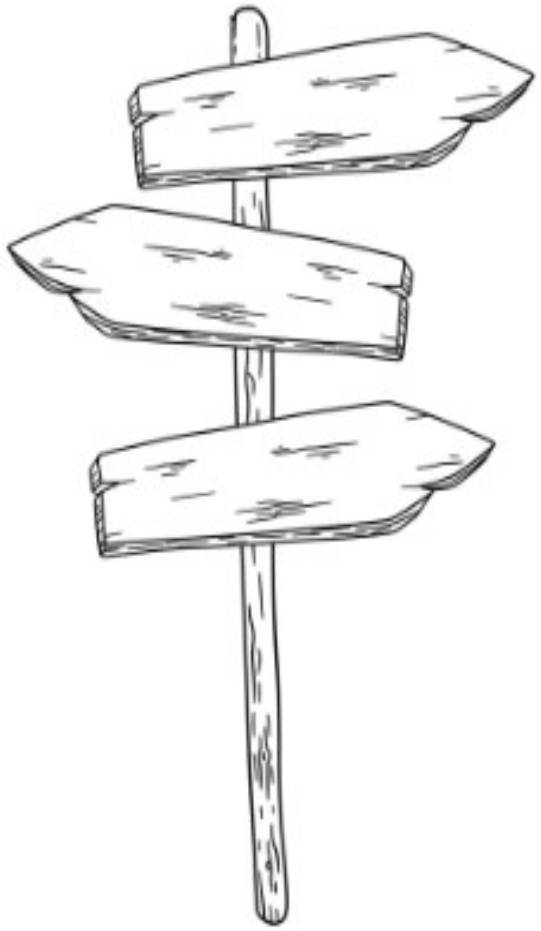
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Attentes envers les chemins de fer du point de vue du régulateur et que peut attendre la branche de la Confédération ?

10 juin 2024, Tobias Hubschmid, Andreas Studer, OFT

Agenda



- Présentation
- Tâches
- Directives souveraines
- Directive CySec-Rail
- Sécurité vs. sûreté
- Attentes
- Principes
- Services et offres

Pourquoi tout cela ?

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.

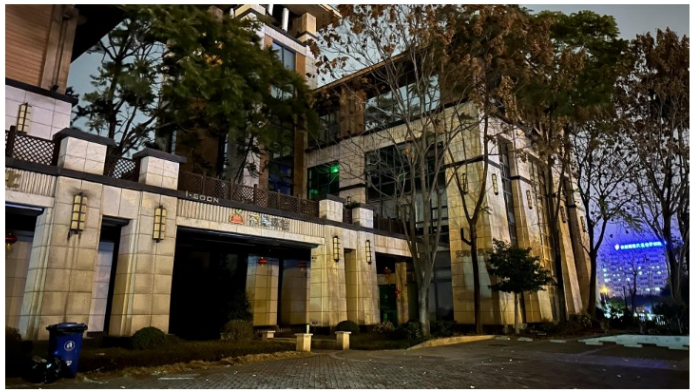
Lukas Mäder
30.03.2024, 21.45 Uhr 3 min

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.

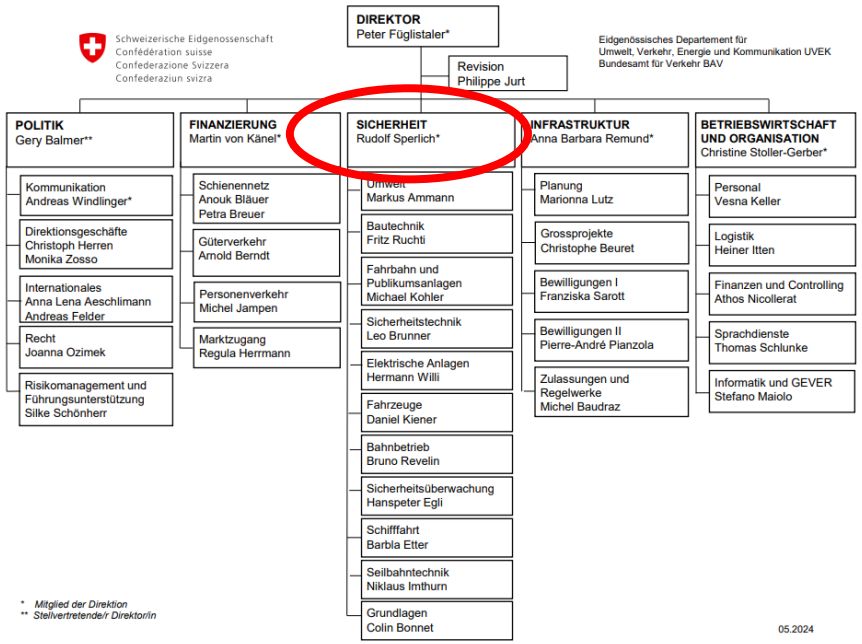
Friedrich Schmidt, Matthias Wyssuwa, Mona Jaeger

03.05.2024, 15:35 Uhr

Présentation - ensemble, nous sommes plus forts !

Tobias Hubschmid
depuis le 1.05.2020 à l'OFT et responsable du centre de compétences en cybersécurité, formation : Ingénieur électricien ETS et ingénieur diplômé en technologies de l'information HES, CAS Cyber Security (EPFZ) et formation d'auditeur spécialisé. Plus de 20 ans d'expérience professionnelle dans le domaine de la sécurité de l'information avec diverses formations continues.

Andreas Studer
depuis le 1.03.2023 à l'OFT et responsable du centre de compétences en cybersécurité, formation : Ingénieur HES en biotechnologie, chargé de validation de systèmes informatiques certifié, CAS Cybersécurité et Information Risk Management (FHNW), chargé de sécurité IT BSI, formation d'auditeur spécialisé, 20 ans d'expérience en gestion de la qualité dans l'industrie.



Sicherheitstechnik
Leo Brunner

Centre de compétence CySec

Tâches du centre de compétences CySec OFT

Phase normative

Élaboration et révision de bases légales

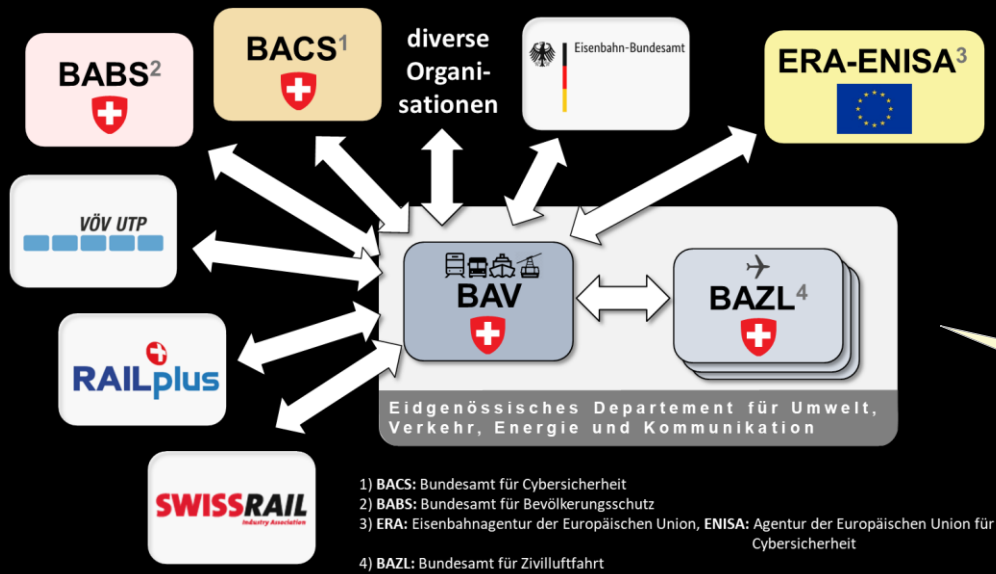
Définition d'exigences minimales dans le domaine de la cybersécurité des transports publics
→ actuellement : directive Cybersécurité ferroviaire (RL CySec-Rail)

Phase préventive

Examen axé sur les risques des autorisations d'exploiter, des procédures d'approbation des plans et des homologations de série en ce qui concerne la cybersécurité (dans le cadre des procédures ordinaires)

Phase d'exploitation

Réalisation de séquences d'audit auprès d'entreprises de transports publics sur le thème de la cybersécurité

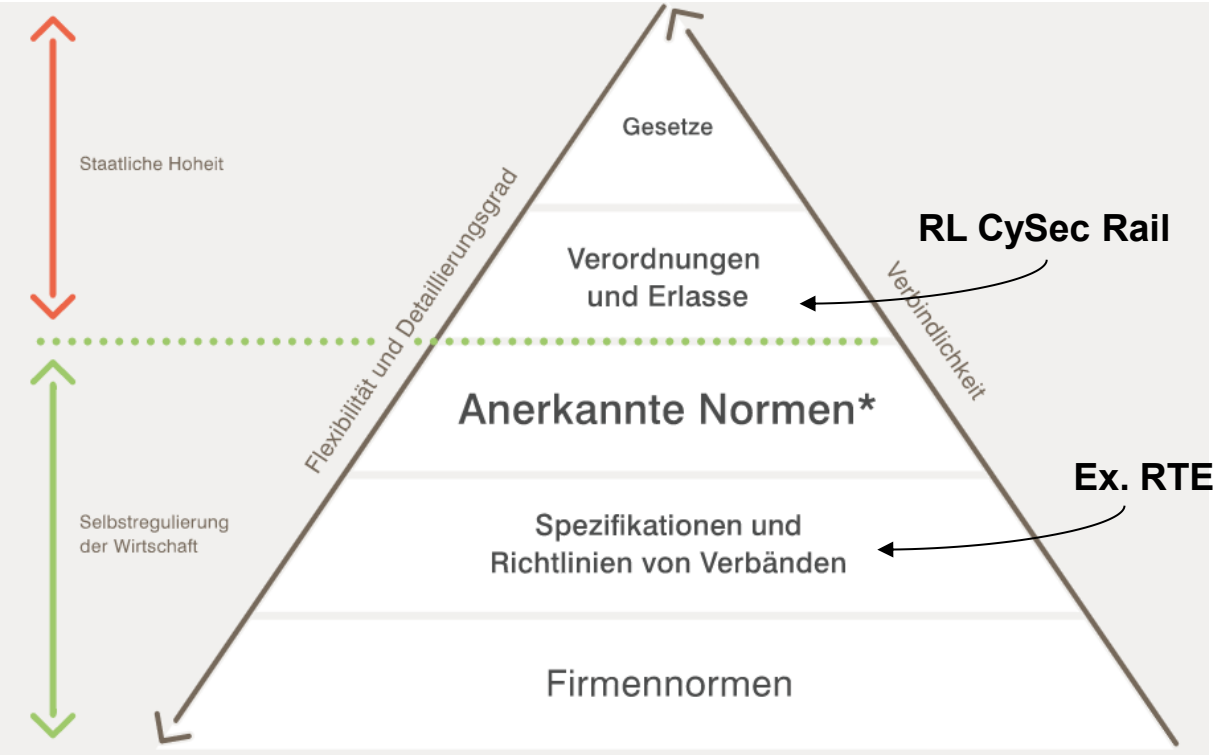


1) **BACS:** Bundesamt für Cybersicherheit
2) **BABS:** Bundesamt für Bevölkerungsschutz
3) **ERA:** Eisenbahnagentur der Europäischen Union, **ENISA:** Agentur der Europäischen Union für Cybersicherheit
4) **BAZL:** Bundesamt für Zivilluftfahrt

Travail d'interfaces & de coordination, sensibilisation

Directives souveraines des chemins de fer

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



- Loi sur les chemins de fer (LCdF, 742.101, 01.07.1958)
- Ordonnance sur la construction et l'exploitation des chemins de fer (OCF, 742.141.1, 01.01.1984)
- Dispositions d'exécution de l'OBE (DE-OBE, 742.141.11, 01.11.2020)

→ La sécurité fait partie intégrante de tous les textes de loi

→ La sécurité TIC n'est mentionnée explicitement qu'une seule fois → DE-OCF art. 5c.1 (jusqu'à présent)

→ Nombreuses normes et standards disponibles dans l'industrie

* Les normes ne sont pas obligatoires en soi ! Leur respect augmente cependant l'acceptation sur le marché.

les normes sont généralement très complètes et formulées de manière très technique

Directive CySec-Rail Source:Directives (admin.ch)

- Aide et complément pour la mise en œuvre des normes existantes. Condensé de NIST CSF, HB CySec UTP, série ISO 2700x, VO 2018/762, nCH-DSG, ISG, CLC TS50701 et IEC62443 → "Standard "Minimal / SGSI «light»

- **Exigences du chapitre 7 :**
  - Stratégie de sécurité de l'information
  - Rôles et responsabilités
  - Directives et organisation
  - Contrôle régulier et PAC
  - Documentation
  - Évaluation et traitement des risques

Attente générale de l'OFT !

- **Mesures de base au chapitre 8 :**
  - Mesures organisationnelles, personnelles, physiques et techniques (B-01 à B-21)
  - Mesures dans le domaine de la technologie opérationnelle (B-22 à B-27)
  - Mesures concernant les systèmes TIC sur les véhicules ferroviaires (B-28 et B-29)

Approche basée sur les risques

Sécurité vs. sûreté

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

RAMS : fiabilité, disponibilité, maintenabilité, sécurité

Sécurité	Sécurité (InfoSec)
Statique, une fois mise en œuvre, la machine ne change pas toutes les semaines	**Dynamique** et évoluant rapidement - l'apparition d'un nouveau point faible dans un produit peut entraîner un risque immédiat.
D'un point de vue légal, la garantie est obligatoire	Un investissement traditionnellement volontaire et influencé par des facteurs économiques (**changement d'époque !**)
Protection des personnes et de l'environnement contre les dommages physiques (RAMS)	Sécurité de l'information, donc en premier lieu **protection des données** (CIA)
La prévention des accidents grâce à **des systèmes et des processus d'exploitation développés en toute sécurité (RAMS)** est au premier plan.	**Les cyberacteurs, avec des motivations, des modèles commerciaux et des capacités différentes**, sont au premier plan.
→ Système pour la **sécurité de fonctionnement**	→ S**écurité de l'information**

Un système qui n'est pas "secure" ne peut pas non plus être "safe" ! (perte de contrôle).

"*Les deux domaines se rejoignent et ne peuvent plus être séparés. Il en résulte de nouveaux défis, ce qui entraîne à son tour de nouveaux profils d'exigences afin de garantir la sécurité à tout moment à l'avenir...*"
Citation de M. Springer, TÜV NORD, chef de projet Security4Safety

Attentes spécifiques au niveau de la stratégie

- La coopération en matière de cybersécurité est encouragée. Une compréhension commune est créée à cet effet dans le secteur (également entre les équipes «Safety» et «Security»).
- Concrètement (voir notamment le chapitre 7 de la Dir. CySec-Rail) :
  - Une stratégie de sécurité de l'information est en place dans l'entreprise.
  - Il doit y avoir au minimum une feuille de route contraignante pour la mise en place du SMSI ! (état mai 2024).
  - Les principaux processus sont appliqués (par ex. Asset-Mgmt, Risk-Mgmt.).
  - Les ressources nécessaires à la réalisation des objectifs de cybersécurité sont mises à disposition par la direction de l'entreprise.
- Des priorités sont fixées : Par exemple, se concentrer sur la cyber hygiène : **faire** ce qui est faisable et, en outre, prêter attention aux points faibles et aux risques majeurs actuels - Consigner par écrit.

Attentes spécifiques au niveau opérationnel

- Les acteurs au niveau opérationnel se préparent à une «excursion dans le domaine» passionnante, variée et stimulante avec d'innombrables étapes et sont prêts à quitter leur zone de confort.
- Passer de la phase de "normalisation" à la phase de "réalisation".
- Le soutien mutuel. La CySec ne concerne pas que certains individus, mais tout le monde.
- Amélioration continue (voir Dir. CySec-Rail, A-05).
- Les GI/ETF de plus grande taille au moins disposent d'un ISMS établi et mis en pratique et peuvent être une aide pour les petites entreprises de transport.

Principes du centre de compétence CySec BAV

Principe I :	L'OFT ne dicte pas le "comment", mais le "quoi". Donner l'orientation et soutenir autant que possible
Principe II :	Approche pragmatique basée sur les risques
Principe III :	une politique de canaux ouverts. E-mail, téléphone, rencontres physiques (informelles) sont possibles

E-mail général : cybersecurity@bav.admin.ch
Téléphone de Tobias : +41 58 48 56490
Téléphone d'Andreas : +41 58 46 25904

Services et offres de l'OFT

- Orientation selon les directives nationales et internationales (p. ex. stratégie cyber nationale, NIS2 (européen), normes, standards) - avec prise d'influence là où c'est possible.
- Développement de directives et d'outils en collaboration avec le secteur et le BACS
- Collaboration établie avec les associations et les représentants d'intérêts sur un pied d'égalité
- Soutenir les travaux des organisations sectorielles (par ex. RTE 28100)
- Audits spécialisés sur place à l'USIC/l'AAE : une chance pour toutes les parties concernées
- Promotion de la coopération/de l'échange d'informations au sein du secteur et entre les secteurs (exemple de la journée ERFA Cybersecurity SA)
- Collecte d'informations sur le thème de la cybersécurité à l'échelle de l'office et du département

→ Attention : délimitation de l'OFT vs BACS (voir diapositive suivante)

Délimitation CySec Expertise OFT-BACS

Expertise CySec OFT https://www.bav.admin.ch/bav/de/home/allgemeine-themen/sicherheit/cybersicherheit.html	**Expertise CySec 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
Connaissances spécifiques aux chemins de fer et aux transports publics, pont vers l'OT et la sécurité (technologies, processus, réglementation, normes, etc.).	Premier point de contact pour l'économie, l'administration, les établissements d'enseignement et la population en ce qui concerne les questions cybernétiques.
Surveillance et responsable de la réglementation dans le secteur ferroviaire et des transports publics (y compris CySec).	Dispose de compétences techniques et méthodologiques étendues et spécifiques en matière de cybersécurité.
Examen des procédures d'autorisation (y compris les questions relatives à la CySec).	Gère le GovCERT, a une longue expérience et dispose d'une expertise appropriée dans la gestion des incidents.
Organisme accrédité pour réaliser des audits spécialisés, y compris des auditeurs certifiés.	Autorité chargée d'attribuer les numéros CVE (gestion des vulnérabilités).
Accès à un réseau dans le domaine des transports publics, ainsi qu'au sein du DETEC et au-delà de l'office.	Accès à un réseau national et international.

Conclusion

En résumé, il faut retenir ce qui suit :

- Objectif commun
- Importance de la coopération
- Les menaces augmentent, les exigences aussi
- Le moment est venu