Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Strassen ASTRA

WEISUNGEN

OT SECURITY GOVERNANCE

Security im Bereich BSA-Systeme

Ausgabe 2022 V1.00
ASTRA 73006

Impressum

Autoren

Jolanda Geringer	ASTRA DS-DTI, Vorsitz
Martin Wyss	ASTRA I-B
Markus Berger	ASTRA I-FU
Manfred Jungo	ASTRA DS
Wolfgang Hoffmann	ASTRA DS-GOV
Bruno Frey	ASTRA DS-GOV
Daniel Gähwiler	CSI Consulting, Zürich

Begleitgruppe

Bernard Crausaz	ASTRA DS-UARS
Mario Pfammatter	ASTRA DS-UARS

Originalsprache
Deutsch

Herausgeber
Bundesamt für Strassen ASTRA
Abteilung Strassennetze N
Standards und Sicherheit der Infrastruktur SSI
3003 Bern

Bezugsquelle
Das Dokument kann kostenlos von www.astra.admin.ch heruntergeladen werden.

Vorwort

Der Fortschritt der Technik und die steigenden Anforderungen an die Strasseninfrastruktur benötigen einheitliche Vorgaben auch im Bereich der Security. Die Sicherheit auf dem Strassennetz, besonders im Bereich von potentiell neuen Angriffspunkten, ist uns ein grosses Anliegen.

Die vorliegenden Weisungen definieren die übergeordnete OT-Security Governance im Bereich BSA mit seinen OT (Operational Technology) Systemen. Ebenfalls wird die Unterscheidung zwischen IT- und OT-Systemen erläutert inkl. deren Einsatzgebiete und Spezifikas.

Diese OT-Security Governance liefert eine übergeordnete Struktur, um die Geschäftsziele bezüglich OT-Security auf strategischer, funktionaler und operativer Ebene zu unterstützen.

Bundesamt für Strassen

Jürg Röthlisberger
Direktor

Inhaltsverzeichnis

1 Einleitung

1.1 Zweck

Diese Weisungen beinhalten das Regelwerk für die OT-Security Governance der Steuer- und Leittechnik der BSA (OT-Systeme). Sie enthalten:

- Die Ziele der OT-Security Governance (siehe Kap. 4.1);
- Die verschiedenen Grundbausteine, um die strategische, funktionale und operative Ebene zu unterstützen;
  - Regeln: Prozesse, Rollen und Organisation;
  - Mensch: Mitarbeiterqualifikationen und –ausbildung;
  - Technologie: Technische Vorgaben;
- Die Differenzierung zwischen IT und OT auf den Nationalstrassen (siehe Kap. 3);
- Die wichtigsten Gremien der OT-Sicherheitsorganisation (siehe Kap. 5.4).

1.2 Geltungsbereich

Die Weisungen gelten für die Planung, die Projektierung, die Realisierung und den Betrieb aller OT-Systeme der Nationalstrassen. Sie sind verbindlich und bei der Integration der Anlagen auf dem IP-Netz BSA zwingend einzuhalten.

Die OT-Systeme der Nationalstrassen sind integraler Bestandteil der Nationalstrassen und unterstehen der Nationalstrassenverordnung. Daher sind diese nicht der BR-Weisung W007 (Weisungen des Bundesrates zu den IKT-Projekten in der Bundesverwaltung und zum IKT-Portfolio des Bundes) unterstellt.

1.3 Gesetzliche Grundlagen, relevante Normen und Standards

Für die Erstellung, den Betrieb und die Nutzung von BSA-Anlagen inkl. den Bereichen Operational Technology müssen gesetzliche Bestimmungen eingehalten werden. Es ist Aufgabe des Bauherrn, der Planer, der Lieferanten und der Betreiber, die für ihren Bereich zutreffenden Vorschriften und Normen einzuhalten (Siehe Literaturverzeichnis).

1.4 Adressaten

Diese Weisungen richten sich in erster Linie an die Mitarbeiter ASTRA und an die Betreiber der OT-Systeme. In zweiter Instanz geben sie den Bauherren, den Projektverfassern und den Planern wichtige Informationen zur OT-Sicherheitsorganisation der Nationalstrassen.

1.5 Inkrafttreten und Änderungen

Die Weisungen treten am 31.10.2022 in Kraft. Die „Auflistung der Änderungen“ ist auf Seite 20 zu finden.

2 Sicherheit in der Bundesverwaltung

2.1 Übersicht der rechtlichen Grundlagen im Bund

Nachfolgende Abbildung zeigt auf, welche rechtlichen Grundlagen zu berücksichtigen sind. Ausnahmen von Informationssicherheits- und Datenschutzvorgaben sind für die spezifischen BSA (Betriebs- und Sicherheitsausrüstungen) vorhanden und werden gezielt umgesetzt.

Abb. 2.1 Informationssicherheits- und Datenschutzvorgaben

2.2 Organisatorische Abstufungen in der Bundesverwaltung

Das Nationale Zentrum für Cybersicherheit (National Cyber Security Centre - NCSC) ist das Kompetenzzentrum des Bundes für Cybersicherheit. Als Fachstelle IKT-Sicherheit des Bundes erlässt das NCSC Vorgaben zur Cybersicherheit innerhalb der Bundesverwaltung (Eigenschutz), überprüft deren Einhaltung und unterstützt die Leistungserbringer bei der Beseitigung von Schwachstellen. Das GS UVEK bricht die übergeordneten Bundesvorgaben auf das Departement und seine Ämter herunter. Das ASTRA definiert die besonderen Vorgaben für das Nationalstrassennetz im Bereich BSA und übernimmt dabei sinngemäss diejenigen Vorgaben, welche für OT-Systeme anwendbar sind.

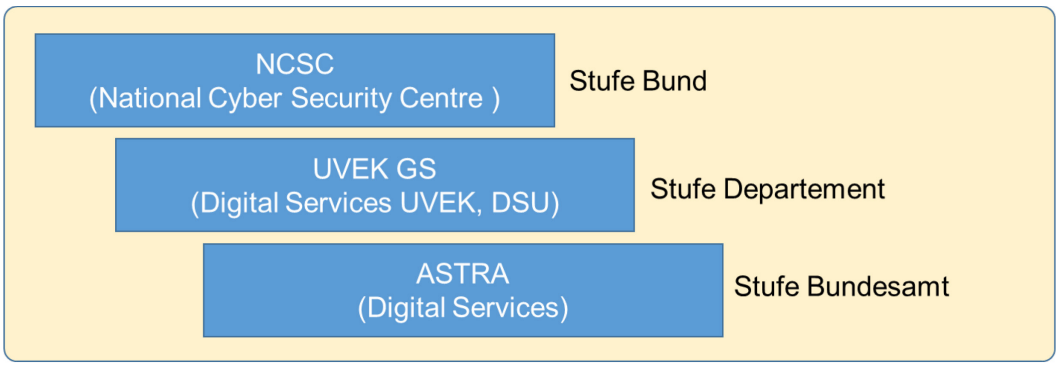

Abb. 2.2 Organisatorische Abstufung in der Bundesverwaltung

Für die OT-Security des ASTRA sind insbesondere folgende Vorgaben relevant:

- Bundesgesetz über den Datenschutz und Verordnung (DSG und VDSG) [1], [4];
- Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) [5];
- Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) [6];
- Verordnung über die digitale Transformation und die Informatik (VDTI) [7];
- Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) [9];
- Si001 – IT-Grundschutz in der Bundesverwaltung (Bundeskanzlei BK, Nationales Zentrum für Cybersicherheit NCSC) [15].

2.3 Umsetzung im ASTRA, Bereich BSA

Im Bereich BSA sind einige Sonderbewilligungen zwecks Gewährleistung der Sicherheit auf den Nationalstrassen vorhanden. Diese dienen der bedürfnisgerechten Umsetzung der rechtlichen Grundlagen, welche Aufgrund der Differenzierung IT/OT (siehe Kapitel 3) vorhanden sind.

In den nachfolgenden Kapiteln werden die ASTRA spezifischen Vorgaben für die Nationalstrassen beschrieben.

3 Differenzierung Information und Operational Technology

3.1 OT-Security in Bezug auf BSA kurz erklärt

OT steht für Operational Technology und ist die Verwendung von Systemen, bestehend aus Hard- und Software zur Steuerung von Anlagen.

Die Betriebs- und Sicherheitsausrüstungen (BSA) umfasst elektromechanische sowie steuer- und leitechnischen Anlagen, welche für den Betrieb und die Sicherheit der Nationalstrassen dienen.

OT umfasst damit die Steuer- und Leittechnik der BSA, die dazu benötigte Infrastruktur (bspw. IP-Netz BSA), die OT-Systeme als auch die Applikationen und Services. OT-Systeme und Aggregate sind Teil der BSA.

3.2 Schwerpunkte IT und OT

Nachfolgend ist aufgezeigt, inwieweit sich IT- zu OT-Thematiken unterscheiden. Dies Erläutert, weshalb diese unterschiedlich geführt und bearbeitet werden.

Abb. 3.3 Unterscheidung IT- zu OT-Thematiken

Einsatzbereiche	**IT**	**OT**
Einsatzschwerpunkte	Bürokommunikation / Automation / Fachanwendungen ohne operative Funktion.	Zuverlässige Steuerung und Regelung, Überwachung und Kontrolle von Maschinen, Anlagen und Prozessen / Fachanwendungen und Applikationen mit operativer Funktion (bspw. Steuerung von Anlagen).
Art der Aktivität	Transaktionale Interaktion zwischen Mensch und Anwendung fokussiert.	Ereignisbasierte Interaktionen zwischen Bedingungen und Prozesssystem.
Sicherheitsthemen	**IT**	**OT**
Security Ziele	Vertraulichkeit Integrität Verfügbarkeit	Funktionale Sicherheit Zuverlässigkeit Verfügbarkeit
Kritische Daten / Informationen	Geschäftsdaten (inkl. Finanzdaten) Personendaten.	Leitsystemdaten (Steuersignale Sensordaten.
Integrität	Kontextuell kritisch.	Integrität kontextuell kritisch. Mögliche Auswirkung auf Leben, Leib und Umwelt
Verfügbarkeit	i.d.R. während Bürozeiten / Ausnahmen im ASTRA bilden Fachanwendungen wie IVZ, ETC, usw.	Hoch, real-time (365 Tage x 24h).
Technologie-Lebensdauer	3-5 Jahre; viele Anbieter; allgegenwärtige Erweiterungen / laufendes Lifecycle Management der eingesetzten Technologien.	10-20 Jahre; normalerweise der gleiche Lieferant über Zeit; Produkt-End-of-Life schafft neue Sicherheitsbedenken.
Änderungsmanagement	Regelmässig und geplant; mit Mindestnutzungszeiten abgestimmt.	Strategische Planung; nicht trivialer Prozess aufgrund von Auswirkungen auf die Produktion.
Physische- und Umweltsicherheit	Reicht von schlecht (Büro-Systeme) bis hervorragend (kritische IT-Systeme).	In der Regel hervorragend für kritische Bereiche; variable Reife basierend auf Kritikalität / Kultur.

4 OT-Security Governance

Die OT-Security Governance (kurz OT-Sec Gov) regelt die Security der OT-Systeme und garantiert die hohe Verfügbarkeit, Integrität und Zuverlässigkeit der Steuer- und Leittechnik der BSA der Nationalstrassen. Ebenso wird sichergestellt, dass die Strategien für die OT-Security mit den Geschäftszielen im Bereich BSA übereinstimmen und diese unterstützen. Auch muss sichergestellt werden, dass die Strategien durch die Einhaltung von Richtlinien und internen Kontrollen mit den geltenden Gesetzen und Vorschriften übereinstimmen und dass entsprechende Verantwortlichkeiten und Kompetenzen zugewiesen sind. D.h. die Governance bestimmt, wer befugt ist, Entscheidungen zu treffen, legt den Rahmen für die Rechenschaftspflicht fest und sorgt für die Überwachung, um sicherzustellen, dass die Risiken angemessen gemindert werden.

4.1 Spezifische Ziele der OT-Security Governance

Aufbau, Pflege und Überwachung des OT-Security Governance-Rahmens, insbesondere:

- Definition, Vorgabe und Überwachung von Standards und „Best Practices“ unter Berücksichtigung der optimalen Balance zwischen Performance und Konformität für alle Disziplinen der Leistungserbringung (OT-Projektgeschäft über alle Phasen als auch OT-Betrieb von Fachanwendungen oder Applikationen mit operativer Funktion) sowie für die Risikobeurteilung;
- Definition, Vorgabe und Prüfung der Einhaltung von Vorgaben. Sicherstellung der adäquaten Begleitung von OT-Projekten und Fachanwendungen oder Applikationen mit operativer Funktion durch Wahrnehmung der Lead-Architekturrolle;
- Der ISBO prüft die freiwillige Umsetzungsrelevanz der IKT-Vorgaben für die Nationalstrassen;
- Sicherstellung der Einhaltung rechtlicher, bundesweiter und departementaler Vorgaben im Zusammenhang mit der OT und den Integrationssystemen.

5 Rahmen und Fundament

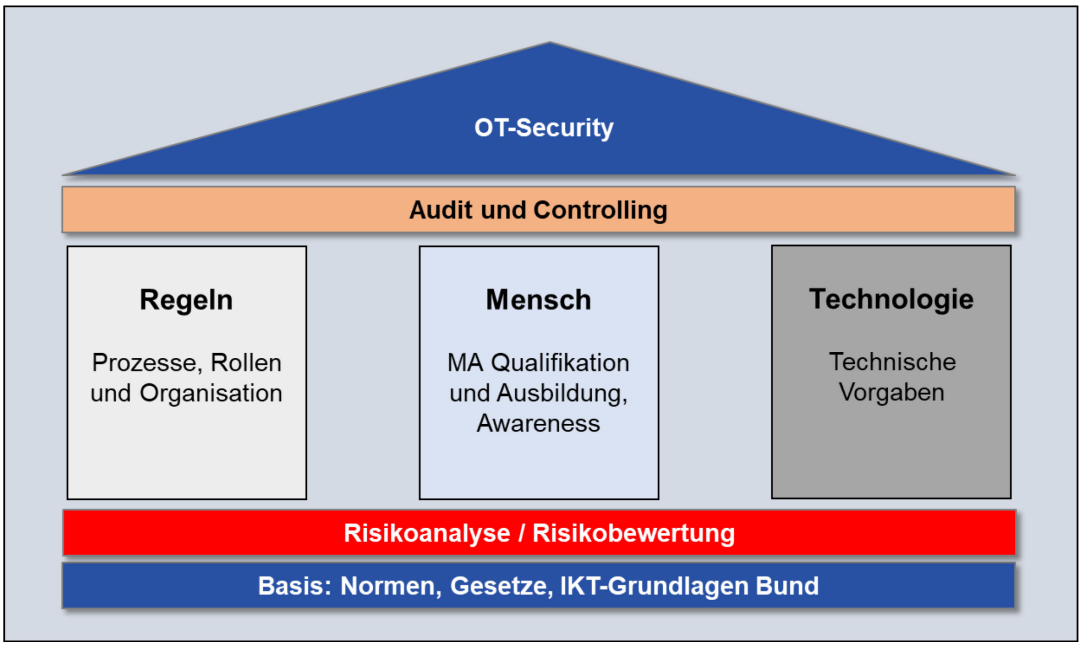

Abb. 5.4 OT- Security Management System (OT-SMS)

5.1 Elemente vom OT-SMS

Die drei Grundbausteine werden von drei wesentlichen Elementen umschlossen, welche in den folgenden Unterkapiteln erläutert werden.

5.1.1 Basis: Normen, Gesetze, IKT-Grundlagen Bund

Ausführungsbestimmungen betreffend Umgang mit den Grundlagendokumenten, insbesondere zum Umgang mit den IKT-Vorgaben des Bundes (Digitale Transformation und IKT Lenkung), wobei die Anwendbarkeit für die Infrastruktur der Nationalstrassen gesondert geprüft wird.

5.1.2 Audit und Controlling

Vorgaben und Bestimmungen bezüglich Audits bzw. regelmässiger Überprüfung des OT-SMS und dessen Umsetzung. Für Audit- und Controllingaufgaben als auch Qualitätssicherungsaktivitäten stehen Prüfpläne, Checklisten und Abnahmeprotokolle zur Verfügung.

5.1.3 Risikoanalyse / Risikobewertung

Die Risikoanalyse und -bewertung legt fest, gegen was man sich in welcher Priorität schützen will. Risikomanagement wird zentral übergeordnet, projektorientiert und aus betrieblicher Sicht betrieben.

Die Risikoanalyse ist die Analyse der durch Risikoidentifikation ermittelten Risiken von unterschiedlichen Sachverhalten und Gefahrensituationen.

Die Risikobewertung ist die von einem Risikoträger oder von Dritten vorgenommene Bewertung eines Einzelrisikos oder des Gesamtrisikos, dem der Risikoträger ausgesetzt ist.

5.2 Grundbausteine OT-SMS

In den folgenden Unterkapiteln werden die Grundbausteine Regeln, Mensch und Technologie erläutert.

5.2.1 Regeln: Prozesse, Rollen und Organisation

Vorgaben und Bestimmungen bezüglich der Rollen, Aufgaben, Kompetenzen und Verantwortlichkeiten, beispielsweise:

- SPoC (Single Point of Contact);
- Eskalationsprozesse;
- Zutritts- und Zugangsregelwerk.

5.2.2 Mensch: MA-Qualifikation und Ausbildung

Vorgaben und Bestimmungen bezüglich Qualifikation und Schulung der Mitarbeiter, beispielsweise:

- Sicherheitstrainings und Sensibilisierungsaktivitäten;
- Knowhow-Sicherstellung.

5.2.3 Technologie: Technische Vorgaben

Vorgaben und Bestimmungen bezüglich technischer Systeme und Umgang mit den Systemen, beispielsweise:

- Security Monitoring (Sammeln und Analysieren von Informationen aus ganz unterschiedlichen (Log-) Quellen, um sicherheitsrelevante Ereignisse, also verdächtiges Verhalten oder nicht autorisierte Systemänderungen im Netzwerk zu erkennen)
- IAM BSA (Identity und Access Management der BSA)
- Log Management (Definieren, Empfangen, Speichern und Löschen von Protokolldaten, welche dem Security Monitoring zugeführt werden).

5.3 Regelwerk

Dieses Regelwerk wird in den Richtlinien, Standards, Fachhandbücher, technischen Merkblätter, Leitfäden und Dokumentationen festgehalten.

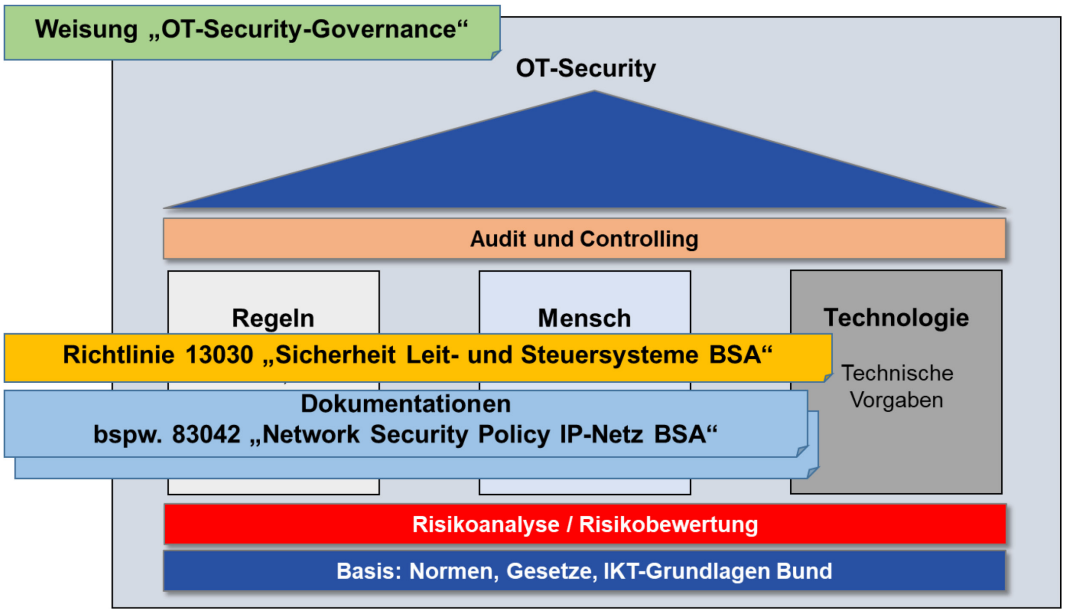

Abb. 5.5 Dokumente des OT-SMS

Das Regelwerk wird in folgenden Dokumenten festgehalten:

- **Weisungen 73006 „OT Security Governance“**

  Diese Weisungen beinhalten das Regelwerk für die OT-Governance der Steuer- und Leittechnik der BSA.

- **Richtlinie 13030 „Sicherheit der Leit- und Steuersysteme BSA“**

  Diese Richtlinie beschreibt das WAS und die grundlegenden Sicherheitskonzepte, um die identifizierten Risiken zu minimieren.

- **Dokumentationen**

  Die Dokumentationen beschreiben das WIE und definieren konkrete Umsetzungsmassnahmen und Sicherheitssysteme wie bspw. das IAM BSA oder die Network Security Policy IP-Netz BSA.

5.4 Organisatorische Strukturen OT-Security Governance (Verantwortlichkeiten)

Die organisatorischen Belange werden in mehrere Bereiche definiert:

- Steuerung: Anpassen, planen und organisieren;
- Umsetzung: Aufbauen, beschaffen und implementieren;
- Betrieb: Bereitstellen, betreiben und unterstützen.

5.4.1 Steuerung

Die übergeordnete Steuerung wird mittels **Change Advisory Board OT-Security (CAB-OT-Sec)** bewerkstelligt. Das Change Advisory Board ist eine Gruppe von Personen, deren Aufgabe es ist, Änderungen in der OT-Umgebung zu bewerten. Einsitz haben Vertreter des ASTRA (Zentrale, Produktmanager IP-Netz BSA Security, Infrastruktur-Betrieb und Filiale) als auch Gebietseinheit.

Nachfolgend die Hauptaspekte:

- Stellt sicher, dass alle notwendigen Sicherheitsdokumente, Weisungen und Richtlinien erarbeitet, wenn nötig aktualisiert und konsequent umgesetzt werden;
- Stellt sicher, dass der Sicherheitsprozess mit dem Unternehmens Risikomanagement Prozess verzahnt, methodisch integriert ist, sowie die Vorgaben aus dem Risiko Management Prozess berücksichtigt werden.

5.4.2 Umsetzung

Die Umsetzung obliegt sowohl den Produktmanagern, der übergeordneten Betriebsorganisation IP-Netz BSA als auch den Projektleitern der Filialen wie auch den Information Security Officer (BSA) der Gebietseinheiten.

Nachfolgend die Hauptaspekte:

- Stellt die Fachführung der Informationssicherheit in Bezug auf OT sicher und legt die Prioritäten der Tätigkeiten der Lage angepasst fest;
- Stellt sicher, dass neue, relevante Sicherheits-Themen identifiziert, analysiert und falls notwendig bearbeitet werden;
- Stellt sicher, dass die Berichterstattung Richtung Geschäftsleitung inhaltlich korrekt, termin-, stufengerecht und systematisch erfolgt.

5.4.3 Betrieb

Der Betrieb obliegt den Gebietseinheiten und der übergeordneten Betriebsorganisation IP-Netz BSA als auch I-B.

Nachfolgend die Hauptaspekte:

- Stellt sicher, dass das entsprechend Know-how und Ressourcen im gesamten Sicherheitsmanagement zur Verfügung stehen;
- Stellt sicher, dass die periodischen Überprüfungen, Audits und Penetration Tests (Verletzlichkeitsanalysen) durchgeführt werden;
- Informationspflicht bei sicherheitsrelevanten Vorfällen.

Glossar

Begriff	Bedeutung
BK	Bundeskanzlei
BSA *EES*	Betriebs- und Sicherheitsausrüstungen *équipements d'exploitation et de sécurité*
CAB	Change Advisory Board
CyRV	Cyberrisikenverordnung
DSG	Datenschutzgesetz /-verordnung
ETC	Easy Way for Traffic Control
GOV	Governance
GS	Generalsekretariat des UVEK
IAM BSA	Identität und Access Management BSA
I-B	Bereich in Abteilung Infrastruktur, Fachbereich Betrieb
ISBD	Informatiksicherheitsbeauftragte der Departemente und Bundeskanzlei
ISBO	Informatiksicherheitsbeauftragte der Organisation
IKT	Informations- und Kommunikationstechnik
IoT	Internet of Things
IP	Internet Protokoll
IT	Information Technology
IVZ	Informationssystem Verkehrszulassung
ISchV	Informationsschutzverordnung
MA	Mensch / MitarbeiterIn
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken
NCSC	Nationale Zentrum für Cybersicherheit (National Cyber Security Centre)
OT	Operational Technology
OT-SMS	Operational Technology Security Management System
SPOC	Single Point of Contact
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VDTI	Verordnung über die digitale Transformation und die Informatik

Literaturverzeichnis

Bundesgesetze

[1] Schweizerische Eidgenossenschaft (1992), „**Bundesgesetz über den Datenschutz (DSG)**“, *SR 235.1*, www.admin.ch.

[2] Schweizerische Eidgenossenschaft (1960), „**Bundesgesetz über die Nationalstrassen (NSG)**“, *SR 725.11*, www.admin.ch.

[3] Schweizerische Eidgenossenschaft (1958), „**Strassenverkehrsgesetz (SVG)**“, *SR 741.01*, www.admin.ch.

Verordnungen

[4] Schweizerische Eidgenossenschaft (1993), „**Verordnung zum Bundesgesetz über den Datenschutz (VDSG)**“, *SR 235.11*, www.admin.ch.

[5] Schweizerische Eidgenossenschaft (2007), „**Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung , ISchV)**“, *SR 510.411*, www.admin.ch.

[6] Schweizerische Eidgenossenschaft (2020), „**Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV)**“, *SR 120.73*, www.admin.ch.

[7] Schweizerische Eidgenossenschaft (2020), „**Verordnung über die digitale Transformation und die Informatik (VDTI)**“, *SR 172.010.58*, www.admin.ch.

[8] Schweizerische Eidgenossenschaft (2007), „**Nationalstrassenverordnung (NSV)**“, *SR 725.111*, www.admin.ch.

Weisungen und Strategiedokumente

[9] Schweizerische Eidgenossenschaft „**Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken**“ (NCS 2018-2022)

[10] Schweizerische Eidgenossenschaft „**Strategie Netzwerke des Bundes**“ vom November 2018.

[11] Schweizerische Eidgenossenschaft „**Weisung über die Betreiber- und Sourcingentscheide im UVEK**“ vom 01.01.2022

[12] Schweizerische Eidgenossenschaft „**Weisung zur Nutzung der Informatikmittel im UVEK**“ vom 01.01.2022.

[13] Schweizerische Eidgenossenschaft „**Weisung zur Steuerung, Führung und Kontrolle der Informatik und Digitalisierung im UVEK**“ vom 01.01.2022.

[14] Schweizerische Eidgenossenschaft „**Weisung Unternehmensarchitektur Management UVEK**“ vom 01.01.2022.

[15] Schweizerische Eidgenossenschaft „**Vorgabe Si001 – IT-Grundschutz in der Bundesverwaltung - Version 5.0**“ vom NCSC vom 23.02.2022.

Auflistung der Änderungen

Ausgabe	Version	Datum	Änderungen
2022	1.00	31.10.2022	Inkrafttreten Ausgabe 2022 (Originalversion in Deutsch).