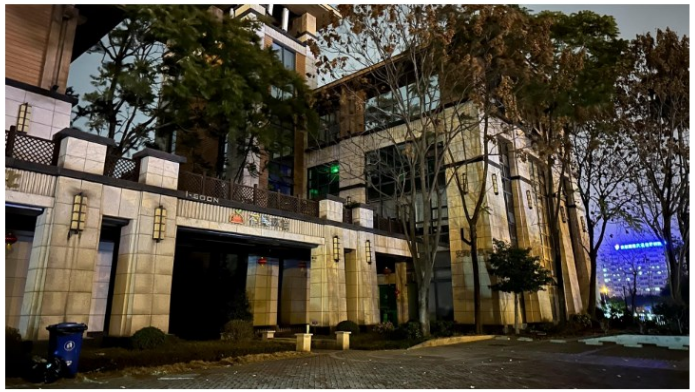
Lukas Mäder
30.03.2024, 21.45 Uhr 3 min

Hören Merken Drucken Teilen

Datenleck enttarnt Chinas Cyber-Armee

von Elisabeth Schmidt, Peking 26.02.2024 | 16:45

Anonym hochgeladene Daten geben erstmals Einblicke, wie private Cyber-Söldner in Chinas Staatsauftrag weltweit spionieren. Im Visier auch europäische Regierungen und die Nato.



Hackern der chinesischen IT-Firma I-Soon ist es offenbar gelungen, in Systeme ausländischer Regierungen einzudringen.

F+ HACKER-ANGRIFF AUF SPD

Bundesregierung macht Russland für Cyber-Attacke verantwortlich

Deutschland und seine Partner beschuldigen Moskau der Cyber-Attacke auf die E-Mail-Postfächer des SPD-Parteivorstandes. Die Bundesregierung kündigt Konsequenzen an. Auch die NATO will reagieren.

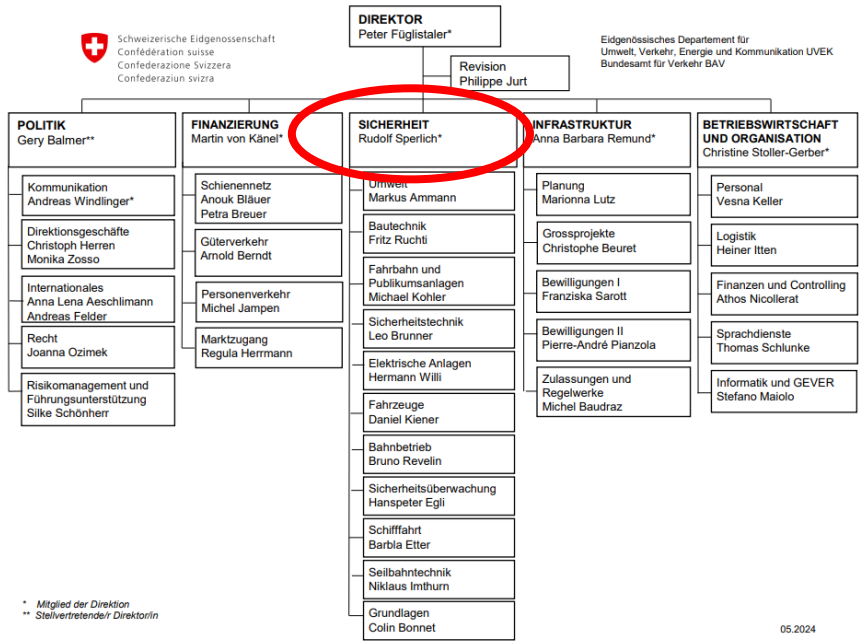
Friedrich Schmidt, Matthias Wyssuwa, Mona Jaeger

03.05.2024, 15:35 Uhr

Vorstellung – gemeinsam sind wir stärker!

Tobias Hubschmid
seit 1.05.2020 beim BAV und zuständig für das Kompetenzzentrum Cybersicherheit, Ausbildung: Dipl. el. Ing. HTL und dipl. Ing. in Informationstechnologie FH, CAS Cyber Security (ETHZ) und Ausbildung zum Fachauditor. Über 20 Jahre Berufserfahrung im Bereich der Informationssicherheit mit diversen Weiterbildungen

Andreas Studer
seit 1.03.2023 beim BAV und zuständig für das Kompetenzzentrum Cybersicherheit, Ausbildung: Dipl. Ing. FH in Biotechnologie, zertifizierter Beauftragter Computersystemvalidierung, CAS Cybersicherheit und Information Risk Management (FHNW), IT Sicherheitsbeauftragter BSI, Ausbildung zum Fachauditor, 20 Jahre Qualitätsmanagementerfahrung in der Industrie



Sicherheitstechnik
Leo Brunner

Kompetenzzentrum CySec

Aufgaben Kompetenzzentrum CySec BAV

Normative Phase

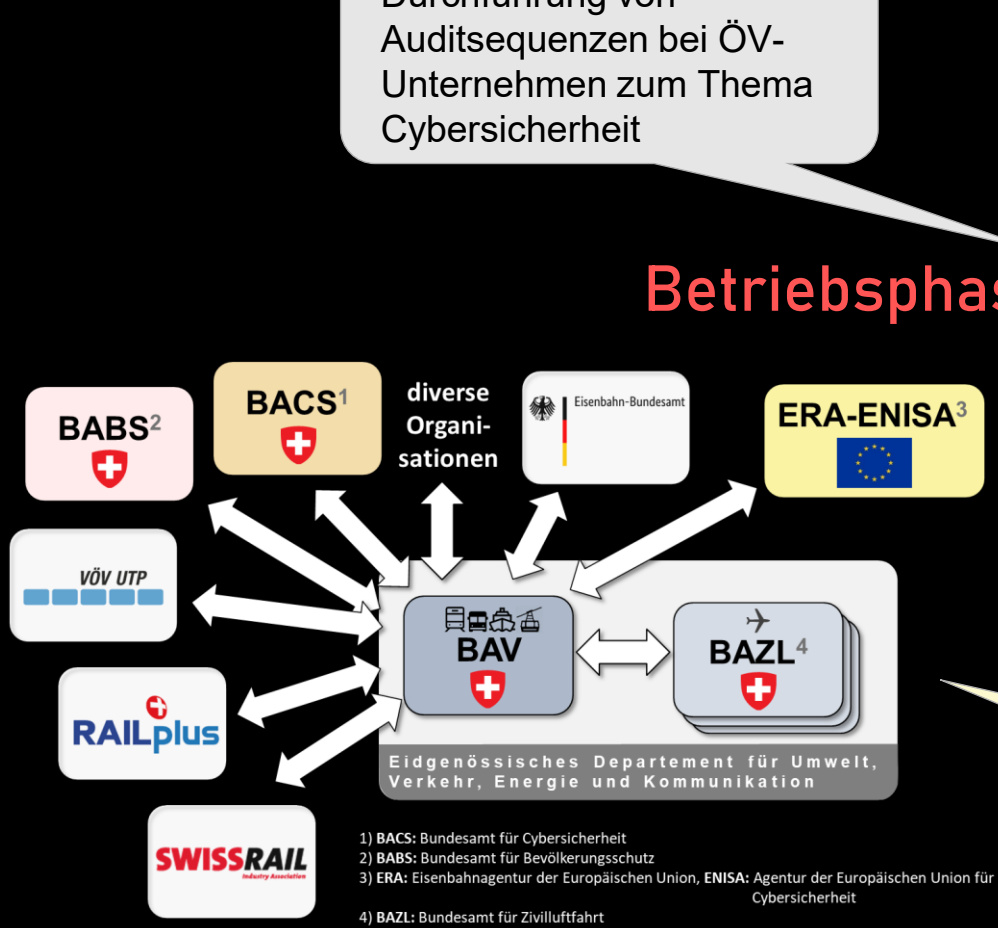
Erstellung und Revision von gesetzlichen Grundlagen

Festlegen von Mindest-anforderungen im Bereich der Cybersicherheit des öV
→ aktuell: Richtlinie Cybersicherheit Eisenbahn (RL CySec-Rail)

Durchführung von Auditsequenzen bei ÖV-Unternehmen zum Thema Cybersicherheit

Betriebsphase

Präventive Phase

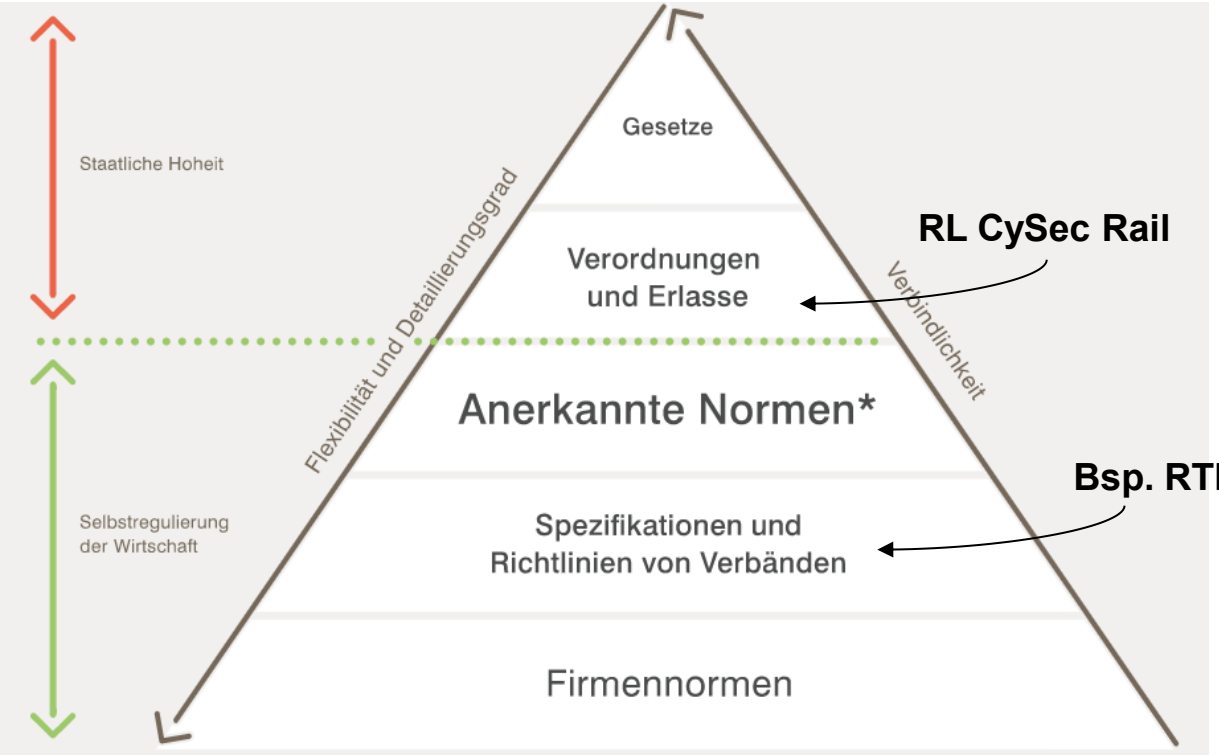


Risikoorientierte Prüfung von Betriebsbewilligungen, Plangenehmigungsverfahren und Typenzulassungen hinsichtlich der Cybersicherheit (innerhalb der ordentlichen Verfahren)

Schnittstellen- & Koordinationsarbeit, Sensibilisierung

Hoheitliche Vorgaben Eisenbahn

Quelle: www.fedlex.admin.ch, www.bav.admin.ch



- Eisenbahngesetz (EBG, 742.101, 01.07.1958)
- Verordnung über Bau und Betrieb der Eisenbahnen (EBV, 742.141.1, 01.01.1984)
- Ausführungsbestimmungen zur EBV (AB-EBV, 742.141.11, 01.11.2020)

→ Sicherheit ist integraler Teil aller Gesetzestexte

→ ICT-Security wird nur 1x explizit erwähnt → AB-EBV Art. 5c.1 (bisher)

→ Zahlreiche Normen und Standards in der Industrie vorhanden

* Normen sind per se nicht zwingend! Deren Einhaltung erhöht jedoch die Akzeptanz auf dem Markt

Normen sind in der Regel sehr umfangreich und technisch anspruchsvoll formuliert

Richtlinie CySec-Rail

Quelle:Richtlinien (admin.ch)

- Hilfsmittel und Ergänzung zur Umsetzung von bestehenden Normen. Kondensat aus NIST CSF, HB CySec VöV, ISO 2700x Reihe, VO 2018/762, CH-DSG, ISG, CLC TS50701 und IEC 62443

→ «Minimal» Standard / ISMS «light»

- **Anforderungen in Kapitel 7:**
  - Informationssicherheitsstrategie
  - Rollen und Verantwortlichkeiten
  - Richtlinien und Organisation
  - Regelmässige Überprüfung und KVP
  - Dokumentation
  - Risikobeurteilung und -behandlung

Generelle Erwartung BAV!

- **Basismassnahmen in Kapitel 8:**
  - Organisatorische, personelle, physische und technische Massnahmen (B-01 bis B-21)
  - Massnahmen im Bereich Operational Technology (B-22 bis B-27)
  - Massnahmen bei ICT-Systemen auf Eisenbahnfahrzeugen (B-28 und B-29)

Risikobasierter Ansatz

Safety vs. Security

Quelle: www.sichere-industrie.de / www.tuev-nord.de

RAMS: Reliability, Availability, Maintainability, Safety

Safety	Security (InfoSec)
Statisch, einmal umgesetzt, ändert sich die Maschine nicht wöchentlich	**Dynamisch** und schnelllebig - beim Aufkommen einer neuen Schwachstelle in einem Produkt kann unmittelbar eine Gefährdung entstehen
Aus gesetzlicher Sicht ist die Gewährleistung zwingend erforderlich	Eine traditionell freiwillige und durch wirtschaftliche Faktoren beeinflusste Investition (**Zeitenwende!**)
Schutz von Mensch und Umwelt vor physischem Schaden (RAMS)	Informationssicherheit, also in erster Linie **Datenschutz** (CIA)
Unfallvermeidung durch **sicher entwickelte Systeme und Betriebsprozesse (RAMS)** steht im Vordergrund.	**Cyberakteure mit unterschiedlicher Motivation, Geschäftsmodellen und unterschiedlichen Fähigkeiten** stehen im Vordergrund.
→ System für die **Betriebssicherheit**	→ **Informationssicherheit**

Ein System, das nicht «secure» ist, kann auch nicht «safe» sein! (Kontrollverlust).

«*Beide Bereiche wachsen zusammen und sind nicht mehr voneinander zu trennen. Daraus ergeben sich neue Herausforderungen, was wiederum zu neuen Anforderungsprofilen führt, um die Sicherheit auch künftig jederzeit zu gewährleisten..*» Zitat M. Springer, TÜV NORD, Projektleiter Security4Safety

Spezifische Erwartungen auf Strategieebene

- Die Zusammenarbeit in der Cybersicherheit wird gefördert. In der Branche wird dazu ein gemeinsames Verständnis geschaffen (auch zwischen Safety- und Security-Teams).
- Konkret (siehe insbesondere Kapitel 7 der RL CySec-Rail):
  - Eine Informationssicherheitsstrategie im Unternehmen ist vorhanden.
  - Minimal muss eine verbindliche Roadmap zur Einführung des ISMS vorhanden sein! (Stand Mai 2024).
  - Die wichtigsten Prozesse werden angewendet (z.B. Asset-Mgmt, Risk-Mgmt.).
  - Die notwendigen Ressourcen für die Zielerreichung der Cybersicherheit werden von der obersten Führungsebene zur Verfügung gestellt.
- Schwerpunkte werden gesetzt: Z.B. Fokus auf die Cyberhygiene: **Machen** was machbar ist und zudem Aufmerksamkeit auf die aktuellen Schwachstellen und Toprisiken – Schriftliches Festhalten.

Spezifische Erwartungen auf operativer Ebene

- Die Akteure auf operativer Ebene stellen sich auf eine spannende, abwechslungs-reiche und herausfordernde «Bergtour» mit unzähligen Etappen ein und sind bereit die Komfortzone zu verlassen.
- Von der «Norming-» in die «Performing Phase» kommen.
- Gegenseitige Unterstützung. Die CySec betrifft nicht Einzelne, sondern alle.
- Kontinuierliche Verbesserung (siehe RL CySec-Rail, A-05).
- Zumindest grössere ISB/EVU verfügen über ein etabliertes und gelebtes ISMS und können für kleinere Transportunternehmen eine Hilfestellung sein.

Grundsätze Kompetenzzentrum CySec BAV

Grundsatz I:	Das BAV gibt nicht das «Wie» vor, sondern das «Was» Stossrichtung vorgeben und soweit möglich unterstützen
Grundsatz II:	Risikobasierter, pragmatischer Ansatz
Grundsatz III:	gelebte Politik der offenen Kanäle. E-Mail, Telefon, physische (informelle) Treffen sind möglich

Generelle E-Mail: cybersecurity@bav.admin.ch
Telefon Tobias: +41 58 48 56490
Telefon Andreas: +41 58 46 25904

BAV-Dienstleistungen und Angebote

- Ausrichtung nach nationalen und internationalen Vorgaben (z.B. Nationale Cyber Strategie, NIS2 (Europäisch), Normen, Standards) - mit Einflussnahme dort wo möglich.
- Weiterentwicklung von Vorgaben und Hilfsmitteln in Zusammenarbeit mit der Branche und dem BACS.
- Etablierte Zusammenarbeit mit den Verbänden und Interessenvertretern auf Augenhöhe.
- Unterstützen der Arbeiten der Branchenorganisationen (z.B. RTE 28100).
- Vor Ort Fachaudits bei ISB/EVU als Chance für alle Beteiligte.
- Förderung der Zusammenarbeit/Informationsaustausch innerhalb der Branche und branchenübergreifend (Beispiel ERFA-Tagung Cybersecurity SA).
- Informationsbeschaffung zum Thema Cybersicherheit amts- und departementsübergreifend.

→ Vorsicht: Abgrenzung BAV vs. BACS (siehe folgende Folie)

Abgrenzung CySec Expertise BAV-BACS

CySec-Expertise BAV https://www.bav.admin.ch/bav/de/home/allgemeine-themen/sicherheit/cybersicherheit.html	**CySec-Expertise BACS** https://www.ncsc.admin.ch/ncsc/de/home/ueber-ncsc/das-ncsc.html https://www.ncsc.admin.ch/ncsc/de/home/ueber-ncsc/strategie-bacs.html
Bahn- und öV-spezifisches Wissen, Brücke zur OT und zur Safety (Technologien, Prozesse, Regelwerk, Normen, etc.).	Erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen.
Aufsicht und zuständig für das Regelwerk im Eisenbahnsektor und im öV (inkl. CySec).	Verfügt über breite sowie spezifische Fach- und Methodenkompetenz in der Cybersicherheit.
Prüfung von Bewilligungsverfahren (inkl. CySec-Belange).	Betreibt das GovCERT, hat langjährige Erfahrungen und verfügt über entsprechende Expertise bei der Vorfallbewältigung.
Akkreditierte Stelle um Fachaudits durchzuführen, inkl. zertifizierte Auditoren.	Autorisierungsstelle zur Vergabe von CVE-Nummern (Schwachstellenmanagement).
Zugriff auf ein Netzwerk im öV-Bereich, wie auch innerhalb UVEK und amtsübergreifend.	Zugriff auf ein nationales und internationales Netzwerk.

Abschluss

Zusammenfassend ist Folgendes mitzunehmen:

- Gemeinsames Ziel
- Wichtigkeit der Zusammenarbeit
- Bedrohungen nehmen zu, darum steigen die Anforderungen
- JETZT ist es an der Zeit