Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC

Ufficio federale dei trasporti UFT
Divisione Sicurezza

Riferimento: BAV-041.4-3/11/6/15/1/4/1/2
Versione 1.1 dal 24.06.2024

Mezzi ausiliari per l'attuazione di un ISMS

Mezzo ausiliario	Osservazione
Manuale di cybersicurezza per le imprese di trasporti pubblici (Manuale UTP del 2020)	Il Manuale dell'UTP, basato sullo standard minimo TIC per diversi settori dell'Ufficio federale per l'approvvigionamento economico del Paese (UFAE[1]), contiene un'introduzione alla sicurezza delle informazioni nel settore dei TP e consente alle imprese di condurre un'autovalutazione
Implementierungsleitfaden ISO/IEC 27001:2022 von ISACA (**guida all'implementazione di ISACA**, solo in ted.)	Funge da mezzo ausiliario per l'implementazione di un ISMS.
ICS Security Kompendium (**compendio sulla sicurezza**, solo in ted.) 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	Con l'ICS Security Kompendium il BSI pubblica un'opera basilare per la sicurezza IT nell'ICS.
Gestione dei punti deboli e dei fornitori: ENISA: - Good Practices for Supply Chain Cybersecurity - Threat Landscape for Supply Chain Attacks CISA: - Known Exploited Vulnerabilities Catalog	
Minacce attuali: UFCS: https://www.ncsc.admin.ch/ncsc/it/home.html Internet Storm Center: https://isc.sans.edu/ **Minacce tendenziali:** ENISA: Foresight Cybersecurity Threats For 2030	Una volta registratesi, le imprese possono iscriversi sulla piattaforma multimodale di cibersicurezza, sulla quale l'UFCS (NCSC) informa in merito alle minacce e ai punti deboli più recenti. Su questa piattaforma, gli utenti registrati hanno la possibilità di scambiarsi informazioni attivamente. Per le richieste di registrazione contattare l'UFCS all'indirizzo useraccounts@ncsc.admin.ch.
Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) MITRE ATT&CK è una guida nella quale sono classificati e descritti gli attacchi informatici e gli hacker pubblicata nel 2013, realizzata e sviluppata dalla Mitre Corporation. Cfr. https://attack.mitre.org/ **Indicators of Compromise (IoC) Database:** https://threatfox.abuse.ch/browse/	Le tattiche sono distinte nelle tre matrici Enterprise, Mobile e ICS (industrial control system, sistema di controllo industriale). Il navigatore ATT&CK basato su web può essere utilizzato per commenti e informazioni sulle matrici ATT&CK nonché per visualizzare la copertura difensiva, la pianificazione dei team rosso/blu, la frequenza delle tecniche scoperte e molto più.
Mezzi ausiliari per le analisi dei rischi (risk assessments): - ISO/IEC 27005	Si veda in proposito anche: https://www.enisa.europa.eu ➔ Risk Management

[1] www.bwl.admin.ch

Mezzo ausiliario	Osservazione
- IEC 62443-3-2 - CLC/TS 50701:2023, cap. 6 e 7 - STRIDE	e specifico alla ferrovia: https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management
Mezzi ausiliari per la segmentazione di reti: - IEC 62443-3-2 e IEC 62443-3-3 - CLC/TS 50701 - Zoning and Conduits for Railways (ENISA, ER-ISAC)	
NIST Cryptography: https://www.nist.gov/cryptography	Informazioni riguardo agli standard di crittografia.
Raccomandazioni BSI su procedure crittografiche e lunghezza delle chiavi (solo in ted.): 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/	
Protezione con password e altre informazioni sulla sensibilizzazione dei collaboratori: https://www.passwortcheck.ch/ https://www.s-u-p-e-r.ch/it/consigli/e-per-elaborare/	Diverse informazioni, tra cui preziose indicazioni per la scelta della password.
Mezzo ausiliario per determinare la maturità della cibersicurezza in un'organizzazione: Standard minimo per le TIC – tool di valutazione	RAILplus dispone di un proprio strumento d'ausilio per determinare la maturità della sicurezza delle informazioni.
Mezzo ausiliario sul tema cloud: - Cloud Security Alliance (CSA) - ENISA: Cloud Cybersecurity Market Analysis - BSI: Mindeststandard des BSI zur Nutzung externer Cloud-Dienste - BSI: Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)	
Tabelle di mappatura per diverse norme: - Standard minimo per le TIC – tool di valutazione - Mapping-Tabelle zwischen ISO/IEC 27019:2020 und ISO/IEC 27002:2022 der Bundesnetzagentur - Mapping Tabelle von ENISA für spezifische Sektoren	Le tabelle di mappatura non sono sempre aggiornate.

Per ulteriori mezzi ausiliari consultare la pagina https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen.html

Molti strumenti d'ausilio per la cibersicurezza sono consultabili su fonti ufficiali e vengono aggiornati per lo più periodicamente. Sempre più ausili sono disponibili anche nel settore.
Il presente allegato è aggiornato sulla pagina Internet dell'UFT.