Die Autobahn

Branchenspezifischer Sicherheitsstandard für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn

(B3S Bundesautobahn oder B3S BAB)

von

Die Autobahn GmbH des Bundes

Version 1.0
Stand: 01.07.2022

Allgemeine Informationen zum vorliegenden Dokument

Bezeichnung	Inhalt	Bearbeitungshinweis
Name des Dokuments (Titel)	Branchenspezifischer Sicherheitsstandard für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn	[Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.]
Herausgeber	Die Autobahn GmbH des Bundes Frank Felde	
Autoren	Autobahn GmbH: Bresser, Ingo; Ehlers, Boris; Estel, Anja; Mahnke, Jens; Meier, Steffen; Mikesic, Tania; Müller-Drenkberg, Jörg; Preisner, Karsten; Rupieper, Nico; Schüttler, Josef; Walter, Stefan	
Nummer des B3S		[Sofern bereits vom BSI vergeben]
Version	1.0	
Status	freigegeben, öffentlich	
Revisionszyklus	alle zwei Jahre	[Revisionszyklus alle 1, 2, 3 Jahre]

Änderungshistorie

Version	Datum	Änderung	Bearbeitet von
0.1 – 0.71	13.12.2021	Initiale Erstellung	Die Autobahn GmbH des Bundes
0.72	22.03.2022	Finaler Entwurf	Tania Mikesic, Stefan Walter, Nico Rupieper / Die Autobahn GmbH des Bundes
1.0	01.07.2022	Freigabe	Frank Felde / Die Autobahn GmbH des Bundes

Die Autobahn

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abkürzung	Erläuterung
AGAP	Alarm- und Gefahrenabwehrpläne
B3S	Branchenspezifischer Sicherheitsstandard
BAB	Bundesautobahnen
BASt	Bundesanstalt für Straßenwesen
BMDV	Bundesministerium für Digitales und Verkehr
BMVBS	Bundesministerium für Verkehr, Bau und Stadtentwicklung
BMVI	Bundesministerium für Verkehr und digitale Infrastrukturen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
CMDB	Configuration Management Database
DIN	Deutsches Institut für Normung
dWiSta	Dynamischer Wegweiser mit integrierten Stauinformationen
EABT	Empfehlungen für die Ausstattung und den Betrieb von Straßentunneln
FStrG	Bundesfernstraßengesetz
GmbH	Gesellschaft mit beschränkter Haftung
IEC	International Electrotechnical Commission
ISMS	Informationssicherheitsmanagementsystem
ISMS-Tool	Informationssicherheitsmanagement-Tool
IT	Informationstechnik

ITSiG	IT-Sicherheitsgesetz
kDL	Kritische Dienstleistung
kDL BAB	Kritische Dienstleistung Bundesautobahn
KRITIS	Kritische Infrastruktur
KRITIS BAB	Kritische Infrastruktur Bundesautobahn
KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen
MARZ	Merkblatt für die Ausstattung von Verkehrsrechnerzentralen und Unterzentralen
PDCA	Plan-Do-Check-Act
RABT	Richtlinien für die Ausstattung und den Betrieb von Straßentunneln
TC57	IEC TC 57
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Technischen Lieferbedingungen für Streckenstationen
UP KRITIS	Öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen
USV	Unterbrechungsfreie Stromversorgung
VBA	Verkehrsbeeinflussungsanlage

1 Einleitung

Am 25. Juli 2015 trat das IT-Sicherheitsgesetz (ITSiG) in Kraft. Dieses Gesetz modifizierte als sogenanntes Artikelgesetz mehrere bestehende Gesetze, auch das BSI-Gesetz (BSIG, siehe Kapitel 9, Nr. 4a).

Laut BSIG sind Kritische Infrastrukturen Anlagen oder Teile davon, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Nach § 8a (1) BSIG müssen deshalb Betreiber Kritischer Infrastrukturen organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten und Prozesse treffen.

Gemäß § 8a (2) Satz 1 BSIG können Betreiber Kritischer Infrastrukturen branchenspezifische Sicherheitsstandards zur Gewährleistung dieser Anforderungen nach § 8a (1) BSIG vorschlagen.

Das vorliegende Dokument ist als branchenspezifischer Sicherheitsstandard für die Betreiber von Bundesautobahnen in Deutschland, kurz B3S BAB, entwickelt und definiert zusammen mit der Anwendung des Dokuments “IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn” (siehe Kapitel 9, Nr. 1) eine mögliche Umsetzung der Anforderung aus § 8a (1) BSIG. Es ist als Rahmenwerk aufgebaut und orientiert sich am IT-Grundschutz mit den BSI-Standards 200-1, 200-2, 200-3 und 100-4 (siehe Kapitel 9, Nr. 2d-2g) und dem IT-Grundschutz-Kompendium 2021 (siehe Kapitel 9, Nr. 2h).

Die Struktur dieses Dokumentes folgt der „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG“ in der Version 1.1 vom September 2021 (siehe Kapitel 9, Nr. 2a).

2 Anwendung

Dieser B3S dient zu einer angemessenen Behandlung aller relevanten Themen zur Umsetzung der gesetzlichen Anforderungen nach § 8a (1) BSIG. Die vollständige Umsetzung dieses B3S ist geeignet, die gesetzlichen Anforderungen nach § 8a (1) BSIG zu erfüllen.

Die Anwendung dieses B3S setzt die Anwendung des "IT-Grundschutzprofil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn" (siehe Kapitel 9, Nr. 1) verpflichtend voraus. Nur die Umsetzung der Anforderungen aus beiden Dokumenten genügt den gesetzlichen Anforderungen.

Zusätzlich zu den Vorgaben des § 8a Abs.1 BSIG werden im § 8a Abs. 1a BSIG Vorgaben für den Einsatz von Systemen zur Angriffserkennung gestellt, die ab dem 1. Mai 2023 erfüllt werden müssen. Die Umsetzung dieser Vorgaben ist nicht Bestandteil dieses B3S. Betreiber Kritischer Infrastrukturen nach dem BSIG müssen diese Vorgaben individuell umsetzen.

2.1 gesetzlicher Rahmen

Den gesetzlichen Umfang für diesen B3S bestimmt die Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV, siehe Kapitel 9, Nr. 4b). Sie bestimmt die Anlagen der Verkehrssteuerungs- und Leitsysteme im Sinne des BSIG §10 (1) für den Sektor Transport und Verkehr als Kritische Infrastruktur (kurz: KRITIS BAB) mit dem Schwellwert Bundesautobahn (vergleiche BSI-KritisV, Anhang 7, Teil 3, Spalte B in Zeile 1.4.1.).

Die Betreiber dieser Anlagen sind demnach Betreiber Kritischer Infrastrukturen. Gemäß BSIG §2 (2) gehören alle informationstechnischen Systeme, Komponenten und Prozesse, die die Anwendung und den Betrieb der Anlagen von Verkehrssteuerungs- und Leitsystemen der Bundesautobahnen umfassen, dazu.

2.2 Anwendungsbereich

Dieser B3S wird auf alle informationstechnischen Systeme, Komponenten und Prozesse des Betreibers angewendet, die maßgeblich für die Funktionsfähigkeit der Anlagen von Verkehrssteuerungs- und Leitsystemen für das Bundesautobahnnetz sind. Damit definiert der Anwendungsbereich die „direkte Einflussnahme auf die Leichtigkeit und Sicherheit des (Personen- und Güter-) Verkehrs auf dem Netz der Bundesautobahnen" als die kritische Dienstleistung Bundesautobahn, kurz kDL BAB.

2.3 Beschreibung des Anwendungsbereiches

In den folgenden Unterkapiteln sind die maßgeblichen informationstechnischen Systeme, Komponenten und Prozesse der KRITIS BAB genauer beschrieben.

Das “IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn” (siehe Kapitel 9, Nr. 1), das zu diesem B3S gehört, verdeutlicht diese Beschreibungen und zeigt auf Profilebene die Branchenspezifika auf.

2.3.1 **Prozesse**

Der Anwendungsbereich umfasst die folgenden Geschäftsprozesse:

- operatives Verkehrsmanagement
  Bestandteile dieses Prozesses sind das Bedienen von Verkehrsbeeinflussungsanlagen, das Bedienen tunnelbetrieblicher Einrichtungen, die Bereitstellung von Verkehrsinformationen und die Durchführung des Störfall- und Ereignismanagements.
- Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur
  Hierunter fallen Prozesse zur Systemüberwachung, Wartung und Instandsetzung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur.
- Durchführung des Straßenbetriebsdienstes
  Teilprozesse sind die Durchführung der Streckenwartung/-kontrolle, die Durchführung des Winterdienstes und die Durchführung von Sofortmaßnahmen am Straßenkörper oder zur Verkehrssicherung aufgrund unvorhergesehener Ereignisse.

2.3.2 **Organisation**

Der Betreiber ist zuständig für ein Autobahnnetz oder Teile des Autobahnnetzes, die sich über das gesamte Bundesgebiet erstrecken können. Je nach Unternehmensgröße des Betreibers können Zuständigkeiten und die oben genannten Prozesse in Abhängigkeit der jeweiligen Aufbauorganisation über viele Standorte verteilt sein. An einem Standort gibt es eventuell keine, eine oder mehrere Organisationseinheiten, die jede für sich KRITIS BAB oder Teile der KRITIS BAB betreiben oder die kDL BAB bereitstellen.

2.3.3 **Personal**

Beim Personal kann unterschieden werden in diejenigen Personen, die

- die Anlagen von Verkehrssteuerungs- und Leitsystemen bedienen und für die bestimmungsgemäße Anwendung der Anlagen – Verkehr lenken und steuern - zuständig sind.
- die Anlagen von Verkehrssteuerungs- und Leitsystemen instand halten und für den technischen Betrieb der Anlagen zuständig sind.

2.3.4 **Technik**

Es gehören alle Komponenten, deren Ausfall oder Beeinträchtigung direkt die Funktionsfähigkeit der Verkehrssteuerungs- und Leitsysteme des Betreibers beeinflussen, zum Anwendungsbereich:

Anwendungen, Systeme, Hardware, Software, Kommunikationsverbindungen, industrielle Komponenten, Netzwerke und die dafür benötigten TK-Komponenten, etc. Vergleiche hierzu auch Kapitel 2 Strukturanalyse des genannten IT-Grundschutz-Profils (siehe Kapitel 9, Nr. 1).

Dabei lassen sich die technischen Komponenten im Wesentlichen in drei Kategorien einteilen:

- Betriebs- und verkehrstechnische Tunnelausstattung
- Verkehrssteuerungs- und -leittechnik
- die dafür notwendige Kommunikationstechnik

Diese können bundesweit verteilt, die dezentralen Anlagen großer Betreiber vielzählig und sehr unterschiedlich sein.

2.3.5 **Standorte**

Gebäude, Räume und Betriebsstätten, in denen KRITIS BAB betrieben oder angewendet werden, gehören ebenfalls zum Anwendungsbereich.

Vergleiche hierzu Kapitel 2.6 des genannten IT-Grundschutz-Profils (siehe Kapitel 9, Nr. 1).

Dabei lassen sich folgende Beispiele für Standorte ableiten:

- Verkehrszentralen
  In diesen Gebäuden oder Räumlichkeiten wird das Verkehrsmanagement umgesetzt.
- Tunnelleitzentralen
  In diesen Gebäuden oder Räumlichkeiten werden die Leistungen zur zentralen Steuerung und Lenkung des Verkehrs in Tunneln erbracht.
- Betriebszentralen
  Diese Gebäude oder Räumlichkeiten umfassen oft die beiden Kerngeschäfte zur Verkehrsbeeinflussung (auf offener Strecke) und Tunnel.

2.3.6 **Intern erbrachte Leistungen**

Wird der Betrieb von Anwendungen, Systemen oder Komponenten, die im Anwendungsbereich dieses B3S liegen, unterstützend in einer Organisationseinheit als Service durchgeführt, dann sollte die Anwendung und Umsetzung dieses B3S durch entsprechende interne Vereinbarungen (OLA/SLA) sichergestellt werden.

2.3.7 **Extern erbrachte Leistungen**

Wird der Betrieb von Anwendungen, Systemen oder Komponenten, die im Anwendungsbereich dieses B3S liegen, nicht selbst vom Betreiber durchgeführt, sondern von Dritten, beispielsweise im Rahmen von Outsourcing, so ist die Anwendung und Umsetzung dieses B3S durch entsprechende Vereinbarungen sicherzustellen. Die Verantwortung in Bezug

auf die Einhaltung dieses B3S verbleibt beim Betreiber (z.B. durch Abschluss einer Dienstleistervereinbarung, deren Inhalt und Umsetzung zu prüfen ist).

Die Wartung und Instandhaltung von betriebs- und verkehrstechnischen Tunnelausstattungen sowie von Verkehrsbeeinflussungsanlagen wird vom Betreiber nicht selten an Dritte vergeben. Der Dritte übernimmt damit die Bewahrung des Ist- bzw. die Wiederherstellung des Sollzustandes dieser Anlagen. Die Anwendung und Umsetzung dieses B3S ist deshalb für die beauftragten Dritten verbindlich und in den entsprechenden Wartungs- und Instandhaltungsverträgen zu fixieren. Der Betreiber selbst bleibt in der Verantwortung über diese extern erbrachten Leistungen.

2.4 Außerhalb des Anwendungsbereiches

Nicht zum Anwendungsbereich des vorliegenden B3S gehören:

- das Autobahnnetz, wenn dort keine Installationen für Verkehrssteuerungs- und Leitsysteme vorhanden sind.
- an das Autobahnnetz grenzende, dezentrale (Einzel-)Systeme wie zum Beispiel Lichtsignalanlagen.
  Hinweis: Sollten sich z.B. Lichtsignalanlagen als Schnittstelle zwischen dem Autobahnnetz und weiteren Informationsverbünden befinden, die sich nicht im Zuständigkeitsbereich des Autobahnbetreibers befinden, ist zu prüfen, wie die Netze physisch oder logisch getrennt sind. Ist dies nicht möglich sind diese Anlagen in den zu betrachtenden Informationsverbund der Autobahn zu integrieren. In diesem Fall kann der Branchenspezifische Sicherheitsstandard für die „Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr“ ergänzend herangezogen werden.
- Abgegrenzte Systeme oder Dienste für Dritte, z.B. Informationsbereitstellung für Dritte.

3 Vorgaben und Regelungen

Hier werden spezifische Regelungen für Betreiber von Verkehrssteuerungs- und Leitsystemen auf BAB aufgeführt, die direkten Einfluss auf den B3S haben (vergleiche auch jeweils Kapitel 9).

Allerdings wird auf eine abschließende Aufzählung allgemein anerkannter, gültiger, technischer Normen und DIN verzichtet.

3.1 Gesetzliche Vorgaben

3.1.1 **BSI-Gesetz**

Das BSIG ist die gesetzliche Grundlage für Kritische Infrastrukturen und §8a für diesen B3S.

3.1.2 **BSI-Kritis-Verordnung**

Die Kritis-Verordnung definiert gemäß §10 BSIG Kritische Infrastrukturen.

3.1.3 **Bundesfernstraßengesetz (FStrG)**

Das FStrG definiert in § 1 Absatz 4 Nummer 1, 3 und 4 Einrichtungen, die zu einer Anlage oder ein System zur Verkehrsbeeinflussung im Straßenverkehr gehören. Die KritisV greift diese Definition im Anhang 7, Teil 1 Nr. 1, 1.20 zur Definition von Verkehrssteuerungs- und Leitsystem auf.

3.2 Sicherheitsstandards und IT-spezifische Regelwerke

3.2.1 **BSI**

Die BSI-Standards 200-1, 200-2, 200-3 und 100-4 definieren zusammen mit dem Kompendium 2021 die IT-Grundschutz-Vorgehensweise.

3.2.2 **IEC 62443**

Die internationale Normenreihe bestimmt die Sicherheitsanforderungen für industrielle Steuerungs- und Automatisierungssysteme.

3.3 Betriebs- und verkehrstechnische Tunnelausstattung

3.3.1 **EABT-80/100**

Grundlage für das (Verkehrs-)Sicherheitsniveau von Tunneln sind die in der Bundesrepublik Deutschland geltenden „Empfehlungen für die Ausstattung und den Betrieb von Straßentunneln“ (EABT, siehe Kapitel 9, Nr. 5b). Diese Empfehlungen beinhalten wesentliche

Anforderungen an Anlagen und IT-Systeme. Die EABT-80/100, Ausgabe 2019 repräsentieren den aktuellen Stand der Technik.

3.3.2 **RABT**

Die „Richtlinien für die Ausstattung und den Betrieb von Straßentunneln“ (RABT, siehe Kapitel 9, Nr. 5a) sind mit der Ausgabe 2006 durch ein Allgemeines Rundschreiben des BMVBS für die Bundesfernstraßen verbindlich eingeführt.

3.4 Verkehrssteuerungs- und -leittechnik

3.4.1 **TLS**

Die „Technischen Lieferbedingungen für Streckenstationen“ (TLS, siehe Kapitel 9, Nr. 5c) beschreiben den strukturellen bzw. hierarchischen Aufbau des Gesamtsystems von verkehrstelematischen Einrichtungen. Sie regeln weiterhin die Datenübertragung zwischen den einzelnen Systemkomponenten bzw. Systemebenen. In den TLS sind damit die Kommunikationsinhalte als auch die anzuwendenden Protokolle (TC57 und TCP/IP) festgelegt. Die TLS 2012 sind durch ein Allgemeines Rundschreiben des BMVBS/BMVI zur verbindlichen Anwendung im Bereich der Bundesfernstraßen eingeführt.

3.4.2 **MARZ**

Im „Merkblatt für die Ausstattung von Verkehrsrechnerzentralen und Unterzentralen“ (MARZ, siehe Kapitel 9, Nr. 5d) sind die notwendigen Festlegungen für Unterzentralen und Verkehrsrechnerzentralen für Bundesfernstraßen enthalten:

- Aufgaben der Zentralen,
- Beschreibung der verkehrstechnischen Anforderungen,
- Systemarchitekturentwurf aus fachlicher Sicht sowie grundsätzliche funktionale und nichtfunktionale Anforderungen an Hard- und Software,
- Art der Kommunikation innerhalb des VRZ-/UZ-Systems sowie zwischen Zentralen und mit Dritten.

Das MARZ 2018 ist im Bereich der Bundesfernstraßen verbindlich anzuwenden.

4 Schutzziele

4.1 KRITIS-Schutzziele

Im Vordergrund der Betrachtung in diesem B3S steht die Versorgung der Allgemeinheit mit Leistungen zum Transport von Personen und Gütern, hier als kDL BAB definierte kritische Dienstleistung Bundesautobahn: Die direkte Einflussnahme auf

- die Leichtigkeit des Verkehrs und
- die Sicherheit des Verkehrs

auf Bundesautobahnen mit Hilfe von Verkehrssteuerungs- und Leitsystemen (siehe Kapitel 2.2).

Diese Dienstleistung ist eine stark informationsorientierte Dienstleistung mit hohem Automatisierungsgrad: Verkehrssteuerung- und -lenkung hängt davon ab, zu welchem Zeitpunkt bestimmte Informationen an welchem Ort oder in welchem Umfeld vorliegen. Die gewonnenen Informationen werden weiterverarbeitet, so dass sie regional zur

- Verbesserung des Verkehrsflusses oder
- Erhöhung der Verkehrssicherheit

genutzt werden können. Nutzer dieser Dienstleistung bzw. Verbesserungseffekte sind die Verkehrsteilnehmer auf den Autobahnen.

Die kDL BAB der Verkehrsoptimierung und Überwachung wird benötigt, um das „normale“ Niveau der Leichtigkeit und Sicherheit des Verkehrs auf BAB herzustellen und zu halten. Ist die kritische Dienstleistung beeinträchtigt, kann sich dies negativ auf die Leichtigkeit und Sicherheit auswirken.

Mit Ausnahme der Autobahntunnel ab einer Länge von 400m und einer Planungsgeschwindigkeit von 80 oder 100 km/h, bei denen eine Sperranlage gemäß der EABT 80-100 (siehe Kapitel 9, Nr. 5b) erforderlich ist, kann eine Unterbrechung der kritischen Dienstleistung durch eine ungeplante Sperrung des Tunnels eintreten. Für diesen Fall sind auf Maßnahmenseite großräumige und lokale Umleitungen in Alarm- und Gefahrenabwehrplänen (AGAP) festzulegen.

Im „IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn“ (siehe Kapitel 9, Nr. 1) werden alle Komponenten und Schnittstellen, welche im Geltungsbereich für den Betrieb der Tunnel notwendig sind, definiert.

Die KRITIS-Schutzziele der kDL BAB sind daher alle physischen, technischen und organisatorischen Objekte, aus denen sich die KRITIS BAB zusammensetzt und die in Kapitel 2.3 ausführlicher beschrieben sind.

4.2 IT-Schutzziele

Die IT-Schutzziele leiten sich aus den oben genannten Eigenschaften der kDL BAB - stark informationsorientierte Dienstleistung mit hohem Automatisierungsgrad - ab. Die Grundwerte Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von Informationen, Geschäftsprozessen, Anwendungen und IT-Systemen, die für die Funktionsfähigkeit der Kritischen Infrastruktur BAB maßgeblich sind, müssen gewährleistet sein. Wobei

- **Verfügbarkeit**
  bedeutet, dass Informationen, Systeme, Komponenten und Prozesse der relevanten Anlagen unter Einhaltung der Anforderungen im vorgegebenen Umfang zur Verfügung stehen.
  Bsp.: Die notwendigen Daten, IT-Systeme, Komponenten und Prozesse für die digitale Steuerung und Lenkung des Verkehrs auf dem Autobahnnetz sind verfügbar und die technischen Anlagen sind funktionsfähig.
- **Vertraulichkeit**
  bedeutet, dass vertrauliche Daten und Informationen ausschließlich Befugten zur Verfügung gestellt werden dürfen.
  Bsp.: Unverschlüsselte Informationen und Daten der verwendeten Steuerungs- und Lenkungs-Anlagen werden vor unbefugter Freigabe an Dritte geschützt.
- **Integrität und Authentizität**
  bedeuten, dass die Korrektheit (Unversehrtheit) der Informationen und die korrekte Funktionsfähigkeit der Systeme sichergestellt ist und diese nachweislich von der Quelle erstellt wurden.
  Bsp.: Der Autobahnverkehr wird auf Basis verbindlicher, unverfälschter Werte zuverlässig gesteuert und gelenkt, deren Quelle eindeutig bekannt und prüfbar ist.

Der Schutz dieser Grundwerte abgebildet auf den Betrieb der KRITIS BAB ergeben die branchenspezifischen IT-Schutzziele. Hierbei ist mindestens zu berücksichtigen, dass die kDL in hohem Maße von Informationen abhängig ist. Die Schutzziele Integrität und Authentizität spielen daher eine wesentliche Rolle, was sich durch höhere Sicherheitsanforderungen für diese Grundwerte im Prozess „operatives Verkehrsmanagement“ ausdrücken muss als z. B. im Vergleich zur Verfügbarkeit (vergleiche IT-Grundschutzprofil, Kapitel 3.1 bzw. 3.1.3).

Der Begriff „Leitzentrale“, der hier im Zusammenhang mit dem B3S genannt wird, bezieht sich ausschließlich auf den Verkehr. In Abgrenzung dazu gibt es die „klassischen“

Rettungsleitstellen, die die Rettungsdienste z. B. der Polizei und Feuerwehr unterstützen.

Hierauf aufbauend sind bei Bedarf im Rahmen des ISMS anlagenspezifische Ausprägungen der oben beschriebenen Schutzziele vom Betreiber abzuleiten bzw. zu erfassen und für IT-Systeme, Komponenten und Prozesse zu berücksichtigen.

5 Branchenspezifische Gefährdungslage

5.1 All-Gefahrenansatz

Im Rahmen des All-Gefahrenansatzes müssen alle relevanten Bedrohungen und Gefährdungen identifiziert werden. Aus den Gefährdungen werden Risiken für die kDL BAB bestimmt, die im Rahmen der Risikoanalyse bewertet und behandelt werden müssen.

Der All-Gefahrenansatz beinhaltet mindestens die Identifikation der relevanten elementaren Gefährdungen nach dem BSI-Standard 200-3 und aufbauend darauf die Ermittlung der möglichen branchenspezifischen Gefährdungen (zusätzliche Gefährdungen).

Die vorgegebenen Bedrohungsszenarien aus dem Abschnitt 5.3 aus der „Orientierungshilfe B3S“ (Stand: September 2021, Version 1.1) zum „Stand der Technik“ müssen dabei mindestens abgedeckt sein.

Kapitel	Bedrohungsszenario
B 1	Ausnutzung von Zero-Day Schwachstellen
B 2	Schadsoftware in E-Mail-Anhängen
B 3	Advanced Persistent Threat (APT)-Angriffe
B 4	Ransomware
B 5	Daten-Exfiltration

Tabelle 1: Bedrohungsszenarien

5.2 Branchenspezifische Relevanz von Bedrohungen und Schwachstellen

Die KRITIS BAB beinhaltet aufgrund ihrer Zusammensetzung folgende typische Gefährdungspotentiale:

Besonderheiten der kDL BAB bzw. KRITIS BAB	Branchenspezifische Gefährdungen
(bundesweit) verteilte Organisation, verteilte Prozesse, verteilte Aufgaben	Organisatorische, räumliche und zeitliche Risiken

Besonderheiten der kDL BAB bzw. KRITIS BAB	Branchenspezifische Gefährdungen
(bundesweit) verteilte Technik, sehr große Anzahl Anlagen, weit verzweigtes Datennetzwerk	betriebs- und anlagentechnische Gefährdungen, Wartungs- und Instandsetzungsrisiken, Gefährdungen bezüglich Abhängigkeit von Dienstleistern, zeitliche Risiken
(bundesweit) verteilte Gebäude	Unberechtigter Zutritt, unberechtigter Zugang unberechtigter Zugriff
Unbeaufsichtigte Gebäude, z. B. Kabelhäuser	Einbruch, Diebstahl, Beschädigungen, Zerstörung, Vandalismus Unbefugtes Eindringen in Räumlichkeiten, unbefugtes Eindringen in IT-Systeme
Einsatz von Automatisierungstechnik	höheres, über die Gefährdungen von Office-IT hinausgehendes Gefährdungspotential

Tabelle 2: Typische Gefährdungspotentiale

Die nachfolgende Tabelle führt beispielhaft Gefährdungen für informationstechnische Systeme, Komponenten oder Prozesse an:

Nr.	Branchenspezifische Gefährdung	Relevanz für kDL BAB oder KRITIS BAB
1	Elementare Gefährdungen - Naturkatastrophen Beispiele Hochwasser Blitzeinschlag Erdbeben	Naturgefahren können zu Schädigung, Zerstörung, Ausfall oder Teilausfall der Verkehrssteuerungs- und Leitsysteme führen. Z. B. verursacht Hochwasser Beeinträchtigung oder Ausfall einer Verkehrsbeeinflussungsanlage (VBA).
2	Elementare Gefährdungen – Höhere Gewalt	Höhere Gewalt kann zur Beeinträchtigung der Verfügbarkeit

Nr.	Branchenspezifische Gefährdung	Relevanz für kDL BAB oder KRITIS BAB
	Beispiele Ausfall von (externen) Dienstleistern Feuer Pandemie	von Personal und der Verkehrssteuerungs- und Leitsysteme führen. Z. B. verursacht Feuer Ausfall von Server- und Automatisierungssystemen, die die Sperrung von Tunnelabschnitten zur Folge haben.
3	Elementare Gefährdungen - Organisatorische Gefährdungen Beispiele Fehlende organisatorische Vorgaben Mangelnde Qualifikation Nicht-Verfügbarkeit von Personal	Organisatorische Mängel können zu Schädigung, Zerstörung, Ausfall oder Teilausfall der Verkehrssteuerungs- und Leitsysteme und menschlichen Fehlhandlungen führen. Z. B. muss für Feuerlöscher eine regelmäßige Wartung festgelegt und bekannt gemacht werden. Ist das nicht der Fall, kann die Funktionsfähigkeit im Brandfall nicht sichergestellt werden.
4	Elementare Gefährdungen - Menschliche Fehlhandlungen Beispiele Fehlbedienung Administration Mangelnde Qualifikation Unachtsame Verkehrsteilnehmer (Unfall auf BAB)	Menschliche Fehlhandlungen können zu Schädigung, Zerstörung, Ausfall oder Teilausfall der Verkehrssteuerungs- und Leitsysteme führen. Z. B. verursacht der Tanklaster-Unfall einen Großbrand, bei dem Wechselverkehrszeichen zerstört werden.
5	Technisches Versagen Beispiele Versagen von Hardware	Technisches Versagen führt zu Schädigung, Zerstörung, Ausfall oder Teilausfall der Verkehrssteuerungs- und Leitsysteme.

Nr.	Branchenspezifische Gefährdung	Relevanz für kDL BAB oder KRITIS BAB
	Überlastung von Systemen Fehlverhalten von Systemen	Z. B. kann Hardware aufgrund des Alters oder dauerhaft zu hoher Belastung versagen.
6	Gezielte IT-Angriffe Beispiele Diebstahl, Beschädigung von Geräten Technische Angriffe Datendiebstahl und -manipulation	IT-Angriffe führen zu Schädigung, Zerstörung, Ausfall oder Teilausfall der Verkehrssteuerungs- und Leitsysteme. Z. B. durch Ransomware werden über das Netz IT-Systeme funktionsunfähig.
7	Krisensituation Beispiele extreme und unvorhergesehene Unwetterereignisse	Unwetterereignisse können zu Schädigung, Zerstörung, Ausfall oder Teilausfall der Verkehrssteuerungs- und Leitsysteme führen. Z. B. irreparable Wasserschäden in Technik- oder Netzanschlussräumen, Beschädigung von VBAs inklusive dWiSta durch Flutkatastrophe
8	Gefährdungen für die BAB Großschadenslagen in der Nähe Katastrophen im Umfeld Beispiele Großbrand Reifenlager neben BAB Tanklaster-Unfall Explosion neben BAB	Gefährdungen BAB können zu Schädigung, Zerstörung, Ausfall oder Teilausfall der Verkehrssteuerungs- und Leitsysteme führen. Z. B. Zerstörung einer VBA durch Explosion im Chemiepark

Tabelle 3: Gefährdungen für informationstechnische Systeme, Komponenten oder Prozesse

5.3 Gefährdungen und Ereignisse ohne Relevanz für den B3S

Beeinträchtigungen der Verfügbarkeit des Autobahnnetzes (Verkehrsinfrastruktur) sind nicht zwingend mit einem Schaden oder einer ungeplanten Beeinträchtigung der kDL BAB verbunden.

Beispiele

Straßensperrung oder Spurreduktionen infolge von Unfällen, liegengebliebenen Fahrzeugen, Personen auf der Fahrbahn, Bränden, besonderen Wettersituationen, Naturkatastrophen, aber auch geplante Aktionen wie Straßenarbeiten oder Baustellen (sofern der Anlass keine Auswirkung auf die KRITIS BAB hat).

5.4 Änderungen der Gefährdungslage

Die zu behandelnden relevanten Gefährdungen sind kontinuierlich zu überprüfen und ggf. anzupassen oder zu ergänzen. Dabei müssen insbesondere berücksichtigt werden:

- Änderungen der allgemeinen Gefährdungslage (neu hinzugekommene Angriffsarten oder Angreifer, Neuausrichtung von Angreifern etc.)
- Änderungen der branchenspezifischen Gefährdungslage
- Bekannt gewordene neue Schwachstellen
- Änderungen der Gefährdungslage durch Veränderungen an der Systemarchitektur bzw. durch den technischen Fortschritt
- Anderweitige Änderungen an der für die Funktionsfähigkeit der maßgeblichen IT oder deren Schnittstellen

Die Überprüfung der Gefährdungslage sollte direkt bei Veränderungen der Sicherheitslage oder Anpassungen an den Systemen erfolgen, muss spätestens bei der intervallmäßigen Neubewertung alle 12 Monate durchgeführt werden.

6 Risikoanalyse

Die Risikoanalyse für die Kritische Infrastruktur KRITIS BAB muss auf Basis des BSI-Standards 200-3 (siehe Kapitel 9, Nr. 2f) erfolgen und beschreibt, unabhängig von anderen ISO-Normen, den kompletten Prozess für die geeignete Beurteilung (Identifizierung, Einschätzung und Bewertung) und die Behandlung aller für die KRITIS BAB relevanten Risiken.

Um den Stand der Technik gemäß §8a Abs. 1 BSIG einzuhalten, muss der BSI-Standard 200-3 vollständig berücksichtigt werden.

Abbildung 1: Prozess der Risikoanalyse nach BSI-Standard 200-3 (vereinfachte Darstellung)

Der Prozess der Risikoanalyse nach BSI-Standard 200-3 beginnt mit der Gefährdungsübersicht, gefolgt von der Risikoeinstufung und der Risikobehandlung, um mit der Konsolidierung zu enden.

6.1 Erstellung einer Gefährdungsübersicht

Zur Vorbereitung auf die Risikoeinstufung müssen in dieser Phase Risiken, welche die Informationssicherheit betreffen und Auswirkungen auf die kDL BAB haben können, erkannt, beschrieben und dokumentiert werden.

Dazu zählen alle Risiken, die sich auf die informationstechnischen Systeme, Komponenten oder Prozesse auswirken, die maßgeblich für den Betrieb und die Funktionsfähigkeit der KRITIS BAB sind. Dabei sind Abhängigkeiten oder Schnittstellen zu oder von anderen IT-Systemen, die Auswirkungen auf die KRITIS BAB haben können, zusätzlich zu berücksichtigen.

Neben den relevanten elementare Gefährdungen nach dem BSI IT-Grundschutz (siehe Kapitel 9, Nr. 2j), müssen insbesondere die branchenspezifischen Gefährdungen für die KRITIS BAB aus Kapitel 5.2 zur Identifikation von Risiken berücksichtigt, auf Vollständigkeit überprüft und um fehlende Gefährdungen ergänzt werden.

6.2 Risikoeinstufung

Ziel der Risikoeinstufung ist es festzustellen, wie hoch die Wahrscheinlichkeit für das Eintreten sowie die potenzielle Schadenshöhe eines Schadensereignisses sind. Anhand dieser Faktoren muss das Risiko für die Objekte unter Berücksichtigung der erstellten Gefährdungsübersicht bewertet werden.

Die Risikoeinstufung muss entsprechend des BSI-Standards 200-3 (siehe Kapitel 9, Nr. 2f) qualitativ erhoben werden.

Die quantitative Risikoeinstufung wird aufgrund der Vollständigkeit kurz beschrieben und wird zur Durchführung der Risikoanalyse nicht weiter berücksichtigt. Diese kann abweichend dieses B3S mit entsprechender Begründung vom Betreiber umgesetzt werden.

- Quantitative Risikoeinstufung - Die quantitative Risikobetrachtung setzt umfangreiches statistisches Datenmaterial voraus. Verglichen mit der qualitativen Risikoanalyse ist eine quantitative Risikoanalyse aufwendiger. Weiterhin führen die Ergebnisse nicht zwangsläufig zu der vom Betreiber gewünschten Erhöhung des Sicherheitsniveaus.
- Qualitative Risikoeinstufung - Ermöglicht anhand zuvor festgelegter Kriterien eine schnelle und effektive Risikoerhebung zur Prioritätensetzung sowie zur Risikobewältigungsplanung.

Jeder Betreiber einer KRITIS BAB kann sowohl die Anzahl der Stufen als auch die Kriterien individuell festlegen und beschreiben. Die Kategorien sollten mit den Fachabteilungen abgestimmt werden.

Zur qualitativen Bewertung von Risiken können beispielhaft die folgenden Kategorien angewandt werden:

Bewertung von Eintrittswahrscheinlichkeiten	**Bedeutung**
selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal im Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Tabelle 4: Bewertung Eintrittswahrscheinlichkeiten

Bewertung von Auswirkungen	**Bedeutung**
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.

Bewertung von Auswirkungen	Bedeutung
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 5: Bewertung Schadensauswirkungen

6.3 Risikobewertung

Im Rahmen der Risikobewertung muss für die KRITIS BAB unter Berücksichtigung festgelegter Kriterien auf Basis der Ergebnisse der Risikoeinstufung eine Feststellung erfolgen, ob das Risiko oder sein Ausmaß akzeptabel ist.

Die Auswertung sollte mithilfe einer durch den Betreiber festgelegten Risikomatrix erfolgen. Daraus ergibt sich das Risiko für jede einzelne Gefährdung für das jeweilige Objekt.

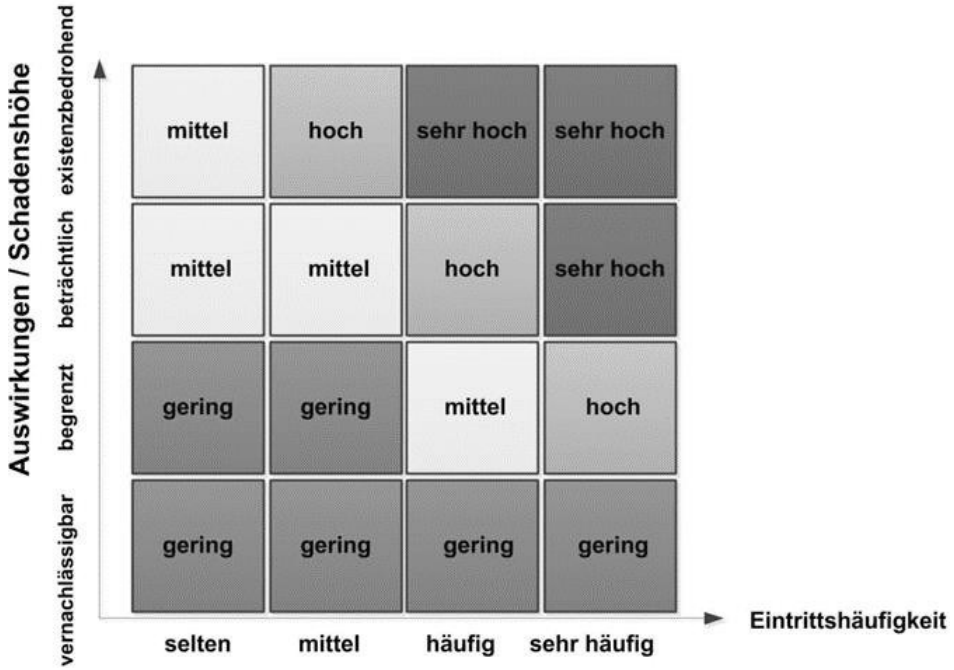

Abbildung 2: Beispiel einer Risikomatrix aus dem BSI-Standard 200-3

Das Beispiel der Risikomatrix aus dem BSI-Standard 200-3 besitzt auf der x-Achse die Eintrittshäufigkeiten selten, mittel, häufig und sehr häufig und auf der y-Achse die Auswirkungen / Schadenshöhen vernachlässigbar, begrenzt, beträchtlich und existenzbedrohend. Das sich ergebende Risiko stellt sich als Quadrat dar und kann gering, mittel, hoch oder sehr hoch sein.

Bewertung von Risiken	Bedeutung
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.
sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden sehr hohe Risiken selten akzeptiert.

Tabelle 6: Bewertung von Risiken

Beispielhaft ergeben sich folgende Handlungsempfehlungen entsprechend der Risikokategorien zur Risikobewertung:

- **Hohe oder sehr hohe Risiken**, welche eine häufige/sehr häufige Eintrittswahrscheinlichkeit in Kombination mit einer signifikanten Schadensauswirkung aufweisen, müssen im Rahmen der Verhältnismäßigkeit zeitnah behandelt und reduziert werden.
- Für **Risiken im mittleren Bereich** mit moderater Eintrittswahrscheinlichkeit und Schadensauswirkung müssen die Behandlungsoptionen hinsichtlich Kosten und Nutzen geprüft und die Risiken je nach Verhältnismäßigkeit reduziert oder beseitigt werden.
- **Geringe Risiken**, deren Eintreten entweder sehr unwahrscheinlich oder deren Schadensauswirkungen gering sind, sollten so weit wie möglich behandelt werden. Dies kann unter Berücksichtigung von Kosten und Nutzen erfolgen.

Weitere Informationen zur Risikoanalyse und die genaue Umsetzung der Sicherheitskonzeption für Betreiber von Verkehrssteuerungs- und Leitsystemen für das Netz der Bundesautobahnen werden im ebenfalls öffentlich verfügbaren Dokument „IT-

Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn“ (siehe Kapitel 9, Nr. 1) beschrieben. Der Umgang mit diesem Profil wird in Kapitel 7.2.1 beschrieben.

6.4 Berücksichtigung von Abhängigkeiten bei der Risikoanalyse

Sofern externe Plattformbetreiber sowie Wartungs- und Instandhaltungsdienstleister für die Aufrechterhaltung der kDL BAB und damit der kritischen Geschäftsprozesse erforderlich sind, gelten für die im Rahmen der Leistungserbringung genutzten IT-Systeme und Infrastrukturen die gleichen Anforderungen wie für den KRITIS Betreiber selbst.

Um potenzielle Störungen und informationstechnische Angriffe auf Infrastrukturen Dritter im Rahmen einer Risikoanalyse bewerten zu können, sollten Abhängigkeiten zwischen eigenen Systemen und Prozessen und den Diensten der externen Betreiber und Dienstleister bekannt sein.
Zur Erbringung der Dienstleistung von externen Plattformbetreibern sowie Wartungs- und Instandhaltungsdienstleistern müssen wirksame Verträge bzw. Leistungsvereinbarungen nachweisbar sein. Prüfmöglichkeiten können als möglicher Vertragsbestandteil vorgesehen werden.

6.5 Risikobehandlung

Die Risikobehandlung auf Basis des BSI-Standards 200-3 dient dazu, nicht akzeptierbaren Risiken angemessen zu begegnen. So stehen vier Behandlungsoptionen, wie das Vermeiden, Reduzieren, Transferieren und Akzeptieren von Risiken zur Auswahl.

Für die Betreiber einer KRITIS BAB besteht nach § 8a (1) BSIG die Besonderheit, dass eine eigenständige, dauerhafte Risikoakzeptanz nicht zulässig ist. Für die Umsetzung der technischen und organisatorischen Maßnahmen ist zu berücksichtigen, dass der dafür erforderliche Aufwand in einem angemessenen Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der kDL BAB steht.

Weiterhin dürfen Risiken im Sinne des B3S für Bundesautobahnen nach § 8a (1) BSIG nicht auf Versicherungsnehmer oder andere Dienstleister übertragen werden.

Daraus resultieren die folgenden, verbliebenen Risikobehandlungsoptionen:

- **Risikovermeidung -** Ausschluss der Risikoquelle, zum Beispiel durch Ändern von Geschäftsprozessen oder entfernen von Risikoursachen aus dem Informationsverbund.
- **Risikoreduktion -** Modifizierung des Risikos durch schließen organisatorischer, technischer oder physischer Schwachstellen durch Erarbeitung und Umsetzung geeigneter Sicherheitsmaßnahmen nach dem „Stand der Technik“.

6.6 Konsolidierung

Die Ergebnisse der Risikobehandlung müssen ausreichend dokumentiert und mit dem Sicherheitskonzept konsolidiert werden.

Dies beinhaltet, dass ungeeignete, unpraktische, widersprüchliche, zu aufwändige oder zu teure Maßnahmen verworfen, überarbeitet oder ersetzt werden.

Abschließend erfolgt die Rückführung in den Sicherheitsprozess.

7 Sicherheitsanforderungen nach Stand der Technik und Vorgehensweisen

Die Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG (siehe Kapitel 9, Nr. 2a) enthält Kriterien für eine sachgerechte Prüfung der vom Betreiber umgesetzten Sicherheitsmaßnahmen, um den geforderten Nachweise gemäß §8a BSIG zu erbringen. Der Betreiber muss daher die nachfolgenden Themenfelder, die diesem Anforderungskatalog entnommen sind, abdecken.

7.1 Abzudeckende Themen

7.1.1 **Informationssicherheitsmanagementsystem (ISMS)**

Es ist ein geeigneter Rahmen für die angemessene Behandlung aller relevanten Risiken und Themenfelder zur Umsetzung der Anforderungen nach § 8a Abs. 1 BSIG zu schaffen. Dafür muss ein Informationssicherheitsmanagementsystem nach dem BSI-Standard 200-1eingeführt und betrieben werden.

Das ISMS muss als kontinuierlicher Prozess etabliert werden, dies beinhaltet einen fortlaufenden Verbesserungsprozess z. B. nach dem PDCA-Managementzyklus oder äquivalenten Methoden.
Im Rahmen des ISMS muss der Umgang mit Informationen, Systemen und Software in Informationssicherheitsrichtlinien und Verfahrensanweisungen beschrieben und geregelt sein.
Mit dem Betrieb des ISMS müssen die in diesem Dokument beschriebenen Vorgehensweisen und Randbedingungen beachtet werden.

Alle Dokumente sind von der Unternehmensleitung bzw. vom jeweiligen Verantwortlichen in Kraft zu setzen und den Beschäftigten sowie relevanten externen Parteien bekannt und zugänglich zu machen. Alle Informationssicherheitsrichtlinien werden in geplanten Abständen oder jeweils nach erheblichen Änderungen überprüft, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.

Es kann ein (zentrales) Informationssicherheitsmanagement-Tool (ISMS-Tool) betrieben werden, dass alle Objekte im Anwendungsbereich, deren Bedeutung für die Erbringung der kDL BAB und deren Behandlung dokumentiert.

Für die Vorgehensweise nach dem BSI-Standard 200-2 ist mindestens die Standard-Absicherung anzuwenden und die in der Strukturanalyse definierten Zielobjekte (Prozesse, Anwendungen, IT-Systeme, Netzwerk und Infrastruktur) bilden den grundlegenden Informationsverbund der Kritischen Infrastruktur im ISMS ab. Die Maßnahmen richten sich nach dem Schutzbedarf sowie den in der Risikoanalyse ermittelten Gefährdungen.

7.1.2 **Asset Management**

Ein Asset Management zur (automatisierten) Inventarisierung für den hier betrachteten Anwendungsbereich muss umgesetzt werden. Die Inventarisierung kann sowohl mithilfe einer Softwarelösung (CMDB) als auch mithilfe von Tabellen erfolgen. Maßgeblich hierfür ist, dass alle betrachteten Systeme und Objekte vollständig erfasst und hinsichtlich ihrer Konfigurationen geprüft und betrachtet werden können.

Das Asset Management muss alle relevanten Anforderungen aus dem IT-Grundschutz-Kompendium 2021 berücksichtigen. Hierzu zählen insbesondere die Bausteine:

- OPS.1.1.2 “Ordnungsgemäße IT-Administration"
- APP.6 “Allgemeine Software”

Es sollten die folgenden minimalen Eigenschaftswerte der Assets erfasst werden:

- Asset-Typ
- Hersteller
- Typenbezeichnung/Modell
- Funktion
- Status
- Verantwortlicher

7.1.3 **Continuity- und Notfallmanagement**

Die Sicherheitskonzeption auf Basis des BSI IT-Grundschutzes verfolgt einen ganzheitlichen Ansatz. Der Betreiber muss auf dieser Basis geeignete Prozesse, Verfahren und Maßnahmen zur Aufrechterhaltung des Betriebs der Kritischen Infrastruktur (KRITIS BAB) für die verschiedenen Schadensereignisse - Störung, Notfall, Krise und Katastrophe – aufbauen und etablieren.

Dazu muss er das Continuity- und Notfallmanagement nach dem BSI-Standard 100-4 anwenden.

Dazu gehören im Wesentlichen

- die Initiierung des Notfallmanagement-Prozesses,
- die Konzeption und Umsetzung der Notfallvorsorge,
- das Krisenmanagement und die Notfallbewältigung,
- die Planung und Durchführung von Übungen und Tests und
- die Aufrechterhaltung und kontinuierliche Verbesserung.

Der Betreiber etabliert damit einen Notfallmanagement-Prozess, der nach Konzeption das Notfallvorsorgekonzept umsetzt und ähnlich wie der IS-Prozess des BSI-Standards 200-2

regelmäßig auf seine Wirksamkeit und Effizienz hin überprüft und kontinuierlich verbessert wird. Zudem müssen entsprechende Rollen in der Notfallmanagement-Organisation definiert und besetzt werden. In regelmäßigen Abständen von maximal 12 Monaten müssen Übungen und Tests durchgeführt werden, um Wirksamkeit sowie Umsetzbarkeit der Notfall-Prozesse auch in schwierigen und stressigen Situationen sicherzustellen. Die Prozesse sollten mithilfe von internen Übungen und komplexen Systemtests, Kommunikationsübungen, Plan- oder Krisenübungen geprüft werden. Hierbei sollten sowohl die Einbeziehung von externen Partnern und Dienstleistern berücksichtigt als auch das Szenario „Wegfall eines Dienstleisters“ betrachtet werden.

Für die Wiederherstellung des Normalzustandes der Systeme und Komponenten, die maßgeblich dem Betrieb der KRITIS BAB dienen, sollten sowohl zentrale als auch dezentrale Notfall- und Wiederanlaufhandbücher erstellt und an geeigneter Stelle hinterlegt werden. Dabei sollten Organisationseinheiten und die Systeme und Komponenten der Kritischen Infrastruktur (KRITIS BAB) unterschieden werden.

So sollten Handbücher je Organisationseinheit und je Komponente, die maßgeblich für den Betrieb der KRITIS BAB benötigt wird, durch den Betreiber erstellt werden. Diese sollten bei Änderungen angepasst, jedoch regelmäßig spätestens alle 12 Monate auf Ihre Aktualität geprüft, bei den zuständigen Stellen bekannt gemacht werden und wenn möglich geübt werden.

Zum Aufbau eines Notfallmanagements kann zusätzlich das „Umsetzungsrahmenwerk zum Notfallmanagement“ (Stand: Version 1.0, siehe Kapitel 9, Nr. 2i) herangezogen werden.

Sobald der BSI-Standard 200-4 als Nachfolger des BSI-Standards 100-4 final veröffentlicht wird, sollte das Continuity- und Notfallmanagement nach Möglichkeit und Ressourcen in einem bestimmten Zeitraum an die neuen Vorgaben angepasst werden. Wenn sie veröffentlicht wurden, sollten dabei vom BSI bereit gestellte Unterlagen zur Hilfestellung, z. B. Migrationskonzepte genutzt werden.

7.1.4 **Technische Informationssicherheit**

Die Absicherung der Kritischen Infrastruktur sollte nach dem BSI IT-Grundschutz erfolgen. Die Maßnahmen sind dem Schutzbedarf entsprechend umzusetzen. Das Ergebnis der Risikoanalyse bei einem hohen oder sehr hohen Schutzbedarf und der daraus ermittelten Maßnahmen müssen bei der Umsetzung berücksichtigt werden.

Die vorgegebenen Maßnahmenkategorien aus den Abschnitten 5.2.1 und 5.3 aus der „Orientierungshilfe B3S“ (Stand: September 2021, Version 1.1) zum „Stand der Technik“ oder die relevanten Bausteine aus dem „IT-Grundschutz-Profil für die Verkehrssteuerungs- und

Leitsysteme der Bundesautobahn“ (siehe Kapitel 9, Nr. 1) müssen dabei mindestens abgedeckt sein.

Nachfolgend werden den genannten Maßnahmen der Orientierungshilfe die Bausteine aus dem IT-Grundschutz-Kompendium 2021 zugeordnet. Eine genaue Zuweisung ist von jedem Betreiber individuell zu prüfen und bei Bedarf zu ergänzen.

	Kapitel	Maßnahme	Beispiele
Absicherung von Netzübergängen	A 1.1	Inventarisierung aller Netzzugänge	NET.1.1
	A 1.2	Netztrennung und Segmentierung, besonders im ICS-Umfeld	NET.1.1
	A 1.3	Absicherung der Fernzugriffe, Remote Access	OPS.1.2.5
	A 1.4	Sicheres Sicherheitsgateway, Firewall	NET.3.2
	A 1.5	Härtung und sichere Basiskonfigurationen	NET.3.1
	A 1.6	Schnittstellenkontrolle, Intrusion Detection/Prevention (IDS, IPS)	DER.1
	A 1.7	Absicherung mobiler Netzzugänge, mobile Sicherheit, Telearbeit, ggf. BYOD	OPS.1.2.4, SYS.3.2.2, CON.7
	A 1.8	DDoS-Mitigation	NET.1.1
	A 1.9	Network Access Control (NAC)	NET.2.1
	A 1.10	Einsatz von Routern und VPN-Gateways	NET.3.1, NET.3.3
Sichere Interaktion im Internet	A 2.1	Browser-Virtualisierung, Exploit Protection	APP.1.2
	A 2.2	Web-Filter	NET.3.1, NET.3.2
	A 2.3	Virtuelle Schleuse	NET.1.1.A4, NET.3.1.A18
	A 2.4	Sichere Dokumentenerstellung	NET.1.1, APP.1.2, APP.3.1, APP.3.2
	A 2.5	Detektionswerkzeuge für gezielte Angriffe auf Webseiten bzw. über E-Mails	OPS.1.1.4

	Kapitel	Maßnahme	Beispiele
	A 2.6	Security Information and Event Management (SIEM)	NET.1.2
Sichere Software (insbesondere Vermeidung von offenen Sicherheitslücken)	A 3.1	Spam-Abwehr, Content Filtering	APP.1.2, APP.5.2, APP.5.3
	A 3.2	Toolunterstützte Inventarisierung von Hardware und Software	APP.6, OPS.1.1.2
	A 3.3	Zentrales Patch- und Änderungsmanagement, Konfigurationsmanagement	OPS.1.1.3
	A 3.4	Schutz vor Schadsoftware	OPS.1.1.4
	A 3.5	Softwaretest und Freigabe	OPS.1.1.6
	A 3.6	Software Development Security (sichere Software-Entwicklung)	APP.7
	A 3.7	Security Operations	APP.* je nach Ausstattung und Schutzbedarf
	A 3.8	Sichere Beschaffung und Aussonderung (sicheres Löschen, Überwachung, Datensicherung und -wiederherstellung (Backup), Archivierung)	APP.6
Sichere und zuverlässige Hardware	A 4.1	Sichere Beschaffung und Aussonderung	SYS.*/IND.* je nach Ausstattung und Schutzbedarf
	A 4.2	Geeignete Aufstellung, Schutz vor Umwelteinflüssen, Zugriffsschutz und Einsatz von Diebstahlsicherungen	SYS.*/IND.* je nach Ausstattung und Schutzbedarf
	A 4.3	Schutz von Schnittstellen, inkl. Verhinderung der unautorisierten Nutzung von Schnittstellen, wie z. B. integrierten Mikrofonen, Kameras, Sensoren, UMTS etc.	SYS.*/IND.* je nach Ausstattung und Schutzbedarf

	Kapitel	Maßnahme	Beispiele
	A 4.4	Geregelte Außerbetriebnahme	SYS.*/IND.* je nach Ausstattung und Schutzbedarf
	A 4.5	Redundanzen, inklusive entsprechender Lieferanten- und Wartungsvereinbarungen, und vertrauenswürdige Lieferanten- und Logistikketten sowie qualifizierte Hersteller	SYS.*/IND.* je nach Ausstattung und Schutzbedarf
	A 4.6	Speicher- und Tamper-Schutz	SYS.4.3.A16
	A 4.7	Patch-, Änderungs- und Konfigurationsmanagement für Firmware	OPS.1.1.3
Sichere Authentisierung	A 5.1	Identitäts- und Rechtemanagement	ORP.4
	A 5.2	Multifaktor-Authentisierung (Zweifaktor-Authentisierung)	ORP.4
	A 5.3	Zugriffskontrolle (Sicheres Login)	ORP.4, CON.10
	A 5.4	Rollentrennung (Getrennte Administrator-Konten)	OPS.1.1.2, OPS.1.2.5
Verschlüsselung	A 6.1	Kryptografische Absicherung (Data in Rest, Data in Motion)	CON.1
	A 6.2	Cloud-Daten-Verschlüsselung (Cloud-Encryption)	CON.1, OPS.2.2
	A 6.3	Verschlüsselung der Kommunikationsverbindungen (z.B. Voice Encryption)	CON.1, NET.1.1
	A 6.4	E-Mail-Verschlüsselung	CON.1, APP.5.3
	A 6.5	Verschlüsselung der Datenträger z. B. Festplattenverschlüsselung	CON.1, SYS.1.1, SYS.2.1, SYS.2.2
Sonstiges	A 7.1	Sensibilisierung und Schulungen	ORP.3
	A 7.2	Übungen	ORP.3

	Kapitel	Maßnahme	Beispiele
	A 7.3	Aufrechterhaltung des aktuellen Informationsstands durch Bezug von Warnungen, CERT-Meldungen, Lagebild	ISMS.1
	A 7.4	Verfügbarkeit notwendiger Ressourcen	ISMS.1, OPS.1.1.2
	A 7.5	Interne Audits und Penetrationstests	DER.3.1, DER.3.2, OPS.1.1
	A 7.6	Sicherheitsstrategie und Sicherheitsleitlinie	ISMS.1
Besonders zu betrachtende Maßnahmenkategorien	A 9.1	Detektions- / Suchmöglichkeiten auf Infektionen	DER.1
	A 9.2	Innere Sensorik (zur Detektion von IT-Angriffen)	DER.1
	A 9.3	Client-Isolation	NET.2.1
	A 9.4	Härtung von Verzeichnisdiensten wie bspw. dem Microsoft Active Directory	APP.2.2
	A 9.5	Backup-Konzept inklusive Offline-Backups	SYS.*/IND.* je nach Ausstattung und Schutzbedarf

Tabelle 7: Zuordnung Bausteine zu Maßnahmen der Orientierungshilfe A 1 bis A 7 und A 9

7.1.5 **Personelle und organisatorische Sicherheit**

Informationssicherheit muss in allen Bereichen eines Unternehmens umgesetzt und gelebt werden. Die Umsetzung der personellen und organisatorischen Sicherheit erfordert klare Regelungen und führt zu einer sicheren Unternehmenskultur.

Hierzu sind zum Beispiel folgende Maßnahmen aus dem IT-Grundschutz-Kompendium 2021 oder die relevanten Bausteine aus dem „IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn“ (siehe Kapitel 9, Nr. 1) zu berücksichtigen:

- Das Personal muss auf geeignete Art und Weise hinsichtlich der Zuverlässigkeit sowie der fachlichen Kompetenz ausgewählt werden. In besonders sensiblen Bereichen muss ggf. eine Sicherheitsüberprüfung durchgeführt werden (vgl. Baustein ORP.2).
- Eine Rollenzuweisung wird bei Dienstantritt durchgeführt. Bei einem Dienstpostenwechsel erfolgt eine geregelte Rollenänderung (vgl. Baustein ORP.4).

- Alle notwendigen Rechte, Befugnisse und Kompetenzen werden in Abhängigkeit der zugewiesenen Rolle festgelegt (vgl. Baustein ORP.4).
- Bei der Berechtigungsvergabe muss das Prinzip der minimalen Berechtigung angewandt werden - so wenig Berechtigungen wie möglich, nur so viele wie zwingend erforderlich (vgl. Baustein ORP.4).
- Für Neuzugänge sowie Abgänge muss ein geregeltes Verfahren für die Vergabe und den Entzug der Berechtigungen existieren (vgl. Baustein ORP.4).
- Es werden regelmäßige Schulungs- und Sensibilisierungsmaßnahmen für alle Beschäftigten durchgeführt (vgl. Baustein ORP.3).
- Die Vorgaben zur personellen und organisatorischen Sicherheit werden an geeigneter Stelle veröffentlicht und bekanntgegeben.
- Es wird ein Verständnis für die Informationssicherheit auf allen Ebenen des Unternehmens (Leitung, IT, Beschäftigte, Dienstleister, …) geschaffen (vgl. Baustein ORP.3).
- Die Vorgaben zur Vorfallsmeldung werden erstellt und bekanntgegeben (z.B.: Meldewege, Ansprechpersonen, …) (vgl. Baustein DER.1).

7.1.6 **Bauliche/physische Sicherheit**

Neben der Absicherung der IT-Systeme, die zum Betrieb der KRITIS BAB notwendig sind, muss auch die bauliche/physische Sicherheit dieser Systeme über geeignete Maßnahmen gewährleistet werden.

Hierzu sind zum Beispiel folgende Maßnahmen aus dem IT-Grundschutz-Kompendium 2021 oder die relevanten Bausteine aus dem „IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn“ (siehe Kapitel 9, Nr. 1) zu berücksichtigen:

- Das Aufstellen von Zutrittsregelungen für sensible Bereiche wie beispielsweise Technik-, Server- oder Kontrollräume. Nur autorisierte Beschäftigte dürfen die entsprechenden Räume betreten (vgl. Baustein INF.1).
- Bei Maßnahmen innerhalb der sensiblen Bereiche durch Dritte sind die Arbeiten zu beaufsichtigen (vgl. Baustein ORP.1).
- Besucher müssen sich anmelden (vgl. Baustein INF.1).
- Die sicherheitstechnischen Anlagen wie die Brandmelde- und Löschtechnik werden gemäß den rechtlichen Vorgaben eingebaut. Zusätzlich werden Wartungen und Funktionstests zur Sicherstellung der Funktionsfähigkeit durchgeführt (vgl. Baustein INF.1/INF.2).
- Die Installation der elektrotechnischen Anlagen (Sicherungsschränke, Verkabelung, …) erfolgt normengerecht und ordnungsgemäß mit Überspannungsschutz und entsprechender Notstromversorgung (vgl. Baustein INF.12).

- Das Betriebsgebäude ist mithilfe einer Einbruchmeldeanlage sowie einbruchhemmenden Fenstern und Türen gesichert und in Sicherheitszonen unterteilt (vgl. Baustein INF.5).
- Bei Räumen, in denen IT-Systeme oder sonstige Anlagen aufgestellt werden, die eine große Abwärme erzeugen (z.B.: Serverräume), ist eine ausreichend dimensionierte Klimaanlage installiert (vgl. Baustein INF.2).

Die vorgegebenen Maßnahmenkategorien aus dem Abschnitt 5.2.2 aus der „Orientierungshilfe B3S“ (Stand: September 2021, Version 1.1) zum „Stand der Technik“ müssen dabei mindestens abgedeckt sein.

Nachfolgend werden den genannten Maßnahmen der Orientierungshilfe die Bausteine aus dem IT-Grundschutz-Kompendium 2021 zugeordnet. Eine genaue Zuweisung ist von jedem Betreiber individuell zu prüfen und bei Bedarf zu ergänzen.

Kapitel	Maßnahme	Beispiele
A 8.1	Zugangskontrolle	ORP.4
A 8.2	Notstromversorgung (USV)	INF.2
A 8.3	Netzersatzanlagen	INF.2

Tabelle 8: Zuordnung Bausteine zu Maßnahmen Orientierungshilfe Kapitel A 8

7.1.7 Vorfallerkennung und -bearbeitung

Um die relevanten IT-Systeme, die für die Erbringung der KRITIS BAB genutzt werden, schützen zu können, müssen sicherheitsrelevante Ereignisse rechtzeitig erkannt und behandelt werden. Um Ausfälle oder Beeinträchtigungen, die aufgrund von unvorhersehbaren Ereignissen eintreten können, zu behandeln, sind geeignete Prozesse zur Vorfallerkennung und -bearbeitung zu definieren sowie Meldewege gemäß §8b BSIG zu implementieren.

Schwachstellenmeldungen, Sensibilisierungen, Hilfestellungen oder nützliche Hinweise zu aktuellen Themen, die die Betreiber kritischer Infrastrukturen betreffen, können u.a. auf

- der Webseite des BSI (https://www.bsi.bund.de/),
- dem Melde- und Informationsportal des BSI (https://mip.bsi.bund.de/),
- bekannten IT-News-Seiten (z.B.: https://www.heise.de/),
- den Webseiten der Hersteller oder
- der Webseite des CERT-Bund (https://www.cert-bund.de/)

abgerufen werden.

Die Vorfallerkennung und -bearbeitung lässt sich in vorbeugende und eingreifende Maßnahmen unterteilen.

Zu den präventiven Maßnahmen zählen beispielsweise:

- Die Sensibilisierung und Schulung der Beschäftigten zur Erkennung eines Vorfalls.
- Eine ausreichende Protokollierung aller für die Erbringung der KRITIS BAB relevanten Systeme.
- Einrichtung einer Notfallnummer.
- Ein geeignetes Verfahren zur Detektion von Angriffen sowie der Überwachung des Netzwerkverkehrs auf Unregelmäßigkeiten.
- Die Etablierung eines Verfahrens zur Analyse von Schwachstellenmeldungen von Herstellern oder staatlichen Einrichtungen (BSI, CERT, …).

Zu den reaktiven Maßnahmen zählen beispielsweise:

- Direkte Abarbeitung der Meldewege zur Information aller Beteiligten.
- Die Benachrichtigung der betroffenen Stellen u.a. mit definierten Sofortmaßnahmen.
- Ein Verfahren zur Reaktion auf Angriffe. Hierzu zählen die Sperrung von Geräten oder die Trennung wichtiger Systeme vom Netzwerk.
- Durchführung der Maßnahmen unter Beachtung der Notfallpläne.

7.1.8 **Überprüfung im laufenden Betrieb**

Um die Funktionsfähigkeit der KRITIS BAB zu gewährleisten, müssen die Maßnahmen der relevanten informationstechnischen Systeme, Komponenten und Prozesse regelmäßig auf ihre Wirksamkeit überprüft werden. Die Prüfungen werden anlassbezogen und/oder in regelmäßigen Abständen alle 12 Monate durchgeführt.

Anlassbezogene Prüfungen werden durchgeführt, wenn beispielsweise

- Schwachstellenmeldungen von Herstellern oder staatlichen Einrichtungen (BSI, CERT, …) dies erfordern.
- sich die Bedrohungs- oder Gefährdungslage geändert hat,
- nicht zuverlässig erklärbaren Beeinträchtigungen der KRITIS BAB oder der zugehörigen IT-Systeme vorliegen,
- erfolgreich oder möglicherweise erfolgreiche Angriffe stattgefunden haben oder
- Änderungen an den IT- oder Kommunikationssystemen durchgeführt wurden.

Regelmäßige Prüfungen werden durchgeführt, wenn

- rechtliche Vorgaben diese erfordern,
- entsprechende interne Prüfzyklen definiert wurden oder
- Audits oder Teilbereichsprüfungen stattfinden.

7.1.9 Lieferanten, Dienstleister und Dritte

Die Sicherheitskonzeption des Betreibers ist nicht ausschließlich auf die internen Maßnahmen und Konzepte begrenzt, sondern ist auch für die Vergabe im Bereich der KRITIS BAB an externe Dienstleister von besonderer Bedeutung.

Die Sicherheitsanforderungen an Lieferanten, Dienstleister und Dritte müssen vertraglich geregelt werden. Diese sind auf die Einhaltung der Informationssicherheitsanforderungen des Unternehmens zu verpflichten.

Ergänzend können die „Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen“ (siehe Kapitel 9, Nr. 3a) des UP KRITIS bei der Vertragsgestaltung berücksichtigt werden.

7.1.10 Branchenspezifische Technik und (Kern-)Komponenten

Wie in den weiteren KRITIS-Sektoren wird auch im Anwendungsbereich der Kritischen Infrastruktur im Bereich der Autobahn branchenspezifische Technik eingesetzt. Neben dem Einsatz von IT-Komponenten ist der Einsatz verschiedener Steuerungssysteme sowie die Infrastruktur von besonderer Bedeutung.

Die branchenspezifische Technik und wichtige Komponenten der Infrastruktur sind in dem separaten “IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn“ (siehe Kapitel 9, Nr. 1) beschrieben.

7.2 Anwendungshinweise für Betreiber als Anwender eines B3S

Wichtig ist, dass mit der Anwendung dieses B3S auch die Anwendung des IT-Grundschutzprofils BAB verpflichtend ist.

Darüber hinaus muss dieser B3S vom Betreiber der KRITIS BAB an die eigenen Gegebenheiten angepasst werden, um den „Stand der Technik“ umzusetzen.

7.2.1 Anpassung des IT-Grundschutz-Profils durch den KRITIS BAB-Betreiber

Das Dokument „IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn“ (siehe Kapitel 9, Nr. 1) stellt die Referenzarchitektur und -organisation eines Autobahnbetreibers, der zugleich Betreiber einer KRITIS BAB ist, dar. Der dort beschriebene

Geltungsbereich umfasst ausschließlich Verkehrssteuerungs- und Leitsysteme wie sie im §8a (1) BSIG als maßgeblich und als Anhang 7 in der KritisV bestimmt sind. Diese können bei jedem Betreiber variieren.

Wenn der Betreiber diesen B3S zur Umsetzung des “Standes der Technik” nutzen will, muss er das Profil vollständig anwenden. Es ist als Schablone aufgebaut und wird - angereichert um die jeweiligen individuellen Differenzen – als Basis für das ISMS des Betreibers genutzt.

Strukturanalyse: Wenn der zu schützende Informationsverbund des Betreibers von der beschriebenen Referenzarchitektur abweicht, ist zu analysieren, welche Objekte des Profils nicht vorhanden, zusätzlich vorhanden oder abweichend vom beschriebenen Einsatzzweck vorhanden sind. Diese Objekte sind zu dokumentieren und deren Abweichung zu begründen. Objekte, die vom beschriebenen Einsatzzweck abweichen, sind genauso zu behandeln wie deren Originale. Es sei denn, die Abweichung ist erheblich, dann sollte man ein gesondertes Objekt hinzufügen (zusätzliches Objekt). Nicht vorhandene Objekte werden nicht gelöscht, sondern bleiben nach Dokumentation unbehandelt.

Schutzbedarf und Modellierung: Zusätzliche Objekte müssen nach der Sicherheitskonzeption wie im BSI-Standard 200-2 beschrieben behandelt werden. Diesen Objekten werden ein angemessener Schutzbedarf und geeignete Bausteine des IT-Grundschutz-Kompendiums 2021 zugeordnet.

Die aus den Bausteinen abgeleiteten Anforderungen werden in Abhängigkeit des festgestellten Schutzbedarfs umgesetzt. Ausgewählte Anforderungen können konkretisiert, nicht vorhandene beschrieben werden.

Prozessbausteine: Das gleiche gilt für Abweichungen, wenn diese den organisatorischen Bereich des Betreibers oder die Prozessbausteine betreffen. Es ist zu analysieren, welche Bausteine des Profils nicht modelliert oder für den Geltungsbereich des Betreibers zusätzlich modelliert werden. Die Abweichungen werden begründet, das Ergebnis wird dokumentiert und fließt in die Phase der Modellierung ein. Die abgeleiteten Anforderungen werden in Abhängigkeit des festgestellten Schutzbedarfs angepasst. Ausgewählte Anforderungen können wie oben beschrieben konkretisiert, nicht vorhandene beschrieben werden.

Analoges gilt für alle Anpassungen des Profils, auch die des Schutzbedarfs und seiner Ableitung (Vererbung).

Idealerweise finden derlei Anpassungen der „Schablone“ samt Dokumentation auch in einem ISMS-Tool statt. Änderungen des Profils können dort festgehalten und dokumentiert werden. Anhand einfacher Kriterien sollte im Tool gut und schnell (für Dritte) erkennbar sein, was zum IT-Grundschutz-Profil gehört und was davon abweicht. Wichtig ist, dass alle Abweichungen vollständig dokumentiert sind. Den Nachweis für letzteres kann man mit einfachen Mitteln aus den Tabellen des IT-Grundschutz-Profils führen.

7.2.2 **Konkretisierung des Anwendungsbereichs durch die Betreiber**

Der Anwendungsbereich dieses B3S muss von dem Betreiber der KRITIS BAB mit dem Geltungsbereich konkretisiert und die Infrastruktur detailliert dargestellt werden.

7.2.3 **Fortschreibung und Erfahrungen der Anwender**

Die Fortschreibung dieses B3S erfolgt auf Basis der Erfahrungen der Anwender innerhalb der Autobahn GmbH des Bundes spätestens alle zwei Jahre.

8 Glossar

Begriff	Quelle	Definition
Anlagen	KritisV §1	Anlagen sind a) Betriebsstätten und sonstige ortsfeste Einrichtungen, die für die Erbringung einer kritischen Dienstleistung notwendig sind. b) Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen, die für die Erbringung einer kritischen Dienstleistung notwendig sind. Einer Anlage sind alle vorgesehenen Anlagenteile und Verfahrensschritte zuzurechnen, die zum Betrieb notwendig sind, sowie Nebeneinrichtungen, die mit den Anlagenteilen und Verfahrensschritten in einem betriebstechnischen Zusammenhang stehen und die für die Erbringung einer kritischen Dienstleistung notwendig sind.
Betreiber	KritisV §1	Betreiber ist eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.
Betriebszentrale		Umfasst oft die Kerngeschäfte der Verkehrs– und Tunnelleitzentrale der Verkehrsbeeinflussung (auf offener Strecke) und Tunnel.
BSI-Standards		Die BSI-Standards liefern die Vorgehensweise zum Aufbau eines ISMS und bilden mit dem IT-Grundschutz-Kompendium die Sicherheitskonzeption nach dem IT-Grundschutz ab.
IT	BSIG §2 (1)	Die Informationstechnik (IT) im Sinne dieses Gesetzes umfasst alle technischen Mittel zur Verarbeitung von Informationen.
IT-Grundschutz		Standardvorgehensweise zum Aufbau eines ISMS

IT-Grundschutz-Kompendium		Das IT-Grundschutz-Kompendium wird jährlich in einer aktualisierten Version veröffentlicht und liefert konkrete Anforderungen zum Aufbau eines ISMS. Es bildet mit den BSI-Standards den IT-Grundschutz ab.
Kritische Dienstleistung (allgemein)	KritisV §1	Kritische Dienstleistung ist eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren nach den §§ 2 bis 8, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde.
Kritische Dienstleistung (Sektor Verkehr)	KritisV §8 (1)	Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens ist im Sektor Transport und Verkehr die Versorgung der Allgemeinheit mit Leistungen zum Transport von Personen und Gütern (Personen und Güterverkehr) kritische Dienstleistung im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes.
Kritische Infrastrukturen (Sektor Verkehr, allgemein)	KritisV §8 (3)	Im Sektor Transport und Verkehr sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die 1. den in Anhang 7 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und die für den Personen- oder Güterverkehr in den in Absatz 2 genannten Verkehrsträgern sowie im ÖPNV, in der Logistik oder sonst erforderlich sind und 2. den Schwellenwert nach Anhang 7 Teil 3 Spalte D erreichen oder überschreiten.
Lichtsignalanlage	StVO §37	Wechsellichtzeichen
Branchenspezifischer Sicherheitsstandard oder (kurz) B3S	BSIG §8a (2)	Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach den Absätzen 1 und 1a vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach den Absätzen 1 und 1a zu gewährleisten.

Straßenkörper	FStrG §1 (4)	Das sind besonders der Straßengrund, der Straßenunterbau, die Straßendecke, die Brücken, Tunnel, Durchlässe, Dämme, Gräben, Entwässerungsanlagen, Böschungen, Stützmauern, Lärmschutzanlagen, Trenn-, Seiten-, Rand- und Sicherheitsstreifen.
Tunnel	EABT 80/100	Tunnel mit einer Planungsgeschwindigkeit von 80 km/h oder 100 km/h.
Tunnelleitzentrale		Gebäude oder Räumlichkeiten, in denen die Leistungen zur zentralen Steuerung und Lenkung des Verkehrs in Tunneln erbracht werden.
Verkehrsbeeinflussungsanlagen	BASt	Verkehrsbeeinflussungsanlagen werden auf Bundesfernstraßen zur Erhöhung der Verkehrssicherheit und Verbesserung des Verkehrsflusses eingesetzt.
Verkehrssteuerungs- und Leitsystem	KritisV Anhang 7, Teil 1 1.20)	Eine Anlage oder ein System zur Verkehrsbeeinflussung im Straßenverkehr einschließlich der in § 1 Absatz 4 Nummer 1, 3 und 4 des Bundesfernstraßengesetzes genannten Einrichtungen, zum Beispiel Verkehrs-, Betriebs- und Tunnelleitzentralen, Entwässerungsanlagen, intelligente Verkehrssysteme und Fachstellen für Informationstechnik und -sicherheit im Straßenbau, sowie der Telekommunikationsnetze der Bundesautobahnen.
Verkehrszentrale		Gebäude oder Räumlichkeiten, in denen das Verkehrsmanagement umgesetzt wird.

9 Literaturhinweise und mitgeltende Dokumente

Neben den Formularen, die für den Antrag auf Eignung beim BSI notwendig sind, gelten folgende Dokumente mit:

9.1 IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn (IT-Grundschutz-Profil BAB)

Version 1.0 von 22.06.2022,
Herausgeber: Frank Felde, Gesamt-Informationssicherheitsbeauftragter in Stellvertretung für Die Autobahn GmbH des Bundes

9.2 Bundesamt für Sicherheit in der Informationstechnik - Dokumente

a) Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG, Version 1.1 von September 2021
b) Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG, Version 1.1 vom 21.08.2020
c) Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen, Version 1.0 vom 28.02.2020
d) Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 200-1, Version 1.0, Oktober 2017
e) IT-Grundschutz-Methodik, BSI-Standard 200-2, Version 1.0, Oktober 2017
f) Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 200-3, Version 1.0, Oktober 2017
g) Notfallmanagement, BSI-Standard 100-4, Version 1.0, November 2008
h) IT-Grundschutz-Kompendium 2021, Stand Februar 2021
i) Umsetzungsrahmenwerk zum Notfallmanagement, Version 1.0
j) Elementare Gefährdungen, Stand Dezember 2020

9.3 UP KRITIS - Dokumente

k) Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen, Version 3.0 vom November 2021

9.4 Gesetze, Verordnungen

l) Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)
   BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert
m) Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)
   BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), zuletzt durch Artikel 1 der Verordnung vom 6. September 2021 (BGBl. I S. 4163) geändert

n) Bundesfernstraßengesetz (FStrG)

Bundesfernstraßengesetz in der Fassung der Bekanntmachung vom 28. Juni 2007, zuletzt geändert durch Artikel 11 des Gesetzes vom 10. September 2021

9.5 Technische Standards

o) RABT
Richtlinien für die Ausstattung und den Betrieb von Straßentunneln
Herausgeber: Forschungsgesellschaft für Straßen- und Verkehrswesen, Ausgabe 2006
ISBN: 3-937356-87-8

p) EABT
Empfehlungen für die Ausstattung und den Betrieb von Straßentunneln
Herausgeber: Forschungsgesellschaft für Straßen- und Verkehrswesen, Version EABT-80/100, Ausgabe 2019
ISBN: 978-3-86446-235-1

q) TLS
Technische Lieferbedingungen für Streckenstationen, Version 2012
Herausgeber: Bundesministerium für Verkehr, Bau und Stadtentwicklung, heute BMVI Download über die Seiten der Bundesanstalt im Straßenwesen (BaSt):
BASt - Fachthemen – Verkehrstechnik - TLS 2012, zuletzt aufgerufen am 08.12.2021

r) MARZ
Merkblatt für die Ausstattung von Verkehrsrechnerzentralen und Unterzentralen, Version 2018
Herausgeber: Bundesministerium für Verkehr, Bau und Stadtentwicklung, heute BMVI, Download über die Seiten der Bundesanstalt im Straßenwesen (BaSt):
BASt - Publikationen - Merkblatt für die Ausstattung von Verkehrsrechnerzentralen und Unterzentralen MARZ 2018, zuletzt aufgerufen am 08.12.2021