Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

ASTRA Sicherheitskonzept IT/OT BSA

Gebietseinheit VII

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Strassen ASTRA

Version 1.5 / 08. November 2022

Impressum

Version	1.5
Autoren	Roger Züger Patrik Keller Fabio Caspani bw digitronik, Robert Klein
Fachliche Mitwirkung	Roger Züger
Herausgeber	Baudirektion Kanton Zürich Tiefbauamt, GE VII - Nationalstrassenunterhalt Betriebsleitzentrale Werkhofstrasse 1 8902 Urdorf 044 736 54 11
Dateiname	IT-OT-Sicherheitskonzept GEVII.docx
Zweck	IT/OT Sicherheitskonzept gemäss ASTRA Merkblatt 26 010-04002
Letzte Änderung / von	8. November 2022 / Fabio Caspani
Genehmigt am / von	9. November 2022 / Roger Züger
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 bezweckt die systematische und nachvollziehbare Benennung und Meldung von Handlungsbedarf zur Erreichung der definierten Schutzziele gemäss Technischem Merkblatt BSA 26 010-04002 «IT/OT-Sicherheitskonzept für den Betrieb der BSA».

1.2. Definitionen

1.2.1. 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.

1.2.2. 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.

1.2.3. Lieferanten

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

1.2.4. Systeme

Dieses Konzept bezeichnet mit IT-System eine oder mehrere Maschinen, welche der Datenverarbeitung dienen und über eine IP-Adresse mit anderen IT-Systemen verbunden sind.

Dieses Konzept bezeichnet mit OT-System eine oder mehrere Maschinen, welche durch automatische Datenübermittlung oder -verarbeitung Steuerungsaufgaben beeinflussen oder übernehmen. Beispiele dafür sind Sensoren, Steuerungen, Signalisation.

1.2.5. Inventar

Dieses Konzept bezeichnet als Inventar ein IT-System, welches der Gebietseinheit dazu dient, diejenigen IT-Systeme systematisch zu erfassen, welche direkt durch Mitarbeitende oder indirekt durch Lieferanten der Gebietseinheit betrieben werden.

1.3. Gültigkeit

Dieses Konzept wird mit der Abnahme im Rahmen des Projektes «F4 IP Netz BSA_IT/OT Sicherheitskonzept» für die Gebietseinheit erstmals gültig. Ohne Änderungen an den Vorgaben bleibt das Konzept gültig und wird mindestens jährlich auf Änderungsbedarf geprüft. Wird ein Bedarf festgestellt, wird dieser umgehend analysiert, notwendigen Massnahmen abgeleitet und das vorliegende Sicherheitskonzept entsprechend ergänzt.

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.

Wenn in diesem Konzept die männliche Form gewählt wird, gelten die Anweisungen für alle Personen, welche in den Geltungsbereich fallen.

1.4. Geltungsbereich

In den Geltungsbereich dieses Konzeptes fallen alle BSA-Nutzer in der Gebietseinheit und die IT-Systeme im Inventar der Gebietseinheit und daran angeschlossene OT-Systeme.

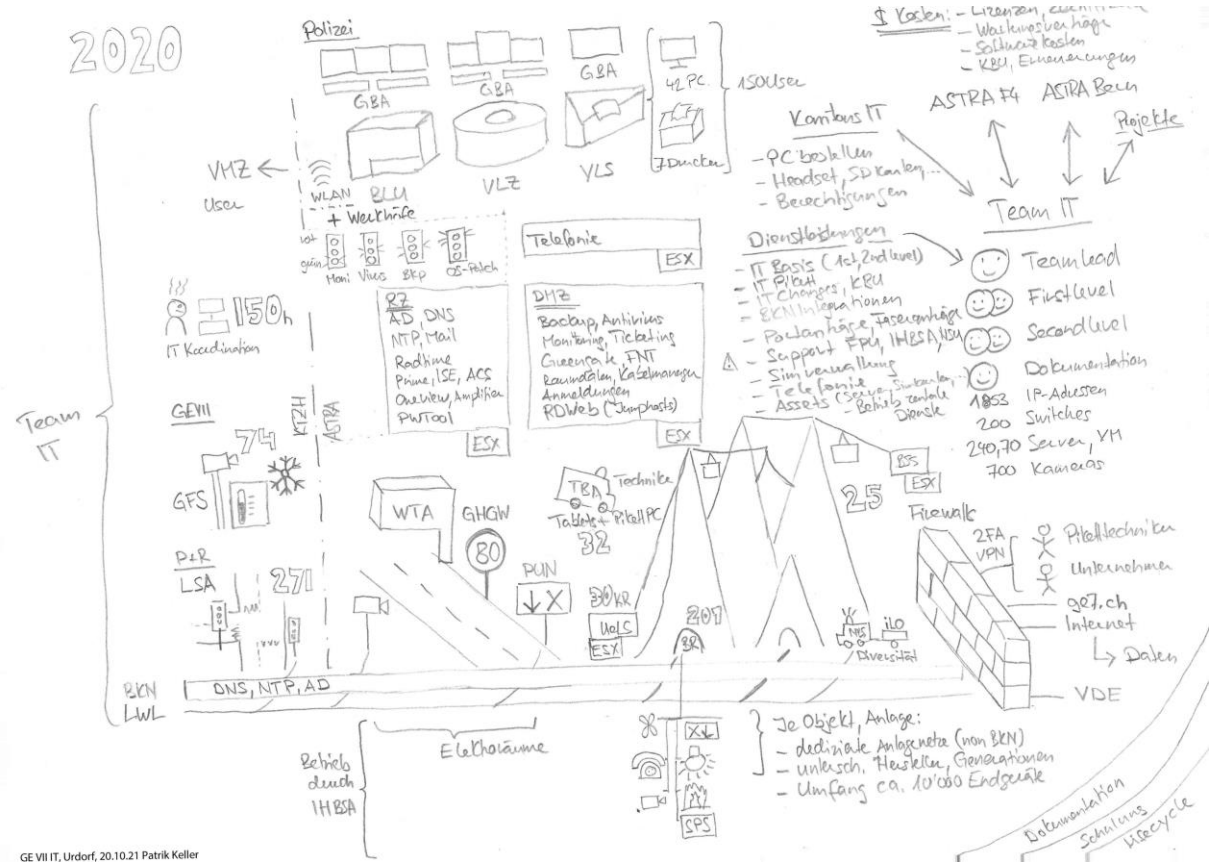

Figure 1 - Wimmelbild zum Geltungsbereich

Das Wimmelbild gibt einen ersten Überblick über die Menge und Vielfalt an technischen Komponenten und Services, welche für die Leistungserbringung der GE erforderlich sind.

UeLS, BKN und NBS bilden die Basis für die Kommunikation. Darunter sind Elektroräume, welche von IH-BSA betrieben werden, und Bereichsrechner eingezeichnet. Dieses Konzept regelt, wie diese Bereiche und die angeschlossenen Komponenten in Betrieb genommen und betrieben werden sollen.

1.5. Rahmenbedingungen

1.5.1. Klassifikation

Das Sicherheitsmanagement ist differenzierter möglich, wenn eine Klassifikation der inventarisierten Systeme erfolgt. Aktuell sind keine Vorgaben bekannt, welche unterschiedliche Schutzmassnahmen für unterschiedliche Schutzbedürfnisse verlangt.

1.5.2. 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.

1.5.3. 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.

Konflikte werden zuerst bei den Schutzzielen SZ5 und SZ6 in Table 2 sichtbar. Kapitel 3 und 4 zeigen den erkannten Handlungsbedarf.

1.6. Anspruchsgruppen

Wenn in diesem Konzept nicht anders definiert, erfolgt die Kommunikation zwischen den Rollen der Gebietseinheit gemäss nachfolgender Darstellung.

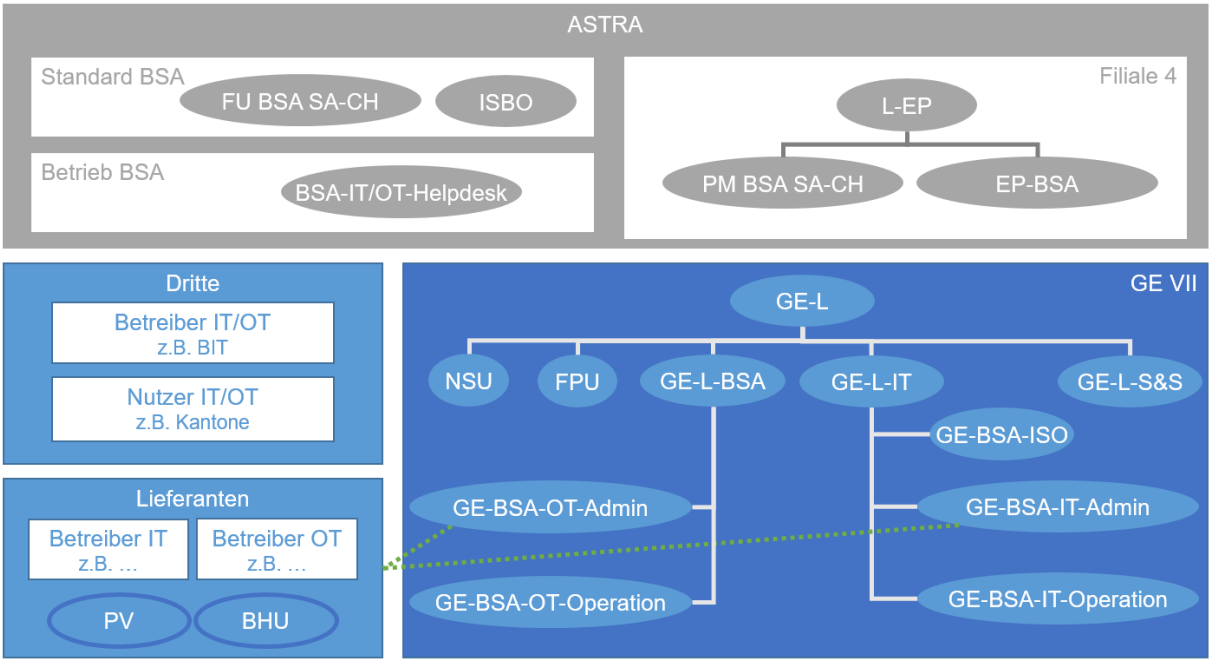

Figure 2 - Rollen und Anspruchsgruppen

Grün strichliert ist dargestellt, für welche Rollen die Verbindungen der Gebietseinheit zu deren Lieferanten definiert ist.

1.7. Rollen innerhalb der Gebietseinheit

Die nachfolgende Tabelle zeigt, die Rollen in der Gebietseinheit, deren Aufgaben und deren Besetzung.

Kürzel	Bezeichnung und Beschreibung	Zuständigkeit	Besetzung
GE-L	**Leiter Gebietseinheit** Er kann Teile seiner Aufgaben an den GE-L-BSA und/oder den GE-L-IT delegieren.	Der Leiter-GE ist das Bindeglied zwischen ASTRA und GE.	unverändert
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.	Infrastructure-Management Platform-Management Continuity-Management Improvement-Management Service Request-Management Ref.: Betriebsverantwortliche, Allgemeine management Praktiken, Infrastructure, platform & service request management	unverändert

Kürzel	Bezeichnung und Beschreibung	Zuständigkeit	Besetzung
GE-L-BSA **GE-L-IT**	**Gruppenchef BSA** **Teamleiter IT** Er stellt die operative Umsetzung des IT/OT-Sicherheitskonzeptes in der GE sicher. Rapportiert dem Leiter BSA resp. Leiter IT über alle Aspekte der I/OT-Sicherheit und überwacht die Schulung der MA.	Betriebsreporting Asset Management Service Validation & Testing (Sicherstellung von Abnahmen) Ref.: strategy, transition und management Praktiken service, technische management Praktiken, measurement and reporting, service continuity management	unverändert
GE-BSA-ISO	Er ist der IT-Spezialist in der GE und erarbeitet die Sicherheitsziele zuhanden der GE, respektive deren Leitungsebene. Er überprüft die internen Abläufe auf das bestehenden IT/OT-Sicherheitskonzept und meldet Verbesserungsvorschläge oder Differenzen. Er stellt sicher, dass das interne Know-how den Anforderungen genügt, organisiert Schulungen und fördert so das Bewusstsein der Mitarbeiter für Informationssicherheit. Bei Projekten ist er Ansprechpartner für die Überprüfung bezüglich der Übereinstimmung mit dem IT/OT-Sicherheitskonzept der GE. Er nimmt an der GE AG-BSA-IT teil und stellt den Wissenstransfer mit dem ASTRA und unter den GE sicher. Er identifiziert, bewertet und überwacht Risiken bezüglich der IT/OT-Sicherheit.	Information Security Change Enablement Ref.: continual service improvement, change enable	neu
GE-BSA-IT/OT-Admin	Er hat die Übersicht über alle IT/OT-Komponenten (Inventar), stellt die Dokumentation und deren Aktualisierung sicher Er ist der Ansprechpartner für Changes, Release, Problems und	Release Management Deployment Management Ref.: asset, process, change, release, problem & incident manager, release & deployment management	offen

Kürzel	Bezeichnung und Beschreibung	Zuständigkeit	Besetzung
	Incidents, sowie die Organisation deren Bearbeitung.		
GE-BSA-IT/OT-Operation	Er stellt den 1st, 2nd, 3rd Level Support sicher, nimmt Störmeldungen entgegen, organisiert die Behebung und informiert die entsprechenden Stellen (Anlageverantwortliche, Nutzer usw.). Er übernimmt das nötige Monitoring und stellt die entsprechenden Daten zur Verfügung.	Operation Service Design Asset Management (u.a. IP-Adressierung) Service Desk Monitoring & Event Management Ref.: operation & design service, technischer Analytiker & Störungsbeheber, service desk, monitoring & event management	offen
GE-BSA-BLZ	Er unterstützt das BSA-IT Team bei den Aufgaben bezüglich der Überwachung der Anlagen, der Störungsmeldung und Behebung. Er ist zuständig für das An- und Abmelden von Dritten. Er wird bei der Überwachung der Systeme und dem Ticketmanagement durch GE-BSA-IT-Operatoren unterstützt.	Service Desk Monitoring & Event Management Ref.: service desk, monitorer, störungskoordinator, technischer operator	Zentralisten GE (wie bisher)

Table 1 – Rollenbesetzung

Alle Aufgaben werden heute von Personen in der GE wahrgenommen. Offen ist die Festlegung, welche Person in welcher Rolle tätig ist, da die, im Merkblatt des ASTRA, vorgegebenen Rollen eine andere Organisationsstruktur abbilden als die der GE VII. Normalerweise ist die IT der IH-BSA untergeordnet resp. in dieser integriert. In der GE VII stellt IT & Kommunikation eine eigene Abteilung mit ausgewiesenen IT-Fachspezialisten (mind. Informatiker EFZ und Informatik Ingenieure), wobei der GE-L-IT direkt dem GE-L unterstellt ist. Entsprechend sind die Schnittstellen respektive die Zuständigkeiten der IT/OT Dienste zwischen dem GE-L-IT und GE-L-BSA abzustimmen.

1.7.1. BSA Nutzer

Der BSA-Nutzer ist ein Mitarbeiter des ASTRA, der GE oder Dritten (Behörden, Unternehmungen usw.), der informationstechnische Systeme zur Erledigung seiner Aufgaben benutzt. IT/OT-Nutzer und Nutzer sind hierbei als Synonyme zu betrachten, da heutzutage nahezu jeder Mitarbeiter eines Unternehmens bzw. einer Behörde informationstechnische Systeme während der Erledigung seiner Tätigkeiten benutzt.

1.7.2. GE-BSA-BLZ

Der Leiter GE-L-S&S zeichnet sich für die Betriebsleitzentrale respektive deren Prozesse verantwortlich.

1.7.3. GE-BSA-ISO

Der GE BSA ISO ist eine von der GE Leitung benannte Person, die im Auftrag der Leitungsebene dafür sorgt, dass die speziellen Sicherheitsanforderungen im Bereich der IT/OT Infrastruktur (u.a. Firewall) mit ihren industriellen Steuerungen abgedeckt sind und die Sicherheitsorganisation aus dem Bereich ISO in das Gesamt-ISMS (Information Security Management System) eingebunden ist.

Die Besetzung der Rolle ist noch nicht abgeschlossen.

Vorläufig nehmen Personen die Aufgaben dieser Rolle wahr, welche bereits einen engen Bezug zu IT- und OT-Themen in der Gebietseinheit haben.

1.7.4. GE-FPU

Die Fach- und Projektunterstützung der GE stellt das Bindeglied zwischen der GE VII und den laufenden Projekten des ASTRA dar. Das FPU Team informiert das PM ASTRA eines Projektes unter anderem über vorhandene Vorgaben, wie z.B. das vorliegende IT/OT-Sicherheitskonzept.

1.7.5. PM ASTRA

Während der Projektphase zeichnet sich das Projektmanagement des ASTRA, mit dem Projektleiter des ASTRA und dem BHU, für die korrekte Umsetzung und Erstellung des Gewerkes resp. der Anlage verantwortlich.

1.7.6. CAB

Das Change Advisory Board CAB koordiniert die IT/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.

Folgende Vertreter sind im CAB: BSA-IT/OT-Helpdesk, Standard BSA, FU BSA SA-CH und ISBO, sowie für die Gebietseinheit GE-L-IT als Vertreter aus dem Betrieb BSA.

2. ISMS (Informations-Sicherheits-Management-System)

2.1. Informationssicherheit

2.1.1. Schutzziele

Der Eigentümer der Nationalstrassen, ASTRA, hat folgende Schutzziele SZ definiert:

Nummer	Schutzziel
SZ1	Schutz der Reputation des ASTRA
SZ2	Vermeidung von Rechtsstreitigkeiten
SZ3	Vermeidung von direktem monetärem Schaden
SZ4	Vermeidung von Zusatzaufwand (Manpower)
SZ5	Vermeidung von Systemausfällen. Gewährleistung der Geschäftstätigkeit
SZ6	Schutz der Integrität der Daten und Prozesse

Table 2 - Schutzziele

2.1.2. 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 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.

Table 3 - Leitlinien

2.1.3. Grundsätze der IT/OT Architektur

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

Table 4 – Grundsätze zur Verfügbarkeit

Beispiele sind

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

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

Table 5 – Grundsätze zur Vertraulichkeit

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.

Table 6 – Grundsätze zur Integrität

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

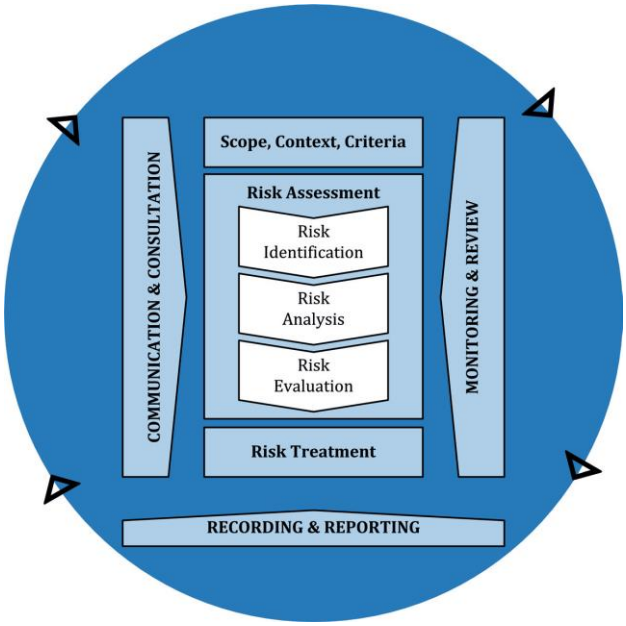

Figure 3 – Prozess zum Risikomanagement gemäss ISO 31000

2.2.1. «Communication and Consultation»

Der GE-BSA-ISO nimmt gemäss Table 1 im Gremium GE AG-BSA-IT 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 gemäss Table 1 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 der GE-BSA-BLZ oder dem GE-BSA-ISO.

Die GE-BSA-BLZ leitet Meldungen, welche die Schutzziele der Eigentümerin verletzen können, an den BSA-GE-ISO weiter. Dieser prüft die Meldung und informiert bei einer offensichtlichen Verletzung der Schutzziele den ASTRA BSA-IT/OT-Helpdesk.

Die GE-BSA-BLZ stellt sicher, dass der GE-BSA-ISO die gemeldeten Abweichungen erhält.

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

Der GE-BSA-ISO bewirtschaftet die Risiken der Gebietseinheit auf Basis gemeldeter Abweichungen und gemäss seinen Aufgaben in Table 1.

Alle anderen Aktivitäten in diesem Bereich des Risikomanagements werden vom Eigentümer wahrgenommen.

2.2.4. «Monitoring and Review»

Betriebseinheiten und Lieferanten 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 gemäss Kapitel 0 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 Standard BSA
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 EP-BSA PM ASTRA EP-BSA
AG4	Temporäre Lösung	mittels kurzfristiger Konfigurationsanpassung, wie während einer Störung, beispielsweise eine vorübergehende Beschränkung des Fernzugriffs	GE-BSA-IT/OT-Operation
AG5	Notbetrieb herstellen	Falls verfügbar und nötig, mittels Entscheid der Notfallorganisation, beispielsweise während einer Krise	offen

Table 7 – Arten von 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.

2.3. 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 kann mit zusätzlichen Massnahmen unterstützt werden, beispielsweise Schulungen, Workshops, Plakaten, Aufklebern, Gadgets, Phishing-Kampagnen oder Penetrationstests mit einer Komponente im Social Engineering.

3. Organisation und Betriebssicherheit

M-Nr.	Beschreibung	Organisation	Technik
M01	Secure Endgeräte	3.4.4	4.1.1
M02	Malwarescanner auf allen Zentralsystemen	3.4.4	4.1.1
M03	Sämtliche Systeme sind mit Passwort gegen unerlaubten Zugriff geschützt	3.3.1	4.3.3
M04	Periodische Überprüfung der Alarmfunktionalität	3.5.3	
M05	Keine funktionalen Einschränkung durch Ausfälle zentraler Systeme und Bereitstellung von Notfallprozessen für Ausfall der Zentralsysteme	3.5.4	
M06	Security Patching Prozesse für sämtliche Systeme etablieren	3.4.2	4.3.4, 4.4.4
M07	Periodische Aktualisierung der Software (sämtliche Systeme)	3.4.2	4.3.4
M08	Definierte Verantwortlichkeiten und Betriebsprozesse für sämtliche Systeme (auch Krisenmanagement)	3.1.1, 3.3.1	4.3.1
M09	Schulung der Betreiber. Knowhow Transfer zum Betrieb	3.2.1	
M10	Logfiles bereitstellen. Logfiles auswerten	3.5.2	
M11	Backup etablieren. Periodischen Restore durchführen	3.3.2	4.2.1, 4.3.2
M12	Automatisierte Funktionsüberwachung	3.4.3	4.2.3, 4.4.1
M13	Reduktion der Komplexität des Gesamtsystem	3.1.2	4.2.4
M14	Strukturierte, dokumentierte Verbindungen zwischen BSA und Aussenwelt. (Fernzugriff)	3.1.4.2	4.4.5
M15	Periodische Sicherheitsprüfung der BSA IT-Infrastruktur	3.5.1	
M16	Inventarisierung (HW/SW)	3.1.4.1	4.1.3, 4.2.20
M17	Zweitwegerschliessung wo notwendig	3.5.4	
M18	Physischer Zutritt	3.1.3	4.5
M19	Kommunikationsprotokolle	3.1.4.2	
M20	Protokollierung von Administrativen Arbeiten	3.5.2	

M-Nr.	Beschreibung	Organisation	Technik
M21	Einschränkung der User-Berechtigung	3.3.1	4.1.2
M22	Berechtigungskonzept	3.1.3	4.2.5, 4.4.2
M23	Change Management	3.4.1	

Table 8 – Inhalte zur Organisation und Technik nach Themen

3.1. Organisation

ORP.1 Organisation
ORP.4 Identitäts- und Berechtigungsmanagement
ORP.5 Compliance Management

3.1.1. Kompetenzen und Verantwortlichkeiten

M08 – GE-L-IT

Definierte Verantwortlichkeiten und Betriebsprozesse für sämtliche Systeme (auch Krisenmanagement)

Die Betriebsverantwortung für sämtliche Systemkategorien ist festgelegt. Je nach Komplexität der Systeme kann die Verantwortung über mehrere Stellen verteilt sein (OS, DB, Anwendung etc.). In diesem Fall sind die AKV's der Beteiligten vertieft zu regeln.

Die Verantwortlichkeit für Gesamtanlagen, Netzwerke und Verbindungen zur Aussenwelt (Firewall Regeln und Protokolle) sind explizit auszuweisen. Die Aufgabenerfüllung muss stets nachvollziehbar sein.

Fragestellungen

- Sind in der IT/OT-Organisation die Kompetenzen und die Verantwortlichkeiten mit dem IT/OT Sicherheitskonzept GE für die BSA eindeutig geregelt und dokumentiert?
- Hat ihre Organisation einen FaS GE BSA IT/OT-ISO?

IST-Zustand

Die Verantwortlichkeiten werden in der GE wahrgenommen. Die konkrete Zuteilung der vorgegebenen Rollen und notwendigen Verantwortlichkeiten auf die Organisation der GE VII ist noch nicht abgeschlossen.

Die Abnahme des Sicherheitskonzeptes ist noch offen. Das fertige Dokument wird durch die Leitung genehmigt und vom CAB freigegeben.

Der GE-BSA-ISO hat in seiner Rolle begonnen und arbeitet sich ein.

Risiko

Funktionsausfall der Zentralsysteme, Leittechnik, Alarmierung Ausfall dezentraler Systeme

Technisch bedingte Fehlfunktion

Störung der Alarmsysteme löst Falsch-/ Fehlalarme aus

Soll-Zustand
Dieses Sicherheitskonzept ist gültig und wirksam. Die Verantwortung ist nachvollziehbar geregelt. Die Rolle GE-BSA-ISO ist etabliert. Sicherheitsmeldungen gehen an den jeweils Verantwortlichen und dann an den GE-BSA-ISO. Der GE-BSA-ISO adressiert erkannten Handlungsbedarf.
Gegenmassnahme
Die folgenden Massnahmen werden jährlich, bei Bedarf auch unterjährig, umgesetzt: 1. Der GE-BSA-ISO prüft das Sicherheitskonzept mindestens jährlich und macht bei Bedarf Anpassungen. 2. Der GE-L-IT würdigt bei Bedarf die Änderungen des GE-BSA-ISO am Sicherheitskonzept und empfiehlt es zur Freigabe. 3. Das CAB gibt das Sicherheitskonzept bei Bedarf frei. 4. Der GE-L-IT bestätigt mindestens jährlich die Ressourcen und Verantwortlichkeiten.

Table 9 – Kompetenzen und Verantwortlichkeiten

3.1.2. Sicherstellung der Einhaltung des Konzeptes

M13 – GE-L-IT
Reduktion der Komplexität des Gesamtsystems Eine tiefe Komplexität wird als Design-Ziel des Gesamtsystems verbindlich festgelegt. Dieses beinhaltet eine strukturierte Systemarchitektur, möglichst wenige Komponenten und Hersteller, möglichst wenige Softwareprodukte und harmonisierte Versionen der Software. Die Tools für Systemwartung sind über verschiedene Lieferanten und Softwareversionen zu harmonisieren und zu standardisieren.
Fragestellungen
• Wird der FaS GE BSA IT/OT-ISO in IT/OT-Projekten zur Stellungnahme aufgefordert und meldet er die Differenzen dem FaS FU? • Berücksichtigen externe Planer und Unternehmer das IT/OT-Sicherheitskonzept GE in den Projekten? • Funktioniert die Zusammenarbeit mit dem FaSKoB und dem EP BSA bezüglich der laufenden Überprüfung des IT/OT-Sicherheitskonzeptes auf den Stand der Technik. • An wen werden Sicherheitsprobleme gemeldet?

IST-Zustand

Die Interessen der GE VII werden von der GE-FPU bei den Projekten vertreten. Diese verweist auf die aktuellen Standards der GE, wobei die Einhaltung dieser nicht eindeutig geregelt ist. Zudem gibt es seitens er GE einen «Normalienserver», auf welchem verschiedene Dokumente abgelegt sind, an welchen sich die Projekte orientieren sollten. Auch dies wird von den einzelnen Projekten unterschiedlich gehandhabt und umgesetzt.

Die Vorgaben der GE werden teilweise vom ASTRA an Lieferanten kommuniziert. Da die Zeitspanne zwischen der Projektausschreibung (ASTRA) und der Umsetzung (Projekt) sehr gross sein kann, sind diese Vorgaben teilweise schon veraltet.

Gespräche mit FaSKoB und EP BSA finden statt.

Betriebliche Sicherheitsprobleme werden via GE-L-IT und andere via Projektleiter kommuniziert.

Risiko

Technisch bedingte Fehlfunktion

Menschliche Fehlmanipulation

Soll-Zustand

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. Für Projekte ist festgelegt, zu welchem Zeitpunkt der GE-BSA-ISO miteinbezogen werden muss. Dadurch verfügt er über ausreichende Informationen, um die Komplexität zu reduzieren und die Sicherheit zu erhöhen. D.h. FaSKoB und EP BSA berücksichtigen die Vorgaben der GE und stellen deren Einhaltung im Rahmen von Projekten sicher. Der GE-BSA-ISO berät sie dabei.

Der GE-BSA-ISO führt eine Liste von Mängeln zwecks Behebung. FaSKoB und EP-BSA werden regelmässig über den Stand in Kenntnis gesetzt. Das ASTRA hat Interesse an der wirksamen Behebung von Mängeln, um Komplexität und IT-Sicherheitsrisiken zu senken. Deshalb hilft FaSKoB, angemessene Massnahmen zu empfehlen oder passt übergeordnete Richtlinien an, und EP-BSA hilft bei der Priorisierung und Beschaffung der erforderlichen Mittel. FaSKoB und EP-BSA informieren den GE-BSA-ISO so, dass er den GE-L-IT jederzeit über den aktuellen Stand informieren kann.

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[1]. 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.

[1] Bei Bedarf kann die GE-FPU weitere FaS der GE VII hinzuziehen.

Gegenmassnahme
5. Der GE-BSA-ISO prüft periodisch und systematisch die Einhaltung des Sicherheitskonzeptes, beispielsweise jährlich mit einer externen Sicherheitsprüfung. 6. Der GE-BSA-ISO kann Projekte hinsichtlich Einhaltung dieses Konzeptes prüfen, beispielsweise im Rahmen einer Sicherheitsprüfung. 7. Der GE-BSA-ISO führt eine Mängelliste und meldet periodisch (z.B. quartalsweise) den Fortschritt an den GE-L-IT, FaSKoB und EP-BSA. 8. Mit der Kenntnisnahme der Mängelliste anerkennt der GE-L-IT jeden Mangel im Sinne einer befristeten Ausnahme. Für Einträge, für welche er keine Bewilligung erteilen kann oder will, folgt ein Antrag auf Ausnahmebewilligung bei der nächsthöheren zuständigen Stelle. Beispielsweise ISBO, BSA-Standard oder Leiter-IT im ASTRA. 9. Auf Basis dieses Konzeptes werden Prüfpläne für die Systeme erstellt. Im Rahmen des Betriebes werden diese durch die GE-BSA-IT/OT-Admins erstellt und angepasst. Im Rahmen eines Projektes liegt diese Tätigkeit in der Verantwortung des PM ASTRA und seiner Lieferanten. 10. Der GE-BSA-ISO meldet Verstösse des EP-BSA oder FaSKoB 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. 11. BSA-Nutzer melden erkannte Verstösse gegen dieses Konzept wahlweise an den Vorgesetzten oder direkt an den GE-BSA-ISO.

Table 10 – Sicherstellung der Einhaltung des Konzeptes

3.1.3. Berechtigungskonzept und physischer Zutritt

M18, M22 – GE-BSA-ISO
Berechtigungskonzept Ein Berechtigungskonzept pro BSA ist zu erstellen. Für jedes in der Domäne BSA betriebene System muss ein Berechtigungskonzept vorliegen, das die Berechtigungsvergabe anhand der Prinzipien need to know und need to use regelt. **physischer Zutritt** Der physische Zutritt zu technischen Räumen und der IT/OT-Infrastruktur darf für unbefugte nicht zugänglich sein. → Schliesskonzept
Fragestellungen
aus Kapitel 3.4 • Wird der Zugriff von externen Dienstleistern / Mitarbeitern reglementiert und wie wird dieser eingeschränkt? • Wie ist sichergestellt, dass externe Lieferanten / Dienstleister / Mitarbeiter nur auf die notwendigen Systeme Zugriff haben? aus Kapitel 4.5 • Ist der physische Zutritt zu den Räumen eingeschränkt?

IST-Zustand

Die Berechtigungsvergabe erfolgt grundsätzlich nach dem «Benutzerkonzept für Bereichs-rechner»[2]. Die restlichen Berechtigungen werden nach good practice vergeben, sind jedoch nicht formalisiert.

Zugriff wird durch das AD sowie die ISE eingeschränkt und ist dokumentiert (vgl. Cisco AnyConnect). Mittels der ISE wird die Zugriffberechtigungen geregelt (IP basierte Accesslisten).

Zonenbasierter Zugriff: RDS-Zugriff öffnet den Zugriff in der jeweiligen Zone (Abschnitt und Technik).

Der physische Zutritt folgt den Ausführungen im Schliesskonzept, welches auch technisch implementiert ist.

Risiko

Menschliche Fehlmanipulation

Unbefugte erhalten Einsicht in Daten der Nationalstrassen

Nicht geschützte Komponenten der BSA werden manipuliert

Soll-Zustand

Zusätzlich zum bestehenden Schliesskonzept[3] wird das folgende Berechtigungskonzept umgesetzt.

Grundsätzlich erfolgen alle Zugriffe mittels persönlichem Benutzerkennung.

Privilegierte Benutzer werden für die dafür vorgesehene Tätigkeit verwendet, d.h. nicht für tägliche Arbeiten mit Office, Mail oder Internet. Die Anmeldung mit einem privilegierten Benutzer von Extern ist nur mit Mehrfaktorauthentisierung möglich.

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.

Grundsätzlich sind alle persönlichen Benutzerkennungen in den Berechtigungen eingeschränkt, beispielsweise hat ein Domain Admin keine Adminrechte auf Servern oder auf Netzwerkgeräten (Tier-Architektur).

Sollten lokal definierte Adminbenutzer erforderlich sein, können diese nur über entsprechende Berechtigungen in der Domäne eingerichtet und verwaltet werden (LAPS).

Alle Rechte einer Person sind dokumentiert. Die Berechtigungsvergabe erfolgt nachvollziehbar. Wer Rechte beantragt, darf diese nicht selbst bewilligen, was technisch sicherzustellen ist (4-Augen Prinzip). Nur interne Mitarbeitende dürfen Anträge bewilligen. Die Rechte bewilligt, wer im

[2] https://normalien.ge7.ch/download/benutzerkonzept-bereichsrechner/

[3] Dokument: Schliesskonzept der GEVII

Inventar für das jeweilige Systeme, auf welchem die Rechte wirken, als Systemeigner[4] erfasst ist oder sein Stellvertreter.
Gegenmassnahme
12. Der GE-BSA-IT/OT-Admin prüft die Dokumentation der vergebenen Rechte mindestens jährlich auf Vollständigkeit und Wirksamkeit. 13. Vorgesetzte prüfen mindestens jährlich für jeden ihrer Mitarbeitenden die Dokumentation der Rechte auf mögliche Konflikte oder unnötige Häufung von Rechten, eine sogenannte Rechte-Rezertifizierung. Bei Bedarf legen sie geeignete Gegenmassnahmen fest. 14. Der GE-BSA-ISO stellt mindestens jährlich eine Prüfung der Systeme sicher, welche für die Rechtevergabe oder deren Dokumentation benutzt werden, z.B. im Rahmen einer technischen Sicherheitsprüfung. Dies gilt für Zutrittssysteme wie auch die beiden zentralen Zugriffverwaltungssysteme, Domain Controller und Cisco ISE.

Table 11 – Berechtigungskonzept

3.1.4. Inventar

3.1.4.1. Hardware und Software

M16 – GE-BSA-IT/OT-Admin
Inventarisierung (HW/SW) Um eine vollständige Übersicht der BSA-Informatik zu gewährleisten, muss eine vollständige Inventarisierung der verwendeten Komponenten sichergestellt werden. Es ist dabei zu klären und festzulegen welche Daten wo notwendig sind und wer was macht (Zuständigkeit Gebietseinheit und ASTRA). Insbesondere müssen Doppelspurigkeiten vermieden werden. Es darf immer nur einen Datenmaster geben.
Fragestellungen
• Keine
IST-Zustand
In der GE VII gibt es, im Rahmen der Applikation Greengate, ein Inventar, welches auf den Daten der ASTRA Applikation «FA BSA» beruht, mit welchem die IH-BSA Abteilung arbeitet. Die IT hat verschiedene Lösungen für ein Hardware-Inventar im Einsatz, wobei sich keine Lösung als zentrales Inventar etablieren konnte. Deshalb gibt es Inkonsistenzen zwischen den verschiedenen Tools. Ein Software-Inventar existiert im Kaspersky Security Center. Die Software aller Geräte, welche dem Virenschutz ausgestattet sind, wird dort automatisch erfasst. Zudem ist eine rudimentäre Installation von DocuSnap für regelmässige Scan des Netzwerkes vorhanden, welche aber erst einen Teil der gesamten Infrastruktur erfassen kann.

[4] Präzisierung: Grundsätzlich gehören sämtliche Anlagen dem ASTRA In diesem und dem nachfolgenden Kontext ist als Systemeigner der Systemverantwortliche zu verstehen, welcher im Sinne und nach Vorgaben des Eigentümers, die Systeme betreibt.

Risiko
Technisch bedingte Fehlfunktion Menschliche Fehlmanipulation
Soll-Zustand
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. Der GE-BSA-IT/OT-Admin erfasst im Inventar alle seine von der GE oder deren Lieferanten 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. 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 gemäss Kapitel 0. Wenn also ein höherer Schutzbedarf - als von diesem Konzept vorgegeben - erkannt wird, ist dieser im Inventar ausgewiesen.
Gegenmassnahme
15. GE-BSA-IT/OT-Admins prüfen ihre Inventareinträge mindestens jährlich auf Vollständigkeit und Aktualität und passen diese bei Bedarf an. Sie melden erkannte Mängel an den GE-BSA-ISO, beispielsweise bei erkanntem, höheren Schutzbedarf. 16. Der GE-BSA-ISO prüft mindestens jährlich, dass alle Systeme im Inventar erfasst sind, beispielsweise aufgrund eines Abgleichs mit einem Netzwerkscan.

Table 12 – Hardware und Software

3.1.4.2. Datenflüsse

M14, M19 – GE-BSA-ISO
Strukturierte, dokumentierte Verbindungen zwischen BSA und Aussenwelt. (Fernzugriff) Der (Fern)zugriff ist über den standardisierten Zugriffspunkt zu gewähren (Umgehung von Zugriffsbeschränkung via alternative Wege, z.B. Modem, sind nicht zulässig). Schnittstellen zur Aussenwelt sind auf ein Minimum zu reduzieren, zu strukturieren und aktuell zu dokumentieren. Der Zugriffe in die Prozesszone erfolgt ausschliesslich durch ausgesuchte Protokolle → GE Konzept zu den unterschiedlichen Anlagen (Alter) **Kommunikationsprotokolle** Innerhalb der Prozesszone sind nur die vom ASTRA vorgegebenen Protokolle zulässig. Die Identität des Kommunikationspartners muss überprüft werden, wenn diese Funktionalität vom Protokoll angeboten wird.

Fragestellungen

- Gibt es klare Regeln im Umgang mit IT/OT-Systemen und IT/OT-Sicherheit für alle Mitarbeiter / externe Lieferanten / Dienstleister?

IST-Zustand

VPN Zugriffe erfolgen für interne Mitarbeiter stets über eine Zweifaktorauthentifizierung. Externe Lieferanten und Planer erhalten lediglich einen zeitlich beschränkten Zugriff, dieser soll im Verlauf des nächsten Jahres ebenfalls noch mittels Zweifaktorauthentifizierung verifiziert werden.

Wer als externer Partner einen VPN-Zugang beantragt muss dies über ein «VPN-Antragsformular»[5] machen. Darin enthalten ist ebenfalls eine Sicherheitserklärung, welche sich der Benutzer verpflichtet einzuhalten, während dieser den VPN-Zugang benutzt. Zusätzlich muss jeder Unternehmer einmalig eine Datenschutzvereinbarung unterzeichnen. Diese ist integraler Bestandteil des VPN-Antrages.

Für Änderungen der Firewall-Regeln gibt es ebenfalls ein Formular[6], welches der Antragsteller ausfüllen und begründen muss.

Risiko

"Malware oder Ransomware im IP-Netz Malware wird über die BSA Geräte in das Client Netz des ASTRA verbreitet"

Unbefugte erhalten Einsicht in Daten der Nationalstrassen

Funktionsausfall der Zentralsysteme, Leittechnik, Alarming Ausfall dezentraler Systeme

Technisch bedingte Fehlfunktion

Nicht geschützte Komponenten der BSA werden manipuliert

Soll-Zustand

Die Richtlinie 13030 dient als Grundlage für die folgenden Definitionen.

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.

Alle Datenflüsse zwischen dem Netzwerk der GE und einem Netzwerk Dritter oder Lieferanten sind auf Protokolle und IP-Adressen beschränkt, d.h. in den Firewallregeln ist die Angabe «any» nicht zulässig.

Datenflüsse zwischen den Netzwerken Dritter oder Lieferanten über das BKN-Netzwerk der GE werden als missbräuchlich bewertet und sind nicht zulässig.

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,

---

[5] https://normalien.ge7.ch/download/vpn-antragsformular/

[6] https://normalien.ge7.ch/download/antrag-firewall-change/

- 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.

Datenflüsse zwischen Netzsegmenten im Netzwerk der GE sind auf bewilligte Protokolle und mindestens für eines der Segmente auf IP-Adressen beschränkt.

Alle bestehenden Freischaltungen für Datenflüsse zwischen Netzsegmenten sind dokumentiert und aktuell. Änderungen und neue Freischaltungen sind nachvollziehbar beantragt, bewilligt und deren korrekte Umsetzung überprüft.

Widerspricht eine Freischaltung gegen eine der Regeln und ist sie betrieblich notwendig, kann der GE-L-IT eine Ausnahme bewilligen. Eine Ausnahmebewilligung ist immer befristet und ist ein Mangel, welcher behoben werden muss. Ist eine Freischaltung aufgrund einer betrieblichen Störung dringend erforderlich, darf der Antrag ausnahmsweise im Nachhinein gestellt werden.

Gegenmassnahme

17. Der GE-BSA-ISO nimmt Anträge für Freischaltungen entgegen, prüft diese und gibt diese allenfalls unter Auflagen zur Umsetzung frei. Anträge des GE-BSA-ISO dürfen nur von einem Stellvertreter freigegeben werden (4-Augen-Prinzip). Es dürfen nur Anträge für Freischaltungen, denen ein dringendes betriebliches Ereignis (IT-Störungsticket) zugrunde liegt, im Nachhinein gestellt werden.
18. Der GE-BSA-IT/OT-Admin für die Firewall konfiguriert die bewilligten Anträge im System, oder stellt die Einholung eines Antrages sicher, wenn dies erforderlich ist, beispielweise wegen der Behebung einer betrieblichen Störung.
19. Der GE-BSA-ISO prüft regelmässig, dass nur bewilligte Freischaltungen konfiguriert sind, beispielsweise im Rahmen einer Sicherheitsprüfung. Er kann bei Bedarf zusätzlich die administrativen Zugriffe auf die Firewall auswerten, um die Einhaltung dieses Konzeptes zu prüfen.

Table 13 - Datenflüsse

3.2. Personal

ORP.3 Sensibilisierung und Schulung

3.2.1. Sensibilisierung und Schulung

M09 – GE-BSA-ISO

Schulung der Betreiber. Know-How Transfer zum Betrieb

Die in Massnahme M07 beschriebenen Stellen müssen über das für ihre Aufgaben notwendige KnowHow verfügen. Dies ist mittels Schulungen sicherzustellen und aktuell zu halten.

Fragestellungen

- Sind im GE Schulungsprogramm fachspezifische IT/OT-Sicherheitsschulungen enthalten?
- Welche IT/OT-spezifische Ausbildung hat das eingesetzte Personal?
- Wie werden die Mitarbeiter zum Thema IT/OT-Sicherheit geschult?

IST-Zustand

Es sind keine fachspezifischen IT/OT-Sicherheitsschulungen im GE Schulungsprogramm enthalten.

Das intern eingesetzte Personal verfügt über Qualifikationen im Bereich der Informatik (EFZ/HF/FH). Es kann nicht abgeschätzt werden, über welche Ausbildung das externe Personal verfügt.

Mitarbeiter werden derzeit im Rahmen einer kurzen kantonalen Pflichtausbildung zum Thema IT/OT-Sicherheit geschult. Es gibt von der GE VII eine Datenschutzvereinbarung, welche den grundsätzlichen Umgang mit Daten regelt. Weiterführende grundsätzliche Regeln im Umgang mit IT/OT-Systemen für Mitarbeiter und Lieferanten sind nicht definiert.

Risiko

Funktionsausfall der Zentralsysteme, Leittechnik, Alarmierung Ausfall dezentraler Systeme

Technisch bedingte Fehlfunktion

Störung der Alarmsysteme löst Falsch-/ Fehlalarme aus

Menschliche Fehlmanipulation

Soll-Zustand

Alle BSA-Nutzer, d.h. Mitarbeitende, Lieferanten 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.

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.

Bei Bedarf erfolgen gezielte Ausbildungen («Training-off-the-Job»).

Gegenmassnahme
20. Der GE-BSA-ISO empfiehlt dem GE-L-IT Massnahmen zur Sensibilisierung und gezielten Ausbildung. Eine Kopie der Empfehlungen geht jeweils an den ISBO. 21. Der GE-L-IT ermöglicht mindestens einmal jährlich eine Sensibilisierungsmassnahme und gezielte Ausbildungen nach Bedarf. Der GE-BSA-ISO sendet seine Einschätzung zur Wirksamkeit der umgesetzten Massnahmen zusammen mit der Kopie der Empfehlungen an den ISBO. 22. Der GE-BSA-ISO macht sich ein Bild über die Sorgfalt und das Verhalten von Lieferanten im Zusammenhang mit der Sicherheit und gibt Empfehlungen an den GE-L-IT ab.

Table 14 – Schulung

3.3. Datenverwaltung

CON.1 Kryptokonzept
CON.2 Datenschutz
CON.3 Datensicherungskonzept
CON.6 Löschen und Vernichten
CON.7 Informationssicherheit auf Auslandsreisen
CON.8 Software-Entwicklung
CON.9 Informationsaustausch
CON.5 Entwicklung und Einsatz von Individualsoftware
CON.4 Auswahl und Einsatz von Standardsoftware

3.3.1. Zugriffschutz für Systeme

M03, M08, M21 – GE-BSA-IT/OT-Admin
Sämtliche Systeme sind mit Passwort gegen unerlaubten Zugriff geschützt Sämtliche Systeme die über TCP/IP erreichbar sind, verfügen über einen PIN/Passwortschutz. Passwörter sind individuell, persönlich und unterliegen einer bestimmten Komplexität. Die Qualität des Zugangsschutzes sowie die Periodizität der Erneuerung ist geregelt. Die Passwörter der individuellen, eindeutig einem Benutzer zuordenbaren Accounts werden vom jeweiligen Benutzer definiert und verwaltet. Es steht dafür keine zentrale Verwaltungslösung bereit. Die Passwörter müssen die Vorschriften aus „Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB“ erfüllen. **Definierte Verantwortlichkeiten und Betriebsprozesse für sämtliche Systeme** Die Betriebsverantwortung für sämtliche Systemkategorien ist festgelegt. Je nach Komplexität der Systeme kann die Verantwortung über mehrere Stellen verteilt sein (OS, DB, Anwendung etc.). In diesem Fall sind die AKV’s der Beteiligten vertieft zu regeln. Die Verantwortlichkeit für Gesamtanlagen, Netzwerke und Verbindungen zur Aussenwelt (Firewall Regeln und Protokolle) sind explizit auszuweisen. Die Aufgabenerfüllung muss stets nachvollziehbar sein. **Einschränkung der User-Berechtigung** Die Berechtigungen der User / Benutzer sind auf das Minimum / Notwendige zu reduzieren. Die Kontrolle der Zugrifferlaubnis und Zugriffverwendung muss jederzeit nachvollziehbar sein. Systeme in der Netzwerkzone «Prozess» müssen so konstruiert sein, dass ein Benutzer nur vorgesehene Aktivitäten durchführen kann. Insbesondere ist dafür zu sorgen, dass ein Benutzer nicht auf die Betriebssystem-Ebene gelangt und dort beliebige Aktionen ausführt. Es ist auch zu

verhindern, dass ein Benutzer mit einem Web-Browser andere als vordefinierte URLs anwählen kann.

Fragestellungen

- Wie wird der Zugriff auf die Daten und deren Integrität gewährleistet?
- Ist der Zugriff auf besonders schützenswerten Daten klar geregelt (z.B. Videodaten)?
- Wie werden nicht mehr benötigte oder defekte Datenträger sicher gelöscht / vernichtet?

IST-Zustand

Die Dokumentationen werden grösstenteils auf einer Ablage, welche vom Amt für Informatik (AFI) zur Verfügung gestellt wird, abgelegt. Der Zugriffsschutz ist über die kantonale Domäne geregelt.

Die Restlichen Daten liegen auf Servern im BKN-Netzwerk. Hier wird der Zugriff über die BKN-Domäne eingeschränkt.

Offen sind die Touch-Panels (Vor-Ort-Bedienungen) und der Status auf den Anlagen ist unklar.

Die GE VII verwaltet keine besonders schützenswerten Daten, da die Videobilder nicht hochauflösend genug sind, um Details wie Gesichter erkennen zu können. Bei der Positionierung der Kameras wird darauf geachtet, dass keine Personen, resp. Autonummern erkennbar sind.

Alle Datenträger, welche zur GE zurückkommen, werden vernichtet. Es besteht aber kein Überblick, was mit den restlichen Datenträgern passiert.

Risiko

Unbefugte erhalten Einsicht in Daten der Nationalstrassen

Nicht geschützte Komponenten der BSA werden manipuliert

Menschliche Fehlmanipulation

Unbefugte erhalten Einsicht in Daten der Nationalstrassen

Soll-Zustand

Es finden nur authentisierte Zugriffe auf Systeme statt, beispielsweise mit Benutzerkennung und Passwort, oder Maschinenzertifikaten oder API-Key und Token.

Soll ein Benutzer eine Aktivität mit privilegierten Rechten ausführen, erfolgt diese nach expliziter Freigabe (UAC). Das vermeidet versehentliche Fehler oder das automatische Ausführen von Programmen, beispielsweise Malware.

Die Mindestanforderungen des ASTRA an eine ausreichende Authentisierung sind technisch erzwungen, beispielsweise die Passwortkomplexität oder die Deaktivierung von Standardbenutzern. Ausnahmen sind bekannt und werden so verwaltet, dass trotzdem ein angemessener Schutz erreicht wird.

Datenflüsse, welche die BKN-Netzwerke der GE in das öffentliche Netz verlassen, sind verschlüsselt.

Ob auf den durch die GE betriebenen Systemen besonders schützenswerte Daten gespeichert sind, wird systematisch geprüft. Bei erkanntem, erhöhten Schutzbedarf werden angemessene Vorgaben erstellt und umgesetzt.

Die Verpflichtung zur Einhaltung von Mindestanforderungen bei der Vernichtung von Datenträgern ist sichergestellt, beispielsweise durch eine schriftliche Bestätigung.
Gegenmassnahme
23. Der GE-BSA-IT/OT-Admin stellt für seine Systeme sicher, dass die Authentisierung und Verschlüsselung dem definierten Sollzustand entspricht oder eine bewilligte Ausnahme vorliegt. Sie prüfen mindestens jährlich, ob besonders schützenswerte Daten auf ihren Systemen gespeichert sind. Sie stellen sicher, dass Datenträger ihrer Systeme gemäss Vorgaben vernichtet werden. 24. Der GE-BSA-ISO prüft periodisch mit Stichproben, ob die Authentisierung, Verschlüsselung und Datenträgervernichtung gemäss Vorgaben erfolgt, beispielsweise jährlich im Rahmen einer Sicherheitsprüfung.

Table 15 – Passwortschutz

3.3.2. Backup und Restore

M11 – GE-L-IT
Backup etablieren. Periodischen Restore durchführen Einstellungen und Daten wichtiger Systeme werden periodisch gesichert. Die Vollständigkeit der Sicherung sowie der Prozess des Rückspielens wird regelmässig getestet.
Fragestellungen
• Gibt es ein Konzept zur Sicherung und Wiederherstellung der Daten? • Welche Daten werden regelmässig gesichert und wie lange sind diese Datensicherungen verfügbar?
IST-Zustand
Es werden alle Windows-Maschinen regelmässig gesichert. Von den Linux-Clients sind nur einzelne gesichert, da die Anbindung an die Sicherungssoftware nicht im Leistungsumfang der Lieferanten enthalten ist. Dies müsste mittels zusätzlichem Auftrag erfolgen. Es werden jährlich stichprobenartig einzelne Wiederherstellungsprozesse getestet. Grundsätzlich werden alle Backup-Clients gleichbehandelt. Es gibt keinen Unterschied in den Datensicherungen zwischen den verschiedenen Rechnern. Es gibt verschiedene Backupintervalle: - Tägliches Backup; 30 Tage verfügbar - Monatliches Backup; 12 Monate Verfügbar - Jährliches Backup; mehrere Jahre verfügbar In regelmässigen Abständen werden die Daten zusätzlich auf ein externes, räumlich getrenntes, Bandlaufwerk geschrieben (Tape-Library). Aktuell wird eine regelmässige Auslagerung dieser Datentapes geprüft. Die Konfigurationen der Cisco-Geräte werden in einem Cisco-proprietären Tool gesichert. Eine Ransomware geschützte Sicherungslösung ist in Arbeit.
Risiko

Die Daten zur BSA-Steuerung gehen verloren
Soll-Zustand
Es existiert ein konsistentes Backup-Konzept, in welchem definiert ist, welche Geräte, in welchem Ausmass, wie gesichert werden müssen. 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. Es ist bekannt, wie lange es vom Entscheid für die Wiederherstellung bis zu deren Umsetzung dauert (RTO Recovery-Time-Objective). Sicherungen der Konfiguration werden so lange behalten, wie eine konsistente Wiederherstellung möglich ist. 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. Sicherungen sind vor versehentlicher Löschung oder Ransomware geschützt, beispielsweise mit Datenträgern, welche offline aufbewahrt werden, oder anderen geeigneten Bedingungen für den Zugriff auf Backups.
Gegenmassnahme
25. Der BSA-IT/OT-Admin für die Backup-Software prüft das Backupkonzept mindestens jährlich und macht bei Bedarf Anpassungen. 26. Der GE-BSA-ISO würdigt bei Bedarf die Änderungen des GE-BSA-IT/OT-Admin für die Backup-Software, welche am Backupkonzept vorgenommen wurden, und empfiehlt es zur Freigabe. 27. Der GE-L-IT gibt das Backupkonzept bei Bedarf frei. 28. Der GE-L-IT bestätigt mindestens jährlich die Ressourcen und Verantwortlichkeiten für die Umsetzung allfälliger Änderungen am Backupkonzept und die Einhaltung des Backupkonzepts.

Table 16 – Backup und Restore

3.4. Betriebsprozesse

OPS.1 Eigener Betrieb
OPS.2 Betrieb von Dritten
OPS.3 Betrieb für Dritte

3.4.1. Change-Management

M23 – GE-BSA-IT/OT-Admin
Change-Management Für Änderungen ist ein Change-Management Prozess zu erstellen. Die Changes sind zu dokumentieren. Umfangreiche Changes sind über das CAB zu genehmigen.
Fragestellungen
• Wie werden Änderungen an den IT/OT-Systemen dokumentiert?

- Gibt es Prozesse, welche das Änderungsmanagement/Change Management unterstützen?

IST-Zustand

Es existieren wenige Formulare, über welche Lieferanten einige Changes beantragen können. Diese werden grundsätzlich auch für interne Prozesse verwendet. Ein standardisierter Change-Management-Prozess im Bereich IT konnte jedoch noch nicht etabliert werden. Insbesondere Changes auf Systemen die ein Lieferant liefert oder eine Erweiterung, welche ein Projekt auf ihrem Projektperimeter plant, wurden bis jetzt nicht systematisch erfasst und geprüft. Es ist auch unklar mit welchem Mengengerüst hier gerechnet werden müsste.

Der GE fällt es schwer einen Change-Management-Prozess zu etablieren, da nicht alle Rollen des Prozesses bei der GE sind.

Risiko

Technisch bedingte Fehlfunktion

Störung der Alarmsysteme löst Falsch-/ Fehlalarme aus

Die Daten zur BSA-Steuerung gehen verloren

System kann nicht mehr gestartet werden

Soll-Zustand

Ein Change ist eine Änderung eines Gerätes, welches von der GE überwacht und/oder betrieben wird.

Changes sind systematisch erfasst, beispielsweise mittels Logging. Es ist definiert, wie lange Änderungen nachvollziehbar sind.

Die Einführung eines Change-Managements wird, nach Ansicht der GE, weitreichende (businesskritische) Folgen für die Projekte und somit auch die ASTRA Filiale haben. Deshalb schlägt die GE vor ein Changemanagement in mehreren Schritten einzuführen.:

I. Vor jedem Change muss die Arbeit bei der GE angemeldet werden. Falls eine solche Änderung keine betriebliche Störung oder kein aussergewöhnliches Risiko zur Folge hat, beispielsweise wegen ausreichender Redundanz, rascher Umsetzung mittels Automation oder geringer Bedeutung des Systems, kann auf eine Freigabe der GE verzichtet werden.
   Alle anderen Changes erfordern die Freigabe der GE.
   Einzige Ausnahme bilden Emergency Changes, dies sind Anpassungen zur Behebung einer Störung oder wenn Gefahr im Verzug ist, beispielsweise eine Umgehungslösung oder eine Sicherheitsaktualisierung. Solche Änderungen können im Nachhinein beantragt und bewilligt werden.
II. Die GE etabliert einen Change-Management-Prozess nach ITIL für Sicherheitskritische Changes an produktiven Systemen, beispielsweise Änderungen an Firewall-Regeln.
III. Die GE etabliert einen Changemanagement-Prozess nach ITIL für sämtliche Changes in Zusammenarbeit mit dem ASTRA. Ausnahmen, welche keine Freigabe, erfordern sind klar dokumentiert.

Gegenmassnahme

29. Der GE-BSA-ISO führt eine Liste von Systemen, welche keine Freigabe oder Antragstellung für Changes benötigen. Er definiert für welche Systeme eine Freigabe zwingend ist und ob die Freigabe im 4-Augen-Prinzip erfolgen muss, beispielsweise bei IT-Systemanpassungen auf Firewalls oder am Berechtigungssystem.
30. GE-BSA-IT/OT-Admin stellt sicher, dass seine Systeme Änderungen nachvollziehbar aufzeichnen und die Aufzeichnungen entsprechend lange aufbewahrt bleiben. Er stellt sicher, dass Änderungsanträge für seine Systeme vollständig und nachvollziehbar sind, es sei denn, es kann darauf verzichtet werden (System ist auf der Liste mit Ausnahmen).

Table 17 – Protokollierung administrative Arbeiten

3.4.2. Periodische Aktualisierung

M06, M07 – GE-BSA-IT/OT-Operation

Security Patching Prozesse für sämtliche Systeme etablieren

Es ist definiert, wer über welche Kanäle über Sicherheitslücken der Systeme informiert wird, wie solche Schwachstellen beurteilt und über deren Relevanz für die Systeme des ASTRA entschieden wird.

Es ist geklärt wer über die Umsetzung entscheidet und wer in welcher Zeitfrist die Umsetzung durchführt.

Periodische Aktualisierung der Software (sämtliche Systeme)

Für sämtliche Systeme die über TCP/IP erreichbar sind, ist im Grundsatz eine periodische Aktualisierung der Software vorzusehen.

Die Periodizität der Aktualisierung ist für sämtliche Systemkategorien abschliessend festgelegt. Ebenfalls geregelt ist wer in welcher Zeitfrist die Umsetzung durchführt. Um den Aktualisierungsprozess zu vereinfachen sind die verwendeten Softwareprodukte und die verwendeten Versionen auf das notwendige reduziert (siehe auch Massnahme 4.13).

Für Unterhaltsarbeiten sind Wartungsfenster festgelegt.

Fragestellungen

- Welche Systeme werden regelmässig gepatcht?
- Gibt es Systeme die nicht regelmässig gepatcht werden (können)?

IST-Zustand

Mit dem Tool Ivanti Patchmanagement ist man in der Lage Windowsserver bezüglich Betriebssystems effizient zu patchen. Dies wird durch die GE VII für die Standardserver im RZ und der DMZ so angewandt.

Rechner der BSA Systeme (sprich KR, BR, AR) werden, wie bisher üblich, nicht gepatcht. Die Rechner wurden durch die Auftraggeber über Projekte beschafft. Die Rechner wurden zum grössten Teil mit ein Patchlevel > 1 Jahr alt in den Betrieb übergeben. Es war nicht Bestandteil des Pflichtenhefts einfach patchbare Systeme zu liefern. Die Lieferanten warnen, die Rechner in Eigenregie zu patchen. Erste Erfahrungen mit dem Patchen eines einzelnen Windowsrechners sind vorhanden. Die Systeme bilden Bestandteile der BSA Systeme, welche noch nach dem Ansatz «Never touch/change a running System» entwickelt wurden. Um Linux Rechner effizient zu patchen, fehlen der GE VII aktuell die Tools.

Da aus Garantiegründen die Rechner von den Lieferanten nicht durch die GE VII gepatcht werden dürfen[7], ist dies ebenfalls mit externen Kosten verbunden und stellt ein hohes Sicherheitsrisiko dar, welche von den Projekten nicht berücksichtigt wird.

Risiko

"Malware oder Ransomware im IP-Netz Malware wird über die BSA-Geräte in das Client Netz des ASTRA verbreitet"

Unbefugte erhalten Einsicht in Daten der Nationalstrassen

Funktionsausfall der Zentralsysteme, Leittechnik, Alarmierung Ausfall dezentraler Systeme

Technisch bedingte Fehlfunktion

Soll-Zustand

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.

Jeder Systemeigner erhält für seine Systeme zeitnah vom Lieferanten oder Hersteller Informationen, ob und wie Sicherheitslücken geschlossen werden können.

Wo dies nötig und eine aktuelle Testumgebung verfügbar ist, wird die Aktualisierung zuerst in einer Testumgebung vorgenommen, um die Auswirkungen festzustellen.

Für jedes System ist bekannt, wieviel Vorlaufzeit für eine Einspielung von Aktualisierungen erforderlich ist.

Allenfalls kann eine Aktualisierung aufgrund von Altlasten auch erst bei einer vollständigen Systemerneuerung erfolgen. In solchen Fällen sind kompensierende Massnahmen zum Schutz zu prüfen.

In dringenden Fällen entscheidet der GE-BSA-IT/OT-Admin nach Beratung mit dem GE-BSA-ISO, ob eine Umgehungslösung oder eine kurzfristige Aktualisierung als Emergency Change umgesetzt wird.

[7] Gemäss Aussage einiger Lieferanten und Unternehmer. Teilweise wird, auch von den PM ASTRA, auf die Ausschreibung resp. den Projektauftrag hingewiesen, bei der ein Patchen der Systeme (oder den Rückbau von alten, nicht mehr benötigten Systemen) nicht explizit gewünscht wurde und deshalb ein Einbringen eines Sicherheitsupdates einen Garantieverlust zur Folge haben könnte.

Gegenmassnahme
31. Der GE-BSA-IT/OT-Admin dokumentieren für jedes seiner Systeme die verfügbaren Wartungsfenster oder begründen deren fehlen. Er berät sich bei Bedarf mit dem GE-BSA-ISO zu Sofortmassnahmen und leitet deren Umsetzung in die Wege. 32. GE-BSA-IT/OT-Operation aktualisiert während eines Wartungsfensters die entsprechenden Systeme. Es können auch Lieferanten oder GE-BSA-IT/OT-Admin beteiligt sein. 33. Der GE-BSA-ISO prüft periodisch, beispielsweise jährlich, den Softwarestand. Bei Bedarf nimmt er Handlungsbedarf in die Mängelliste zur Behebung auf, beispielweise Umgehungslösungen wie eine Platzierung in einem getrennten Netzwerksegment hinter einer Firewall.

Table 18 – Periodische Aktualisierung

3.4.3. Systemüberwachung

M12 – GE-BSA-IT/OT-Operation
Automatisierte Funktionsüberwachung Die Funktionalität kritischer Anlagen wird überwacht. Die Funktionsüberwachung unterscheidet sich vom Alarming dahingehend, dass nicht Störungen, sondern der aktuelle Betriebszustand übermittelt wird. Die Prüfung der Daten wird in die Betriebsprozesse integriert. Die Systeme müssen so weit protokolliert werden, dass Anomalien ausgewertet und erkannt werden.
Fragestellungen
• Werden die Informationen über den Status der Schutzsoftware (z.B. aktueller Schutz, erkannte Schadprogramme, etc.) und an zentraler Stelle protokolliert und ausgewertet?
IST-Zustand
Die GE betreibt ein Monitoring Tool, bei welchem alle im BKN, und künftig am «IP-Netz-BSA», angeschlossenen Geräte überwacht werden. Die Überwachung der Antivirensoftware geschieht zentral auf je einem Server im BKN, sowie in der DMZ. Die eingesetzte Software ist proprietär zu den verwendeten Virenschutzprogrammen auf den Clients.
Risiko
Technisch bedingte Fehlfunktion Menschliche Fehlmanipulation Hinweise auf bevorstehenden Ausfall eines Systems/Komponente/Anlage[8] Unklare Aussage über Systemverfügbarkeiten[9]

[8] Zusätzliches Risiko, dass nicht auf der Risikoliste des ASTRA Merkblattes aufgelistet ist
[9] Zusätzliches Risiko, dass nicht auf der Risikoliste des ASTRA Merkblattes aufgelistet ist

Soll-Zustand
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. Ereignisse auf Systemen werden systematisch aufgezeichnet und zentral gespeichert, vgl. Kapitel 3.5.2. Sie dienen der Erkennung von Anomalien oder der Analyse von Ursachen für Systemstörungen. 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.
Gegenmassnahme
34. Der GE-BSA-ISO definiert, ob und welche Überwachung inkl. Scanning und Aufzeichnung er auf welchen Systemen verlangt, beispielsweise im Rahmen einer Sicherheitsprüfung. 35. GE-BSA-IT/OT-Admin stellt sicher, dass seine Systeme bei der Übernahme in die Systemüberwachung so integriert werden, dass der Betrieb deren Verfügbarkeit überwachen kann. 36. GE-BSA-IT/OT-Operation stellt die Überwachung der Systemverfügbarkeit, sowie die zentrale Speicherung der Logdaten sicher. Er prüft auf Verdacht die Aufzeichnungen und meldet Anomalien. 37. Der GE-BSA-ISO prüft periodisch, ob alle Systeme gemäss Inventar in der Systemüberwachung berücksichtigt sind, beispielsweise bei einer jährlichen Bestandsaufnahme.

Table 19 – Systemüberwachung

3.4.4. Malware

M01, M02 – GE-BSA-ISO
Secure Endgeräte Für Unterhaltsarbeiten kommen nur Secure Endgeräte zum Einsatz. Dies sind prioritäre managed Clients. Müssen Endgeräte der Partner verwendet werden, so müssen diese auf aktuellem Sicherheitsstand (Patching) und mit aktuellem Malwareschutz ausgerüstet sein. Dies wird vertraglich mit Pönalen bei Zuwiderhandlung eingefordert. **Malwarescanner auf allen Zentralsystemen**[10] Auf Zentralsystemen der BSA ist ein Malwarescanner installiert. Dieser erhält periodisch (täglich) neue Signaturen und meldet Ereignisse in die Zentrale Malwareüberwachung. Zugänge von extern sind gegen Malware geschützt. Insbesondere dann, wenn Daten ins BSA-Netz geladen werden können. → Die Basisdienste sind anzuwenden (zum Beispiel Zeit-Synchronisation, Adress-Vergabe etc.).

[10] Als Zentralsystem ist in diesem Zusammenhang ein Systeme zu verstehen, welches für den Betrieb, die Datenauswertung, die Datenerfassung und/oder Datenverarbeitung von zentraler Bedeutung ist. Typischerweise handelt es sich um ein System mit einem Windows oder Linux Betriebssystem.

Fragestellungen
• Für welche Systeme gibt es einen Schutz vor Schadprogrammen (z.B. Trojaner, Viren, Malware, etc.)? • Welche Systeme sind nicht vor Schadprogrammen (z.B. Trojaner, Viren, Malware, etc.) geschützt? • Wie wird der Schutz vor Schadprogrammen aktuell gehalten?
IST-Zustand
Die Antivirensoftware ist auf den meisten Servern, sowie internen Clients im Netzwerk installiert. Durch die proprietäre Managementsoftware können alle Antivirenprogramme überwacht und bei Bedürfnis aktualisiert werden. Für die externen Partner gibt es eine Sicherheitserklärung, bei welcher diese garantieren müssen, dass ihre Geräte einen aktuellen Virenschutz installiert haben.
Risiko
"Malware oder Ransomware im IP-Netz Malware wird über die BSA-Geräte in das Client Netz des ASTRA verbreitet" Funktionsausfall der Zentralsysteme, Leittechnik, Alarming Ausfall dezentraler Systeme Technisch bedingte Fehlfunktion
Soll-Zustand
Zugriffe auf Systeme im BKN-Netz der GE erfolgen remote über definierte Zugänge, beispielsweise VPN, RDS, Jumphost oder ähnliches, nicht mit mobilen Endgeräten. In seltenen Fällen kann es erforderlich sein, ein mobiles Endgerät ausnahmsweise direkt im Netz der GE anzuschliessen. Solche Zugänge sind ein aussergewöhnliches Risiko und werden über das Change-Management gemeldet. Bei Bedarf folgt auf einen solchen Zugriff ein Netzwerk- und Verwundbarkeitsscan. Die Server und wenigen stationären Clients sind als Endgeräte ständig im Netz der GE verbunden. Für diese Geräte wird ein einheitlicher Malware-Schutz installiert.
Gegenmassnahme
38. Der GE-BSA-ISO wertet regelmässig, beispielsweise jährlich im Rahmen einer Sicherheitsprüfung, aus, in welchem Verhältnis die Nutzung von Fernzugriffen, stationärer Clients und ausnahmsweise lokal angeschlossener, mobiler Endgeräte ist. Bei Bedarf wird der Einsatz mobiler Endgeräte analysiert und Massnahmen empfohlen, deren Gebrauch im BKN-Netz der GE zu reduzieren. 39. GE-BSA-IT/OT-Admin erfassen im Inventar, auf welchen ihrer Systeme ein Malwareschutz aktiv ist. 40. Der GE-BSA-ISO erhebt mindestens einmal jährlich, welche Systeme keinen Malwareschutz haben, welche von der einheitlichen Lösung abweichen und stichprobenartig, ob die Einstellungen der übrigen Systeme einen angemessenen Schutz bieten.

Table 20 – Malwarescanner

3.5. Sicherheitsvorfälle und Notfallmanagement

DER.1 Detektion von sicherheitsrelevanten Ereignissen
DER.2 Security Incident Management
DER.3 Sicherheitsprüfungen
DER.4 Notfallmanagement

3.5.1. Technische Sicherheitsprüfungen

M15 – GE-BSA-ISO

Periodische Sicherheitsprüfung der BSA IT-Infrastruktur

Der Sicherheitsstand der Systeme ist periodisch zu überprüfen und auszuweisen.

Fragestellungen

- Hat Ihre Organisation eine spezifische Sicherheitsrichtlinie erstellt?
- Wie wird die Organisation ihrer IT/OT-Security (auch ISMS - Information Security Management System) geprüft?
- Wie wird die Umsetzung der Sicherheitsmassnahmen geprüft?

IST-Zustand

Die GE hat auf ihrem Normalien-Server verschiedene technische Dokumente veröffentlicht, welche u.a. die IT-Sicherheit adressieren. Eine dedizierte Sicherheitsrichtlinie der GE ist noch nicht vorhanden.

Die Security-Aspekte werden bei der Abnahme eines Projektes einmalig überprüft, anschliessende Überprüfungen finden «on-the-fly» und bei Bedarf, beispielsweise bei neu entdeckten Sicherheitslücken statt.

Risiko

"Malware oder Ransomware im IP-Netz Malware wird über die BSA-Geräte in das Client Netz des ASTRA verbreitet"

Unbefugte erhalten Einsicht in Daten der Nationalstrassen

Funktionsausfall der Zentralsysteme, Leittechnik, Alarming Ausfall dezentraler Systeme

Technisch bedingte Fehlfunktion

Soll-Zustand

Es existieren technische Vorgaben, deren Einhaltung überprüft wird. Erkannter Handlungsbedarf wird systematisch erfasst und adressiert.

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.

Die Aktualisierung der technischen Sicherheitsvorgaben ist sichergestellt.

Gegenmassnahme
41. Der GE-BSA-ISO prüft periodisch die Aktualität technischer Vorgaben in der GE, beispielsweise im Rahmen der jährlichen Überarbeitung dieses Sicherheitskonzeptes. Er gibt Feedback zu technischen Vorgaben des ASTRA für IT/OT-Systeme. 42. Der GE-L-IT gibt geänderte technische Vorgaben der GE frei. 43. GE-BSA-IT/OT-Admin prüfen die Einhaltung technischer Vorgaben im Rahmen von Projekten, beispielsweise im DAW und melden Handlungsbedarf an den GE-BSA-ISO.

Table 21 – Sicherheitsprüfung

3.5.2. Logfiles

M10, M20 – GE-BSA-ISO
Logfiles bereitstellen. Logfiles auswerten Die Logfiles wichtiger Systeme werden periodisch auf kritische Ereignisse ausgewertet. Wo nötig ist dies mit einer Alarmierung gekoppelt. Die Reaktion auf einen Incident ist geregelt. Die Systeme müssen soweit protokolliert werden, dass Anomalien ausgewertet und erkannt werden. (siehe auch Massnahme M12) **Protokollierung administrative Arbeiten** Alle administrativen Tätigkeiten (Unterhalt & Konfiguration) auf einem System müssen protokolliert werden. Wenn technisch nicht umsetzbar, dann kann diese Aufgabe an die Basis-Dienste BSA ausgelagert werden. Diese Möglichkeit gilt nicht für Systeme, die Zugriff auf andere Systeme gewährleisten (zum Beispiel Abschnittsrechner). Wenn Teile einer Aufgabe von einem nachgelagerten System erfüllt werden (backend server), muss die Identität des verursachenden Endbenutzers so mit übertragen werden, dass sie vom Empfängersystem einfach für die Zugriffskontrolle verwendet werden kann (zum Beispiel mittels WS-Trust). Ist dies aus technischen Gründen nicht möglich, muss das aufrufende System die Aktivitäten protokollieren.
Fragestellungen
• Haben Sie einen Plan zur Elimination eines APT (Advanced Persistent Thread) und wie prüfen sie diesen? • Ist jede Störung dokumentiert und sind die getätigten Arbeiten nachvollziehbar dokumentiert?
IST-Zustand
Die GE verfügt über keinen konkreten Plan um einem APT zu eliminieren. Implizit würden wahrscheinlich die kritische Infrastruktur komplett vom öffentlichen Netz getrennt, da die Grundfunktionalität auch ohne Verbindung ins Internet funktioniert. Es gibt ebenfalls keine systematische Auswertung von Logfiles. IT-Störungen werden über ein Ticketing-Tool abgewickelt. Somit ist jede Störung einheitlich erfasst und es ist nachvollziehbar, wie die Störung behoben wurde.
Risiko
Unbefugte erhalten Einsicht in Daten der Nationalstrassen Nicht geschützte Komponenten der BSA werden manipuliert

Technisch bedingte Fehlfunktion Menschliche Fehlmanipulation
Soll-Zustand
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. Zur Erkennung von APT bleiben die Aufzeichnungen mindestens 3 Jahre gespeichert und sind vor unberechtigtem Zugriff sowie Veränderung geschützt. Anomalien können erkannt werden. Sicherheitsrelevante Störungen sind in den Aufzeichnungen nachvollziehbar. In einem umsetzbaren Konzept soll geregelt werden, wie Logging-Informationen zur Behandlung von IT- und sicherheitsrelevanten Störungen systematisch erhoben werden sollen. Arbeiten, beispielsweise Umgehungslösungen, sind dadurch dokumentiert und bei Bedarf werden Massnahmen empfohlen (Problem Management nach ITIL).
Gegenmassnahme
44. Der BSA-IT/OT-Admin für das Logmanagement prüft das Logmanagement-Konzept mindestens jährlich und macht bei Bedarf Anpassungen. 45. Der GE-BSA-ISO würdigt bei Bedarf die Änderungen des GE-BSA-IT/OT-Admin für das Logmanagement, welche am Logmanagement-Konzept vorgenommen wurden, und empfiehlt es zur Freigabe. 46. Der GE-L-IT gibt das Logmanagement-Konzept bei Bedarf frei. 47. Der GE-L-IT bestätigt mindestens jährlich die Ressourcen und Verantwortlichkeiten für die Umsetzung allfälliger Änderungen am Logmanagement-Konzept und die Einhaltung des Logmanagement-Konzepts.

Table 22 - Logfiles

3.5.3. Alarmfunktionalität

M04 – GE-BSA-IT/OT-Operation
Periodische Überprüfung der Alarmfunktionalität Die Alarmfunktion ist dahingehend überwacht, dass Störungen und Ausfall präventiv detektiert werden können. Die Alarmfunktionalität wird periodisch überprüft.
Fragestellungen
• Wie werden alle Mitarbeiter auf die Detektion von Sicherheitsvorfällen geschult? • Hat ihre Organisation eine ausgereifte Eskalationsstrategie für Sicherheitsvorfälle? • Wird die Alarmfunktion dahingehend überwacht, dass Störungen und Ausfall präventiv detektiert werden können und wird die Alarmfunktionalität periodisch geprüft?
IST-Zustand
Die Mitarbeiter wurden bis anhin nicht für die Detektion von Sicherheitsvorfällen geschult. Eine konkrete, formelle Eskalationsstrategie für IT-Sicherheitsvorfälle existiert nicht. Aus dem Verständnis der GE-IT wird die folgende Eskalation angewandt: GE-IT-Pikett -> GE-L-IT -> GE-L -> ELA (Einsatzleiter ASTRA).

Es gibt verschiedene Alarmfunktionen in der GE. Zum einen werden betriebliche relevante Alarme vom UeLS alarmiert. Diese Alarme werden regelmässig im Rahmen von Wartungsarbeiten (gemäss Vorschrift ASTRA) überprüft.

Des Weiteren betreibt die IT eigene Monitoring-/Alarming-Tools, welche die «Gesundheit» der Geräte überwachen. Diese alarmieren bei Abnormalen Betriebszuständen, welche jedoch nicht zwingend eine Störung zur Folge haben (Bsp.: Temperaturanstieg, Ausfall von RAID-Festplatte). Diese Funktionen werden jedoch nicht explizit getestet, da sie Grundsätzlich von einer Fehlfunktion ausgehen.

Risiko

Funktionsausfall der Zentralsysteme, Leittechnik, Alarming Ausfall dezentraler Systeme

Technisch bedingte Fehlfunktion

Störung der Alarmsysteme löst Falsch-/ Fehlalarme aus

Soll-Zustand

Die Systemüberwachung stellt sicher, dass Systemausfälle ausreichend schnell erkannt werden.

Der Malware-Schutz stellt sicher, dass Schadsoftware rasch erkannt oder deren Ausführung sofort blockiert wird.

Die Überprüfung von Aufzeichnungen ermöglicht die Erkennung von Anomalien.

Erkannte Störungen werden nach einem geregelten Verfahren eskaliert.

Gegenmassnahme

48. Der GE-BSA-IT/OT-Operation alarmiert bei technischen Störungen je nach Dokumentation den GE-BSA-IT/OT-Admin oder den Lieferanten, wenn für die angetroffene Situation keine Umgehungslösung definiert ist oder deren Umsetzung nicht wirksam ist. Die Eskalation erfolgt an die jeweils definierte Stelle, beispielsweise IT-Pikett oder Notfallnummer des Lieferanten.
49. Der GE-BSA-IT/OT-Operation oder der IT-Pikett eskaliert bei Bedarf, beispielsweise wenn Gefahr für Leib und Leben besteht, die Störung weiter an die Notfallorganisation der GE.

Table 23 – Alarmfunktionalität

3.5.4. Notfallmanagement

M05, M17 – GE-BSA-IT/OT-Admin

Keine funktionale Einschränkung durch Ausfälle zentraler Systeme und Bereitstellung von Notfallprozessen für Ausfall der Zentralsysteme

Systeme in der Netzwerkzone «Prozess», insbesondere die Steuerungsanlagen, müssen so konstruiert sein, dass der Ausfall eines Basis-Dienstes BSA (zum Beispiel Zeit-Synchronisation, IAM etc.) keine funktionalen Einschränkungen bewirkt. So darf zum Beispiel der Ausfall eines zentralen LDAP Verzeichnisses nicht dazu führen, dass auf den Streckensystemen keine Authentisierung mehr durchgeführt werden kann. Es sind präventiv Prozesse und Verantwortlichkeiten definiert, welche bei Ausfall von Zentralsystemen zur Anwendung kommen. Diese beinhalten auch Wiederanlaufpläne.

Zweitwegerschliessung wo notwendig

Bedarfsabklärung einer Zweitwegerschliessung auch hinsichtlich der Bedürfnisse der BSA durchführen.

Fragestellungen

- Sind im BSA Betriebskonzept Eventualplanungen für das Notfallmanagement bei weitreichendem Ausfall von Netzwerkwerkinfrastruktur oder Dienstleistern enthalten?

IST-Zustand

Im Falle eines weitreichenden Ausfalls von BKN Komponenten greift die GE auf das Notbetriebssystem NBS zurück. Dieses ist nicht mit dem BKN gekoppelt, also komplett unabhängig. **Selbst wenn im UeLS die redundanten und hochverfügbaren Systeme ausfallen, so können sicherheitskritische Systeme noch immer über das NBS gesteuert werden.**

Das NBS ist auch, Aufgrund der Unabhängigkeit zum UeLS und BKN, bei einem Malware-Befall, nach einer kurzen Ausfallzeit, wieder vollumfänglich benutzbar. Mit einem Cluster- resp. hochverfügbaren (virtuellen) System ist dies nicht möglich.

Risiko

Unbefugte erhalten Einsicht in Daten der Nationalstrassen

Nicht geschützte Komponenten der BSA werden manipuliert

Hohes Risiko für Leib und Leben[11]

Ressourcen des KAPO und des NSU zur Tunnelüberwachung und Intervention vor Ort über mehrere Tage notwendig[12]

Ausfall der Verbindung zum Zentralsystem

Soll-Zustand

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.

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.

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.

[11] Zusätzliches Risiko, dass nicht auf der Risikoliste des ASTRA Merkblattes aufgelistet ist.
[12] Zusätzliches Risiko, dass nicht auf der Risikoliste des ASTRA Merkblattes aufgelistet ist.

Gegenmassnahme
50. Der GE-BSA-ISO führt und prüft einen Eskalationsplan, welcher für IT mit dem GE-L-IT und für OT mit dem GE-L-BSA abgestimmt ist. Er berücksichtig dabei bestehende Eskalationsstrukturen, beispielsweise den IT/OT-Helpdesk des ASTRA. 51. Der GE-L-IT und der GE-L-BSA definieren den IT-Eskalationsplan für die GE. Dazu gehören IT-Pikett, OT-Pikett und Notfallorganisation. Sie stellen sicher, dass bestehende Eskalationsstrukturen der GE eingebunden werden können. Sie führen mindestens jährlich einen Test durch, um die Erreichbarkeit der Betroffenen festzustellen und die Handlungsfähigkeit sicherzustellen. 52. Der GE-BSA-IT/OT-Admin definiert und dokumentiert für seine Systeme die technischen Handlungsmöglichkeiten in einem Notfall, d.h. den Notbetrieb. Beispielsweise können das Teilnetz der Bereichsrechner bewusst vom BKN-Netz getrennt werden oder Dienste über eine redundante Netzwerkverbindung erreichbar sein oder ein eingeschränkter Funktionsumfang für einen Notbetrieb vorgesehen werden. Falls auf einen Notbetrieb verzichtet wird, begründet er dies. 53. Der GE-BSA-IT/OT-Admin testet in definierten Zeitintervallen, beispielsweise jährlich, ob die definierten technischen Notfallpläne für seine kritischen Systeme tauglich sind. Er passt bei Bedarf den Plan an.

Table 24 - Notfallmanagement

4. Infrastruktur (Software, Hardware, Zutritt)

4.1. Software Anwendungen

APP.1 Client-Anwendung
APP.2 Verzeichnisdienst
APP.3 Netzbasierende Dienste
APP.4 Buseiness Anwendungen
APP.5 E-Mail/Groupware/Kommunikation

4.1.1. Clientanwendungen

M01, M02, – GE-BSA-ISO
Secure Endgeräte Für Unterhaltsarbeiten kommen nur Secure Endgeräte zum Einsatz. Dies sind prioritäre managed Clients. Müssen Endgeräte der Partner verwendet werden, so müssen diese auf aktuellem Sicherheitsstand (Patching) und mit aktuellem Malwareschutz ausgerüstet sein. Dies wird vertraglich mit Pönalen bei Zuwiderhandlung eingefordert. **Malwarescanner auf allen Zentralsystemen** Auf Zentralsystemen der BSA ist ein Malwarescanner installiert. Dieser erhält periodisch (täglich) neue Signaturen und meldet Ereignisse in die Zentrale Malwareüberwachung. Zugänge von extern sind gegen Malware geschützt. Insbesondere dann, wenn Daten ins BSA-Netz geladen werden können. → Die Basisdienste sind anzuwenden (zum Beispiel Zeit-Synchronisation, Adress-Vergabe, etc.).
Fragestellungen
• Werden im BSA Bereich Office-Produkte (Clients) eingesetzt? • Sind die eingesetzten Office-Produkte (Clients) aktuell (neuster Patch-Level)? • Sind die eingesetzten Office-Produkte (Clients) von Dritten / Partner auf dem aktuellen Sicherheitsstand (Patching) und mit aktuellem Malwareschutz ausgerüstet? • Werden im BSA Bereich Webbrowser eingesetzt? • Sind die / Ist der eingesetzte Webbrowser aktuell (neuster Patch-Level)?
IST-Zustand
Im BSA-Bereich werden keine Office-Produkte eingesetzt, da dies für den Betrieb nicht notwendig ist. Für die Bedienung des UeLS wird Firefox 46 verwendet. Ein Update ist hier nicht vorgesehen, da die Bestimmungen vorgeben, dass das UeLS auf dieser Firefox-Version läuft. Die Clients, welche Firefox 46 installiert haben, sind jedoch hinter einer Firewall und haben keinen Internetzugang (siehe dazu auch *3.4.2 Periodische Aktualisierung*).
Gegenmassnahme / Bemerkung für die Massnahmentabelle
Keine erforderlich, nicht anwendbar

Table 25 - Clientanwendungen

4.1.2. Benutzerberechtigungen

M21 – GE-BSA-IT/OT-Admin
Einschränkung der User-Berechtigung Die Berechtigungen der User / Benutzer sind auf das Minimum / Notwendige zu reduzieren. Die Kontrolle der Zugrifferlaubnis und Zugriffverwendung muss jederzeit nachvollziehbar sein. Systeme in der Netzwerkzone «Prozess» müssen so konstruiert sein, dass ein Benutzer nur vorgesehene Aktivitäten durchführen kann. Insbesondere ist dafür zu sorgen, dass ein Benutzer nicht auf die Betriebssystem-Ebene gelangt und dort beliebige Aktionen ausführt. Es ist auch zu verhindern, dass ein Benutzer mit einem Web-Browser andere als vordefinierte URLs anwählen kann.
Fragestellungen
• Ist ein zentrales Benutzermanagement/ein zentraler Verzeichnisdienst vorhanden? • Verwenden die BSA Systeme das zentrale AD?
IST-Zustand
Ein zentrales AD wird bereits für die grosse Mehrheit der Benutzer verwendet. Die AD-Benutzer sind ebenfalls alle persönlich. Das AD wird auch für die BSA-Geräte, bis auf Stufe Rechner, eingesetzt ("Windows-Anmeldung", "LDAP-Anmeldung" für Linux wo immer möglich auch mit Einschränkungen).
Gegenmassnahme / Bemerkung für die Massnahmentabelle
i. Der GE-BSA-IT/OT-Admin für AD stellt Auswertungen für Prüfungen gemäss Kapitel 3.1.3 zur Verfügung.

Table 26 - Benutzerberechtigungen

4.1.3. Softwareinventar

M16 – GE-BSA-IT/OT-Admin
Inventarisierung Um eine vollständige Übersicht der BSA-Informatik zu gewährleisten, muss eine vollständige Inventarisierung der verwendeten Komponenten sichergestellt werden. Es ist dabei zu klären und festzulegen welche Daten wo notwendig sind und wer was macht (Zuständigkeit Gebietseinheit und ASTRA). Insbesondere müssen Doppelspurigkeiten vermieden werden. Es darf immer nur einen Datenmaster geben.
Fragestellungen
• Wie viele unterschiedliche Softwareprodukte werden im BSA Umfeld eingesetzt? • Wie werden die eingesetzten Softwareprodukte inventarisiert?
IST-Zustand
Ein dediziertes Softwareinventar existiert in der GE nicht. Alle Clients, welche Kaspersky installiert haben, haben ihre Software im Kaspersky Security-Center inventarisiert.

Gegenmassnahme / Bemerkung für die Massnahmentabelle	
ii.	Der GE-BSA-ISO prüft, ob und wofür DocuSnap als Werkzeug für die Inventarisierung der von der GE betriebenen Systeme zum Einsatz kommt.
iii.	Der GE-L-IT legt fest, wer für welches System die Rolle GE-BSA-IT/OT-Admin übernimmt.
iv.	GE-BSA-IT/OT-Admin übernehmen ihre Systeme ins Inventar gemäss Massnahme 15. Diese Massnahme ist abhängig von ii. und iii.

Table 27 - Softwareinventar

4.2. Server

SYS.1 Server
SYS.2 Desktop-Systeme
SYS.3 Mobile Devices
SYS.4 Sonstige Systeme

4.2.1. Backup

M11 - GE-BSA-IT/OT-Admin	
Backup etablieren. Periodischen Restore durchführen	
Einstellungen und Daten wichtiger Systeme werden periodisch gesichert. Die Vollständigkeit der Sicherung sowie der Prozess des Rückspielens wird regelmässig getestet.	
Fragestellungen	
• Werden an einzelnen, wichtigen Servern regelmässig (z.B. einmal pro Jahr) Restore-Tests durchgeführt? • Werden die Server, ihrer Wichtigkeit nach regelmässig gebackupt?	
IST-Zustand	
Es gibt ein zentrales Backupsystem für die Server. Eine Unterscheidung nach Wichtigkeit der Systeme wird nicht vorgenommen. Die Systeme werden jedoch alle täglich gesichert. Es werden auch jährliche Restore-Tests durchgeführt, jedoch an zufällig ausgewählten Systemen. Beim UeLS werden diese Aufgaben vom Lieferanten übernommen.	
Gegenmassnahme / Bemerkung für die Massnahmentabelle	
v.	Der GE-BSA-IT/OT-Admin für das Backupsystem erstellt ein Backupkonzept gemäss Kapitel 3.3.2 auf Basis des Inventars.

Table 28 - Serverbackup

4.2.2. Inventar

M16 - GE-BSA-IT/OT-Admin
Inventarisierung
Um eine vollständige Übersicht der BSA-Informatik zu gewährleisten, muss eine vollständige Inventarisierung der verwendeten Komponenten sichergestellt werden. Es ist dabei zu klären und festzulegen welche Daten wo notwendig sind und wer was macht (Zuständigkeit Gebietseinheit

und ASTRA). Insbesondere müssen Doppelspurigkeiten vermieden werden. Es darf immer nur einen Datenmaster geben.
Fragestellungen
• Existiert eine Übersicht über alle eingesetzten Betriebssysteme auf den einzelnen Komponenten/Systemen? • Ausserbetriebnahme: Ist die Ausserbetriebnahme einer Komponente (insbesondere eines Server Systems) in einem Prozess geregelt? • Wie wird wirksam kontrolliert ob beliebige Datenträger an ein System angeschlossen werden?
IST-Zustand
Innerhalb des BKN ist der GE bekannt, welche Betriebssysteme eingesetzt werden. In den Tunnelnetzen liegt die Übersicht beim Lieferanten. Für die Ausserbetriebnahme gibt es kein konkretes Konzept. Der Rückbau wird jeweils von Projekten vorgenommen und pro Projekt unterschiedlich gehandhabt. Die Clients erlauben externe Datenträger nur dort, wo die Polizei anwesend ist. Bei den Servern setzt man auf die Zutrittsbeschränkung. Diese schützt jedoch nicht vor unabsichtlichem Fehlverhalten.
Gegenmassnahme / Bemerkung für die Massnahmentabelle
Inventarpflege siehe Kapitel 4.1.2 vi. Der GE-BSA-ISO stellt eine generische Checkliste für die Ausserbetriebnahme zur Verfügung. vii. Der GE-BSA-IT/OT-Admin benutzt für die Ausserbetriebnahme die Checkliste des GE-BSA-ISO. Diese Massnahme ist abhängig von vi. viii. Der GE-BSA-IT/OT-Admin für den Schutz der Endpunkte (Kaspersky) prüft regelmässig dessen Wirksamkeit für Maschinen, welche den Anschluss externer Datenträger zulassen. Er meldet Mängel, welcher er nicht sofort selbst beheben kann dem GE-BSA-ISO mit einer Empfehlung, beispielsweise wenn ein kostenpflichtiger Zusatz erforderlich ist.

Table 29 - Inventar

4.2.3. Automatische Funktionsüberwachung

M12 – GE-BSA-IT/OT-Operation
Automatisierte Funktionsüberwachung Die Funktionalität kritischer Anlagen wird überwacht. Die Funktionsüberwachung unterscheidet sich vom Alarming dahingehend, dass nicht Störungen, sondern der aktuelle Betriebszustand übermittelt wird. Die Prüfung der Daten wird in die Betriebsprozesse integriert. Die Systeme müssen so weit protokolliert werden, dass Anomalien ausgewertet und erkannt werden.
Fragestellungen
• Komponenten: Findet ein aktives Monitoring der Systeme statt?

IST-Zustand
Die Systeme, welcher am BKN angeschlossen sind, werden mittels PRTG-Überwachungssoftware von der GE überwacht. Die Anlagesysteme werden direkt vom UeLS überwacht.
Gegenmassnahme / Bemerkung für die Massnahmentabelle
ix. Der GE-BSA-IT/OT-Operation filtert Alarmierungen aus der automatischen Funktionsüberwachung, wenn ihm Arbeiten am System bekannt sind, beispielsweise während eines angemeldeten Changes. x. Der GE-BSA-IT/OT-Operation meldet dem GE-BSA-ISO, wenn Weiterleitungen und Eskalationen unbearbeitet bleiben.

Table 30 - Automatische Funktionsüberwachung

4.2.4. Reduktion der Komplexität des Gesamtsystems

M13 – GE-BSA-ISO
Reduktion der Komplexität des Gesamtsystems Eine tiefe Komplexität wird als Design-Ziel des Gesamtsystems verbindlich festgelegt. Dieses beinhaltet eine strukturierte Systemarchitektur, möglichst wenige Komponenten und Hersteller, möglichst wenige Softwareprodukte und harmonisierte Versionen der Software. Die Tools für Systemwartung sind über verschiedene Lieferanten und Softwareversionen zu harmonisieren und zu standardisieren.
Fragestellungen
• Komponenten: Gibt es Vorgaben (insbesondere zu Serversystemen) von der GE?
IST-Zustand
Es existieren verschiedene Normalien der GE. Speziell für Server gibt es die «BR-Normalie», welche sich auf die Bereichsrechner fokussiert.
Gegenmassnahme / Bemerkung für die Massnahmentabelle
xi. Der GE-BSA-ISO erfasst im Kontext mit Projekten eine mögliche Zunahme der Komplexität, beispielsweise wenn gegen die Normalien verstossen wird, und nimmt den Sachverhalt als Mangel auf.

Table 31 - Reduktion der Komplexität des Gesamtsystems

4.2.5. Berechtigungskonzept Server

M22 – GE-BSA-ISO
Berechtigungskonzept Ein Berechtigungskonzept pro BSA ist zu erstellen. Für jedes in der Domäne BSA betriebene System muss ein Berechtigungskonzept vorliegen, das die Berechtigungsvergabe anhand der Prinzipien need to know und need to use regelt.
Fragestellungen
• Rollentrennung: Findet eine Trennung von Rollen statt?

• Rollentrennung: Welche Rollen gibt es in der GE?
IST-Zustand
Im AD gibt es «normale» und «admin» Benutzer. Externe Lieferanten haben nur «admin»-Benutzer und kommen mit diesen lediglich auf ihre eigenen Rechner. Im Leitsystem werden vier verschiedene Benutzertypen unterschieden. Hier gibt es «admin», «superuser», «operator» und «read-only».
Gegenmassnahme / Bemerkung für die Massnahmentabelle
xii. Der GE-BSA-IT/OT-Admin berät für seine Systeme den GE-BSA-ISO bei der Rollenbildung und –vergabe im Zusammenhang mit Kapitel 3.1.3.

Table 32 – Berechtigungskonzept Server

4.3. Steuerungen

IND.1 Betriebs- und Steuerungstechnik
IND.2 ICS-Komponenten

4.3.1. Verantwortlichkeiten für Steuerungen

M08 – GE-L-BSA
Definierte Verantwortlichkeiten und Betriebsprozesse für sämtliche Systeme Die Betriebsverantwortung für sämtliche Systemkategorien ist festgelegt. Je nach Komplexität der Systeme kann die Verantwortung über mehrere Stellen verteilt sein (OS, DB, Anwendung etc.). In diesem Fall sind die AKV's der Beteiligten vertieft zu regeln. Die Verantwortlichkeit für Gesamtanlagen, Netzwerke und Verbindungen zur Aussenwelt (Firewall Regeln und Protokolle) sind explizit auszuweisen. Die Aufgabenerfüllung muss stets nachvollziehbar sein.
Fragestellungen
• Wer ist verantwortlich für die IT/OT-Sicherheit der SPS/PLC-Komponenten? • Gibt es IT/OT-Security Vorgaben der GE für SPS/PLC-Komponenten? • Sind alle SPS/PLC-Komponenten vor physischem Zugriff geschützt?
IST-Zustand
Für die IT/OT-Sicherheit ist während des Projekts der Lieferant zuständig, danach geht die Verantwortung, nach dem Verständnis der GE, an den Bauherren (ASTRA Filiale) über. Innerhalb der GE sind diesbezüglich keine Verantwortlichkeiten definiert/bekannt. Ausser den impliziten Vorgaben, welche sich aus verschiedenen Richtlinieren und Normen ableiten lassen, gibt es keine Sicherheitsvorschriften für SPS/PLC-Komponenten. Es sind alle SPS/PLC-Komponenten bis zu einem gewissen Grad vor physischem Zugriff geschützt.

Gegenmassnahme / Bemerkung für die Massnahmentabelle
xiii. Der GE-L-BSA legt fest, wer für welches Steuerungssysteme die Rolle GE-BSA-IT/OT-Admin übernimmt. xiv. GE-BSA-IT/OT-Admin übernehmen ihre Systeme ins Inventar gemäss Massnahme 15. Diese Massnahme ist abhängig von ii. und xiii. xv. Der GE-L-ISO berät den GE-L-BSA bei der Erstellung von Vorgaben zu den Steuerungssystemen. physischer Zutritt gemäss Kapitel 4.5

Table 33 – Verantwortlichkeiten für Steuerungen

4.3.2. Backup von Steuerungssystemen

M11- GE-BSA-IT/OT-Admin
Backup etablieren. Periodischen Restore durchführen Einstellungen und Daten wichtiger Systeme werden periodisch gesichert. Die Vollständigkeit der Sicherung sowie der Prozess des Rückspielens wird regelmässig getestet.
Fragestellungen
• SPS/PLC: Gibt es eine Datensicherung (siehe Fragestellung im Kapitel 3.2 – Themen «Datensicherung»)?
IST-Zustand
Seitens der GE VII existieren für einen Grossteil der SPS/PLC-Komponenten selbst angefertigte Datenbackups (teilweise aber ohne Source-Code). Eine vollständige Datensicherung (inkl. Source-Code) ist teilweise nur über die Lieferanten möglich. Es gibt jedoch keinen Nachweis- über solche Sicherungen, ebenso ist der Zugriff der GE VII auf die Sicherungen nicht sichergestellt.

Gegenmassnahme / Bemerkung für die Massnahmentabelle
xvi. Der GE-BSA-IT/OT-Admin stellt für seine Steuerungssysteme sicher, dass die GE-BSA Zugriff auf die Sicherungen hat.

Table 34 - Backup von Steuerungssystemen

4.3.3. Zugriffschutz für Steuerungssysteme

M03 - GE-BSA-IT/OT-Admin
Sämtliche Systeme sind mit Passwort gegen unerlaubten Zugriff geschützt Sämtliche Systeme die über TCP/IP erreichbar sind, verfügen über einen PIN/Passwortschutz. Passwörter sind individuell, persönlich und unterliegen einer bestimmten Komplexität. Die Qualität des Zugangsschutzes sowie die Periodizität der Erneuerung ist geregelt. Die Passwörter der individuellen, eindeutig einem Benutzer zuordenbaren Accounts werden vom jeweiligen Benutzer definiert und verwaltet. Es steht dafür keine zentrale Verwaltungslösung bereit. Die Passwörter müssen die Vorschriften aus „Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB“ erfüllen.
Fragestellungen
• Verfügen sämtliche Systeme die über TCP/IP erreichbar sind, einen PIN/Passwortschutz?
IST-Zustand
Es besitzen fast alle Geräte, welche über eine IP-Adresse im BKN erreichbar sind einen PIN/Passwortschutz. Ausnahmen sind z.B. die Vor-Ort Bedienpanels (Touch-Panels). Zu den Geräten in den Lokalen Anlagenetzen kann keine Angabe gemacht werden.
Gegenmassnahme / Bemerkung für die Massnahmentabelle
Gemäss Massnahme 23.

Table 35 - Zugriffschutz für Steuerungssysteme

4.3.4. Wartung der Steuerungssysteme

M06, M07- GE-BSA-IT/OT-Admin
Security Patching Prozesse für sämtliche Systeme etablieren Es ist definiert, wer über welche Kanäle über Sicherheitslücken der Systeme informiert wird, wie solche Schwachstellen beurteilt und über deren Relevanz für die Systeme des ASTRA entschieden wird. Es ist geklärt wer über die Umsetzung entscheidet und wer in welcher Zeitfrist die Umsetzung durchführt.

Periodische Aktualisierung der Software (sämtliche Systeme) Für sämtliche Systeme die über TCP/IP erreichbar sind, ist im Grundsatz eine periodische Aktualisierung der Software vorzusehen. Die Periodizität der Aktualisierung ist für sämtliche Systemkategorien abschliessend festgelegt. Ebenfalls geregelt ist wer in welcher Zeitfrist die Umsetzung durchführt. Um den Aktualisierungsprozess zu vereinfachen sind die verwendeten Softwareprodukte und die verwendeten Versionen auf das notwendige reduziert. Für Unterhaltsarbeiten sind Wartungsfenster festgelegt.
Fragestellungen
• SPS/PLC: Wie werden regelmässig IT/OT-Security-Patches eingespielt? • SPS/PLC: Werden regelmässige Wartungsarbeiten vorgenommen und welche?
IST-Zustand
Security-Patches werden bei Bedarf vom Lieferanten oder gemäss dessen Vorgaben eingespielt. Gleichermassen werden Wartungsarbeiten durchgeführt. Die GE VII macht höchstens Sichtkontrollen, solange keine Störung vorliegt.
Gegenmassnahme / Bemerkung für die Massnahmentabelle
gemäss Kapitel 3.4.2

Table 36 – Wartung der Steuerungssysteme

4.4. Netze und Kommunikation

NET.1 Netze
NET.2 Funknetze
NET.3 Netzkomponenten
NET.4 Telekommunikation

4.4.1. Netzwerküberwachung

M12 - GE-BSA-IT/OT-Operation
Automatisierte Funktionsüberwachung Die Funktionalität kritischer Anlagen wird überwacht. Die Funktionsüberwachung unterscheidet sich vom Alarming dahingehend, dass nicht Störungen, sondern der aktuelle Betriebszustand übermittelt wird. Die Prüfung der Daten wird in die Betriebsprozesse integriert. Die Systeme müssen soweit protokolliert werden, dass Anomalien ausgewertet und erkannt werden.
Fragestellungen
• Allgemein: Ist das IP Netzwerk der GE vollständig überwacht (in Bezug auf Ausfall und Performance)?
IST-Zustand
Das BKN ist vollständig überwacht, Verbindungsstörungen des Leitsystems sind sogar doppelt überwacht, vom IT-Monitoring (PRTG) sowie vom Leitsystem selbst.

Gegenmassnahme / Bemerkung für die Massnahmentabelle	
xvii.	Der GE-BSA-IT/OT-Operation filtert Alarmierungen aus der automatischen Funktionsüberwachung, wenn ihm Arbeiten am System bekannt sind, beispielsweise während eines angemeldeten Changes.
xviii.	Der GE-BSA-IT/OT-Operation meldet dem GE-BSA-ISO, wenn Weiterleitungen und Eskalationen unbearbeitet bleiben.

Table 37 - Netzwerküberwachung

4.4.2. Berechtigungen zu Netzwerkkomponenten

M22 - GE-BSA-IT/OT-Admin

Berechtigungskonzept

Ein Berechtigungskonzept pro BSA ist zu erstellen. Für jedes in der Domäne BSA betriebene System muss ein Berechtigungskonzept vorliegen, das die Berechtigungsvergabe anhand der Prinzipien need to know und need to use regelt.

Fragestellungen

- Netzwerk: Ist der Zugang zum Netzwerk nur für registrierte und der GE im Vorfeld bekannte Endgeräte zugelassen?
- Gibt es aktive Netzwerkkomponenten ausserhalb von geschlossenen Räumen?
- Ist der physische Zugang zu den Netzwerkkomponenten eingeschränkt?

IST-Zustand

Der Anschluss einzelner Geräte muss bei der GE beantragt werden, mittels Portantrag. Grundsätzlich sind die Switchports auf eine MAC-Adresse fixiert oder ausgeschaltet. Es gibt jedoch Ports, welche für Servicearbeiten genutzt werden können und diese Restriktion nicht gilt. Zudem kann keine Aussage gemacht werden zu Netzwerken, welche sich noch bei Projekten befinden.

Die Netzwerkkomponenten der GE befinden sich grundsätzlich alle an zugriffsgeschützten Orten. Die klassischen Netzwerkgeräte befinden sich grösstenteils in geschlossenen Räumen. Es gibt jedoch auch Router und Switches, welche sich auf der Strecke in abgeschlossenen Schränken befinden, sowie Endgeräte, wie Kameras, Verkehrszähler, etc., welche draussen sind. Diese Standorte sind teilweise leicht zugänglich.

Gegenmassnahme / Bemerkung für die Massnahmentabelle	
xix.	Der GE-BSA-IT/OT-Admin für die Zugriffsberechtigungen auf Netzwerkkomponenten (Cisco ISE) berät den GE-BSA-ISO bei der Rollenbildung und –vergabe im Zusammenhang mit Kapitel 3.1.3 für seine Systeme.
xx.	Der GE-BSA-IT/OT-Admin für die Zugriffsberechtigungen auf Netzwerkkomponenten (Cisco ISE) wertet regelmässig aus, ob und auf welchen Switch-Ports keine Einschränkungen konfiguriert wurden. Er meldet Abweichungen, welche er nicht selbst sofort beheben kann, dem GE-BSA-ISO.

physischer Zutritt gemäss Kapitel 4.5

Table 38 - Berechtigungen zu Netzwerkkomponenten

4.4.3. Netzwerkinventar

M16 - GE-BSA-IT/OT-Admin
Inventarisierung Um eine vollständige Übersicht der BSA-Informatik zu gewährleisten muss eine vollständige Inventarisierung der verwendeten Komponenten sichergestellt werden. Es ist dabei zu klären und festzulegen welche Daten wo notwendig sind und wer was macht (Zuständigkeit Gebietseinheit und ASTRA). Insbesondere müssen Doppelspurigkeiten vermieden werden. Es darf immer nur einen Datenmaster geben.
Fragestellungen
• Kann zu jeder aktiven IP-Adresse eine Komponente eindeutig zugeordnet und lokalisiert werden?
IST-Zustand
Grundsätzlich kann die GE alle Geräte im BKN-Netzwerk identifizieren. Zudem gibt es für jedes Netzwerkgerät einen Hostnamen. Bekanntlich gibt es jedoch keine Regel ohne Ausnahme. Die GE verfügt noch über kein IPAM-Tool (IP-Adress-Management).
Gegenmassnahme / Bemerkung für die Massnahmentabelle
xxi. Der GE-BSA-ISO prüft, welches Werkzeug für die Inventarisierung der von der GE verwendeten IP-Adressen zum Einsatz kommt. xxii. Der GE-BSA-IT/OT-Admin für die Zugriffsberechtigungen auf Netzwerkkomponenten (Cisco ISE) pflegt abhängig von Gegenmassnahme xx. die IP-Adressliste im IPAM-Tool. Inventarpflege für die Netzwerkkomponenten selbst, gemäss Kapitel 4.1.2

Table 39 - Netzwerkinventar

4.4.4. Verwaltung von Netzwerkkomponenten

M06 - GE-BSA-IT/OT-Admin
Security Patching Prozesse für sämtliche Systeme etablieren Es ist definiert, wer über welche Kanäle über Sicherheitslücken der Systeme informiert wird, wie solche Schwachstellen beurteilt und über deren Relevanz für die Systeme des ASTRA entschieden wird. Es ist geklärt wer über die Umsetzung entscheidet und wer in welcher Zeitfrist die Umsetzung durchführt.
Fragestellungen
• Netzwerk: Gibt es einen Prozess für die Inbetriebnahme/Ersatz von Endgeräten am Netzwerk? • Gibt es einen Prozess für die Ausserbetriebnahme von Endgeräten? • Werden regelmässig Security-Patches auf Netzwerkkomponenten eingespielt?

IST-Zustand
Um Endgeräte ans BKN anzuschliessen, gibt es einen Integrationsprozess von Seiten der GE. Die Geräte werden vom Lieferanten, in Rücksprache mit der GE, ans BKN angeschlossen. Netzwerkendgeräte werden meist von Projekten rückgebaut. Einen konkreten Prozess seitens der GE gibt es nicht. Die Netzwerkgeräte werden mindestens jährlich gepatcht. Dies wurde beim Netzwerk schon von Beginn weg so geplant, zudem gestaltet sich dies wesentlich einfacher als bei den Servern, da einheitliche Produkte eingesetzt werden.
Gegenmassnahme / Bemerkung für die Massnahmentabelle
xxiii. Der GE-BSA-IT/OT-Admin für das jeweilige Endgerät stellt bei der Inbetriebnahme sicher, dass seine Systeme richtig im Netzwerkinventar verknüpft sind. xxiv. Der GE-BSA-IT/OT-Admin für die Zugriffsberechtigungen auf Netzwerkkomponenten (Cisco ISE) stellt sicher, dass beispielsweise Lieferanten, seine Systeme regelmässig aktualisieren. xxv. Der GE-BSA-IT/OT-Admin für die Zugriffsberechtigungen auf Netzwerkkomponenten (Cisco ISE) stellt sicher, dass die Ausserbetriebnahme den Vorgaben des GE-BSA-ISO entspricht. Diese Massnahme ist abhängig von vi.

Table 40 – Verwaltung von Netzwerkkomponenten

4.4.5. Externe Zugänge

M14 - GE-BSA-IT/OT-Admin
Strukturierte, dokumentierte Verbindungen zwischen BSA und Aussenwelt Der (Fern)zugriff ist über den standardisierten Zugriffspunkt zu gewähren (Umgehung von Zugriffsbeschränkung via alternative Wege, z.B. Modem, sind nicht zulässig). Schnittstellen zur Aussenwelt sind auf ein Minimum zu reduzieren, zu strukturieren und aktuell zu dokumentieren. Der Zugriffe in die Prozesszone erfolgt ausschliesslich durch ausgesuchte Protokolle.
Fragestellungen
• Firewall: Sind die externen Netzzugänge mit entsprechenden Firewall-Komponenten vollständig gesichert? • Firewall: Sind Zugriffe über die Firewall restriktiv konfiguriert? • Firewall: Wird der Betrieb der Firewall durch die GE intern erbracht? • Werden auf dem Perimeter der GE WLANs betrieben? • Wer steuert/reglementiert den Zugriff auf das WLAN? • Ist der Zugriff von einem WLAN direkt auf das BSA Netzwerk (IP Netz GE) möglich?
IST-Zustand
Externe Netzzugänge sind nur mittels VPN möglich. Die Firewall wird von der GE betrieben. Man hat das Know-How intern und möchte dies auch nutzen. Die Firewall-Regeln sind auch restriktiv gesetzt. Es gibt keine Wildcard-Regeln. Das Team IT der GE betreibt eigene WLAN-Netzwerke. Die Netzwerke dienen jedoch lediglich als Carrier für VPN Verbindungen ins BKN und sind nicht direkt am BKN angebunden. Trotzdem muss sich jeder Benutzer des WLANs authentifizieren.

Gegenmassnahme / Bemerkung für die Massnahmentabelle
xxvi. Der GE-BSA-IT/OT-Admin für die Zugriffsberechtigungen auf Netzwerkkomponenten (Cisco ISE) stellt sicher, dass externe Zugriffe technisch nur mit Mehrfaktor-Authentisierung möglich sind. Die Freischaltungen erfolgen gemäss Kapitel 3.1.4.2

Table 41 – Externe Zugänge

4.5. Zutritt

INF.1 Allgemeines Gebäude
INF.2 Rechenzentren sowie Serverraum
INF.3 Elektrotechnische Verkabelung
INF.4 IT/OT-Verkabelung
INF.5 Raum sowie Schrank für technische Infrastruktur
INF.6 Datenträgerarchiv
INF.7 Büroarbeitsplatz
INF.8 Häuslicher Arbeitsplatz
INF.9 Mobiler Arbeitsplatz
INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume

M18 – GE-L-S&S
M18 - Physischer Zutritt Der physische Zutritt zu technischen Räumen und der IT/OT-Infrastruktur darf für unbefugte nicht zugänglich sein. → Schliesskonzept
Fragestellungen
• Ist der physische Zutritt zu den Räumen eingeschränkt? • Haben nur berechtigte Personen physischen Zutritt zu den Systemen? • Ist der Zutritt zu zentralen Räumen mit übergeordneten IT/OT-Systemen eingeschränkt, überwacht und protokolliert? • Wie ist die Freigabe für den Zutritt zu zentralen Räumen mit übergeordneten IT/OT-Systemen geregelt (z.B. Zutritt nur in Begleitung von IT/OT-Personal, Bewilligung durch IT/OT-Verantwortlichen, etc.)? • Wird unterschieden wer Zugriff auf Schränke mit zentraler IT/OT- oder Netzwerk-Infrastruktur hat?
IST-Zustand
Der physische Zutritt ist wie folgt eingeschränkt: • Allgemeines Gebäude: Badge • Rechenzentrum sowie Serverraum: Badge oder Schlüssel • Elektrotechnische Verkabelung / IT/OT Verkabelung: in den Räumlichkeiten zugänglich; Kabel sind zwischen den Gebäuden geschützt verlegt (Vorgabe) • Raum sowie Schrank für technische Infrastruktur: mindestens Sicherheitsschloss vorgeschrieben • Datenträgerarchiv: Schlüssel • Büroarbeitsplatz: nur mit Badge • Häuslicher Arbeitsplatz: 2FA (2-Faktor-Authentifizierung und VPN • Mobiler Arbeitsplatz: 2FA und VPN

• Besprechungs-, Veranstaltungs- und Schulungsräume: entweder GE-Büro oder Polizei Die Badges sind Passepartout für alle Badge-Zutritte. Diese besitzen alle technischen Mitarbeiter der GE. Externe Lieferanten können einen bei der GE beantragen, dieser kann für gewisse Zeiten freigeschaltet werden. Die Schlüssel werden einzeln an die Mitarbeiter ausgegeben. Die externen Lieferanten können ebenfalls einzelne Schlüssel für gewisse Zeiträume beantragen. Die Zutrittsverwaltung wird von der Zentrale der GE gemacht. Sämtliche Badge-Leser protokollieren ihre Aktivitäten. Die Benutzung der Schlüssel kann nicht überwacht werden. Um einen Badge-Zugang zu erhalten, muss der Lieferant einen Antrag bei der GE stellen und dieser muss bewilligt werden. Die Schlüssel werden gemäss Schliesskonzept der GE vergeben. Schränke mit zentraler IT/OT-Infrastruktur besitzen ein zusätzliches Schloss, um den Schrank zu öffnen. Schränke mit weniger kritischer Infrastruktur sind nicht speziell gesichert, hier vertraut man auf den Zutrittsschutz des Raumes.
Gegenmassnahme / Bemerkung für die Massnahmentabelle
xxvii. Der GE-BSA-IT/OT-Operation für das Schliesssystem, der GE-L-S&S, stellt die korrekte Funktion des Systems sicher und handelt gemäss dem Schliesskonzept der GE.

Table 42 – Physischer Zutritt

Änderungsverzeichnis

Version	Datum	Ersteller	Bemerkung
0.1	24.11.2021	TBA-GEVII, R. Züger	Grundstruktur um erarbeitete Daten abfüllen zu können.
0.2	06.12.2021	Robert Klein, bw digitronik ag	Kapitel 1 und 2
0.3	10.12.2021	Robert Klein, bw digitronik ag	Kapitel 3.1 bis 3.3
0.4	16.12.2021	Robert Klein, bw digitronik ag	Kapitel 3.4 und 3.5
0.5	20.12.2021	Robert Klein, bw digitronik ag	Rückmeldung zu Kapitel 3 einarbeiten
0.6	21.12.2021	TBA-GEVII, F. Caspani	Kapitel 4
0.7	22.12.2021	TBA-GEVII, F. Caspani Robert Klein, bw digitronik ag	Einarbeitung Feedback GE-L-IT
1.0	22.12.2021	TBA-GEVII, F. Caspani	Aussortieren Abkürzungsverzeichnis
1.1	03.01.2022	TBA-GEVII, F. Caspani	Liste der Gegenmassnahmen im Kap.4 Nummerierung korrigiert
1.2	24.01.2022	TBA-GEVII, R. Züger	Komplette Review und kleinere Anpassungen (Präzisierungen / Textkorrekturen)
1.3	27.01.2022	TBA-GEVII, F. Caspani	Review übernehmen, Dokumentparameter anpassen, Dokument formatieren
1.4	08.11.2022	TBA-GEVII, F. Caspani	Kleinere Korrekturen (Text, Grammatik, Formatierung)

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung
AD	Active Directory
ASTRA	Bundesamt für Strassen
BHU	Bauherrenunterstützung
BKN	Betriebskommunikationsnetzwerk
BR	Bereichsrechner
BSA	Betriebs- und Sicherheitsausrüstung
CAB	Change-Advisory-Board (Entscheidungsgremium)
DAW	Dokumentation des ausgeführten Werks
FaSKob	ASTRA Fachspezialist Kontrolle Betrieb
GBA	Grossbildanzeige
GE VII	Gebietseinheit VII
HW	Hardware
IT Basis	Betrieb und Pflege von Rechnern, Netzwerkkomponenten und Betriebssystemen
Kapo ZH	Kantonspolizei Zürich
NAS	Network Attached Storage
OS	Operating System, Betriebssystem
SPS	Speicherprogrammierbare Steuerung
UeLS	Übergeordnetes Leitsystem
VM	Virtual Machine
VMZ-CH	Verkehrs Management Zentrale Schweiz
VPN	Virtual Private Network
ZTS	Zentrales Testsystem