Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation
Bundesamt für Strassen ASTRA
Filiale 4

OT-Sicherheitskonzept GE VII

Gebietseinheit VII

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Strassen ASTRA

Version 2.0 / 27. Februar 2025

Impressum

Version	2.0
Autoren	Roger Züger Fabio Caspani
Fachliche Mitwirkung	Roger Züger
Herausgeber	Baudirektion Kanton Zürich Tiefbauamt, GE VII - Nationalstrassenunterhalt Betriebsleitzentrale Werkhofstrasse 1 8902 Urdorf
Dateiname	OT-Sicherheitskonzept GEVII.docx
Zweck	OT-Sicherheitskonzept gemäss ASTRA Merkblatt 26 010-04002
Letzte Änderung / von	27. Februar 2025 / Fabio Caspani
Genehmigt am / von	27. Februar 2025 / Robert Hämmerli, Martin Wyss
Gültigkeit	Es gilt die jeweils neuste, von der GE VII publizierte Version dieses Dokumentes, unabhängig von der Laufzeit eines Projektes. Die Adressaten informieren sich selbst über die aktuelle Version.

Inhaltsverzeichnis

1 Einleitung

1.1 Zweck

Dieses Konzept beschreibt, mit welchen Massnahmen, die in der ASTRA Richtlinie 13030 [1] vorgegebenen Ziele und Strategien verfolgt werden sollen aus Sicht der GE VII. Das Sicherheitskonzept beschreibt ausschliesslich den Zielzustand und wird anhand des ASTRA Merkblattes «26010-04002 OT-Sicherheitskonzept für den Betrieb der BSA» [2] aufgebaut und geführt.

1.2 Aufbau

Die Struktur dieses Dokuments orientiert sich an der Vorgabe aus dem ASTRA Merkblatt 26010-04002 [2].
Das Dokument beinhaltet öffentliche und interne Informationen. Es existieren somit immer zwei Ausgaben dieses Konzeptes. Interne Informationen werden in der öffentlichen Version geschwärzt.

1.3 Definitionen

Sicherheitsmanagement
Dieses Konzept bezeichnet mit Sicherheitsmanagement die Erfüllung der Aufgabe, ein sozio-technisches System in einen definierten Zustand zu überführen und so zu erhalten, dass ein wirksamer Schutz der Leistungserbringung vor Ausfall (Verfügbarkeit), Kompromittierung (Integrität) oder Verletzung der Vertraulichkeit (Vertraulichkeit) entsteht.

Dritte
Dieses Konzept bezeichnet als Dritten einen Dienstleister, der seine Leistungen im Auftrag eines anderen als der Gebietseinheit erbringt. Bezüger von Dienstleistungen der Gebietseinheit sind ebenfalls als Dritte bezeichnet. Beispiele sind das Bundesamt für Informatik, die Verkehrsmanagementzentrale oder eine Kantonspolizei.

Unternehmer
Dieses Konzept bezeichnet als Unternehmer einen Dienstleister, der Services, welche zur Erbringung des Leistungs- und Betriebsauftrages der Gebietseinheit notwendig sind und durch die Gebietseinheit beauftragt werden.

1.4 Gültigkeit

Ohne Änderungen an den Vorgaben bleibt das Konzept gültig und wird regelmässig auf Änderungsbedarf geprüft. Wird ein Bedarf festgestellt, wird dieser umgehend analysiert, notwendigen Massnahmen abgeleitet und das vorliegende Konzept entsprechend ergänzt. Es gilt immer die aktuelle Version.

Alle Beteiligten haben in ihrem Einflussbereich die Einhaltung des Sicherheitskonzepts sicherzustellen. Bei einer Abweichung von diesen Vorgaben ist bei der zuständigen Stelle eine begründete Ausnahme einzuholen.

Systeme, welche in den BSA der GE-Systeme betrieben werden und entweder veraltet sind oder nicht aktualisiert werden dürfen/können, werden als Ausnahme ins Inventar aufgenommen. Für solche Systeme kann dieses Konzept nur in dem Sinn angewendet werden, dass kompensierende Massnahmen getroffen werden müssen, beispielsweise die Verschiebung der Systeme in ein Netzwerksegment hinter einer Firewall.

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in diesem Dokument die männliche oder weibliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter.

1.5 Rahmenbedingungen

1.5.1 Klassifikation

Das Sicherheitsmanagement erfolgt anhand einer Klassifikation der inventarisierten Systeme. Die Klassifikation der Systeme erfolgt durch den Eigentümer.

1.5.2 Umfang Netzwerk

Dieses Konzept gilt grundsätzlich für alle Geräte auf dem Perimeter der GE VII, welche an ein Netzwerk angeschlossen sind (nicht standalone). Die GE hat die Hoheit über das BKN und IP-Netz-BSA-GE. Die Unternehmer verwalten gemeinsam mit dem Fachspezialisten IH-BSA die Anlagenetze unterhalb der Bereichsrechner.

1.6 Lebenszyklen

Zyklen im Strassenbau sehen Lebensspannen im Bereich von Jahrzehnten und Wartungsintervalle im Bereich mehrerer Jahre vor. Die bestehenden Systeme benötigen wesentlich dichtere Wartungsintervalle zur Sicherstellung der Sicherheit.
Die Hauptversion eines Betriebssystems wird zwischen drei und maximal sieben Jahren vom Hersteller unterstützt. Sicherheitspatches müssen jederzeit eingeplant und nach einem standardisierten Verfahren eingespielt werden können.

1.7 Zielkonflikte

Die Gebietseinheit wird beim Bau berücksichtigt und ist für den Betrieb zuständig. Bau-, IT-Konzept- und IT-Architekturmängel verschieben sich, automatisch (systembedingt), nach der Inbetriebnahme in die Zuständigkeit der Gebietseinheit. Das gilt auch für die Wirksamkeit dieses Konzeptes für IT/OT-Systeme, wenn letztere so gebaut werden, dass sie nicht angemessen gewartet werden können.

1.8 Stellen, Gremien und Rollen

Die nachfolgende Tabelle beschreibt die wichtigsten Stellen, Gremien und Rollen des Sicherheitsprozesses ASTRA und GE VII:

Kürzel	Bezeichnung	Beschreibung
CAB	Change Advisory Board	Das CAB koordiniert die OT-Sicherheit für den Betrieb der BSA und übernimmt das Changemanagement für die übergeordneten Funktionen. Es werden auch Empfehlungen oder Entscheidungen bezüglich den GE-Aufgaben getroffen, welche die Sicherheit betreffen.
GE AG-BSA-OT	GE Arbeitsgruppe BSA	Mit der AG-BSA-OT wird der Wissenstransfer zwischen dem ASTRA und den BSA-OT MA bei den GE sichergestellt. Aktuelle OT-Themen werden behandelt.
Risk-Manager	EP-BSA oder PM BSA SA-CH	Der Risk Manager befasst sich mit der Analyse, Beurteilung und Steuerung von Risiken. Er identifiziert Schwachstellen, die das ASTRA unter finanziellen, operativen oder sicherheitstechnischen Aspekten schädigen könnten, beugt ihnen vor und koordiniert Lösungsvorschläge bei der Umsetzung. Er ist verantwortlich für die Entwicklung von Strategien, Prozessen und Systemen für Risk-Management und - überwachung zum Schutz der Geschäftskontinuität.

Kürzel	Bezeichnung	Beschreibung
GE-L	Leiter Gebietseinheit	Der Leiter-GE ist das Bindeglied zwischen ASTRA und GE.
GE-L-BSA **GE-L-IT**	Leiter BSA Gebietseinheit Leiter IT Gebietseinheit	Er stellt sicher, dass die IT/OT-Betriebsorganisation über die nötigen Ressourcen verfügt, damit die Rollen und Aufgaben erfüllt werden können. Er kann Teile seiner Aufgaben an den GE-L-IT delegieren und vice-versa.
GE-BSA-ISO	Fachsupport BSA GE ISO (Information Security Officer)	Der ISO ist eine von der GE-Leitung benannte Person, die im Auftrag der Leitungsebene dafür sorgt, dass die Sicherheitsanforderungen im Bereich der OT-Infrastruktur (u.a. Firewall) mit ihren industriellen Steuerungen abgedeckt sind und die Sicherheitsorganisation aus dem Bereich ISO in das OT-SMS (OT-Security Management System) eingebunden ist - Risikoassessments - Incident Management
OT-Engineer	Weitere GE BSA-OT Mitarbeiter (2nd Level Support)	Ein GE-BSA-OT-Engineer ist für Einrichtung, Betrieb und Wartung der OT-Systeme zuständig. Zu den Aufgaben gehören: - Störungsanalyse und -behebung (Incident/Problem) - Change-, release & deployment management
OT-Operator	Weitere GE BSA-OT Mitarbeiter (1st Level Support)	Der GE-BSA-OT-Operator ist für Betrieb, Überwachung und Wartung der OT-Systeme/Tools zuständig. Zu den Aufgaben gehören: - Supportanfragen (service requests) - Infrastruktur-/Service-Monitoring (u.a. NMS) - Systembetreuung - Access Manager (u.a. IAM BSA) - Managen und pflegen des OT-Inventar (u.a. IP-Adressierung)
OT-Support	Unternehmer	Der Unternehmer übernimmt diverse Aufgaben für seine Anlagen im Bereich der Wartung und 3rd Level Support.

Tabelle 1: Stellen, Gremien und Rollen

2 ISMS

2.1 Informationssicherheit

Schutzziele
Der Eigentümer der Nationalstrassen, das ASTRA, hat in der Richtlinie 13030 "OT SECURITY" [1] die Schutzziele in Kapitel 4 definiert.

Leitlinie
Die Gebietseinheit unterstützt die Schutzziele des Eigentümers, ASTRA, hinsichtlich Informationssicherheit entlang folgender Leitlinien.

Nummer	Leitlinie
LL1	Jeder BSA-Nutzer leistet seinen Beitrag zur Informationssicherheit.
LL2	Die Leitungsebene der Gebietseinheit stellt die Einhaltung dieses Konzeptes im Einflussbereich der Gebietseinheit sicher.
LL3	Wenn in diesem Konzept nicht anders definiert, werden • Aufgaben zur Informationssicherheit auf der untersten möglichen Stufe ausgeführt und • die korrekte Einhaltung auf der nächsthöheren Stufe geprüft.
LL4	Wenn in diesem Konzept nicht anders definiert, werden • Abweichungen vom Konzept systematisch dokumentiert, • von der Leitungsebene der Gebietseinheit zur Kenntnis genommen, • Handlungsbedarf adressiert und • falls angemessen an den Eigentümer eskaliert.

Tabelle 2: Leitlinien

Grundsätze der IT/OT Architektur

Verfügbarkeit	Ein einzelnes Ereignis erzeugt nur in einem vordefinierten Bereich Schaden.

Beispiele sind
- Systemgrenzen zwischen Streckenabschnitten
- Trennung von Netzwerksegmenten
  - unterschiedlicher Arten von Systemen
  - unterschiedlicher Betreiber
- Einsatz von diversitären (unterschiedlichen) parallelen Systemen

Vertraulichkeit	Es werden keine besonders schützenswerten Personendaten gesammelt. Es werden keine Personenprofile gebildet.

Beispiele sind
- fristgerechte Vernichtung von Videoaufzeichnungen
- Unkenntlichkeit von Nummernschildern und Personen in den Aufzeichnungen (Streams)
- Aufzeichnung von Videostreams nur auf / mit freigegeben und definierten Anlagen

Integrität	Jeder Zutritt und jeder privilegierte Zugriff erfolgen authentisiert.

Beispiele sind
- Unpersönliche Benutzerkonten erfordern vor deren Verwendung eine persönliche Authentisierung.
- Innerhalb gesicherter Bereiche werden nur Personen angetroffen, deren Identität bekannt ist und denen der Zutritt erlaubt ist.

2.2 Risikomanagement

2.2.1 «Communication and Consultation»

Der GE-BSA-ISO nimmt im Gremium CAB ASTRA teil, beispielsweise berät er sich mit anderen Teilnehmern zur Informationssicherheit und informiert die Leitungsebene über Handlungsbedarf.
Der GE-L resp. der GE-L-BSA und der GE-L-IT ist das Bindeglied zum ASTRA, beispielsweise für Eskalationen.
Alle anderen Aktivitäten in diesem Bereich des Risikomanagements werden vom Eigentümer wahrgenommen.

2.2.2 «Recording and Reporting»

Sobald ein BSA Nutzer Abweichungen von diesem Konzept erkennt, meldet er dies dem GE-BSA-ISO. Dieser prüft die Meldung und informiert bei einer offensichtlichen Verletzung der Schutzziele die Eigentümer.

2.2.3 «Scope, Context, Criteria», «Risk Assessment»

Der GE-BSA-ISO unterstützt den Risk-Manager bei der Bewirtschaftung der Risiken der Gebietseinheit auf Basis gemeldeter Abweichungen und gemäss seinen Aufgaben.
Alle anderen Aktivitäten in diesem Bereich des Risikomanagements werden vom Eigentümer wahrgenommen.

2.2.4 «Monitoring and Review»

Betriebseinheiten und Unternehmer unterstützen in der Erfüllung ihrer Aufgaben das Risikomanagement, beispielsweise mit technischen Massnahmen zur systematischen Überwachung von Risiken.
Der GE-BSA-ISO benutzt Prüfmethoden zur Beurteilung der Einhaltung dieses Konzeptes, beispielsweise mit Stichproben, Prüfpunkten während und nach Projekten, sowie Audits. Er stellt mittels Review die Gültigkeit des Konzeptes sicher.

2.2.5 «Risk Treatment»

Der GE-BSA-ISO empfiehlt in der Liste erkannter Abweichungen geeignete Gegenmassnahmen. Folgende Arten von Gegenmassnahmen sind möglich.

Nummer	Bezeichnung	Beschreibung	Adressat, z.B.
AG1	Vorgabe ändern	mittels Antrag an die bewilligende Stelle	GE-L-BSA GE-L-IT CAB ASTRA
AG2	Prüfung ändern	mittels Anpassung eines Arbeitsmittels, z.B. einer Checkliste	GE-BSA-ISO
AG3	System ändern	mittels ordentlichem Verfahren, d.h. Sofortmassnahme mit Mitteln der Gebietseinheit betriebliche Mittel der Erhaltungsplanung EP Systembau mittels Projektänderungsantrag	GE-L GE-L-BSA GE-L-IT Risk-Manager
AG4	Temporäre Lösung	mittels kurzfristiger Konfigurationsanpassung, wie während einer Störung, beispielsweise eine vorübergehende Beschränkung des Fernzugriffs	OT-Operator OT-Engineer
AG5	Notbetrieb herstellen	Falls verfügbar und nötig, mittels Entscheid der Notfallorganisation, beispielsweise während einer Krise	offen

Tabelle 3: Gegenmassnahmen

Je nach Art der Gegenmassnahme und Eskalationsstufe ist ein anderer Entscheidungsträger für die Umsetzung zuständig. Für AG5 ist kein Notbetrieb von IT/OT-Systemen und somit kein Adressat definiert.

Der GE-L-IT prüft die Angemessenheit und Wirksamkeit der empfohlenen Gegenmassnahmen aus Sicht der Gebietseinheit und stellt im Rahmen seiner Rolle die richtige Eskalation sicher, beispielsweise wenn die Schutzziele im Zusammenhang mit der Informationssicherheit nicht mehr erreicht werden können.

2.2.6 Bewusstseinsbildung

Mit der Umsetzung dieses Konzeptes und der regelmässigen Prüfung dessen Einhaltung entsteht für die BSA-Nutzer eine erhöhte Sichtbarkeit des Themas Informationssicherheit. Damit und mit einem wirksamen Einsatz von Mitteln rückt die Informationssicherheit ins Bewusstsein aller Beteiligten. Die Wirkung soll mit zusätzlichen Massnahmen unterstützt werden, beispielsweise Schulungen, Workshops, Plakaten, Aufklebern, Gadgets, Phishing-Kampagnen oder Penetrationstests mit einer Komponente im Social Engineering.

3 Regeln (Prozesse, Rollen und Organisation)

3.1 Informationen

3.1.1 Einsatz geeigneter Systeme

Anforderungen

USS.A01	Die Risiken der Komponenten sind vor der Beschaffung bekannt und mit der Eigentümerin abgesprochen.
USS.A02	Der Einsatz kryptographischer Algorithmen ist von der Eigentümerin bewilligt und mit der GE abgesprochen.
USS.A03	Kryptographische Verfahren werden sinnvoll eingesetzt.
USS.A04	[nur GE VII intern relevant]

Vorgaben aus übergeordneten Richtlinien

- GS-5.1 Geschäftsrelevante Informationen dürfen nur auf OT-Systemen gespeichert und verarbeitet werden, deren Inhaber entweder eine Verwaltungseinheit der Bundesverwaltung oder für die die Einhaltung der sicherheitstechnischen Anforderungen aus dieser Vorgabe vertraglich geregelt ist (z.B. im Rahmen einer RZ-Lösung). [1]
- GS-6.1 Die eingesetzten OT-Systeme müssen geeignet sein, den Schutz der Vertraulichkeit und Integrität der Informationen zu gewähren. [1]
- GS-6.2 Der Einsatz von kryptografischen Verfahren ist nur dort vorzusehen, wo dies aufgrund des Schutzbedarfs absolut notwendig ist. [1]
- GS-6.3 Werden Informationen verschlüsselt, dann müssen die dazu verwendeten Schlüssel so verwaltet werden, dass eine Wiederherstellung und damit eine Entschlüsselung der Informationen jederzeit möglich ist. In der Regel bedingt das eine aufwändige Schlüsselverwaltung (mit einem «Key Recovery»-Mechanismus) sowie ein periodisches Austesten der Wiederherstellbarkeit der Informationen. [1]

3.1.2 Backup und Restore

Anforderungen

BAR.A01	Für Server- und Clientsysteme gelten die Backupvorgaben gemäss «Rechner-Normalie» [3]
BAR.A02	Von den Netzwerkkomponenten muss eine Konfigurationsdatei der aktuellen Konfiguration abgelegt sein, wenn immer möglich im proprietären Tool (z.B. Cisco IND oder Prime).
BAR.A03	Die Quellcodes für sämtliche Steuerungen werden einheitlich abgelegt und periodisch gesichert.
BAR.A04	Es ist bekannt, welcher der jeweils letzte Zeitpunkt ist, auf den eine konsistente Wiederherstellung möglich ist (RPO Recovery-Point-Objective). Dabei werden jeweils so viele Systeme berücksichtigt, wie gemeinsam wiederhergestellt werden müssen.
BAR.A05	Es ist bekannt, wie lange es vom Entscheid für die Wiederherstellung bis zu deren Umsetzung dauert (RTO Recovery-Time-Objective).
BAR.A06	Sicherungen der Konfiguration werden so lange behalten, wie eine konsistente Wiederherstellung möglich ist.
BAR.A07	Sicherungen der Daten werden so lange behalten, wie es der Systemeigner jeweils für sein System definiert. Externe Anforderungen und interne Abhängigkeiten sind dokumentiert. Es ist möglich, dass Systeme betrieben werden, deren Daten nicht gesichert werden müssen. Auch in diesem Fall ist die Begründung dokumentiert.
BAR.A08	Sicherungen sind vor versehentlicher Löschung oder Ransomware geschützt, beispielsweise mit Datenträgern, welche offline aufbewahrt werden, oder anderen geeigneten Bedingungen für den Zugriff auf Backups.
BAR.A09	`[ nur GE VII intern relevant ]`
BAR.A10	`[ nur GE VII intern relevant ]`
BAR.A11	Die Wiederherstellung eines Systems muss geprüft werden. Systeme, welche keinen Restore-Test durchlaufen, werden grundsätzlich als nicht wiederherstellbar angesehen.

Vorgaben aus übergeordneten Richtlinien

- GS-7.1 Die Verfügbarkeit von geschäftsrelevanten Informationen muss jederzeit dem Schutzbedarf entsprechend sichergestellt sein. [1]
- GS-7.2 Der für Informationen verantwortliche Betreiber muss über eine Backup-Strategie verfügen und diese auch umsetzen. Diese Strategie muss ein Mehrgenerationen-Prinzip und eine offline Speicherung wichtiger Datenbestände vorsehen, so dass Daten auch im Falle von datenverschlüsselnder Malware («Ransomware») wiederhergestellt werden können. [1]
- GS-7.3 Die Wiederherstellung von Daten (Restore) muss mindestens einmal jährlich getestet werden. Zusätzlich ist die Wiederherstellung immer dann zu testen, wenn sich die OT-Systeme grundlegend ändern. [1]

3.1.3 Mobile Datenträger

Anforderungen

USB.A01	Wechselträger kommen nur dort zum Einsatz, wo nicht anders möglich.
USB.A02	Ein Wechseldatenträger ist als ein "kurzlebiges" Medium zu betrachten. Der Datenträger muss vor der Verwendung formatiert werden und darf nur die zu übertragenden Dateien enthalten.
USB.A03	Wechseldatenträger, welche sensitive Daten enthalten sind zu verschlüsseln und nach der Verwendung sofort zu löschen.
USB.A04	Ausnahmefälle müssen bei der GE beantragt und bewilligt werden. Dies gilt auch für GE-Mitarbeiter.
USB.A05	Der Einsatz von Wechseldatenträgern sollte wo möglich deaktiviert sein.

Vorgaben aus übergeordneten Richtlinien

- GS-8.2 Die Verwendung von mobilen Datenträgern wie USB-Sticks, etc. ist nicht gestattet. [1]

3.2 OT-System

3.2.1 Design

Anforderungen

DSN.A01	Security by Design: IT-Security-Probleme werden in der Planugsphase bereits berücksichtigt und adressiert.
DSN.A02	"Security by Obscurity" ist keine Security.
DSN.A03	Unnötige Komplexität wird ebenfalls als Sicherheitsproblem eingestuft.

Vorgaben aus übergeordneten Richtlinien

- GS-10.1 Die produktive Umgebung des OT-Systems muss von einer allenfalls vorhandenen nicht produktiven Umgebung (z.B. für Entwicklung und/oder Test) getrennt sein. [1]

3.2.2 Change-Management

Anforderungen

CMG.A01	[nur GE VII intern relevant]
CMG.A02	[nur GE VII intern relevant]

Vorgaben aus übergeordneten Richtlinien

- GS-9.2 Sicherheitskonfigurationen und -einstellungen dürfen nur autorisiert aktiviert, geändert, deaktiviert und deinstalliert werden. [1]
- GS-14.1 Für jegliche Änderungen an einem OT-System ist ein definierter Change Management Prozess einzuhalten. Im ordentlichen Betrieb ist dafür die Gebietseinheit zuständig, im Projektmodus erfolgen die Änderungen gemäss den Vorgaben der Filiale. Für zentrale Systeme der Management Ebene sind die entsprechenden Leistungserbringer zuständig. [1]

3.2.3 Netzwerkintegration

Anforderungen

INT.A01	Die Systemintegration erfolgt strikte nach dem definierten Prozess der GE.
INT.A02	Die Projekte und Unternehmer unterstützen die GE in diesem Prozess gemäss Vorgabe.
INT.A03	Falls die GE Abweichungen vom vorgegebenen Prozess oder den Sicherheitsrichtlinien feststellt, hat sie ein "Veto-Recht" und kann die Integration unterbrechen.
INT.A04	Es vor der Integration bekannt, welche Auswirkungen ein Teilsystem auf das restliche System haben kann.
INT.A05	Die zu integrierenden Systeme weisen keine Sicherheitsmängel mehr auf. Ins Netzwerk integrierte Systeme weisen keine Sicherheitsmängel mehr auf.
INT.A06	Sobald ein Gerät ins BKN/IP-Netz-BSA integriert ist, gelten sämtliche Sicherheitsrichtlinien. Abweichungen davon werden bei Bedarf eskaliert.

Vorgaben aus übergeordneten Richtlinien

- GS-9.1 Ein OT-System muss vor der Inbetriebnahme in der Produktivumgebung so konfiguriert und eingestellt sein, dass es vor unberechtigtem Zugriff geschützt ist, es soweit technisch möglich gehärtet ist und in einer zur Aufgabenerfüllung erforderlichen und vom Benutzer nicht veränderbaren Minimalkonfiguration betrieben wird (d.h. nicht genutzte Schnittstellen, Module, Dienste und Funktionen müssen deaktiviert sein), und wichtige sicherheitsrelevante Aktivitäten und Ereignisse (mit Zeitangaben) aufgezeichnet und zeitnah ausgewertet werden. [1]

3.2.4 Ausserbetriebnahme

Anforderungen

DEC.A01	Die Ausserbetriebnahme von Geräten ist der GE bekannt.
DEC.A02	Alle Datenträger müssen entsprechend der höchst-klassifizierten Information auf dem Datenträger, entsorgt werden.
DEC.A03	`[ nur GE VII intern relevant ]`

Vorgaben aus übergeordneten Richtlinien

- GS-8.1 Die Datenträger, auf denen geschäftsrelevante Informationen gespeichert sind, müssen jederzeit dem Schutzbedarf der Informationen entsprechend geschützt sein. Namentlich für die Reparatur und Entsorgung von Datenträgern müssen geeignete Prozesse definiert und umgesetzt sein. [1]

3.2.5 Wartung der Systeme

Anforderungen

MTN.A01	Die GE betreibt ausschliesslich Systeme und Systemarchitekturen, für welche das Patching technisch möglich und organisatorisch und finanziell geregelt ist. Dies wird bereits auf Projektstufe berücksichtigt.
MTN.A02	Jeder Systemeigner erhält für seine Systeme zeitnah vom Unternehmer oder Hersteller Informationen, ob und wie Sicherheitslücken geschlossen werden können.
MTN.A03	Für jedes System ist bekannt, wieviel Vorlaufzeit für eine Einspielung von Aktualisierungen erforderlich ist. Entsprechend sind periodische Wartungsfenster zu definieren.
MTN.A04	Allenfalls kann eine Aktualisierung aufgrund von Altlasten auch erst bei einer vollständigen Systemerneuerung erfolgen. In solchen Fällen sind kompensierende Massnahmen zum Schutz zu prüfen.
MTN.A05	In dringenden Fällen entscheidet der OT-Engineer nach Beratung mit dem GE-BSA-ISO, ob eine Umgehungslösung oder eine kurzfristige Aktualisierung als Emergency Change umgesetzt wird.

Vorgaben aus übergeordneten Richtlinien

- GS-11.1 Für ein OT-System und ihre Komponenten (z.B. Software-Bibliotheken, Treiber) müssen während der ganzen Lebensdauer eine professionelle Wartung und Pflege sichergestellt sein. Darunter fällt insbesondere auch die Einspielung von regelmässigen und betrieblich oder sicherheitstechnisch notwendigen Updates und Fehlerkorrekturen (Patches). Die dafür notwendigen Wartungs- und Supportverträge sind vorzusehen. [1]
- GS-11.2 Hardware und Software ist grundsätzlich vor End of Support zu ersetzen. [1]
- GS-15.1 Das OT-System muss unter Berücksichtigung von branchenüblichen Sicherheitsvorgaben und -empfehlungen («Best Practices») betrieben werden. [1]

3.2.6 Patchmanagement

Anforderungen

PTM.A01	Sämtliche Systeme sind so zu konzipieren, dass Sicherheitspatches jederzeit eingespielt werden können.
PTM.A02	Systeme sind, wenn möglich, immer auf dem aktuellen Stand zu halten.

Vorgaben aus übergeordneten Richtlinien

- GS-11.1 Für ein OT-System und ihre Komponenten (z.B. Software-Bibliotheken, Treiber) müssen während der ganzen Lebensdauer eine professionelle Wartung und Pflege sichergestellt sein. Darunter fällt insbesondere auch die Einspielung von regelmässigen und betrieblich oder sicherheitstechnisch notwendigen Updates und Fehlerkorrekturen (Patches). Die dafür notwendigen Wartungs- und Supportverträge sind vorzusehen. [1]

3.2.7 Malware

Anforderungen

VIR.A01	Die Server und Clients sind als Endgeräte ständig im Netz der GE verbunden. Für diese Geräte wird ein einheitlicher Malware-Schutz installiert.
VIR.A02	Die Malware-Schutz-Software für BSA-Geräte ist zentral zu verwalten.
VIR.A03	Externe Partner garantieren mittels Sicherheitserklärung, dass ihre Geräte einen aktuellen Virenschutz installiert haben.

Vorgaben aus übergeordneten Richtlinien

--

3.2.8 Software-Anwendungen

Anforderungen

SWA.A01	Neu entwickelte Software läuft stabil.
SWA.A02	Es sind auch Fehlerfälle in die Teststrategie eingebunden.
SWA.A03	Unnötige Funktionalität ist deaktiviert/deinstalliert.
SWA.A04	Proprietäre Sicherheitsmechanismen sind aktiviert.
SWA.A05	Die Software nutzt wo immer möglich Ressourcen und Komponenten des Basissystems (OS) wie z.B. die Zeitsynchronisation oder den DNS.

Vorgaben aus übergeordneten Richtlinien

--

3.2.9 Notfallmanagement

Anforderungen

EMG.A01	Für die Erhaltung der Sicherheit im Verantwortungsgebiet der GE sind verschiedene Szenarien definiert, welche für den Notfall einen getesteten Plan vorlegen können. Für das Szenario eines IT/OT-Notfalles sind IT/OT-Notbetrieb, sowie IT/OT-Wiederanlauf geplant und getestet.
EMG.A02	Notbetrieb bedeutet, dass die Sicherheit für IT/OT-Systeme über alternative technische Lösungen sichergestellt ist. Mindestens für geeignete, kritische Systeme wird dafür das NBS eingesetzt.
EMG.A03	Mindestens für kritische IT/OT-Basisfunktionen sind solche Pläne definiert und geprüft. Es existiert eine eigenständige Rückfallebene zum UeLS (momentan NBS), über welches die sicherheitskritischen Funktionen unabhängig vom UeLS gesteuert werden können.

Vorgaben aus übergeordneten Richtlinien

- GS-12.2 Wird ein Integritätsverlust festgestellt, muss das OT-System vom Netzwerk getrennt, gesichert und untersucht werden. Im Falle einer bestätigten Kompromittierung muss je nach OT-System und erhaltener Malware das weitere Vorgehen geprüft werden (Neuaufsetzen, Ersatz, etc.). [1]
- GS-12.3 Das OT-System muss in ein Malwareschutzkonzept eigebunden sein, das insbesondere auch regelt, wie bei einem Malwarebefall vorzugehen ist und welche Stellen wie informiert werden müssen. [1]
- GS-13.1 Für betriebskritische OT-Systeme sind für einen Ausfall oder Teilausfall dieser Systeme Notfallprozesse und Wiederanlaufszenarien vorzubereiten. Insbesondere für Safetyrelevante OT-Systeme sind diese Notfallprozesse und Wiederanlaufszenarien regelmässig zu üben und zu verbessern. [1]

3.2.10 Audits

Anforderungen

AUD.A01	Es existieren technische Vorgaben, deren Einhaltung überprüft wird. Erkannter Handlungsbedarf wird systematisch erfasst und adressiert.
AUD.A02	Organisatorische Massnahmen stellen sicher, dass technische Prüfungen vollständig und wirksam durchgeführt werden. Der Fortschritt in der Umsetzung der Mängelliste wird überwacht und bei Bedarf eskaliert.
AUD.A03	Die Aktualisierung der technischen Sicherheitsvorgaben ist sichergestellt.

Vorgaben aus übergeordneten Richtlinien

--

3.3 OT-Grundinfrastruktur

3.3.1 Identitäts- und Berechtigungsmanagement

Ein zentrales Identitäts- und Berechtigungsmanagement ermöglicht dem Betreiber eine einheitliche Verwaltung der einzelnen Entitäten. Dadurch können Fehler und Inkonsistenzen vermieden werden, welche bei heterogenen, dezentralen Individuallösungen beinahe unumgänglich sind.

Anforderungen

IDA.A01	Alle Identitäten werden zentral verwaltet. Die Anzahl der Identity-Stores ist auf ein Minimum zu beschränken.
IDA.A02	Grundsätzlich erfolgen alle Zugriffe mittels persönlicher Benutzerkennung.
IDA.A03	Die Verwendung unpersönlicher Benutzerkennungen ist zulässig, wenn nachvollziehbar ist, wer sich jeweils mit der unpersönlichen Benutzerkennung authentisiert hat, beispielsweise auf einem Gateway (VPN, …) oder Jumphost (RDS, …), oder nach Zugriff auf einen Passwortsafe mit entsprechenden Logging-Eigenschaften.
IDA.A04	`[ nur GE VII intern relevant ]`
IDA.A05	`[ nur GE VII intern relevant ]`
IDA.A06	Sollten lokal definierte Adminbenutzer erforderlich sein, können diese nur über entsprechende Berechtigungen in der Domäne eingerichtet und verwaltet werden (z.B. LAPS).
IDA.A07	Alle Rechte einer Person sind dokumentiert. Die Berechtigungsvergabe erfolgt nachvollziehbar (für Server nach dem «Benutzerkonzept für Bereichsrechner»).
IDA.A08	`[ nur GE VII intern relevant ]`
IDA.A09	User, welche sich seit über 12 Monaten nicht mehr angemeldet haben, werden deaktiviert.

Vorgaben aus übergeordneten Richtlinien

- GS-16.1 Für jedes in der Domäne nationalstrassen.admin.ch betriebene OT-System muss ein Berechtigungskonzept vorliegen, das die Berechtigungsvergabe anhand des Prinzips «Need-to-Know» regelt. Die Berechtigungen sind so zu vergeben, dass ein Benutzer nur vorgesehene Aktivitäten durchführen kann. [1]
- GS-16.2 [...] Insbesondere müssen die Benutzeridentitäten mindestens jährlich in Bezug auf Notwendigkeit und Richtigkeit überprüft und nicht mehr benötigte Benutzer gelöscht werden. [1]
- GS-16.3 Alle Zugriffsrechte auf ein OT-System müssen im Rahmen eines definierten und dokumentierten Prozesses verwaltet und stets aktuell gehalten werden. Insbesondere müssen die Rechte mindestens jährlich in Bezug auf Notwendigkeit und Richtigkeit durch den Betreiber überprüft und nicht mehr benötigte Rechte entfernt werden. [1]
- GS-17.1 Der Zugriff auf OT-Systeme basiert auf persönlichen Logins. [1]
- GS-17.3 Gruppen-Accounts/-logins werden grundsätzlich nicht zugelassen. [1]

3.3.2 Zugriffsschutz

Anforderungen

ACP.A01	Es finden nur authentisierte Zugriffe auf Systeme statt, beispielsweise mit Benutzerkennung und Passwort, oder Maschinenzertifikaten oder API-Key und Token.
ACP.A02	`[ nur GE VII intern relevant ]`

ACP.A03 [nur GE VII intern relevant]

Vorgaben aus übergeordneten Richtlinien

- GS-16.2 Die Benutzeridentitäten und Benutzerrollen müssen über das IAM BSA verwaltet werden. [...]. [1]
- GS-17.2 Die Authentifikation eines Benutzers gegenüber einem OT-System muss mittels einer 2-Faktoren-Authentifikation erfolgen. Erfolgt die Anmeldung eines Benutzers von einer festen Bedienstation, welche direkt am OT-Netz angeschlossen ist, innerhalb eines überwachten Raumes der GE/ASTRA aus, so genügt eine Authentifikation mittels Benutzer-ID und Passwort. [1]
- GS-18.1 Das Passwort ... [1]
- GS-18.2 Ein administrativ gesetztes Initialpasswort muss bei seinem Erstgebrauch geändert werden. [1]
- GS-18.3 Wenn das Passwort geändert wird, muss sichergestellt sein, dass das neue Passwort keinem der 10 zuletzt verwendeten Passwörtern entspricht. [1]
- GS-18.4 Nach maximal 5 Fehleingaben muss das Passwort gesperrt und darf nur im Rahmen eines definierten Prozesses wieder freigegeben werden. [1]
- GS-18.5 Bei Verdacht (oder Bestätigung) auf Kenntnisnahme durch Unberechtigte oder Missbrauch muss das Passwort umgehend geändert werden. [1]
- GS-18.6 Server-seitig muss sichergestellt sein, dass das Passwort nie im Klartext ausgelesen oder im Rahmen eines anderen Angriffs leicht kompromittiert werden kann. [1]
- GS-18.7 Passwörter müssen nur dann geändert werden, wenn ein Verdacht auf Missbrauch vorliegt. [1]
- GS-18.8 Auto-Logout oder Sperrbildschirm nach einer inaktiven Zeitspanne von xy min.(ausser spezielle Clients z.B. Zentrale) [1]
- GS-19.1 Administrative Zugriffe auf OT-Systeme müssen auf eine dokumentierte und kontrollierte Art und Weise erfolgen. Insbesondere müssen solche Zugriffe mittels sicherer Protokolle erfolgen, nachvollziehbar aufgezeichnet und ausgewertet werden können. [1]
- GS-19.2 Die Nutzung der entsprechenden (privilegierten) Konti muss einer Person zugeordnet werden können. Zudem dürfen die Konti nur über minimal erforderliche und möglichst kurzlebige Zugriffsrechte verfügen. [1]

3.3.3 Monitoring

Anforderungen

MON.A01	Wenn nicht anders im IT-Inventar angegeben, sind alle Systeme kritisch hinsichtlich Systemverfügbarkeit und werden laufend auf ihren Betriebszustand überwacht, beispielsweise durch ein Monitoring mittels Ping, SNMP, Skripts zur Feststellung, ob SSH oder HTTPS verfügbar sind.
MON.A02	Ereignisse auf Systemen werden systematisch aufgezeichnet und zentral gespeichert. Sie dienen der Erkennung von Anomalien oder der Analyse von Ursachen für Systemstörungen.
MON.A03	Der Stand der Systeme wird regelmässig erhoben, beispielsweise durch Netzwerkscans oder Meldungen von Agents auf den Systemen. Zusätzlich werden Verwundbarkeitsscans durchgeführt, um Handlungsbedarf zu erkennen.

Vorgaben aus übergeordneten Richtlinien

- GS-20.1 Sämtliche OT-Systeme müssen, soweit dies technisch machbar ist, aktiv überwacht (Monitoring-Konzept) werden. [...]. [1]

3.3.4 Logfiles

Anforderungen

LOG.A01	Aufzeichnungen von Systemereignissen werden systematisch erhoben. Die Mindestanforderung betrifft sicherheitsrelevante Ereignisse, wie Meldungen zur Authentisierung, das Starten systemkritischer Prozesse, Verbindungsversuche aus und in das BKN-Netz der GE und jeweils die Kommunikationspartner dazu.
LOG.A02	Anomalien können erkannt werden. Sicherheitsrelevante Störungen sind in den Aufzeichnungen nachvollziehbar.
LOG.A03	`[ nur GE VII intern relevant ]`

Vorgaben aus übergeordneten Richtlinien

- GS-20.1 [...] Ebenso muss ein Logging aktiviert sein und Logs müssen systematisch und zeitnah auswertet werden, damit Anomalien wie zum Beispiel Angriffsversuche, Fehlverhalten, Hardware-Probleme etc. frühzeitig entdeckt werden können. [1]
- GS-20.2 Log-Files bzw. Loggings müssen mindestens 12 Monate aufbewahrt werden. Dabei ist sicherzustellen, dass die Log-Daten geschützt bleiben und nicht manipuliert werden. [1]

3.3.5 Alarmfunktionalität

Anforderungen

ALA.A01	Die Systemüberwachung stellt sicher, dass Systemausfälle ausreichend schnell erkannt werden.
ALA.A02	Der Malware-Schutz stellt sicher, dass Schadsoftware rasch erkannt oder deren Ausführung sofort blockiert wird.
ALA.A03	Die Überprüfung von Aufzeichnungen ermöglicht die Erkennung von Anomalien.
ALA.A04	Erkannte Störungen werden nach einem geregelten Verfahren eskaliert.

Vorgaben aus übergeordneten Richtlinien

--

4 Mensch (Know-How, Ausbildung und Awareness)

4.1 Sensibilisierung und Schulung

4.1.1 Awareness

Da die Menschen eine zentrale Rolle im Bereich der Cybersicherheit spielen, ist es wichtig, dass diese entsprechend ihrer Funktion sensibilisiert und geschult werden.

Anforderungen

AWR.A01	Alle BSA-Nutzer, d.h. Mitarbeitende, Unternehmer und Projekt-Beteiligte (mit direktem Bezug zum BKN) werden mit Massnahmen zur Sensibilisierung im Thema IT/OT-Sicherheit erreicht. Dazu gehört die Kenntnis von Regeln oder das Verhalten im Umgang mit IT/OT-Sicherheit (Passwörter, etc.). Mögliche Massnahmen sind Web-Based-Trainings, Plakate, «Give-away», gezielte Teilnahme im Rahmen des GE-Schulungsprogramms.
AWR.A02	Fachpersonen mit Rollen im Thema IT/OT-Systeme erhalten während der Erfüllung ihrer Aufgaben («Training-on-the Job») Informationen zu aktuellen Entwicklungen der IT-Security, beispielsweise im Austausch mit Externen während der Behebung von Mängeln.
AWR.A03	Bei Bedarf erfolgen gezielte Ausbildungen («Training-off-the-Job»).

Vorgaben aus übergeordneten Richtlinien

- GS-1.1 Alle Benutzerinnen und Benutzer von OT-Systemen müssen im Bereich der OT-Sicherheit stufen- bzw. funktionsgerecht sensibilisiert und geschult sein. [1]
- GS-1.2 Sie müssen die für OT-Systeme relevanten Einsatzrichtlinien kennen und sind zu deren Einhaltung verpflichtet. [1]
- GS-1.3 Sie müssen jährlich ein Training zum bewussten Umgang mit OT-Systemen absolvieren (Awareness-Training). [1]

4.2 Meldepflicht

4.2.1 Anforderungsmanagement

Anforderungen

REQ.A01	Die Einhaltung der Vorgaben in diesem Konzept bewirkt eine Reduktion der Komplexität des Gesamtsystems. Der GE-BSA-ISO wird von Projekten, Vorgesetzten und BSA-Nutzern in seiner Rolle berücksichtigt und unterstützt.
REQ.A02	Für Projekte ist festgelegt, zu welchem Zeitpunkt die GE-IT miteinbezogen werden muss. Dadurch verfügt man über ausreichende Informationen, um die Komplexität zu reduzieren und die Sicherheit zu erhöhen. D.h. FaSKoB und EP BSA berücksichtigen die Bemerkungen und stellen deren Einhaltung im Rahmen von Projekten sicher. Der GE-BSA-ISO berät sie dabei.
REQ.A03	[nur GE VII intern relevant]
REQ.A04	[nur GE VII intern relevant]
REQ.A05	Das PM ASTRA stellt während der Umsetzung seiner Vorhaben die Wirksamkeit der Vorgaben sicher, beispielsweise durch Beratung mit dem GE-BSA-ISO oder durch Einbezug der Projektbeteiligten und der GE-FPU. Er stellt bei seiner Arbeit die Einhaltung der technischen Vorgaben mindestens mit der gleichen Sorgfalt sicher, als wären es bauliche Vorgaben. Der GE-BSA-ISO hat das Recht jederzeit in einem laufenden Projekt eine Sicherheitsprüfung durchzuführen oder durchführen zu lassen.
REQ.A06	Auf Basis dieses Konzeptes werden Prüfpläne für die Systeme erstellt. Im Rahmen des Betriebes werden diese durch die OT-Engineer erstellt und angepasst. Im Rahmen eines Projektes liegt diese Tätigkeit in der Verantwortung des PM ASTRA und seiner Unternehmer.
REQ.A07	[nur GE VII intern relevant]
REQ.A08	Der GE-BSA-ISO meldet Verstösse gegen das vereinbarte Vorgehen an den GE-L-IT. Beispielsweise, wenn ein Projekt nicht oder zu spät dem GE-BSA-ISO zur Kenntnis gebracht wird.
REQ.A09	BSA-Nutzer melden erkannte Verstösse gegen dieses Konzept wahlweise via den Vorgesetzten oder direkt an den GE-BSA-ISO.

Vorgaben aus übergeordneten Richtlinien

- GS-2.1 Alle Benutzerinnen und Benutzer von OT-Systemen müssen Ereignisse, wie z.B. anormales und verdächtiges Systemverhalten oder physischer Verlust, möglichst zeitnah der dafür zuständigen Stelle melden. [1]

4.3 Personensicherheitsprüfung

4.3.1 Benutzeranträge

Anforderungen

USR.A01	Um einen System-Zugang zu erhalten, muss der Zugang mittels Formulars bei der GE beantragt werden. Die Person bestätigt dabei die Datenschutzerklärung sowie die Geheimhaltungspflicht einzuhalten.
USR.A02	Die Identität der Person wird über bekannte Identitäten geprüft, indem eine der GE bekannte Person den Antrag signiert.

Vorgaben aus übergeordneten Richtlinien

- GS-3.1 Personensicherheitsprüfungen sind grundsätzlich nicht notwendig. [1]
- GS-3.2 Die Personensicherheitsprüfung erfolgt nur bei Personen in sicherheitsempfindlichen Funktionen mit Zugang zu klassifizierten Informationen, Materialien oder Anlagen. [2]

4.4 Security-Rollen und -Organisation

4.4.1 Organisation

Geregelte Verantwortungen helfen den Betrieb koordiniert zu steuern und zu überwachen. In diesem Zusammenhang sind die Rollen und Verantwortlichkeiten innerhalb der Gebietseinheit zusammen mit ihren Stakeholdern definiert.

Anforderungen

ORG.A01	Dieses Sicherheitskonzept ist gültig und wirksam. Die Verantwortung ist nachvollziehbar geregelt.
ORG.A02	Gültig ist immer die aktuelle Version dieses Konzeptes. Das Framework wird regelmässig auf Vollständigkeit und Aktualität geprüft und bei Bedarf aktualisiert.
ORG.A03	`[ nur GE VII intern relevant ]`
ORG.A04	`[ nur GE VII intern relevant ]`
ORG.A05	`[ nur GE VII intern relevant ]`

Vorgaben aus übergeordneten Richtlinien

- GS-4.1 Die Security Rollen gem. Kap. 5.2 sind zu besetzen. [1]

5 Technologie

5.1 Netzwerk / Netzwerkzonen

5.1.1 Inventar

Anforderungen

INV.A01	Es gibt eine konsistente Inventarlösung über alle Systeme (Hard- und Software). Aufgrund der technischen Gegebenheiten und Anforderungen kann es sinnvoll sein, mehrere Inventare zu verwenden. Es muss jedoch klar geregelt sein, welches Inventar für welches System / welche Komponenten verwendet werden. Doppelte Inventarisierungen sind aus konsistenzgründen verboten.
INV.A02	Der OT-Operator erfasst im Inventar alle seine von der GE oder deren Unternehmer betriebenen IT- oder OT-Systeme, welche über eine IP-Adresse erreichbar sind, sowie das jeweilige Betriebssystem und die installierten Softwarepakete. Die Software kann auch in einem separaten Tool erfasst werden, sofern darin ein eindeutiger Bezug zum Hardware-Inventar hergestellt werden kann und die verschiedenen Inventare keine Inkonsistenzen zulassen. An einem solchen System angeschlossene OT-Systeme ohne IP-Adressierung werden summarisch erfasst. Jeder Eintrag im Inventar hat einen solchen Systemeigner, welcher die Vollständigkeit und Aktualität seiner Einträge sicherstellt.
INV.A03	Die Systemeigner erkennen und dokumentieren im Inventar, ob und welche Abhängigkeiten zwischen zwei Systemen bestehen. Bei dieser Form der Klassifikation berücksichtigen sie die Grundsätze der IT/OT-Architektur. Wenn also ein höherer Schutzbedarf - als von diesem Konzept vorgegeben - erkannt wird, ist dieser im Inventar ausgewiesen.
INV.A04	Externe Systeme sind ebenfalls zu inventarisieren.

Vorgaben aus übergeordneten Richtlinien

- GS-24.2 Die OT-Systeme müssen inventarisiert sein. (gilt für die neuen Netze IP-Netz BSA GE, nicht anwendbar auf die bestehenden Netze der GE). [1]

5.1.2 Netzwerkpläne

Anforderungen

NPL.A01	`[ nur GE VII intern relevant ]`
NPL.A02	Zu jedem produktiven System ist ein aktueller Netzwerkplan verfügbar.
NPL.A03	Der Entwickler eines Systems ist zuständig, dass der entsprechende Netzwerkplan korrekt erstellt wird.

Vorgaben aus übergeordneten Richtlinien

--

5.1.3 Segmentierung

Anforderungen

SEG.A01	Netzsegmente der GE sind verschiedene Adressbereiche, welche Routingfunktionalität benötigen, um Datenflüsse zwischen ihnen zu ermöglichen. Dies dient der schnellen und einfachen Trennung von technologischen Abschnitten, - wenn ein Notfall dies erfordert oder - wenn die Sicherheit von Systemen in einem Abschnitt eine Trennung erfordert, beispielsweise, weil der Hersteller keine Sicherheitspatches mehr ausliefert oder - wenn die Datenflüsse verschiedener Systeme einander nicht beeinflussen dürfen, beispielsweise Notfallkommunikation, Backup oder Administration von kritischen Systemen.
SEG.A02	Das Core- und Distribution-Netzwerk sind komplett redundant erschlossen.
SEG.A03	Das Netzwerk ist in klar definierte Zonen unterteilt.
SEG.A04	Der Verkehr zwischen den Zonen erfolgt ausschliesslich über Firewalls.
SEG.A05	Funktechnologien übertragen nur verschlüsselte Daten
SEG.A06	In der BKN Normalie der GE VII [4] ist die Netzwerksegmentierung beschrieben.

Vorgaben aus übergeordneten Richtlinien

- GS-21.1 Das IP-Netz BSA ist als geschlossenes Netz im Sinne eines OT-Netzes zu betreiben. Die Trennung von den Office-Netzen ist dabei strikt einzuhalten. Die Vorgaben erfolgen in der ASTRA Richtlinie 13040 IP-Netz BSA. (gilt analog auch für die bestehenden Netze der GE) [1]
- GS-22.1 Das IP-Netz BSA setzt ein Zonenmodell konform zum Zonenmodell Bund um. (gilt für die neuen Netze IP-Netz BSA GE, nicht anwendbar auf die bestehenden Netze der GE) [1]
- GS-24.1 Jedes OT-System muss einer Netzwerkzone zugehören und die entsprechenden Policy-Anforderungen aus der Network Security Policy IP-Netz BSA (NSP IP-Netz BSA) erfüllen und gemäss der NSP IP-Netz BSA betrieben werden. (gilt für die neuen Netze IP-Netz BSA GE, nicht anwendbar auf die bestehenden Netze der GE) [1]

5.1.4 Netzwerkzugriffe

Anforderungen

NAC.A01	`[ nur GE VII intern relevant ]`
NAC.A02	Ungenutzte Netzwerkports sind deaktiviert und in einem separaten VLAN.

Vorgaben aus übergeordneten Richtlinien

- GS-25.1 WLAN ist grundsätzlich zugelassen und erfolgt gemäss den Vorgaben der Network Security Policy IP-Netz BSA. (gilt analog auch für die bestehenden Netze der GE) [1]

5.2 Perimeterschutz

5.2.1 Fernzugriff

Anforderungen

RMT.A01	Die externen Zugriffe erfolgen alle über denselben standardisierten Weg mit 2-Faktor-Authentifizierung.
RMT.A02	`[ nur GE VII intern relevant ]`
RMT.A03	VPN-Zugriffe sind für externe Unternehmer zeitlich beschränkt.
RMT.A04	Zeitlich unbeschränkte VPN-Zugänge sind nur für Partnerorganisationen mit entsprechenden Wartungsverträgen zulässig.

Vorgaben aus übergeordneten Richtlinien

- GS-26.1 Der Fernzugriff (Remote Access) erfolgt zentral über die beiden Zugangspunkte in den Basisdiensten IP-Netz BSA BD A/B gemäss den Vorgaben aus der NSP IP-Netz BSA. [1]
- GS-26.2 Der Fernzugriff erfolgt immer mittels 2-Faktor Authentisierung. [1]
- GS-26.3 In der Migrationsphase IP-Netz BSA dürfen die Fernzugriffe noch über die lokalen externen Zugänge in den Netzen der Gebietseinheiten erfolgen. Grundsätzlich sind auch da die Vorgaben aus der NSP IP-Netz BSA zu befolgen. [1]
- GS-26.4 Grundsätzlich dürfen die Fernzugriffe (Remote Access) nur zeitlich begrenzt geöffnet werden und müssen überwacht sein. Es ist sicherzustellen, dass sich ein Benutzer nach max. 24h erneut anmelden muss. [1]
- GS-26.5 Während eines Fernzugriffes müssen sich die Benutzer beim Verlassen des Arbeitsplatzes abmelden. [1]
- GS-26.6 Jumphosts müssen für Fernzugriffe verwendet werden, um auf OT-Systeme zuzugreifen. Administrative Tools für Wartungen, Diagnose und Konfiguration sind auf diesen Jumphosts zu installieren. [1]
- GS-26.7 Fernzugriffe und Datentransfers sind separat freizuschalten. Daten dürfen nur mit Rücksprache des Betreibers transferiert werden. [1]

5.2.2 Datenflüsse

Anforderungen

DAF.A01	Alle Datenflüsse zwischen dem Netzwerk der GE und einem Kommunikationspartner im Internet enden auf einer Maschine in einem isolierten Segment («DMZ»), d.h. auf einem Gateway oder Proxy.
DAF.A02	[nur GE VII intern relevant]
DAF.A03	Datenflüsse zwischen den Netzwerken Dritter oder Unternehmer über das BKN-Netzwerk der GE werden als missbräuchlich bewertet und sind nicht zulässig.
DAF.A04	Datenflüsse zwischen Netzsegmenten im Netzwerk der GE sind auf bewilligte Protokolle und mindestens für eines der Segmente auf IP-Adressen beschränkt.
DAF.A05	[nur GE VII intern relevant]
DAF.A06	[nur GE VII intern relevant]
DAF.A07	[nur GE VII intern relevant]

Vorgaben aus übergeordneten Richtlinien

- GS-23.1 Die ASTRA Dokumentation 83042 Network Security Policy IP-Netz BSA (NSP IP-Netz BSA) regelt den Aufbau und den Betrieb des Zonenmodells. Sie gilt als Policy für sämtliche im Perimeter IP-Netz BSA umgesetzten Zonen. Abweichungen davon müssen durch die jeweiligen Betreiber begründet und schriftlich festgehalten werden. Eine Freigabe erfolgt durch das CAB OT Security. (gilt für die neuen Netze IP-Netz BSA GE, nicht anwendbar auf die bestehenden Netze der GE) [1]
- GS-27.1 Direkte Zugänge von Internet auf OT-Systeme im IP-Netz BSA werden nicht zugelassen. Ebenso werden keine direkten Zugänge von OT-Systemen im IP-Netz BSA auf das Internet zugelassen. [1]
- GS-27.2 Internetverbindungen sind auf ein Minimum zu beschränken und erfolgen über die DMZ-Infrastruktur der Basisdienste gemäss den Vorgaben der NSP IP-Netz BSA. [1]

5.3 Physische Infrastruktur / Zutritt

5.3.1 Physischer Zutritt

Anforderungen

PAC.A01	Sämtliche Komponenten sind durch bauliche Massnahmen vor unberechtigtem Zugriff geschützt.
PAC.A02	[nur GE VII intern relevant]

Vorgaben aus übergeordneten Richtlinien

- GS-28.1 Der physische Zugang zu BSA-Systemen steht nur berechtigten Personen zu. [1]
- GS-29.1 Die OT-Systeme müssen in abschliessbaren Räumen oder Behältnissen untergebracht sein. Zwingend offen installierte Sensoren oder Aktoren müssen von der zugehörigen Steuerung auf unerlaubte Zugriffe und Manipulationen überwacht werden. [1]
- GS-29.2 Operatoren Arbeitsplätze, Server- und Storage-Systeme müssen in geschützten und abschliessbaren Räumen betrieben werden. [1]
- GS-30.1 Technikräume und Tunnelzentralen sind nach definierten ASTRA-Standards zu bauen und zu betreiben. [1]
- GS-31.1 Der Zutritt zu Technikräumen in Werkhöfen, Stützpunkten, Zentralen, etc. oder der Zugang zu Kabinen, Steuerkästen, etc. mit OT-Systemen ist einzuschränken und klar zu regeln. [1]
- GS-31.2 Die Zutritte zu Technikräumen mit Serversystemen müssen nachvollziehbar sein (Logging). [1]
- GS-31.3 Schliess- und Zutrittskonzepte müssen vorhanden sein. Allenfalls Videoüberwacht, wenn nur physischer Schlüsselzugang möglich ist. [1]

5.4 Serversysteme, Clients und Mobile-Devices

5.4.1 Allgemeine Server

Anforderungen

SRV.A01	Grundsätzlich ist die Standardhardware der GE zu verwenden.
SRV.A02	Der Server muss an einem Ort betrieben werden, zu dem nur berechtigte Personen Zutritt haben (z.B. in einem Serverschrank).
SRV.A03	Für die Anmeldung von Benutzern und Diensten muss ein Authentisierungsverfahren gem. übergeordneter Richtlinie eingesetzt werden. Begründete Ausnahmen sind von der zuständigen Stelle zu bewilligen und zu dokumentieren.
SRV.A04	Der Virenschutz muss ab der Systemintegration aktiviert sein. Begründete Ausnahmen müssen von der zuständigen Stelle bewilligt und dokumentiert werden.
SRV.A05	Der Server muss mittels SNMP überwacht werden können. Die SNMP-Überwachung darf das System nicht beeinflussen. SNMP ist nur Read-Only zulässig.

Vorgaben aus übergeordneten Richtlinien

- GS-12.1 Die Integrität der auf dem OT-System eingesetzten Softwarekomponenten muss sichergestellt sein (z.B. mit Hilfe von digitalen Signaturen). Insbesondere muss jedes Server-System mit erhöhtem Schutzbedarf regelmässig einer Integritätsprüfung unterzogen werden. [1]

5.4.2 Mobile-Devices

Anforderungen

MOB.A01	Zugriffe auf Systeme im BKN-Netz der GE erfolgen remote und über definierte Zugänge, beispielsweise VPN, RDS, Jumphost oder ähnliches, nicht mit mobilen Endgeräten.
MOB.A02	[nur GE VII intern relevant]

Vorgaben aus übergeordneten Richtlinien

- GS-32.1 Externe Clients (nicht von der OT betriebene Geräte) erhalten keinen direkten Zugang zum IP-Netz BSA und werden immer als Fremdgeräte betrachtet (gilt auch für Geräte von Systemlieferanten). Der Zugang erfolgt über den Perimeterschutz. [1]
- GS-32.2 Ein direkter Zugang auf OT-Systeme bspw. für Inbetriebnahmen oder Notfälle durch ein Fremdgerät ist nur dann gestattet, wenn dies explizit durch den Betreiber freigegeben wird. [1]
- GS-33.1 Mobile Devices erhalten keinen direkten Zugang zum IP-Netz BSA und werden immer als Fremdgeräte betrachtet (gilt auch für Geräte von Systemlieferanten und für Geräte des eigenen Betriebs). Der Zugang erfolgt immer über den Perimeterschutz. [1]

6 Betriebsorganisation IP-Netz BSA

Das Kap. 6 soll zum besseren Verständnis die Grundsätze und den Aufbau der Betriebsorganisation IP-Netz BSA aufzeigen. Weitere Information sind im Betriebskonzept IP-Netz BSA beschrieben.

Dieses Kapitel wird ergänzt, sobald der Umgang mit dem IP-Netz BSA im Betrieb geklärt ist. Zurzeit befindet sich das zuständige Projekt noch in der Konzeptphase (Stand Juli 2024).

Für das BKN sind die Betriebskonzepte in der BKN-Normalie [4] und der Rechner-Normalie [3] geregelt. Ebenfalls befinden sich dort detailliertere Vorgaben zu einzelnen Themenblöcken.

7 Literaturverzeichnis

[1] Bundesamt für Strassen ASTRA, „Richtlinie 13030 OT Security," 2024.
[2] Bundesamt für Strassen ASTRA, „OT-Sicherheitskonzept für den Betrieb der BSA," 2024.
[3] Gebietseinheit VII, „Rechner-Normalie," 2024.
[4] Gebietseinheit VII, „BKN-Normalie," 2023.

8 Tabellenverzeichnis