Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Verkehr BAV
Abteilung Sicherheit

Aktenzeichen: BAV-041.4-3/11/6/15/1/4/1/2
Version 1.1 vom 24.06.2024

Hilfsmittel für die Umsetzung eines ISMS

Hilfsmittel	Bemerkung
Handbuch Cybersecurity für Betriebe des öffentlichen Verkehrs (Handbuch VöV vom 2020)	Das Handbuch VöV dient als Einführung in die Informationssicherheit im ÖV-Sektor und ermöglicht den Unternehmen eine Selbsteinschätzung durchzuführen. Das Handbuch basiert auf dem branchenübergreifenden IKT-Minimalstandard des Bundesamts für wirtschaftliche Landesversorgung (BWL[1]).
Implementierungsleitfaden ISO/IEC 27001:2022 von ISACA	Dient als Hilfsmittel zur Implementierung eines ISMS.
ICS Security Kompendium: 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	Mit dem ICS Security Kompendium veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Grundlagenwerk für die IT-Sicherheit in ICS.
Schwachstellen- und Lieferantenmanagement: ENISA: - Good Practices for Supply Chain Cybersecurity - Threat Landscape for Supply Chain Attacks CISA: - Known Exploited Vulnerabilities Catalog	
Aktuelle Bedrohungen: BACS: https://www.ncsc.admin.ch Internet Storm Center: https://isc.sans.edu/ **Bedrohungstrends:** ENISA: Foresight Cybersecurity Threats For 2030	Unternehmen können sich beim Cyber Security Hub nach erfolgter Registrierung anmelden. Das BACS (NCSC) informiert darin über aktuelle Bedrohungen und Schwachstellen. Registrierte Nutzer und Nutzerinnen haben die Möglichkeit, aktiv Informationen auf dieser Plattform auszutauschen. Anträge für die Registrierung nimmt das BACS unter folgender Adresse entgegen: useraccounts@ncsc.admin.ch
Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) MITRE ATT&CK ist ein Leitfaden zur Klassifizierung und Beschreibung von Cyberangriffen und Eindringlingen. Er wurde von der Mitre Corporation erstellt, im Jahr 2013 veröffentlicht und weiterentwickelt. Siehe https://attack.mitre.org/ **Indicators of Compromise (IoC) Database:** https://threatfox.abuse.ch/browse/	Bei den Taktiken wird zwischen Enterprise, Mobile und ICS (Industrielle Control Systeme) unterschieden. Es gibt den webbasierten ATT&CK Navigator zur Kommentierung und Erkundung von ATT&CK-Matrizen. Er kann zur Visualisierung der Defensivabdeckung, der Planung von roten/blauen Teams, der Häufigkeit der entdeckten Techniken und mehr verwendet werden.

[1] www.bwl.admin.ch

Hilfsmittel für Risikoanalysen (Risk Assessments): - ISO/IEC 27005 - IEC 62443-3-2 - CLC/TS 50701:2023, Kapitel 6 und 7 - STRIDE	Siehe auch: https://www.enisa.europa.eu ➔ Risk Management und eisenbahnspezifisch: https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management
Hilfsmittel für die Netzwerksegmentierung: - IEC 62443-3-2 und IEC 62443-3-3 - CLC/TS 50701 - Zoning and Conduits for Railways (ENISA, ER-ISAC)	
NIST Cryptography: https://www.nist.gov/cryptography	Informationen bezüglich Kryptografie-Standards.
BSI Empfehlungen zu kryptographischen Verfahren und Schlüssellängen: 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/	
Passwortschutz und weiterführende Informationen zur **Mitarbeitersensibilisierung**: https://www.passwortcheck.ch/ https://www.s-u-p-e-r.ch/de/tipps/e-wie-einloggen/	U.a. hilfreiche Hinweise für die Passwortwahl.
Hilfsmittel für die Maturität der Cybersicherheit in einer Organisation zu bestimmen: IKT-Minimalstandard – Assessment Tool	RAILplus verfügt über ein eigenes Hilfsmittel zur Bestimmung der Maturität der Informationssicherheit.
Hilfsmittel zum Thema 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)	
Mapping-Tabellen für verschiedene Normen: - IKT-Minimalstandard – Assessment Tool - Mapping-Tabelle zwischen ISO/IEC 27019:2020 und ISO/IEC 27002:2022 der Bundesnetzagentur - Mapping Tabelle von ENISA für spezifische Sektoren	Die Aktualität der Mapping-Tabellen ist nicht immer gegeben.

Weitere Hilfsmittel siehe https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen.html

Viele Hilfsmittel zur Cybersicherheit sind aus öffentlichen Quellen abrufbar und werden mehr oder weniger aktuell gehalten. Auch in der Branche sind zunehmend Hilfsmittel vorhanden.
Dieser Anhang wird auf der BAV-Webseite aktuell gehalten.