Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC

Office fédéral des transports OFT
Division Sécurité

Référence : BAV-041.4-3/11/6/15/1/4/1/2
Version 1.1 de 24.06.2024

Auxiliaires pour la mise en œuvre d'un SMSI

Auxiliaire	Remarque
Manuel sur la cybersécurité destiné aux entreprises de transports publics (manuel UTP de 2020)	Le manuel UTP sert d'introduction à la sécurité de l'information dans le secteur des transports publics et permet aux entreprises de procéder à une auto-évaluation. Le manuel est basé sur la norme minimale TIC intersectorielle de l'Office fédéral pour l'approvisionnement économique du pays (OFAE[1]).
***Implementierungsleitfaden* ISO/IEC 27001:2022** de l'ISACA (en allemand)	Sert d'auxiliaire en vue de l'implémentation d'un SMSI.
ICS Security Kompendium *(en allemand et en anglais)* : https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Allgemeine-Empfehlungen/allgemeine-empfehlungen_node.html	L'*ICS Security Kompendium* de l'Office fédéral (allemand) de la sécurité des technologies de l'information (BSI) est un ouvrage de base pour la sécurité informatique dans les SCI.
Gestion des points faibles et des fournisseurs : ENISA : - *Good Practices for Supply Chain Cybersecurity* - *Threat Landscape for Supply Chain Attacks* CISA : - *Known Exploited Vulnerabilities Catalog*	
Menaces actuelles : OFCS : https://www.ncsc.admin.ch *Internet Storm Center* : https://isc.sans.edu/ **Tendances des menaces :** ENISA : *Foresight Cybersecurity Threats For 2030*	Une fois inscrites, les entreprises peuvent se connecter au *Cyber Security Hub*. L'OFCS (NCSC) y fournit des informations sur les menaces actuelles et les points faibles. Les utilisateurs enregistrés ont la possibilité d'échanger activement des informations sur cette plate-forme. Les demandes d'enregistrement peuvent être transmises à l'OFCS via l'adresse électronique suivante : useraccounts@ncsc.admin.ch
Adversarial tactics, techniques, and common knowledge *(ATT&CK)* MITRE ATT&CK est un guide qui propose une classification et une description des cyberattaques et des intrusions. Il a été élaboré par Mitre Corporation, publié en 2013 puis perfectionné. Voir https://attack.mitre.org/ ***Indicators of Compromise (IoC) Database :*** https://threatfox.abuse.ch/browse/	En termes de tactiques, on fait la distinction entre *Enterprise*, *Mobile* et *ICS* (systèmes de contrôle industriels). Il existe un navigateur ATT&CK basé sur le Web pour commenter et explorer les matrices ATT&CK. Il peut être utilisé pour visualiser la couverture défensive, la planification des équipes rouges/bleues, la fréquence des techniques découvertes et plus encore.
Auxiliaires pour des analyses des risques (*risk assessments*) : - ISO/IEC 27005:2022	Cf. également : http://www.enisa.europa.eu ➔ *risk management*

[1] https://www.bwl.admin.ch

- IEC 62443-3-2 - CLC/TS 50701, chap. 6 et 7 - *STRIDE*	et spécifiquement ferroviaire : https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management
Auxiliaires en matière de segmentation des réseaux : - IEC 62443-3-2 et IEC 62443-3-3 - CLC/TS 50701 - *Zoning and Conduits for Railways* (ENISA, ER-ISAC)	
***NIST Cryptography* :** www.nist.gov/cryptography (en anglais)	Informations concernant les normes de chiffrement.
Recommandations du BSI concernant les procédures de chiffrement et les longueurs de clé : https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html	
***IEEE Cryptography* :** https://standards.ieee.org/ (en anglais)	
Protection par mot de passe et informations complémentaires sur la **sensibilisation des collaborateurs** : https://www.passwortcheck.ch/ https://www.s-u-p-e-r.ch/fr/tipps/e-comme-equiper/	Notamment des indications utiles concernant le choix des mots de passe.
Auxiliaire permettant de déterminer la maturité de la cybersécurité d'une organisation : Norme minimale pour les TIC	RAILplus dispose de son propre outil pour déterminer la maturité de la sécurité de l'information.
Auxiliaires sur le sujet du *cloud* : - *Cloud Security Alliance* (en anglais) - ENISA : *Cloud Cybersecurity Market Analysis* (en anglais) - BSI : *Mindeststandard des BSI zur Nutzung externer Cloud-Dienste* (en allemand et anglais uniquement) - BSI : *Kriterienkatalog C5* (*cloud computing compliance criteria catalogue*) ; en anglais et en allemand	
Tableaux de mapping pour différentes normes : - Norme minimale pour les TIC – outil d'évaluation - *Mapping-Tabelle zwischen ISO/IEC 27019:2020 und ISO/IEC 27002:2022 der Bundesnetzagentur* (en allemand et en anglais) - *Mapping of OES security requirements to specific sectors*, de l'ENISA (en anglais)	Il n'est pas toujours garanti que les tableaux de mapping soient à jour.

Autres auxiliaires : cf. https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen.html

De nombreux auxiliaires concernant la cybersécurité proviennent de sources publiques et sont plus ou moins mis à jour. Le secteur propose également de plus en plus d'auxiliaires.

La présente annexe est tenue à jour sur le site Web de l'OFT.