Branchenspezifischer Sicherheitsstandard für die Siedlungsabfallentsorgung
B3S SAE

Nach § 8a Abs. 2 BSI-Gesetz

Stand: 16.10.2025
Version: 0.9 zur Eignungsprüfung

Impressum

Herausgeber:

UP KRITIS Branchenarbeitskreis Sektor Siedlungsabfallentsorgung mit Beteiligung von Mitgliedern der folgenden Verbände

BDE
Bundesverband der Deutschen Entsorgungs-, Wasser- und Kreislaufwirtschaft e. V.

ITAD
Interessengemeinschaft der Thermischen Abfallbehandlungsanlagen in Deutschland e.V.

VKU
Verband kommunaler Unternehmen e. V.

Verfasser:

Der Branchenspezifische Sicherheitsstandard Siedlungsabfallentsorgung (B3S SAE) wurde von der Arbeitsgruppe B3S SAE des Branchenarbeitskreises Sektor Siedlungsabfallentsorgung in Zusammenarbeit mit der admeritia GmbH erstellt.

Inhalt

Vorwort ... 6
1 Anwendungsbereich und Adressaten des B3S ... 8
2 Normative Verweise, Begriffe und Abkürzungen ... 9
2.1 Normative Verweise ... 9
2.2 Begriffe ... 10
2.2.1 Siedlungsabfälle ... 10
2.2.2 Bereiche der Siedlungsabfallentsorgung im Sinne der BSI-KritisV ... 11
2.2.3 Anlagen ... 11
2.2.4 Gemeinsame Anlage ... 11
2.2.5 Kritische Dienstleistung ... 12
2.2.6 Kritische Infrastrukturen ... 13
2.2.7 Geltungsbereich zum Nachweisen gemäß § 8a Absatz 3 BSIG ... 13
2.2.8 Informationstechnische Systeme, Komponenten und Prozesse ... 15
3 Grundlagen ... 17
3.1 Allgemeines ... 17
3.2 Schutzziele ... 17
3.3 Managementsystem zur Informationssicherheit (ISMS) ... 18
3.4 Betriebliches Kontinuitätsmanagement (BCM) ... 19
3.5 Risikoeinschätzung und – Bewertung (inkl. Bedrohungsanalyse) ... 20
3.6 Risikobehandlung ... 24
4 Angriffserkennung ... 25
4.1 Allgemeine Anforderungen ... 25
4.2 Umfang der Angriffserkennung („risikobasierter Ansatz“) ... 25
4.3 Komponenten und Methoden der Angriffserkennung ... 26
4.3.1 Statische Angriffsmustererkennung ... 26
4.3.2 Anomalie-Erkennung ... 27
4.3.3 Korrelation ... 27
5 Organisatorische Anforderungen ... 28
5.1 Informationssicherheitspolitik und -richtlinien ... 28
5.2 Informationssicherheitsrollen und -verantwortlichkeiten ... 28
5.3 Aufgabentrennung ... 28
5.4 Verantwortlichkeiten der Leitung ... 28
5.5 Kontakt mit Behörden ... 29
5.6 Kontakt mit speziellen Interessensgruppen ... 29
5.7 Informationen über die Bedrohungslage ... 29

5.8 Informationssicherheit im Projektmanagement 29
5.9 Inventar der Informationen und anderer damit verbundener Werten 29
5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten 30
5.11 Rückgabe von Werten 30
5.12 Klassifizierung von Information 30
5.13 Kennzeichnung von Information 31
5.14 Informationsübermittlung 31
5.15 Zugangssteuerung 31
5.16 Identitätsmanagement 31
5.17 Authentisierungsinformationen 32
5.18 Zugangsrechte 32
5.19 Informationssicherheit in Lieferantenbeziehungen 32
5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen 32
5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette 33
5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen 33
5.23 Informationssicherheit für die Nutzung von Cloud-Diensten 33
5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen 33
5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse 33
5.26 Reaktion auf Informationssicherheitsvorfälle 34
5.27 Erkenntnisse aus Informationssicherheitsvorfälle 34
5.28 Sammeln von Beweismaterial 34
5.29 Informationssicherheit bei Störungen 34
5.30 IKT-Bereitschaft für Business-Continuity 34
5.31 Juristische, gesetzliche, regulatorische und vertragliche Anforderungen 34
5.32 Geistige Eigentumsrechte 34
5.33 Schutz von Aufzeichnungen 34
5.34 Datenschutz und Schutz von personenbezogenen Daten (PbD) 35
5.35 Unabhängige Überprüfung der Informationssicherheit 35
5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit 35
5.37 Dokumentierte Betriebsabläufe 35
6 Personenbezogene Anforderung 36
6.1 Sicherheitsüberprüfung 36
6.2 Beschäftigungs- und Vertragsbedingungen 36
6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung 36
6.4 Maßregelungsprozess 36

6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung 37
6.6 Vertraulichkeits- und Geheimhaltungsvereinbarungen 37
6.7 Remote-Arbeit 37
6.8 Meldung von Informationssicherheitsereignissen 37
7 Physische Anforderungen 38
7.1 Physische Sicherheitsperimeter 38
7.2 Physischer Zutritt 38
7.3 Sichern von Büros, Räumen und Einrichtungen 38
7.4 Physische Sicherheitsüberwachung 38
7.5 Schutz vor physischen und umweltbedingten Bedrohungen 39
7.6 Arbeiten in Sicherheitsbereichen 39
7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren 39
7.8 Platzierung und Schutz von Geräten und Betriebsmitteln 39
7.9 Sicherheit von Werten außerhalb der Räumlichkeiten 40
7.10 Speichermedien 40
7.11 Versorgungseinrichtungen 40
7.12 Sicherheit der Verkabelung 40
7.13 Instandhaltung von Geräten und Betriebsmitteln 41
7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln 41
8 Technische Anforderungen 42
8.1 Endpunktgeräte des Benutzers 42
8.2 Privilegierte Zugangsrechte 42
8.3 Informationszugangsbeschränkung 42
8.4 Zugriff auf den Quellcode 42
8.5 Sichere Authentisierung 42
8.6 Kapazitätssteuerung 43
8.7 Schutz gegen Schadsoftware 43
8.8 Handhabung von technischen Schwachstellen 43
8.9 Konfigurationsmanagement 43
8.10 Löschung von Informationen 44
8.11 Datenmaskierung 44
8.12 Verhinderung von Datenlecks 44
8.13 Sicherung von Information 44
8.14 Redundanz von informationsverarbeitenden Einrichtungen 44
8.15 Protokollierung 44
8.16 Überwachung von Aktivitäten 45

8.17 Uhrensynchronisation 45
8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten 45
8.19 Installation von Software auf Systemen im Betrieb 46
8.20 Netzwerksicherheit 46
8.21 Sicherheit von Netzwerkdiensten 46
8.22 Trennung von Netzwerken 46
8.23 Webfilterung 47
8.24 Verwendung von Kryptographie 47
8.25 Lebenszyklus einer sicheren Entwicklung 47
8.26 Anforderungen an die Anwendungssicherheit 47
8.27 Sichere Systemarchitektur und Entwicklungsgrundsätze 47
8.28 Sichere Codierung 47
8.29 Sicherheitsprüfung bei Entwicklung und Abnahme 47
8.30 Ausgegliederte Entwicklung 48
8.31 Trennung von Entwicklungs-, Test- und Produktionsumgebung 48
8.32 Änderungssteuerung 48
8.33 Testdaten 48
8.34 Schutz der Informationssysteme während Tests im Rahmen von Audits 48
Anhänge 49
A.1 Branchenspezifische Risiken 49
A.1.1 Sammlung & Beförderung 50
A.1.2 Verwertung & Beseitigung 58
A.2 Empfehlungen für Betreiber einer Kritischen Infrastruktur zur Meldung von IT-Sicherheitsvorfällen gegenüber dem BSI 66
A.3 Bedrohungsszenarien, elementare Gefährdungen und Schwachstellen 67
A.3.1 Besonders zu berücksichtigende Bedrohungsszenarien 67
A.3.2 Elementare Gefährdungen 69
A.3.3 Schwachstellen 76
A.4 Abkürzungen 80

Vorwort

Eine verlässliche und leistungsfähige Siedlungsabfallentsorgung ist für unsere Gesellschaft essenziell. Die Entsorgungssicherheit ist aus verschiedenen Gründen, etwa Hygiene und Seuchenprävention, ein hohes Gut. Störungen in der Siedlungsabfallentsorgung können sich unmittelbar auf die Funktionsfähigkeit des öffentlichen Lebens auswirken. Aus diesem Grund wurde die Siedlungsabfallentsorgung als Kritische Infrastruktur (KRITIS)-Sektor in das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) aufgenommen.

In Zeiten zunehmender Digitalisierung lassen sich durch den verstärkten Einsatz von Informationstechnologie (IT) bei den Prozessen der Siedlungsabfallentsorgung Effizienz steigern und der Ressourceneinsatz optimieren. Gleichzeitig wächst mit zunehmender Durchdringung der Abläufe mit Informationstechnik das Risiko, dass ein Ausfall oder eine Störung der Informationstechnik die Erbringung der Siedlungsabfallentsorgung maßgeblich behindern kann. Mit dem IT-Sicherheitsgesetz[1] fordert der Gesetzgeber wirksame Schutzmechanismen für die so genannten Kritischen Infrastrukturen in Deutschland.

§ 8a Abs. 2 BSI-Gesetz (BSIG) bietet den Branchen die Möglichkeit, zum Schutze ihrer IT-Systeme – insbesondere der für die Aufrechterhaltung der Kritischen Infrastruktur und der kritischen Dienstleistung erforderlichen informationstechnischen Systeme, Komponenten oder Prozesse – einen Branchenspezifischen Sicherheitsstandard zu entwickeln.

Der vorliegende Branchenspezifische Sicherheitsstandard für den gesamten Sektor Siedlungsabfallentsorgung (B3S SAE) orientiert sich an der DIN EN ISO/IEC 27001:2024[2] und dient als Grundlage für die Risikoabschätzung und die Durchführung von Maßnahmen zum Schutz der informationstechnischen Systeme, Komponenten oder Prozesse für die kritischen Dienstleistungen „Sammlung und Beförderung“ sowie „Verwertung und Beseitigung.“ Eine Umsetzung des B3S erfordert nicht zwingend die Einhaltung der Umsetzungshinweise der DIN EN ISO/IEC 27002:2024. Vielmehr ist die Einhaltung der Umsetzungshinweise gemäß den festgestellten Risiken zu empfehlen. Darüber empfiehlt sich in Bezug auf industrielle Steuerungssysteme (OT) die DIN EN ISO/IEC 62443 zu berücksichtigen.

Der Branchenstandard ist konkret zu dem Zweck erstellt worden, Unternehmen der Siedlungsabfallentsorgung, die gemäß den Vorgaben der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) Kritische Infrastrukturen betreiben, bei der Umsetzung der Anforderungen aus dem BSIG zu unterstützen. Andere Unternehmen der Siedlungsabfallentsorgung steht es frei, sich an diesem Branchenstandard zu orientieren.

Dieser Branchenspezifische Sicherheitsstandard für die Siedlungsabfallentsorgung wurde durch die Arbeitsgruppe „B3S“ des UP KRITIS Branchenarbeitskreises Siedlungsabfallentsorgung erarbeitet.

Erfahrungen und Kommentare zur Anwendung dieses Branchenspezifischen Sicherheitsstandards sind erbeten und können an folgende Stellen gerichtet werden:

UP KRITIS Branchenarbeitskreis Sektor Siedlungsabfallentsorgung

[1] siehe Gesetze zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG)
Quelle: https://www.bsi.bund.de/dok/6776460

[2] Deutsche Übersetzung der englischen Fassung ISO/IEC 27001:2022

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) die Eignung des B3S für den Sektor Siedlungsabfallentsorgung festgestellt.

1 Anwendungsbereich und Adressaten des B3S

Der Anwendungsbereich dieses B3S umfasst die in der BSI-KritisV als Kritische Infrastruktur definierte Anlagenkategorien des Sektors der Siedlungsabfallentsorgung. Diese sind in den Bereichen Sammlung und Beförderung sowie Verwertung und Beseitigung definiert. Daher werden diese Bereiche in diesem B3S in den Blick genommen.

Betreiber haben ausgehend von ihrer Betroffenheit von den in der BSI-KritisV definierten Anlagekategorien individuell und unabhängig vom Anwendungsbereich dieses B3S den Geltungsbereich ihrer kritischen Infrastruktur zu beschreiben. Nähere Informationen dazu bietet das Dokument „Zur Dokumentation des Geltungsbereiches bei KRITIS-Betreibern“[3] des BSI. [siehe hierzu weiter unter 2.2.7].

Der Branchenspezifische Sicherheitsstandard Siedlungsabfallentsorgung (B3S SAE) gilt für die Ermittlung von Maßnahmen zum Schutz der informationstechnischen Systeme, Komponenten oder Prozesse, die für die Erbringung der kritischen Dienstleistungen Sammlung und Beförderung sowie Verwertung und Beseitigung notwendig sind. In diesem Zusammenhang ist der „All-Gefahren-Ansatz“ im Rahmen des Risiko- und Krisenmanagements anzuwenden, welcher über die reine IT-Perspektive hinausgeht und alle (bekannten) Gefahren berücksichtigt.

Die Adressaten dieses B3S sind Unternehmen der Siedlungsabfallentsorgung, die nach der BSI-KritisV als Betreiber von Kritischer Infrastruktur gelten. Darüber hinaus kann der B3S SAE Unternehmen der Branche, die keine Kritische Infrastruktur nach BSI-KritisV betreiben, als Orientierung für die Umsetzung von Maßnahmen im Bereich der Informationssicherheit dienen. Wer die Betreibereigenschaft im Falle von Unterbeauftragungen hat oder anderen Geschäftsverhältnissen, die die klare Identifizierung erschweren, ist im Einzelfall zu prüfen.

Dieser Branchenspezifische Sicherheitsstandard Siedlungsabfallentsorgung umfasst keine Aspekte des Datenschutzes.

[3] Version 2.0 vom 15.08.24, abgerufen am 23.07.2025 unter folgendem Link: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/sdt-1-geltungsbereich.pdf?__blob=publicationFile&v=8

2 Normative Verweise und Begriffe

Im Folgenden werden in diesem B3S verwendete normative Verweise und Begriffe erläutert.

2.1 Normative Verweise

Die folgenden zitierten Dokumente sind für die Anwendung dieses Branchenspezifischen Sicherheitsstandards für die Siedlungsabfallentsorgung zusätzlich zu Rate zu ziehen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die jeweils aktuelle Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

Gesetze & regulatorische Vorgaben:

Die folgenden Gesetze und regulatorischen Vorgaben bilden die Grundlage für den Anwendungsbereich und die Themengestaltung dieses B3S und beziehen sich übergreifend auf das gesamte Dokument:

BSI-Gesetz – BSIG, Gesetz über das Bundesamt für Sicherheit in der Informationstechnik

BSI-Kritisverordnung – BSI-KritisV, Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz

Standards & Normen:

Die Relevanz der im Folgenden aufgelisteten Standards und Normen für die einzelnen Kapitel dieses B3S wird in nachstehender Tabelle dargestellt:

Standard / Norm	**Relevanz für B3S Kapitel**
BSI-Standard 200-1, Managementsysteme für Informationssicherheit (ISMS)	Kap. 3.3
BSI-Standard 200-2, IT-Grundschutz-Methodik	Kap. 5 bis 8
BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz	Kap. 3.5
BSI-Standard 200-4, Business Continuity Management	Kap. 3.4
BSI IT-Grundschutz-Kompendium 2023	Kap. 3.6, A.1 und A.3
BSI ICS-Security-Kompendium	
DIN EN ISO 22301, Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (ISO 22301:2019); Deutsche Fassung EN ISO 22301:2019	Kap. 3.4
DIN EN ISO/IEC 27001 – Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen	Kap. 3.3

IEC 62443-Normenreihe, IT-Sicherheit für industrielle Automatisierungssysteme	Kap. 4 Kap. 5 bis 8
NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide	Kap. 4
DIN EN ISO/IEC 27002 – Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen	Kap. 5 bis 8
DIN ISO/IEC TR 27019, Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Managementsystem von Steuerungssystemen der Energieversorger auf Grundlage der ISO/IEC 27002	Kap. 5 bis 8

2.2 Begriffe

Im Folgenden werden die in diesem B3S verwendeten, relevanten Begriffe erläutert.

2.2.1 Siedlungsabfälle

Siedlungsabfälle sind grundsätzlich gemäß § 3 Absatz 5a Kreislaufwirtschaftsgesetz (KrWG) weit definiert und umfassen gemischt und getrennt gesammelte Abfälle aus privaten Haushaltungen, insbesondere Papier und Pappe, Glas, Metall, Kunststoff, Bioabfälle, Holz, Textilien, Verpackungen, Elektro- und Elektronik-Altgeräte, Altbatterien und Altakkumulatoren sowie Sperrmüll, einschließlich Matratzen und Möbel, und aus anderen Herkunftsbereichen, wenn diese Abfälle auf Grund ihrer Beschaffenheit und Zusammensetzung mit Abfällen aus privaten Haushaltungen vergleichbar sind.

Die BSI-KritisV knüpft grundsätzlich an diese Definition an, schränkt allerdings die in den Geltungsbereich der BSI-KritisV fallenden Abfallströme ein. Die BSI-KritisV richtet sich explizit nicht nach den etablierten Abfallschlüsseln (siehe weiter unten). Vorrangig aus Gründen des Gesundheitsschutzes und Erwägungen der Stadtsauberkeit wurden nur folgende Abfallströme in den Geltungsbereich der BSI-KritisV aufgenommen und zwar unterschiedlich nach Bereichen:

- Restmüll, Bioabfall (Biotonne), Verpackungen und Kunststoffe, Altglas, PPK (Papier, Pappe, Kartonagen) für den Bereich Abfallsammlung/-beförderung
- Restmüll, Bioabfall (Biotonne), Verpackungen und Kunststoffe für den Bereich Abfallverwertung/-beseitigung

Die so festgelegten Abfälle sind nicht nach Schlüsselnummern nach der Abfallverzeichnisverordnung definiert. Vor dem Hintergrund, dass bestimmte Abfälle dringend gesammelt, d.h. von den Erfassungsstandorten auf der Straße oder an den Grundstücken wegbefördert, und behandelt werden müssen, sind die Abfallfraktionen ganz praktisch „tonnengebunden“ zu verstehen. Das heißt, dass z.B. mit Bioabfällen (Biotonne) der Inhalt der Biotonnen gemeint ist, auch wenn die jeweiligen Biotonnen im Einzelfall Fehlwürfe und damit auch andere Abfälle als Bioabfall, z.B. Plastik oder Metall, enthalten. Gleiches gilt für Restmüll, PPK, Glas und Verpackungen. Wichtig in der Praxis ist, dass Grünabfälle, d.h. Park- und Gartenabfälle, nicht vom Geltungsbereich der BSI-KritisV erfasst sind. Sofern Grünabfälle aber vor Ort in der Biotonne miterfasst werden, sind sie in diesem Rahmen ebenfalls vom Begriff „Bioabfälle (Biotonne)“ erfasst. Nicht erfasst sind demgegenüber Grünabfälle, die in eigenen Grünabfalltonnen oder über die Wertstoffhöfe erfasst werden. Mit Blick auf die Fraktion „Verpackungen“ ist auszuführen, dass diese in den Kommunen primär über die Gelbe Tonne bzw. gelbe Säcke erfasst werden. Damit ist der Inhalt dieser Tonnen oder Säcke als Verpackungsabfall zu verstehen. Sofern die einzelne Kommune über eine sogenannte Wertstofftonne verfügt, die sowohl Verpackungen

als auch stoffgleiche Nichtverpackungen erfasst (etwa Kleiderbügel, Bratpfannen, u.a.), so ist der gesamte Inhalt der Wertstofftonne vom Begriff Verpackungsabfall umschlossen.

2.2.2 Bereiche der Siedlungsabfallentsorgung im Sinne der BSI-KritisV

Die BSI-KritisV[4] gliedert die Anlagenkategorien mit den dazugehörigen Schwellenwerte in verschiedene Bereiche.

Die Siedlungsabfallentsorgung wird in den Bereichen „Abfallsammlung und -beförderung" sowie „Abfallverwertung und -beseitigung“ erbracht.

Die Bereiche sind in Anhang 8 der BSI-KritisV nicht legaldefiniert. Allerdings hält die Begründung zur Verordnung entsprechende Definitionen bereit.[5] Im Folgenden werden diese Definitionen wiedergegeben.

- Die Siedlungsabfallsammlung ist das Einsammeln von Siedlungsabfällen bei den Bürgerinnen und Bürgern sowie dem Gewerbe, einschließlich deren vorläufiger Sortierung und vorläufiger Lagerung zum Zweck der weiteren Beförderung.
- Die Siedlungsabfallbeförderung ist der Transport der gesammelten Siedlungsabfälle von oder zur Abfallbehandlungsanlage einschließlich Vorbehandlungsanlage, sowie zur endgültigen Verwertung oder Beseitigung;
- Die Siedlungsabfallverwertung ist jedes Verfahren, als dessen Hauptergebnis die Siedlungsabfälle einem Zweck zugeführt werden, indem sie entweder andere Materialien ersetzen, die sonst zur Erfüllung einer bestimmten Funktion verwendet worden wären, oder indem die Siedlungsabfälle so vorbereitet werden, dass sie diese Funktion erfüllen, vgl. § 3 Absatz 23 Kreislaufwirtschaftsgesetz (KrWG).
- Die Siedlungsabfallbeseitigung ist jedes Verfahren, das keine Verwertung von Siedlungsabfällen ist, auch wenn das Verfahren zur Nebenfolge hat, dass Stoffe oder Energie zurückgewonnen werden. Zur Verwertung und Beseitigung von Siedlungsabfällen zählen auch die Vorbereitung, insbesondere Vorbehandlungsverfahren, wie die Aufbereitung und Sortierung.

Oftmals werden Verwertung und Beseitigung auch unter dem Begriff der Behandlung zusammengefasst.

2.2.3 Anlagen

Der Begriff der Anlagen wird in § 1 Abs. 1 Nr. 1 BSI-KritisV definiert. Danach sind Anlagen

a) Betriebsstätten und sonstige ortsfeste Einrichtungen,
b) Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen oder
c) Software und IT-Dienste,

die für die Erbringung einer kritischen Dienstleistung notwendig sind.

2.2.4 Gemeinsame Anlage

Gemäß § 1 Abs. 2 BSI-KritisV sind einer Anlage 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

[4] Bundesgesetzblatt Teil 1, Nr. 339, 6.12.2023
(Quelle: https://www.recht.bund.de/bgbl/1/2023/339/regelungstext.pdf?__blob=publicationFile&v=2)
[5] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI3/vo-entwurf-bsi-kritisV-siedlungsabfall.pdf?__blob=publicationFile&v=1

Erbringung der kritischen Dienstleistung notwendig sind. Mehrere Anlagen derselben Kategorie, die durch einen betriebstechnischen Zusammenhang verbunden sind, gelten als gemeinsame Anlage, wenn sie gemeinsam zur Erbringung derselben kritischen Dienstleistung notwendig sind. Betreiben zwei oder mehr Personen gemeinsam eine Anlage, so ist jeder für die Erfüllung der Pflichten als Betreiber verantwortlich.

Darüber hinaus liegt eine Gemeinsame Anlage nach Anhang 8 der BSI-KritisV, Teil 1, Nr. 4 vor, wenn es sich um mehrere Anlagen derselben Art handelt, die in einem engen räumlichen und betrieblichen Zusammenhang stehen. Ein enger räumlicher und betrieblicher Zusammenhang ist gegeben, wenn die Anlagen

- auf demselben Betriebsgelände liegen,
- mit gemeinsamen Betriebseinrichtungen verbunden sind,
- einem vergleichbaren technischen Zweck dienen und
- unter gemeinsamer Leitung stehen.

Erreichen oder überschreiten die Anlagen zusammen die in der BSI-KritisV genannten Schwellenwerte, gilt die gemeinsame Anlage als Kritische Infrastruktur. Hierbei ist es wichtig, dass alle vier oben genannten Bedingungen für eine gemeinsame Anlage erfüllt sein müssen.

2.2.5 Kritische Dienstleistung

Kritische Dienstleistungen sind für die Bevölkerung wichtige, teils lebenswichtige Güter und Dienstleistungen. Bei einer Beeinträchtigung dieser kritischen Dienstleistungen würden erhebliche Versorgungsengpässe, Störungen der öffentlichen Sicherheit oder vergleichbare dramatische Folgen eintreten.

Unabhängig von der gesetzlichen Definition werden die kritischen Dienstleistungen in diesem Branchenstandard als Hilfestellung zur Definition des Geltungsbereichs ihrer kritischen Infrastruktur und zur vereinfachten Betrachtung im Rahmen der Risikoanalyse in folgende Hauptschritte unterteilt:

(a) Sammlung und Beförderung

- Tourenplanung (zeitliche Planung der Sammlung von Siedlungsabfällen aus privaten Haushalten, von Depotcontainerstandplätzen und vom Gewerbe in einem festgelegten Gebiet)
- Personalplanung (Planung des für die Abfallsammlung zuständigen Personals)
- Fahrzeugdisposition (Verwaltung und Zuteilung von Fahrzeugen zur Sammlung von Siedlungsabfällen inkl. der Wartung dieser Fahrzeuge)
- Sammlung und Beförderung (Abholen von Siedlungsabfällen von privaten Haushalten, Depotcontainerstandplätzen oder dem Gewerbe und deren Transport bis zu Umladestationen, Sammel- oder Verwertungsanlagen)
- Lagerung, Zwischenlagerung und Umladen von Abfällen (Lagern von Abfällen zur Erzielung größerer Mengen für den Transportprozess, Umladen von Abfällen in größere Abfalltransportfahrzeugen)

(b) Verwertung und Beseitigung

- Abfallmengenerfassung an der Annahme (Verwiegung vor Abladen an der Verwertungsstelle)
- Abfallvorbehandlung (Vorsortierung, Überprüfung, Durchmischung und ggf. Säuberung von Siedlungsabfällen vor deren Verwertung)
- Lager- und Bunkermanagement (Verwaltung der Lagerstellen, die der Verwertung unmittelbar vorgeschaltet sind)
- Verbrennung (thermische Behandlung von Siedlungsabfällen)

- Sortierung (Trennen von Siedlungsabfällen entsprechend deren Stoffgruppe)
- Behandlung (Anwendung von je nach Abfallart unterschiedlicher Verfahren, die einer umweltschonenden Abfallverwertung oder -beseitigung dienen – bspw. biologische Behandlung)
- Rauchgasreinigung (Entfernen von Schadstoffen aus dem durch die Verbrennung von Siedlungsabfällen entstandenen Rauchgas)

Diese Einteilung der kritischen Dienstleistung im Sektor Siedlungsabfallentsorgung dient als beispielhafte Konkretisierungshilfe, kann vom jeweiligen Betreiber abweichend gewählt werden und hat keinen Einfluss auf die BSI-KritisV. Diese gilt unabhängig davon.

2.2.6 Kritische Infrastrukturen

Kritische Infrastrukturen sind Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und 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 (§ 2 Abs. 10 BSIG).

Die Kritischen Infrastrukturen werden durch die BSI-KritisV näher bestimmt.

2.2.7 Geltungsbereich zum Nachweisen gemäß § 8a Absatz 3 BSIG

Zum Nachweis der Umsetzung der Anforderungen gemäß § 8a Absatz 1 BSIG für seine Anlagen muss der KRITIS-Betreiber einen geeigneten Geltungsbereich für den Prüfgegenstand (Scope) festlegen, die zugrundeliegenden Prozesse feststellen und entsprechende Sicherheitsmaßnahmen planen, umsetzen und dokumentieren.

Die Dokumentation des Geltungsbereichs muss dazu folgende Fragen beantworten:

- Welchen Zweck verfolgt der Betreiber und welche Rolle hat hierbei die KRITIS-Anlage? (Kontext)
- Welche Abläufe bestimmen den Betrieb der KRITIS-Anlage? (Prozesse)
- Wozu dient die IT? (Informationstechnik)
- Welche Zugriffe erfolgen über die Grenzen des Geltungsbereiches hinweg? (Schnittstellen)
- Welche Rolle spielen Externe, z.B. Dienstleister und Lieferanten? (Externe)
- Wie sind die Bestandteile der Anlage vernetzt? (Netzstrukturplan)

Ausführliche Erläuterungen zur Dokumentation des Geltungsbereichs sind auf der BSI-Website veröffentlicht (oder besser siehe BSI-Dokument „Zur Dokumentation des Geltungsbereiches bei KRITIS-Betreibern“).[6]

Als erste Orientierung für den Sektor Siedlungsabfallentsorgung kann die nachfolgende schematische Darstellung des Geltungsbereichs als Ausgangspunkt dienen. Sie zeigt in abstrakter Form die verschiedenen Anlagenkategorien der BSI-KritisV im Kontext der kritischen Dienstleistung. Diese muss für die Nachweiserbringung gemäß § 8a Absatz 3 BSIG anhand der vorgenannten Fragen durch die KRITIS-Betreiber bearbeitet und mit Details aus dem jeweiligen Betrieb versehen werden werden. Ein so dokumentierter Geltungsbereich ist darüber hinaus wesentlicher Bestandteil des Managementsystems für Informationssicherheit (vgl. 3.3).

Der Geltungsbereich (Scope) umfasst in der Regel mindestens die folgenden Aspekte, die direkt zur Sicherstellung der kritischen Dienstleistungen im Sektor Siedlungsabfallentsorgung beitragen:

[6] BSI - KRITIS-Nachweise (bund.de)

- **IT/ OT-Infrastruktur und Kommunikation** (z. B. Netzwerke, Firewalls, Gateways und Router, Systeme zur Angriffserkennung)
- **IT/ OT für die kritischen Dienstleistungen**
    - Sammlung und Beförderung
        - Dispositionssysteme
        - Flottenmanagement
        - Lagermanagement
    - Verwertung und Beseitigung
        - OT-Infrastruktur (z.B. Netztrennung)
        - Regelungs-, Steuerungs- und Leittechnik
        - Mengenmanagement
- **Sonstige relevante Aspekte**
    - Gebäude und Räume
    - Warten und Leitstände
    - Personal
    - Prozesse
- **Extern erbrachte Leistungen**
    - Systemhärtung, Schwachstellen- und Patchmanagement für bereitgestellte Produkte
    - Ausgelagerte System- und Softwareentwicklung
    - Fernzugriff
    - Versorgungsdienstleistungen (z.B. Energie, Wasser, etc.)
    - Personaldienstleistungen
    - Cloud-Anwendungen und -Infrastrukturen
    - Wartungsdienstleistungen
    - Externe Rechenzentren

Nicht im Geltungsbereich enthalten sind:

- Bereiche oder Systeme, die nicht unmittelbar mit den kritischen Dienstleistungen verbunden sind.
- Prozesse und Infrastrukturen, die keinen Einfluss auf die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der für die kritischen Dienstleistungen essenziellen Systeme haben.
- Allgemeine IT-Systeme, die keine Relevanz für die kritischen Dienstleistungen aufweisen.
- Leistungen und Ressourcen, die unabhängig von der spezifischen kritischen Dienstleistung sind (z. B. generelle Verwaltungsprozesse).

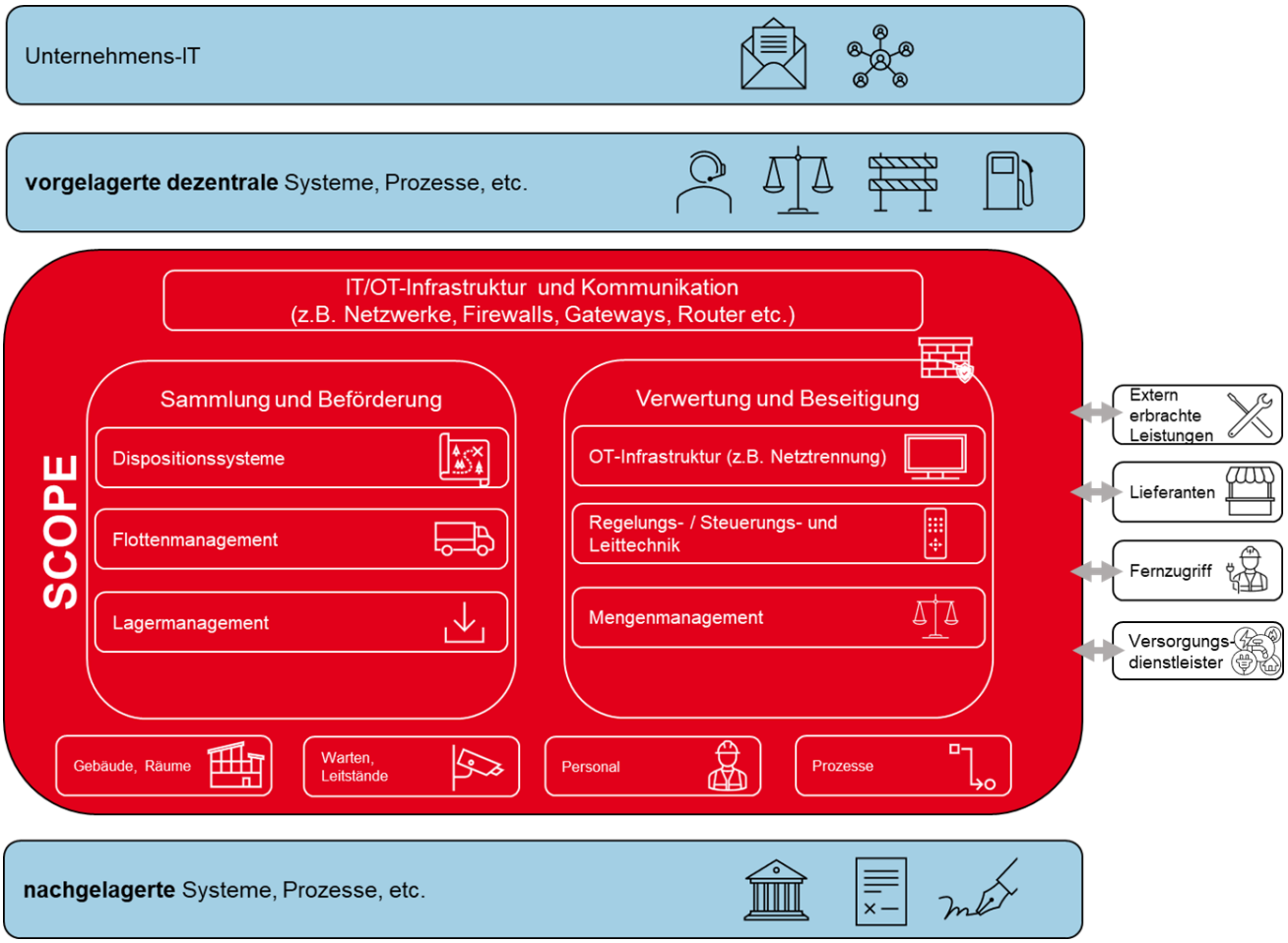

Abbildung 1: Schematische Darstellung des Geltungsbereichs

Im vorliegenden Dokument wird im Wesentlichen der Begriff IT (Information Technology) verwendet. Dieser schließt dabei ausdrücklich die OT (Operational Technology) mit ein, soweit diese für die kritische Dienstleistung relevant ist.

2.2.8 Informationstechnische Systeme, Komponenten und Prozesse

Im Sinne des Informationssicherheitsmanagementsystems sowie der Anforderungen an Betreiber Kritischer Infrastrukturen sind **informationstechnische Systeme, Komponenten und Prozesse** wie folgt zu verstehen:

1. **Informationstechnische Systeme** sind Gesamtheiten aus Hard- und Software, die der Erfassung, Verarbeitung, Speicherung, Übertragung oder Bereitstellung von Informationen dienen und unmittelbar oder mittelbar zur Aufrechterhaltung wesentlicher Geschäfts- oder Versorgungsprozesse beitragen.
2. **Komponenten** sind einzelne technische oder logische Bestandteile informationstechnischer Systeme, deren Funktion für den sicheren Betrieb erforderlich ist. Hierzu zählen insbesondere Anwendungen, Datenbanken, Netzwerkelemente, Schnittstellen sowie sicherheitsrelevante Module.
3. **Prozesse** sind organisatorische oder technische Abläufe, die den Betrieb, die Steuerung oder die Absicherung informationstechnischer Systeme unterstützen oder gewährleisten. Hierunter fallen sowohl automatisierte Abläufe als auch manuelle Verfahren, insbesondere solche der Benutzer- und Rechteverwaltung, des Patch- und Änderungsmanagements, der Datensicherung sowie der Notfallvorsorge.

Informationstechnische Systeme, Komponenten und Prozesse im Sinne dieser Definition sind als schützenswerte Objekte anzusehen, sofern deren Beeinträchtigung, Ausfall oder Manipulation geeignet ist, die Verfügbarkeit, Integrität, Vertraulichkeit oder Authentizität von Informationen oder die Funktionsfähigkeit einer Kritischen Infrastruktur wesentlich zu beeinträchtigen.

3 Grundlagen

Im Nachfolgenden werden die grundlegenden Elemente im Sinne der Nutzung des B3S SAE näher beschrieben.

3.1 Allgemeines

Grundlegendes Ziel im Rahmen der Daseinsvorsorge ist die Sicherstellung der kritischen Dienstleistung, d. h. die Gewährleistung der Entsorgungssicherheit für Siedlungsabfälle. Einen wesentlichen Baustein stellt dabei die Informationssicherheit im Sinne der Wahrung von Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von Informationen dar, d. h. der Schutz der informationstechnischen Systeme, Komponenten, Prozesse.

Ein Informationssicherheitsmanagementsystem (ISMS) nach DIN EN ISO/IEC 27001:2024 unterscheidet organisatorische, personenbezogene, physische und technologische Controls, die in den Kapiteln 5 bis 8 genauer und an die Umstände der Abfallwirtschaft angepasst dargestellt werden. Dieser Branchenspezifische Sicherheitsstandard nimmt in den entsprechenden Kapiteln auf die jeweiligen Abschnitte der DIN EN ISO/IEC 27001:2024 Bezug, welche damit **die wesentliche Grundlage** für die Ableitung der entsprechenden Maßnahmen bildet. Diese Maßnahmen wiederum sind in der DIN EN ISO 27002 aufgeführt. Darüber hinaus stellt der Anhang 1 „Branchenspezifische Risiken“ die Beziehung zwischen Bedrohungen/ Schwachstellen und den Controls aus den Kapiteln 5 bis 8 her.

Mit Blick auf den Schutz der informationstechnischen Systeme, Komponenten, Prozesse und Daten im Allgemeinen und die eingesetzte Sicherheitstechnik bzw. -maßnahmen im Speziellen muss grundsätzlich eine ganzheitliche Betrachtung der angestrebten Schutzziele im Rahmen eines einheitlichen Sicherheitskonzepts erfolgen. Dieses Sicherheitskonzept sollte neben der originären Informationssicherheit auch physische Aspekte (etwa Zutrittsrechte zu bestimmten Räumen) sowie weitere über den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards für Siedlungsabfallentsorgung hinausgehende Aspekte, wie z. B. den Brandschutz berücksichtigen.

Der notwendige Schutz der informationstechnischen Systeme, Komponenten, Prozesse und Daten ist bereits frühzeitig bei Planung und Erstellung entsprechender Systeme, bei der Beschaffung entsprechender Komponenten und insbesondere bei der Beauftragung von Dienstleistern zu berücksichtigen.

In Anhang A.1 werden branchenspezifische Risiken beschrieben, welche durch geeignete Maßnahmen aus den Kapiteln 5 bis 8 behandelt werden. Die Kapitel 5 bis 8 enthalten branchenspezifische Ergänzungen zur DIN EN ISO/IEC 27001:2024, um die branchenspezifischen Risiken zu adressieren. Es ist daher besonders wichtig, dass Betreiber den Anhang A.1 in Bezug auf dessen Übereinstimmung mit den bei ihnen jeweils vorliegenden Bedingungen überprüfen.

3.2 Schutzziele

Der Schutz der informationstechnischen Systeme, Komponenten und Prozesse verfolgt die Schutzziele:

- Verfügbarkeit,
- Integrität,
- Authentizität,
- Vertraulichkeit.

Aus dem Betrachtungswinkel dieses B3S SAE ist die Verfügbarkeit als Schutzziel zur Sicherstellung der Versorgung der Bevölkerung mit der Dienstleistung Siedlungsabfallentsorgung oberstes Schutzziel der Informationssicherheit. Die weiteren Schutzziele Integrität, Authentizität und Vertraulichkeit werden

aufgrund ihrer möglichen Auswirkungen für die Verfügbarkeit mitbewertet. Über diese allgemeinen Schutzziele hinausgehende branchenspezifische Informationssicherheits-Schutzziele bestehen nicht.

Die Schutzziele bestehen darin, dass

- (Teil-)Ausfälle, Ausfallzeiten und Beeinträchtigungen der informationstechnischen Systeme, Komponenten oder Prozesse vermieden werden und ein Zugriff auf die relevanten Daten im Rahmen der für die jeweilige Anlage festgelegten Verfügbarkeit möglich ist,
- die unautorisierte Modifikation der informationstechnischen Systeme, Komponenten oder Prozesse und ihrer Daten verhindert wird (korrekte Funktion der Systeme und Unversehrtheit der Daten),
- die Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit der Daten und ihrer Herkunft gewährleistet wird,
- die Informationen vor unbefugter Preisgabe geschützt sind.

3.3 Managementsystem zur Informationssicherheit (ISMS)

SAE-Betreiber, die Kritische Infrastrukturen betreiben, sind zum Einsatz angemessener technischer und organisatorischer Sicherheitsvorkehrungen, die dem „Stand der Technik“ entsprechen, zum Schutz der KRITIS-Anlagen verpflichtet.

Es ist sicherzustellen, dass das Erreichen und Aufrechterhalten des Stands der Technik für die IT-Systeme des SAE-Betriebs bei Kritischen Infrastrukturen in geeigneter Weise in der Organisation des SAE-Betreibers verankert ist. Im Rahmen der Definition des Anwendungsbereichs des Managementsystems haben SAE-Betreiber die für sie relevanten kDL-Hauptschritte aus Kap. 2.2.5 zu bestimmen und ihr Managementsystem daran auszurichten.

Die Gewährleistung einer ausreichenden Informationssicherheit liegt in der Verantwortung der Unternehmens-/Organisationsleitung und ist daher innerhalb der Organisationsverantwortung von oben nach unten zu organisieren (Top-down-Ansatz).

Diese Anforderungen können zum Beispiel durch Einführung eines ISMS nach DIN EN ISO/IEC 27001:2024 erfüllt werden. Eine formale Zertifizierung ist nach dem BSIG nicht zwingend. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen.

Für Betreiber Kritischer Infrastrukturen ist die Aufstellung und Einführung von Verfahren und Regeln zwingend erforderlich. Dies hat den Zweck die Informationssicherheit zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Ein bestehendes zertifiziertes ISMS kann dies deutlich erleichtern.

Beim Aufbau eines ISMS können die Dokumente

- BSI-Standard 200-1: Managementsysteme für Informationssicherheit
- BSI-Standard 200-2: IT-Grundschutz-Methodik
- BSI-IT-Grundschutz-Kompendium 2023
- BSI-ICS-Security-Kompendium
- DIN EN ISO/IEC 27002
- DIN ISO/IEC TR 27019.

unterstützen

Jedenfalls muss dem BSI durch die Betreiber Kritischer Infrastrukturen entsprechend der relevanten Gesetzgebung nachgewiesen werden, dass angemessene organisatorische und technische

Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse nach dem Stand der Technik getroffen wurden (siehe § 8a Abs. 3 S. 1 BSIG). Dies umfasst auch den Einsatz von Systemen zur Angriffserkennung, § 8a Abs. 1a BSIG. Siehe auch Kapitel 4

Das Assetmanagement ist ein zentraler Bestandteil eines Informationssicherheits-managementsystems, da es die Grundlage für den Schutz von Informationen und Ressourcen bildet. Nur wenn alle relevanten Werte wie Hardware, Software, Daten und Dienstleistungen bekannt und klassifiziert sind, können angemessene Schutzmaßnahmen definiert werden. Ein strukturiertes Assetmanagement unterstützt beispielsweise bei folgenden Vorgängen:

- Erkennung und Bewertung von Risiken im Rahmen der Risikoanalyse
- Erstellung von Notfallplänen im Rahmen des betrieblichen Kontinuitätsmanagements (BCM)
- Festlegung von Verantwortlichkeiten je Asset

3.4 Betriebliches Kontinuitätsmanagement (BCM)

Beim betrieblichen Kontinuitätsmanagement (Englisch: Business Continuity Management) handelt es sich gemäß BSI Standard 200-4 um die Steuerung sämtlicher Aktivitäten, die eine geordnete Geschäftsfortführung nach Schadensereignissen zum Ziel haben,

Zu unterscheiden sind zwei wichtige Bereiche:

1. Vorsorge (Geschäftsprozesse sollten möglichst nicht unterbrochen werden.)
2. Reaktion (Geschäftsprozess sollten nach einem Ausfall in angemessener Zeit wieder hergestellt werden.)

Für die Betreiber Kritischer Infrastrukturen im Sektor Siedlungsabfallentsorgung gelten gemäß § 8a BSIG (vgl. 2.1), unabhängig von den IT-Systemen, Grundanforderungen in Bezug auf die Fortsetzung des Betriebs bei Störungen, die das Einführen eines Business Continuity Management Systems (BCMS) erforderlich machen.

Das BCMS enthält gemäß BSI-Standard 200-4 Strukturen, Regeln und einen Aufbau innerhalb einer Institution, um eine geordnete Geschäftsfortführung nach Schadensereignissen in der Institution zu erreichen. Für den Aufbau eines BCMS können etablierte Standards wie der BSI-Standard 200-4 oder die DIN EN ISO 22301 genutzt werden.

Betreiber kritischer Infrastrukturen haben beispielhaft die folgenden BCM-Aktivitäten in Bezug auf die durch sie betriebene kritische Infrastruktur gemäß BSI-KritisV umzusetzen;

- **Erstellung eines Plans zur Aufrechterhaltung der kritischen Dienstleistung (Continuity Plan)**
  Dokumentation präventiver Maßnahmen und Verfahren, die den Eintritt eines Schadensereignisses verhindern können oder dessen Auswirkungen auf die kritische Dienstleistung reduzieren (darunter zählen bspw. Redundanz- und Härtungsmaßnahmen).

- **Erstellung eines Notfallhandbuchs mit Notfallplänen**
  Dokumentation aller Informationen, die für die Notfallbewältigung benötigt werden und mit denen planbare Ereignisse (bspw. Stromausfall, Naturkatastrophen oder weitreichender Virenbefall) innerhalb eines vorab definierten Notbetriebs bewältigt werden können.

- **Sicherstellung einer geeigneten Verzahnung des BCMS für die kritische Dienstleistung mit dem ISMS für die kritische Infrastruktur**

Bestimmen von gemeinsam nutzbaren Organisationstrukturen und Verantwortlichkeiten inkl. der Vermeidung von redundanten oder widersprüchlichen Vorgaben zur Bewältigung von Notfallsituationen.

- **Durchführen von Business-Impact-Analysen**
  strukturierte Untersuchung mit dem Ziel, (zeit-)kritische Geschäftsprozesse und Ressourcen (Assets) der kritischen Dienstleistung zu identifizieren.
  Hierzu werden diejenigen direkten und indirekten potentiellen Folgeschäden für die SAE-Betreiber ermittelt, die durch den Ausfall von Geschäftsprozessen verursacht werden können. Daraus werden die Anforderungen an den Wiederanlauf von Geschäftsprozessen abgeleitet.

- **Single-Point-of-Failure-Analysen**
  Analysen in Bezug auf Komponenten, deren Ausfall den Ausfall der gesamten Anlage bzw. kritischen Dienstleistung auslösen kann, um geeignete kompensierende oder Redundanzmaßnahmen zu identifizieren.

- **Entwicklung von Kontinuitäts- und Wiederanlaufstrategien und -Plänen**
  Dokumentation, die beschreibt, wie ein SAE-Betreiber ausgefallene Ressourcen, z. B. durch umgesetzte Business-Continuity-Lösungen oder Ersatzlösungen, kompensieren kann, um einen Notbetrieb zu gewährleisten, der die die Fortführung der kritischen Dienstleistung sicherstellt.

Betreiber Kritischer Infrastrukturen gemäß BSI-KritisV haben Vorgehensweisen zur Bewältigung seltener oder besonders folgenreicher Ereignisse (bspw. durch Systemtests, Kommunikationsübungen oder Table-Top-Exercises) zu üben.

3.5 Risikoeinschätzung und – Bewertung (inkl. Bedrohungsanalyse)

Für die im Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards liegenden informationstechnischen Systeme und Prozesse sollte anlassbezogen, mindestens jedoch jährlich, eine Risikoanalyse durchgeführt werden.

Die Risikoanalyse sollte explizit auf die branchenspezifischen Bedrohungen (definiert als potenzielle Gefahr wie bspw. technische Fehler oder Angreifer) und Schwachstellen (Eigenschaft, die von einer Bedrohung ausgenutzt werden kann) eingehen, die für Systeme und Anlagen bestehen, die zur Sammlung bzw- Beförderung oder zur Verwertung bzw. Beseitigung von Siedlungsabfällen genutzt werden.

Dazu ist eine Bedrohungsanalyse durchzuführen mithilfe derer sich die verschiedenen Bedrohungen für IT-Systeme und IT-Prozesse systematisch erfassen, strukturieren und bewerten lassen.

Die Bedrohungsanalyse konzentriert sich als Teil der Gesamtrisikoanalyse auf die einzelnen Bedrohungen von Rechnersystemen, Anwendungen und Kommunikationsnetzen. Aus den identifizierten Bedrohungen lassen sich als Ergebnis die einzelnen Risiken für das Risikomanagement ableiten.

Das grundsätzliche Vorgehen einer Risikoanalyse kann dem BSI Standard 200-3[7] entnommen werden.

[7] vgl. BSI - BSI-Standard 200-3: Risikomanagement - BSI-Standard 200-3

Für IT-Systeme im Sinne dieses Branchenspezifischen Sicherheitsstandards existiert eine Vielzahl möglicher Bedrohungen, die im Rahmen der Bedrohungsanalyse identifiziert, erfasst und in Bezug auf deren Auswirkung auf den Betrieb der kritischen Dienstleistung bewertet werden müssen.

Eine beispielhafte Auflistung der im Rahmen dieses Branchenspezifischen Sicherheitsstandards als relevant eingestuften Bedrohungen, elementare Gefährdungen und Schwachstellen ist Anhang A.3 zu entnehmen. Diese Auswahl von Bedrohungen, elementare Gefährdungen und Schwachstellen ist nicht abschließend und nicht allgemeingültig. Jeder SAE-Betreiber ist angehalten, die für ihn relevanten Bedrohungen und Schwachstellen entsprechend seiner betriebenen Anlagen zu identifizieren.

Die branchenspezifischen Systeme und Prozesse können beispielsweise in Form von technischen Funktionen gebündelt betrachtet werden. Mittels der technischen Funktionen kann der Zusammenhang zwischen den in 2.2.5 beschriebenen Hauptschritten und den eingesetzten informationstechnischen Systemen hergestellt werden.

Technische Funktionen beantworten die Frage „Wer macht was mit welchem System und zu welchem Zweck?“. Ein Beispiel für die funktionsbasierte Vorgehensweise bietet die im Anhang A.1 beschriebene Herleitung der branchenspezifischen Risiken.

SAE-Betreibern ist es dabei freigestellt, zunächst eine sogenannte „Brutto-Risikoanalyse“ durchzuführen, im Rahmen derer vorhandene Schutzmaßnahmen noch nicht bei der Bewertung der Eintrittswahrscheinlichkeit und der Auswirkungen einer Gefährdung berücksichtigt werden. Dieser „Greenfield“-Ansatz macht explizit, wie die Ausgangslage des Betreibers bereits Umstände und Gegebenheiten enthält, die die Risikolage sicherheitswirksam beeinflussen.

SAE-Betreiber müssen aber mindestens eine sogenannte „Netto-Risikoanalyse“ durchführen, im Rahmen derer die aktuelle Risikolage identifiziert wird und die Wirkung bereits implementierter Schutzmaßnahmen berücksichtigt wird. Diese Betrachtung ist maßgeblich dafür, weiteren Handlungsbedarf zur Risikoreduzierung feststellen zu können.

In jedem Fall sind Risikoszenarien zu formulieren, die die Wirkung der branchenspezifischen Bedrohungen und Schwachstellen auf die branchenspezifischen Systeme und Prozesse beschreiben. Die Risikoszenarien müssen dann bezüglich ihrer

- Eintrittswahrscheinlichkeit (definiert als durch geeignetes Fachpersonal geschätzte Wahrscheinlichkeit des Eintritts) und
- Schadensauswirkungen, insbesondere unter Berücksichtigung der Kritikalität der am Szenario beteiligten Systeme und Prozesse, bewertet werden.

Aus der Kategorie (gering, mittel, hoch, sehr hoch) des aus dieser Bewertung resultierenden Risikos leitet sich anschließend die Priorität der Maßnahmen ab, die zur Behandlung der Risikoszenarien geeignet sind. So sind bspw. Maßnahmen zur Reduzierung sehr hoher Risiken höher zu priorisieren als Maßnahmen zur Reduzierung mittlerer oder geringer Risiken.

Zur Validierung der Angemessenheit und Vollständigkeit der durchgeführten Netto-Risikoanalyse, sollten SAE-Betreiber außerdem das sogenannte „Restrisiko“ bestimmen. Das Restrisiko beschreibt das Risiko einer Gefährdung (konkret: die aus der Ausnutzung der Schwachstelle durch die Bedrohung entstehende Gefährdung bzw. das entstehende Gefährdungspotenzial) unter Berücksichtigung der risikoreduzierenden Wirkung bereits umgesetzter und geplanter Maßnahmen. So ist es möglich, festzustellen, ob die geplanten Maßnahmen ausreichend sind, um das Risiko auf ein akzeptables Niveau zu reduzieren.

Bei der Umsetzung der Risikoanalyse wird den SAE-Betreibern empfohlen, sich am BSI-Standard 200-3[8] zu orientieren.

Im Hinblick auf die Eintrittswahrscheinlichkeit und Verwundbarkeit wird auf folgende Unterscheidung verwiesen:

- unwahrscheinlich
  - Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
  - Es gibt praktisch unüberwindbare Hürden (sehr geringer Grad an Vernetzung, Automatisierung und Digitalisierung innerhalb der Anlage).
- mittel
  - Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
  - Es sind viele Hürden zu überwinden (Zugriff nur lokal möglich, mehrstufige Authentifizierung notwendig, spezifisches, nicht öffentlich bekanntes Know-How notwendig, sehr zeitaufwendig und ressourcenintensiv).
- wahrscheinlich
  - Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
  - Es sind manche Hürden zu überwinden (Zugriff aus Büro-IT-Netzwerk möglich, Authentifizierung notwendig, benötigtes Know-How öffentlich in Erfahrung zu bringen, zeitaufwendig mit gewissem Einsatz von Ressourcen).
- sehr wahrscheinlich
  - Ereignis tritt mehrmals im Monat ein.
  - Es sind kaum Hürden zu überwinden (Zugriff aus dem Internet möglich, keine Authentifizierung notwendig, kein dediziertes Know-How notwendig, ohne großen Zeitaufwand und ohne Ressourceneinsatz).

In Bezug auf die Einschätzung der Schadensauswirkungen können sich SAE-Betreiber an folgenden Kategorien orientieren:

- vernachlässigbar - Schadensauswirkungen sind gering und können vernachlässigt werden.
- begrenzt - Schadensauswirkungen sind begrenzt und überschaubar.
- beträchtlich - Schadensauswirkungen können beträchtlich sein.
- existenzbedrohend - Schadensauswirkungen können existenziell bedrohliches, katastrophales Ausmaß erreichen.

Die Einschätzung der Schadensauswirkung muss von jedem SAE-Betreiber **selbst vorgenommen werden**. Bezogen auf die kritischen Dienstleistungen wäre die folgende Einschätzung der Schadensauswirkung eine **erste Orientierung**.

Auswirkung	Sammlung & Beförderung	Verwertung & Beseitigung
Vernach-lässigbar	geringfügige Verzögerung der Sammlung/Beförderung; Vorfälle können mit eigenen Ressourcen bewältigt werden	Verzögerte Abwicklung der Anlieferung und Verarbeitung von Materialien ohne Anlagenstillstand (unter Umständen müssen eigene Lagerkapazitäten zusätzlich in Anspruch genommen werden)

[8] vgl. BSI - BSI-Standard 200-3: Risikomanagement - BSI-Standard 200-3

Begrenzt	erhebliche Verzögerungen der Sammlung/Beförderung; Vorfälle können unter erhöhtem Aufwand oder unter Einsatz unüblicher Ressourcen bewältigt werden	Anlagenstillstand, der durch eigene Lagerkapazitäten abgefangen werden kann
Beträchtlich	Störung der Sammlung/Beförderung in einer Dauer, die zum Erreichen des individuell zu ermittelnden Untragbarkeitsniveaus gem. BSI Standard 200-4 Business Continuity Mangement führt. Dies kann beispielweise der Fall sein, wenn die eigene Sammlungskapazität nicht ausreicht.	Anlagenstillstand in einer Dauer, die zum Erreichen des individuell zu ermittelnden Untragbarkeitsniveaus gem. BSI Standard 200-4 Business Continuity Mangement führt. Dies kann beispielweise der Fall sein, wenn die eigene Lagerkapazität nicht ausreicht
existenz-bedrohend	Ob eine existenzbedrohende Lage möglich ist, muss durch den Betreiber ermittelt werden.	Ob eine existenzbedrohende Lage möglich ist, muss durch den Betreiber ermittelt werden. Eine Existenzbedrohende Lage kann durch einen IT/OT verursachten physischen Schaden, der zum vollständigen Anlagenausfall führt, herbeigeführt werden.

Tabelle 1: Einschätzung der Auswirkungen

Aus der Eintrittswahrscheinlichkeit und der Schadensauswirkung ergibt sich ein 4 x 4 Matrix zur Einstufung der Risiken:

Schadensauswirkung	existenzbedrohend	mittel	hoch	sehr hoch	sehr hoch
	beträchtlich	mittel	mittel	hoch	sehr hoch
	begrenzt	gering	gering	mittel	hoch
	vernachlässigbar	gering	gering	gering	gering
		unwahrscheinlich	mittel	wahrscheinlich	Sehr wahrscheinlich
		Eintrittswahrscheinlichkeit			

Tabelle 2: Risikomatrix in Anlehnung an BSI-Standard 200-3

Die Risikokategorien, die als Ergebnis der Risikobewertung je Risikoszenario bestimmt werden, können wie folgt interpretiert werden:

Risikokategorie	Bedeutung
gering	Die bereits umgesetzten oder zumindest vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz
mittel	Die bereits umgesetzten oder zumindest vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus

hoch	Die bereits umgesetzten oder zumindest vorgesehenen Sicherheitsmaßnahmen bieten möglicherweise keinen ausreichenden Schutz vor dem jeweiligen Risikoszenario
sehr hoch	Die bereits umgesetzten oder zumindest vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor dem jeweiligen Risikoszenario.

Tabelle 3: Risikokategorien in Anlehnung an BSI-Standard 200-3

3.6 Risikobehandlung

Die Risikoermittlung über die Risikomatrix liefert noch keine Risikobewertung. Diese Risikoermittlung ist aber Voraussetzung, dass eine Risikobehandlung stattfinden kann.

Zur Umsetzung einer Risikobewertung kann der BSI Standard 200-3 5.2 herangezogen werden.

Risiken auf die Erbringung der kritischen Dienstleistung sind zwingend zu reduzieren. Organisatorische und technische Vorkehrungen für die Reduzierung der Risiken sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

Eine Akzeptanz oder ein Transferieren von hohen oder sehr hohen Restrisiken ist SAE-Betreibern für ihren festgelegten Geltungsbereich nicht gestattet.

Eine dauerhafte Risikoakzeptanz durch den SAE-Betreiber ist nicht zulässig (BSI-G).

Eine eigenständige dauerhafte Akzeptanz oder ein Transferieren von Risiken für die kritische Dienstleistung selbst ist keine zulässige Option gemäß dem BSIG.

Zur Herleitung risikoreduzierender Maßnahmen kann auf den Annex A der DIN EN ISO/IEC 27001:2024, auf die Umsetzungshinweise der DIN EN ISO/IEC 27002:2024 und auf die Kap. 5 bis 8 dieses Branchenspezifischen Sicherheitsstandards zurückgegriffen werden.

Diese Maßnahmen können im Rahmen eines Risikobehandlungsplans unter Beachtung folgender Parameter geplant werden:

- Zuständigkeiten für die Umsetzung
- Zieldatum
- Verweis auf Annex A der DIN EN ISO/IEC 27001:2024
- Ressourcenbedarf
- Umsetzungsstatus
- Wirksamkeitskontrolle

Bei einer Aufgabenübertragung an Externe durch Outsourcing o. Ä. verbleibt die volle Verantwortung für das Risikomanagement inklusive einer geeigneten Risikobehandlung beim Betreiber.

4 Angriffserkennung

Die Betreiber Kritischer Infrastrukturen sind in Deutschland dazu verpflichtet, Systeme zur Angriffserkennung (SzA) einzusetzen, um ihre Informationssysteme zu schützen.

Das BSIG hält für Angriffserkennungssysteme folgende Definition bereit: „Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten“ (§ 2 Absatz 9b BSIG).

Daraus ergeben sich für Systeme zur Angriffserkennung im Hinblick auf deren Funktionalität die wesentlichen Aufgabenbereiche der Protokollierung, Detektion und Reaktion.

- Die Protokollierung sammelt Informationen z.B. aus dem Netzverkehr sowie Daten der Infrastruktur und zeichnet diese auf.
- Die Detektion erkennt aus der Protokollierung sicherheitsrelevante Ereignisse. Dies kann beispielsweise durch Missbrauchserkennung oder Anomalie-Erkennung erfolgen.
- Im Rahmen der Reaktion sollten Systeme zur Angriffserkennung Maßnahmen implementieren, um Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren. Die technischen Maßnahmen wie z.B. IPS (Intrusion Prevention System) und EDR (Endpoint Detection & Response) sind zu etablieren bzw. bzgl. ihrer Erforderlichkeit und Umsetzbarkeit zu evaluieren.

Der Einsatz von SzA muss die informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, abdecken.

4.1 Allgemeine Anforderungen

Die Anforderungen aus der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung des BSI sind beim Einsatz von Systemen zur Angriffserkennung[9] zu beachten. Für die Feststellung des Umsetzungsgrads des Einsatzes von Systemen zur Angriffserkennung kann die Definition der Umsetzungsgrade der Orientierungshilfe und der BSI-RUN[10] verwendet werden.

4.2 Umfang der Angriffserkennung („risikobasierter Ansatz“)

Bevor eine Angriffserkennung etabliert werden kann, muss deren erforderliche Art und Umfang bestimmt werden. Als Eingangsgrößen (Datenquellen) für technische Werkzeuge zur Angriffserkennung dienen dabei unter anderem Netzwerkmonitoring, Eventlogs und Meldungen von Detection and Response Systemen. Es ist risikobasiert zu prüfen, welche Assets in welchem Umfang aktiv Informationen an eine zentrale Melde- und Auswerteinstanz (engl. Security Information and Event Monitoring, SIEM) senden sollten.

Die Evaluierung für die Angriffserkennung muss:

- die relevanten Angriffsvektoren identifizieren,
- im Umfang als auch in der Tiefe (Sensitivität) definiert werden,
- gewährleisten, dass bei der Implementierung einer Methode berücksichtigt wird, dass es keine Rückwirkung / Beeinträchtigung auf bestehende Systeme geben darf.

[9] „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“, Version 1.1 vom 18.11.2024, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=18

[10] Reife- und Umsetzungsgradbewertung im Rahmen der Nachweisprüfung (RUN), Version 1.0 vom 02.01.2025, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/run.pdf?__blob=publicationFile&v=9

Dabei zu beachten sind folgende Parameter:

- Wie können Angriffe erkannt werden und wo sollte die Erkennung sinnvollerweise erfolgen?
- Gibt es abgeschottete Bereiche, wo Angriffe durch Innentäter erfolgen können und wie können diese adäquat überwacht werden?
- Wie können Angriffserkennungssysteme angelernt und konfiguriert werden, um möglichst alle tatsächlichen Angriffe (True Positives) zu erkennen und gleichzeitig möglichst wenige Fehlalarme (False Positives) zu erzeugen. Betriebsspezifische Situationen müssen Berücksichtigung finden, damit eine Entdeckung von vermeintlichen Angriffen bewertet werden kann (z.B. stellt eine Veränderung eines Programms einer speicherprogrammierbaren Steuerung (SPS-Programm) während des Engineerings in der Regel keinen Angriff dar, während die Veränderung eines SPS-Programms im laufenden Betrieb auf einen Angriff hindeuten würde).
- Welche Methoden der Angriffserkennung können in der Infrastruktur eingesetzt werden? Welche Komponenten und Netzwerkstrukturen liegen vor?

Im Sektor Siedlungsabfallentsorgung orientiert sich der Umfang der Angriffserkennung auch an den Möglichkeiten, die bspw. OT-spezifische Protokolle und Systeme ohne (Remote-)-Logging bieten. Ebenso können Einschränkungen durch Hersteller z.B. in Bezug auf die Installation von Agenten den Umfang weiter einschränken. Die Ableitung von Ersatzmaßnahmen muss dann auf Grundlage einer Risikobetrachtung erfolgen.

Bei der organisatorischen Einbindung von Systemen zur Angriffserkennung ist beispielhaft zu berücksichtigen, dass klare Zuständigkeiten und Prozesse für die Überwachung, Analyse und Reaktion definiert sind. Es sollte festgelegt sein, wer Alarme entgegennimmt, bewertet und gegebenenfalls Eskalationen einleitet. Zudem müssen die Systeme in ein übergeordnetes Sicherheitskonzept integriert und Schnittstellen zu Incident-Management- und Notfallprozessen berücksichtigt werden. Auch Schulungen der Mitarbeitenden und regelmäßige Tests sind wichtig, um die Wirksamkeit sicherzustellen.

4.3 Komponenten und Methoden der Angriffserkennung

Komponenten zur Erkennung von Angriffen sind Netzsensoren und Hostsensoren. Mit Netzsensoren werden Informationen in der Kommunikation zwischen Systemen gesammelt, Hostsensoren sammeln Informationen über ein System und dessen Betriebssystem, die Anwendungen auf einem System und ggf. auch über dessen interne und externe Netzwerkkommunikation.

Netzsensoren haben den Vorteil, dass die Systeme nicht verändert werden. Dafür sind sie nicht in der Lage, Veränderungen an den Host-Systemen zu erkennen oder verschlüsselten Datenverkehr inhaltlich auszuwerten.

Systeme zur Angriffserkennung enthalten außer den Sensoren und Host-Agents noch weitere Komponenten zur Verwaltung, Datensammlung sowie Auswertung der gesammelten Daten.

Methoden zur Angriffserkennung verarbeiten die gewonnenen Informationen, um einen Angriff zu erkennen. Übliche Methoden zur Angriffserkennung sind die statische Mustererkennung, die Anomalie-Erkennung und die Datenkorrelation. Die Kombination von mehreren Methoden zu einem hybriden Ansatz ist heute Stand der Technik.

4.3.1 Statische Angriffsmustererkennung

Bei der statischen Erkennung von Angriffsmustern werden Muster von bereits bekannten Angriffen gesucht. Dies kann in Dateien erfolgen (z. B. signaturbasierter Scan nach Viren) oder auch in Netzwerkverkehr (Verbindungsversuche zu bestimmten IP-Adressen, DNS-Adressen oder URLs).

4.3.2 Anomalie-Erkennung

Durch die Auswertung von Logdateien, durch statistische Methoden oder KI-gestützt werden Abweichung vom Normalbetrieb erkannt, die auf einen Angriff hinweisen können. Beispiele für solche Abweichungen sind Benutzeranmeldungen zu ungewohnter Zeit, Netzwerkverkehr zwischen Systemen, die sonst keine Daten miteinander austauschen, ein starker Anstieg der Systemlast oder eine ungewöhnlich hohe Anzahl an veränderten Dateien. Eine Anomalie-Erkennung kann auch durch Honeypots (Scheinziele) erfolgen, also Systeme, auf die im Normalbetrieb nie zugegriffen wird, so dass jeder Zugriff eine Anomalie darstellt oder über eine Integritätsüberwachung, also zum Beispiel die zyklische Überwachung, ob Dateien unerwartet verändert wurden.

4.3.3 Korrelation

In den gesammelten Daten können durch die Verknüpfung von Daten unterschiedlicher Quellen oder Zeiträumen Muster gefunden werden, die auf einen Angriff hinweisen. Solche Daten sind auch für die forensische Untersuchung von (möglichen) Vorfällen hilfreich.

5 Organisatorische Anforderungen

Das Treffen von geeigneten Maßnahmen zum Schutz der Informationssicherheit ist in der Organisationsverantwortung der Geschäftsführung eines Betriebs. Die Maßnahmen müssen daher in der Betriebsorganisation wirksam verankert und dokumentiert sein.

Im Folgenden werden organisatorische Anforderungen zur Förderung der Informationssicherheit vorgestellt, die zur Ableitung von geeigneten Maßnahmen dienen. Diese wurden aus der DIN EN ISO/IEC 27002:2024 übernommen und teilweise um branchenspezifische Präzisierungen im Sinne von Hinweisen, Ergänzungen oder Beispielen ergänzt. Wenn die Präzisierung sich nicht direkt auf Anlagen oder Anlagenkategorien bezieht, gilt sie für alle Anlagen und Anlagenkategorien im Sektor Siedlungsabfallentsorgung. Die Anforderungen der genutzten Prüfgrundlage (bspw. DIN EN ISO/IEC 27002:2024) sind zu beachten.

In diesem Rahmen geht es zum einen darum, dass klare Verantwortlichkeiten für die Gewährleistung der Informationssicherheit im jeweiligen Unternehmen festgelegt werden. Ferner ist auch wesentlich, dass die im Interesse der Informationssicherheit zu beachtenden innerbetrieblichen Regeln festgelegt, kommuniziert und vollzogen werden und der Informationsfluss im Unternehmen, der für die Gewährleistung der Informationssicherheit relevant ist, funktioniert. Weitere wichtige Aspekte sind die Verwaltung von Hard- und Software (inklusive Zuteilung von Benutzungs- und Zugangsrechten und der Überprüfung von Lieferantendienstleistungen).

5.1 Informationssicherheitspolitik und-richtlinien

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.1 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.1 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.2 Informationssicherheitsrollen und-verantwortlichkeiten

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.2 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.2 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.3 Aufgabentrennung

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.3 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Eine adäquate Aufgabentrennung hat zu erfolgen.

Es gilt, dass eine Aufgabentrennung so weit wie möglich umgesetzt werden muss. In Fällen, in denen dies nicht möglich ist, sind andere Maßnahmen wie Beaufsichtigung, Tätigkeitsüberwachung und Prüfpfade zu nutzen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.3 sind ungeachtet dessen von allen SAE-Betreibern zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.4 Verantwortlichkeiten der Leitung

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.4 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen

Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.4 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.5 Kontakt mit Behörden

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.5 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.5 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.6 Kontakt mit speziellen Interessengruppen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.6 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.6 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.7 Informationen über die Bedrohungslage

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.7 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.7 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.8 Informationssicherheit im Projektmanagement

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.8 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.8 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.9 Inventar der Informationen und anderer damit verbundener Werte

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.9 sind folgende Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Zur Orientierung der üblicherweise relevanten Werte in der Siedlungsabfallentsorgung ist nachfolgend eine Mindestwerteliste aufgeführt.

Werte im Bereich Sammlung und Beförderung umfassen in der Regel mindestens:

- Desktops für den Disponentenarbeitsplatz
- Mobile Endgeräte (Handys, Tablets etc.)
- Festverbaute Bordrechner für Telematiksysteme, Navigation etc.
- Personalplanungssoftware
- Tourenplanungssoftware
- Auftragsverwaltungsanwendungen

Werte im Bereich Verwertung und Beseitigung umfassen in der Regel:

- Leitsysteme (Automatisierung und Bedienen & Beobachten)
- Speicherprogrammierbare Steuerungen (SPS)
- DC Notstromversorgungen / Notstromdieselaggregatoren
- Konfigurationsstationen, Bedienterminals
- Medien- und Protokollkonverter
- intelligente Messsysteme (bspw. Temperatur, Druck, Abgase)

- Waage inkl. Eichprotokollspeicher
- Schnittstellen zu anderen Marktteilnehmern und Sektoren (bspw. Erneuerbare-Energien-Anlagen)
- Betriebsdatenerfassungssysteme
- aktive und passive Netzwerkinfrastruktur der OT
- Rauch-/Gas-/Branddetektion

Jeder SAE-Betreiber hat individuell die für seine Anlagen relevanten Werte und Informationen zu bestimmen.

5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.10 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Werte im Bereich Sammlung und Beförderung beinhalten unter anderem mobile Endgeräte und Apps. Diese kommen in der Regel auch im öffentlichen Raum zum Einsatz und benötigen daher eine Zugangsbeschränkung.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.10 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Sammlung und Beförderung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.11 Rückgabe von Werten

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.11 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.11 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.12 Klassifizierung von Informationen

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.12 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Informationen im Bereich Sammlung und Beförderung beziehen sich auch auf Tourenplanung und Auftragsverwaltung und müssen entsprechend den Informationssicherheitsanforderungen der Organisation klassifiziert werden. Eine sinnvolle Klassifizierung von Informationen kann an folgendem Beispiel nachvollzogen werden:

- **Vertraulichkeit:** Informationen, die Rückschlüsse auf Standorte, Entsorgungswege, Kundendaten oder sicherheitsrelevante Betriebsabläufe zulassen, sind so zu kennzeichnen und zu schützen, dass ein unbefugter Zugriff ausgeschlossen wird.
- **Integrität:** Betriebs- und Prozessdaten (z. B. Tourenpläne, Wiegungen, Abrechnungsdaten) sind gegen Manipulation oder unautorisierte Veränderung abzusichern, um die korrekte und rechtssichere Entsorgung sowie Abrechnung zu gewährleisten.
- **Verfügbarkeit:** Kritische Informationen, wie Einsatz- und Notfallpläne, IT-gestützte Steuerungsdaten für Fahrzeuge und Anlagen, müssen jederzeit in der erforderlichen Qualität verfügbar sein, um eine unterbrechungsfreie Abfallentsorgung zu gewährleisten.

Die Klassifizierung erfolgt nach einem einheitlichen Schema (z. B. **öffentlich – intern – vertraulich – streng vertraulich**) und wird regelmäßig überprüft.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.12 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Sammlung und Beförderung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.13 Kennzeichnung von Informationen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.13 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.13 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.14 Informationsübermittlung

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.14 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Dies betrifft im Bereich Sammlung und Beförderung vor allem Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung beim Einsatz von Subunternehmern von Dienstleistungen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.14 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Sammlung und Beförderung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.15 Zugangssteuerung

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.15 ist folgendes Beispiel für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Dies betrifft im Bereich Sammlung und Beförderung insbesondere die Zugangssteuerung bei mobilen Endgeräten (für Telematiksysteme), die unter anderem im öffentlichen Raum eingesetzt werden.

Falls Komponenten und Protokolle ohne Authentifizierung zum Einsatz kommen, muss dies explizit begründet werden und entsprechend der Risikobewertung Ersatzmaßnahmen (bspw. Zutrittskontrolle oder physische Überwachung) getroffen werden.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.15 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Sammlung und Beförderung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.16 Identitätsmanagement

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.16 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Im Bereich Verwertung und Beseitigung gibt es Komponenten und Protokolle ohne Authentifizierung (z. B. ältere speicherprogrammierbare Steuerungen, nicht gemanagte industrielle Switche oder Modbus/RTU).

Falls Komponenten und Protokolle ohne Authentifizierung zum Einsatz kommen, muss dies explizit begründet werden, und es müssen entsprechend der Risikobewertung Ersatzmaßnahmen (bspw. Zutrittskontrolle oder physische Überwachung) getroffen werden.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.16 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.17 Authentisierungsinformationen

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.17 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Im Bereich Verwertung und Beseitigung gibt es üblicherweise Komponenten und Protokolle ohne Authentifizierung (z. B. ältere speicherprogrammierbare Steuerungen, nicht gemanagte industrielle Switche oder Modbus/RTU). Hier sind entsprechend der Risikobewertung Ersatzmaßnahmen, wie z.B. die physischen Absicherung der Netzwerk- und Benutzerschnittstellen erforderlich.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.17 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.18 Zugangsrechte

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.18 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.18 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.19 Informationssicherheit in Lieferantenbeziehungen

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.19 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

In Fällen, in denen im Bereich Verwertung und Beseitigung keine Alternativen zu Herstellern und Zulieferern von Steuerungs- und Leitsystemen vorhanden sind, sind die Anforderungen in Bezug auf die Bewertung und Auswahl von Produkten oder Dienstleistungen von Lieferanten nur eingeschränkt umsetzbar (weil keine Auswahlmöglichkeit besteht). In solchen Fällen ist insbesondere Wert auf Prozesse und Verfahren für die Pflege der Lieferantenbeziehung sowie für den regelmäßigen Informationsaustausch bzgl. Schwachstellen zu legen. Das Bereitstellen von Schwachstelleninformationen sollte vertraglich vereinbart werden.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.19 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.20 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Im Bereich Verwertung und Beseitigung sollten aufgrund des möglichen, zu verursachenden Schadensausmaß für Zugriffe auf das Leitsystem erhöhte Anforderungen an das durch den Dienstleister eingesetzte Personal gestellt werden z. B. durch schriftlich geregelte Anweisungen und Verpflichtungen zur Einhaltung von Informationssicherheitsmaßnahmen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.20 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.21 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Im Bereich Sammlung und Beförderung umfasst die Informations- und Kommunikationstechnik- (IKT-) Produkt- und Dienstleistungslieferkette in der Regel Lieferanten für mindestens:

- (mobile) Endgeräte
- Telematiksoftware
- Mobilfunk
- Provider Datenleitung bei Telematik als SaaS
- IT-Service Provider

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.21 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Sammlung und Beförderung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

Jeder SAE-Betreiber hat individuell die für seine Anlagen relevanten Lieferanten und Dienstleister zu bestimmen.

5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.22 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.22 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.23 Informationssicherheit für die Nutzung von Cloud-Diensten

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.23 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.23 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.24 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.24 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.25 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.25 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.26 Reaktion auf Informationssicherheitsvorfälle

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.26 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.26 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.27 Erkenntnisse aus Informationssicherheitsvorfällen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.27 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.27 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.28 Sammeln von Beweismaterial

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.28 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.28 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.29 Informationssicherheit bei Störungen

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.29 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für Anlagen im Sektor Siedlungsabfallentsorgung muss bei der Planung der Informationssicherheit während einer Störung darauf geachtet werden, dass vorrangig die Verfügbarkeit der kritischen Anlagenteile und deren unterstützenden informationstechnischen Systeme gewährleistet bleibt.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.29 sind ungeachtet dessen von allen SAE-Betreibern zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.30 IKT-Bereitschaft für Business-Continuity

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.30 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.30 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.31 Juristische, gesetzliche, regulatorische und vertragliche Anforderungen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.31 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.31 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.32 Geistige Eigentumsrechte

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.32 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.32 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.33 Schutz von Aufzeichnungen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.33 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen

Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.33 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.34 Datenschutz und Schutz personenbezogener Daten (pbD)

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.34 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.34 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.35 Unabhängige Überprüfung der Informationssicherheit

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.35 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.35 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.36 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.36 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

5.37 Dokumentierte Betriebsabläufe

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 5.37 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Sektor Siedlungsabfallentsorgung ist es sinnvoll, die Betriebsverfahren für Informationsverarbeitungsanlagen für rudimentäre Tätigkeiten (Reboot, Einspielen eines Backups, o.ä.) so zu dokumentieren, dass Nicht-Fachpersonal die Tätigkeiten durchführen kann.

Dauerhaft besetzte Stellen (bspw. Leitwarten) sind zur Durchführung rudimentärer Tätigkeiten, zur Durchführung von unverzüglichen Meldungen im Rahmen der Meldepflicht aus § 8b Abs. 4 BSIG und zur Entgegennahme von Informationen gemäß § 8b Abs. 2 Nr. 4 BSIG zu befähigen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 5.37 sind ungeachtet dessen von allen SAE-Betreibern zu erfüllen, sofern sie als anwendbar identifiziert wurden.

6 Personenbezogene Anforderung

Oft werden erfolgreiche Angriffe oder eine sonstige Beeinträchtigung der Informationssicherheit auf menschliches Fehlverhalten zurückgeführt. Der Faktor Mensch spielt bei der Gewährleistung der Informationssicherheit folglich eine entscheidende Rolle. Daher sind geeignete personenbezogene Maßnahmen zu ergreifen, um die im jeweiligen Betrieb beschäftigten Personen mit Blick auf Gefahren, die ihr Verhalten für die Informationssicherheit verursachen kann, zu sensibilisieren und entsprechende auch rechtlich durchsetzbare Verhaltensregeln zu schaffen, die die Informationssicherheit befördern. Im Folgenden werden personenbezogene Anforderungen zur Förderung der Informationssicherheit vorgestellt. Diese wurden aus der DIN EN ISO/IEC 27002:2024 übernommen und teilweise um branchenspezifische Präzisierungen im Sinne von Hinweisen, Ergänzungen oder Beispielen ergänzt. Wenn die Präzisierung sich nicht direkt auf Anlagen oder Anlagenkategorien bezieht, gilt sie für alle Anlagen und Anlagenkategorien im Sektor Siedlungsabfallentsorgung. Die Anforderungen der genutzten Prüfgrundlage (bspw. DIN EN ISO/IEC 27002:2024) sind zu beachten.

6.1 Sicherheitsüberprüfung

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 6.1 ist folgendes Beispiel für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Sicherheitsüberprüfungen können beispielsweise aus folgenden Tätigkeiten bestehen, die in Abhängigkeit der Kritikalität der zu besetzenden Stelle zu wählen sind:

- Überprüfung des Lebenslaufs und angegebener Referenzen (bspw. durch Rücksprache mit vorherigem Arbeitgeber)
- Verlangen des Vorlegens eines Führungszeugnisses
- Überprüfung der finanziellen Glaubwürdigkeit (bspw. Einzuholen durch Auskunfteien)

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 6.1 sind ungeachtet dessen von allen SAE-Betreibern zu erfüllen, sofern sie als anwendbar identifiziert wurden.

6.2 Beschäftigungs- und Vertragsbedingungen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 6.2 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 6.2 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

6.3 Informationssicherheitsbewusstsein,-ausbildung und-schulung

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 6.3 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 6.3 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

6.4 Maßregelungsprozess

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 6.4 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 6.4 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 6.5 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 6.5 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

6.6 Vertraulichkeits- und Geheimhaltungsvereinbarungen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 6.6 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 6.6 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

6.7 Remote-Arbeit

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 6.7 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 6.7 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

6.8 Meldung von Informationssicherheitsereignissen

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 6.8 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

SAE-Betreiber haben gemäß § 8b Abs. 4 BSIG die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden:

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,

2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.

Darüber hinaus können Meldungen freiwillig erfolgen.

Die Meldung muss Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, hierbei insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

Die Meldung kann über das Melde- und Informationsportal des BSI (https://mip2.bsi.bund.de) erfolgen. Auch zu Testzwecken können Testmeldungen an das Melde- und Informationsportal des BSI erfolgen. Eine Meldung hat unverzüglich, auch bei noch nicht vollständig vorhandenen Informationen, zu erfolgen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 6.8 sind ungeachtet dessen von allen SAE-Betreibern zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7 Physische Anforderungen

Physische Anforderungen dienen zur Ableitung von praktischen nicht-virtuellen Vor-Ort Maßnahmen, die der Sicherung von Hardware und Software am jeweiligen Standort vor Zugriffen oder Zerstörung dienen. Im Folgenden werden physische Anforderungen zur Förderung der Informationssicherheit vorgestellt. Diese wurden aus der DIN EN ISO/IEC 27002:2024 übernommen und teilweise um branchenspezifische Präzisierungen im Sinne von Hinweisen, Ergänzungen oder Beispielen ergänzt. Wenn die Präzisierung sich nicht direkt auf Anlagen oder Anlagenkategorien bezieht, gilt sie für alle Anlagen und Anlagenkategorien im Sektor Siedlungsabfallentsorgung. Die Anforderungen der genutzten Prüfgrundlage (bspw. DIN EN ISO/IEC 27002:2024) sind zu beachten.

7.1 Physische Sicherheitsperimeter

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.1 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Sektor Siedlungsabfallentsorgung gilt es beim Schutz des Betriebsgeländes zu berücksichtigen, dass branchenüblich Teile der Betriebsgelände für betriebsfremde Personen zugänglich sind. Das ist beispielsweise zu Revisionszeiten der Fall. Bei der Konzeptionierung von Sicherheitsperimetern ist dies entsprechend zu berücksichtigen (z.B. durch Platzierung von Geräten an nicht leicht zugänglichen Stellen oder durch detaillierte Berechtigungsdifferenzierung/Mikrozonierung für die Zutrittskontrolle).

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.1 sind ungeachtet dessen von allen SAE-Betreibern zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7.2 Physischer Zutritt

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.2 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.2 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7.3 Sichern von Büros, Räumen und Einrichtungen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.3 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.3 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7.4 Physische Sicherheitsüberwachung

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.4 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung ist branchenspezifisch üblich, dass kritische Systeme und Komponenten über die Anlage verteilt aufgestellt sind, sodass eine zentrale Überwachung nicht immer möglich ist. In einem solchen Fall sind die damit einhergehenden Risiken zu bestimmen und entsprechende Ersatzmaßnahmen zu treffen (bspw. restriktives Schließkonzept und lokale Überwachungsmaßnahmen).

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.4 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7.5 Schutz vor physischen und umweltbedingten Bedrohungen

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.5 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Sektor Siedlungsabfallentsorgung ist es branchenspezifisch üblich, dass das verarbeitete Material zum großen Teil unbekannt ist. Daraus resultierende physische Gefährdungen im Sinne der Anlagenverfügbarkeit sollten identifiziert und mit geeigneten Maßnahmen (bspw. Stichproben von Material) behandelt werden.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.5 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7.6 Arbeiten in Sicherheitsbereichen

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.6 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung gilt es bei den Sicherheitsmaßnahmen für die Arbeit in Sicherheitsbereichen zu berücksichtigen, dass es z.B. während Revisionszeiten vorkommt, dass sich eine größere Anzahl von betriebsfremden Personen auf dem Betriebsgeländen aufhält. Grundsätzlich muss dafür Sorge getragen werden, dass diese betriebsfremden Personen durch eigenes Personal begleitet wird. Sollte eine Begleitung nicht möglich sein, muss dies entsprechend begründet werden und müssen adäquate Maßnahmen getroffen werden (bspw. Betriebsfremde Personen in solchen Fällen zu Themen der Informationssicherheit unterweisen oder Sicherheitsüberprüfungen analog zu Kap. 6.1 durchführen).

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.6 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.7 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Im Bereich Verwertung und Beseitigung sind Maßnahmen bezüglich des Einrichtens von Bildschirmsperren insbesondere in Mess- und Leitwarten nicht durchgängig umsetzbar. In einem solchen Fall sind Ersatzmaßnahmen, wie z. B. einer physischen Zutrittsbeschränkung umzusetzen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.7 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7.8 Platzierung und Schutz von Geräten und Betriebsmitteln

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.8 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung ist es branchenspezifisch üblich, dass große Fahrzeuge in der Nähe von kritischen Geräten und Betriebsmitteln bewegt werden. Daher sollte der Schutz von Geräten und Betriebsmitteln folgendes berücksichtigen:

- Rammschutz
- Höhenkontrolle

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.8 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

Jeder SAE-Betreiber hat individuell die für seine Anlagen relevanten Schutzvorkehrungen für Geräte und Betriebsmittel zu bestimmen.

7.9 Sicherheit von Werten außerhalb der Räumlichkeiten

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.9 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Sammlung und Beförderung ist es üblich, mobile Endgeräten (bspw. für Telematiksysteme) im öffentlichen Raum einzusetzen. Für diese Werte befinden sich die Sicherheitsparameter nicht in den Händen des Betreibers. Daher ist es für diesen Fall notwendig, zusätzliche Maßnahmen (wie z. B. Datensicherung, zusätzliche Verschlüsselung und Remoteverwaltung inkl. Löschung) zu ergreifen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.9 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Sammlung und Beförderung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7.10 Speichermedien

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.10 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.10 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7.11 Versorgungseinrichtungen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.11 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.11 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7.12 Sicherheit der Verkabelung

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.12 ist **folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:**

Im Bereich Verwertung und Beseitigung ist es üblich, dass Kabelwege überirdisch verlaufen. In solch einem Fall sind Ersatzmaßnahmen (wie z.B. Bodenkabelschutz oder Errichtung von Strommasten) zu ergreifen.

Kabel, die Strom, Daten oder unterstützende Informationsdienste transportieren, sind so zu verlegen, dass sie unter anderem vor Schaden durch

- Feuer und Wärme und
- anliefernde Fahrzeuge
- Eingriffe Dritter

geschützt sind.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.12 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

Jeder SAE-Betreiber hat individuell die für seine Anlagen relevanten Gefährdungen für die Kabelverlegung zu bestimmen.

7.13 Instandhaltung von Geräten und Betriebsmitteln

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.13 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den gesamten Sektor SAE ist es branchenspezifisch üblich, dass verbaute Systeme und Komponenten langjährig eingesetzt werden. In diesem Zeitraum ist es nicht immer möglich, Wartungsdienstleistungen durch Hersteller oder Integratoren für Hard- und Software zu beziehen.

In einem solchen Fall sind die damit einhergehenden Risiken zu bestimmen und entsprechende Ersatzmaßnahmen zu treffen (bspw. Ersatzteilbevorratung kritischer Komponenten, Abkapselung von Systemen oder Betrieb außerhalb von herstellerseitigen Betriebsvorgaben).

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.13 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Sammlung und Beförderung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 7.14 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 7.11 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8 Technische Anforderungen

Technische Anforderungen beschreiben überwiegend automatisierte softwaregestützte Schutzmaßnahmen, die dem Schutz der Informationssicherheit dienen. Diese werden im Folgenden dargelegt. Im Folgenden werden technische Anforderungen zur Förderung der Informationssicherheit vorgestellt. Diese wurden aus der DIN EN ISO/IEC 27002:2024 übernommen und teilweise um branchenspezifische Präzisierungen im Sinne von Hinweisen, Ergänzungen oder Beispielen ergänzt. Wenn die Präzisierung sich nicht direkt auf Anlagen oder Anlagenkategorien bezieht, gilt sie für alle Anlagen und Anlagenkategorien im Sektor Siedlungsabfallentsorgung. Die Anforderungen der genutzten Prüfgrundlage (bspw. DIN EN ISO/IEC 27002:2024) sind zu beachten.

8.1 Endpunktgeräte des Benutzers

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.1 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.1 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.2 Privilegierte Zugangsrechte

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.2 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung ist es branchenspezifisch üblich, dass privilegierte Zugangsrechte auch durch Dienstleister verwaltet werden. Von dieser Praxis ist abzusehen. In jedem Fall sind Vereinbarungen mit dem Dienstleister zu schließen, die dem Betreiber Transparenz und Kontrolle über die Vergabe privilegierter Zugangsrechte verschaffen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.2 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.3 Informationszugangsbeschränkung

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.3 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.3 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.4 Zugriff auf den Quellcode

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.4 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.4 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.5 Sichere Authentisierung

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.5 ist folgendes Beispiel für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung ist es branchenspezifisch üblich, dass nicht alle eingesetzten Systeme und Komponenten in der Lage sind, moderne und damit sichere Authentifizierungsverfahren zu unterstützen.

In einem solchen Fall sind die damit einhergehenden Risiken zu bestimmen, entsprechende Ersatzmaßnahmen zu treffen (bspw. physischer Zutrittsschutz) und dieser Aspekt bei folgenden Neuanschaffungen zu berücksichtigen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.5 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.6 Kapazitätssteuerung

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.6 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.6 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.7 Schutz gegen Schadsoftware

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.7 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung ist es branchenspezifisch üblich, dass nicht alle eingesetzten Systeme und Komponenten in der Lage sind, (moderne) hostbasierte Antivirenlösungen (bspw. Endpoint detection and response – EDR) zu unterstützen.

In einem solchen Fall sind die damit einhergehenden Risiken zu bestimmen, entsprechende Ersatzmaßnahmen zu treffen (bspw. Kapselung von Systemen, netzwerkbasierte Überwachungsmaßnahmen und Netzwerksegmentierung) und dieser Aspekt bei folgenden Neuanschaffungen zu berücksichtigen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.7 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.8 Handhabung von technischen Schwachstellen

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.8 ist folgendes Beispiel für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung ist das Einspielen von Patches zur Behandlung von Schwachstellen aufgrund fehlender Herstellerfreigaben oder aufgrund des Anlagenzustands (bspw. Abhängigkeit von Revisionszeiten) nicht immer zeitnah möglich. Darüber hinaus muss beurteilt werden, ob das Einspielen von Patches Auswirkungen auf die Verfügbarkeit haben.

In einem solchen Fall sind die damit einhergehenden Risiken zu bestimmen, entsprechende Ersatzmaßnahmen zu treffen (bspw. Härtung, Kapselung von Systemen und Netzwerksegmentierung) und dieser Aspekt bei folgenden Neuanschaffungen zu berücksichtigen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.8 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.9 Konfigurationsmanagement

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.9 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen

Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.9 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.10 Löschung von Informationen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.10 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.10 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.11 Datenmaskierung

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.11 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.11 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.12 Verhinderung von Datenlecks

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.12 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.12 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.13 Sicherung von Informationen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.13 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.13 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.14 Redundanz von informationsverarbeitenden Einrichtungen

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.14 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung gibt es oft keine Alternativen zu Herstellern und Zulieferern, weshalb eine Redundanz von Systemen, Geräten und Anlagen unterschiedlicher Hersteller nicht immer möglich ist. Darüber hinaus kann es aufgrund des Alters der eingesetzten Komponenten sein, dass diese keinen redundanten Aufbau unterstützen. Redundanzmaßnahmen sind auch bei Nutzung eines Herstellers oder Zulieferers umzusetzen (bspw. durch die Bevorratung von Ersatzkomponenten).

In einem solchen Fall sind die damit einhergehenden Risiken zu bestimmen, entsprechende Ersatzmaßnahmen zu treffen und dieser Aspekt bei folgenden Neuanschaffungen zu berücksichtigen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.14 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.15 Protokollierung

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.15 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung ist es branchenspezifisch üblich, dass eingesetzte Systeme und Komponenten nicht immer in der Lage sind, Protokollierungsdaten für übliche SIEM-Systeme bereitzustellen.

Wenn eine Protokollierung nur unzureichend auf Systemebene realisierbar ist, ist ein netzbasiertes Logging auf Basis der Ethernet-Verbindungen zu realisieren.

Bei der Umsetzung der Protokollierung auf Kommunikationsebene sind die klassischen Feldbusse (Profibus, …) derzeit nicht zu beachten.

In einem solchen Fall sind die damit einhergehenden Risiken zu bestimmen, entsprechende Ersatzmaßnahmen zu treffen und dieser Aspekt bei folgenden Neuanschaffungen zu berücksichtigen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.15 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.16 Überwachung von Aktivitäten

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.16 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.16 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.17 Uhrensynchronisation

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.17 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Eine Uhrensynchronisation ist mandatorisch. Ist eine Uhrensynchronisierung von einer zentralen Stelle im Netzwerk nicht möglich, sind die damit einhergehenden Risiken zu bestimmen, entsprechende Ersatzmaßnahmen wie z. B. GPS-Firewalls oder geografisch getrennte Zeitquellen zu treffen. Im Verdachtsfall sind ggf. die Uhrzeiten der einzelnen Geräte heranzuziehen. Das Vorhandensein einer Uhrensynchronisation ist bei folgenden Neuanschaffungen zu berücksichtigen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 817 sind ungeachtet dessen von allen SAE-Betreibern zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.18 ist folgendes Beispiel für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung gilt, dass Einschränkungen oder die Deinstallation von Anwendungen mit privilegierten Rechten aufgrund fehlender Herstellerfreigaben nicht immer möglich sind.

In einem solchen Fall sind die damit einhergehenden Risiken zu bestimmen, entsprechende Ersatzmaßnahmen (z.B. Aufnahme der Deinstallation nicht benötigter Hilfsprogramme in Lastenhefte für Hersteller / Wartungsdienstleister oder Überwachung und Unterbindung von nicht benötigten Netzwerkverbindungen zu Systemen mit nicht benötigten Hilfsprogrammen) zu treffen und dieser Aspekt bei folgenden Neuanschaffungen zu berücksichtigen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.18 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.19 Installation von Software auf Systemen im Betrieb

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.19 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.19 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.20 Netzwerksicherheit

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.20 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung ist es branchenspezifisch aufgrund der Abhängigkeit von Herstellern und Dienstleistern nicht immer möglich, alle Netzwerksicherheitsmaßnahmen (bspw. Filterung von Netzwerkverbindungen und Netzwerkgeräten) zu ergreifen.

In einem solchen Fall sind die damit einhergehenden Risiken zu bestimmen, entsprechende Maßnahmen (bspw. Netzwerksegmentierung gemäß Purdue Model inkl. Industrial Demilitarized Zone (IDMZ) und vertikaler Netzwerksegmentierung bspw. zwischen Verbrennungslinien) zu treffen und diesen Aspekt bei folgenden Neuanschaffungen zu berücksichtigen. Darüber hinaus muss der Hersteller / Dienstleister zwingend in die Pflicht genommen werden, dass z.B. Produktverbesserungen umgesetzt werden.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.20 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.21 Sicherheit von Netzwerkdiensten

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.21 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.21 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.22 Trennung von Netzwerken

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.22 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Bereich Verwertung und Beseitigung gilt, dass in einer OT-Umgebung für die IT übliche Anforderungen aufgrund des Alters eingesetzter Systeme nicht immer umsetzbar sind (z.B. die Unmöglichkeit des Einsatzes von Firewalls und Gateways in Netzwerkbereichen ohne Ethernet/IP-Kommunikation).

In einem solchen Fall sind die damit einhergehenden Risiken zu bestimmen, entsprechende Maßnahmen (bspw. Netzwerksegmentierung gemäß Purdue Model inkl. Industrial Demilitarized Zone (IDMZ) und vertikaler Netzwerksegmentierung bspw. zwischen Verbrennungslinien) zu treffen und diesen Aspekt bei folgenden Neuanschaffungen zu berücksichtigen.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.22 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.23 Webfilterung

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.23 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Für den Sektor Siedlungsabfallentsorgung entfällt diese Maßnahme, sofern der Zugriff auf Websites bei Komponenten der kritischen Dienstleistung komplett unterbunden wird.

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.23 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurde.

8.24 Verwendung von Kryptographie

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.24 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.24 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.25 Lebenszyklus einer sicheren Entwicklung

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.25 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.25 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.26 Anforderungen an die Anwendungssicherheit

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.26 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.26 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.27 Sichere Systemarchitektur und Entwicklungsgrundsätze

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.27 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.27 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.28 Sichere Codierung

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.28 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.28 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.29 Sicherheitsprüfung bei Entwicklung und Abnahme

Zusätzlich zu den Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.29 ist folgender Hinweis für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards zu beachten:

Bei einer vorhandenen Netzwerksegmentierung sollte der Test schrittweise je Segment erfolgen. Alternativ können Anlagenstillstände für Tests genutzt werden.

Für Fälle, bei denen keine oder nur begrenzt Tests möglich sind, sollten angemessene Verfahren etabliert werden (z. B. Rollback-Strategie und Vier-Augenprinzip bei Änderungen).

Die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.29 sind ungeachtet dessen von allen SAE-Betreibern (auch solchen, die nicht der Verwertung und Beseitigung zuzuordnen sind) zu erfüllen, sofern sie als anwendbar identifiziert wurde.

8.30 Ausgegliederte Entwicklung

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.30 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.30 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.31 Trennung von Entwicklungs-, Test- und Produktionsumgebungen

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.31 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.31 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.32 Änderungssteuerung

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.32 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.32 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.33 Testdaten

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.33 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.33 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

8.34 Schutz der Informationssysteme während Tests im Rahmen von Audits

Die Beschreibungen und Maßnahmen in DIN EN ISO/IEC 27002:2024 Kap. 8.34 gelten ohne zusätzliche Hinweise oder Beispiele für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards. SAE-Betreiber haben somit die Anforderungen aus DIN EN ISO/IEC 27002:2024 Kap. 8.34 zu erfüllen, sofern sie als anwendbar identifiziert wurden.

Anhänge

A.1 Branchenspezifische Risiken

Die Vorgaben, Ausführungen und Hinweise dieses Branchenspezifischen Sicherheitsstandards basieren auf einer übergeordneten Risikoanalyse der kritischen Dienstleistungen in den Hauptschritten des Sektors Siedlungsabfallentsorgung, die in Kap. 2.2.5 beschrieben werden.

Für jeden Hauptschritt wurde ein sogenanntes „High Consequence Event“ (HCE) – also das schlimmstmöglich anzunehmende Ereignis, welches im Kontext des jeweiligen kDL-Hauptschrittes eintreten könnte, definiert und anhand der in Kap. 3.5 beschriebenen Metrik zur Bestimmung der Auswirkungen eingestuft.

ACHTUNG: Bei der Einstufung der kDL-Hauptschritte (bgl. Kap. 2.2.5) handelt es sich lediglich um einen Vorschlag, den jeder SAE-Betreiber für sich selbst im Rahmen der Risikobewertung zu überprüfen hat.

Daraufhin wurde beschrieben, welche technischen Funktionen üblicherweise an den jeweiligen kDL-Hauptschritten beteiligt sind. Eine Funktion beantwortet an dieser Stelle immer die Frage „Wer macht was mit welchem System und zu welchem Zweck?“.

Für jede festgelegte Funktion wurde bewertet, ob deren Versagen oder deren Manipulation zum festgelegten High Consequence Event führen kann. Das Versagen beschreibt an dieser Stelle einen Zustand, in dem das Schutzziel der Verfügbarkeit beeinflusst wird, während Manipulation eine zusätzliche Beeinflussung der Schutzziele Vertraulichkeit, Integrität und Authentizität enthalten kann.

Anschließend wurde untersucht, durch welche Bedrohungen und Schwachstellen ein Versagen der Funktionen herbeigeführt werden kann und durch welche Bedrohungen und Schwachstellen eine Manipulation. Dabei wurde auf die in Anhang A.3 genannten Bedrohungs- und Schwachstellenkataloge zurückgegriffen.

Aus den Referenzmaßnahmen aus Annex A der DIN EN ISO/IEC 27001:2024 wurden geeignete Maßnahmen ausgewählt, die zur Reduzierung der Bedrohungen und Schwachstellen beitragen können. Dabei wurden die Bedrohungen und Schwachstellen betrachtet, die zum Versagen oder zur Manipulation einer Funktion eines kDL-Hauptschritt führen. Im Anhang A.3 kann die Auswahl der geeigneten Referenzmaßnahmen anhand von Verweisen auf die Kapitel 5 bis 8 zur Reduzierung der Bedrohungen und Schwachstellen nachvollzogen werden.

Für die zugeordneten Referenzmaßnahmen wurde dann überprüft, inwieweit sie durch branchenspezifische Hinweise, Ergänzungen oder Beispiele erweitert werden sollen. Nicht für alle branchenspezifische Bedrohungen und Schwachstellen sind auch branchenspezifische Ergänzungen erforderlich. So wurden in einigen Fällen (geringe Auswirkungen des zugeordneten HCEs) die allgemeinen Anforderungen des Annex A der DIN EN ISO/IEC 27001:2024 als ausreichend erachtet.

A.1.1 Sammlung & Beförderung

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	beispielhafte Referenzmaßnahmen, die den HCE verringern können
statische Tourenplanung	**HCE:** Beschäftigte wissen nicht, wo Abfälle abgeholt werden müssen **Begrenzt** Wenn Beschäftigte nicht wissen, wo Abfälle abgeholt werden müssen, kann das zu erheblichen Verzögerungen der Sammlung/Beförderung führen.	**Tourenplanungs-software:** Software zur Planung von Touren zur Abholung von Software inkl. Bestimmung der Adressen, an denen bestimmte Abfallarten abgeholt werden müssen.	**Versagen:** Ja, ein Versagen der Tourenplanungssoftware kann dazu führen, dass Beschäftigte nicht wissen, wo Abfälle abgeholt werden müssen. **Manipulation:** Ja, eine Manipulation der Tourenplanungs-software kann dazu führen, dass Beschäftigte nicht wissen, wo Abfälle abgeholt werden müssen.	G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.11 Ausfall oder Störung von Dienstleistern G 0.12 Elektromagnetische Störstrahlung G 0.21 Manipulation von Hard- oder Software G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.24 Zerstörung von Geräten oder Datenträgern G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder Systemen G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 2 Schadsoftware in E-Mail-Anhängen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	G 0.14 Ausspähen von Informationen (Spionage) G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.07 Mangelnde Awareness BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme 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	**Versagen:** Vorhaltung Papieraufzeichnung von Tourplanungen Schulung Mitarbeiter zur Nutzung der Papieraufzeichnungen bei Eintritt HCE Dokumentation vorhandenes Erfahrungswissen der Mitarbeitenden mit Ziel des Einsatzes erfahrener Mitarbeitender bei Eintritt HCE **Manipulation:** Vorhaltung Papieraufzeichnung von Tourplanungen Schulung Mitarbeiter zur Nutzung der Papieraufzeichnungen bei Eintritt HCE Dokumentation vorhandenes Erfahrungswissen der Mitarbeitenden mit Ziel des Einsatzes erfahrener Mitarbeitenden bei Eintritt HCE

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	beispielhafte Referenzmaßnahmen, die den HCE verringern können
dynamische Tourenplanung / Auftragsverwaltung	**HCE:** Beschäftigte wissen nicht, wo Abfälle abgeholt werden müssen **Begrenzt** Wenn Beschäftigte nicht wissen, wo Abfälle abgeholt werden müssen, wird die dynamische Tourenplanung gestört und erheblich verzögert.	**Tourenplanungs-software:** Software zur Planung von Touren zur Abholung von Software inkl. Bestimmung der Adressen, an denen bestimmte Abfallarten abgeholt werden müssen.	**Versagen:** Ja, ein Versagen der Tourenplanungssoftware kann dazu führen, dass Beschäftigte nicht wissen, wo Abfälle abgeholt werden müssen. **Manipulation:** Ja, eine Manipulation der Tourenplanungssoftware kann dazu führen, dass Beschäftigte nicht wissen, wo Abfälle abgeholt werden müssen.	G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.11 Ausfall oder Störung von Dienstleistern G 0.12 Elektromagnetische Störstrahlung G 0.21 Manipulation von Hard- oder Software G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.24 Zerstörung von Geräten oder Datenträgern G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder Systemen G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 2 Schadsoftware in E-Mail-Anhängen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	G 0.14 Ausspähen von Informationen (Spionage) G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.07 Mangelnde Awareness BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme 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	**Versagen:** Vorhaltung Aufzeichnung von Dienstleistungsgrundlagen zur Durchführung dynamischen Touren, z.B. Tourenpläne. Schulung Mitarbeiter zur Nutzung der vorgehaltenen Aufzeichnungen bei Eintritt HCE Dokumentation vorhandenes Erfahrungswissen der Mitarbeitenden mit Ziel des Einsatzes erfahrener Mitarbeitender bei Eintritt HCE Regelmäßige Historisierung bzw. Datensicherung von dynamisch geplanten Touren Redundante Server-Strukturen, Datensicherungen oder manuelle Ersatzprozesse wie z.B. durch Nutzung von Papieraufzeichnungen **Manipulation:** Vorhaltung Aufzeichnung von Dienstleistungsgrund-

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	beispielhafte Referenzmaßnahmen, die den HCE verringern können
						lagen zur Durchführung dynamischer Touren Schulung Mitarbeiter zur Nutzung der vorgehaltenen Aufzeichnungen bei Eintritt HCE Dokumentation vorhandenes Erfahrungswissen der Mitarbeitenden mit Ziel des Einsatzes erfahrener Mitarbeitenden bei Eintritt HCE Regelmäßige Historisierung bzw. Datensicherung von dynamisch geplanten Touren Redundante Server-Strukturen, Datensicherungen oder manuelle Ersatzprozesse wie z.B. durch Nutzung von Papieraufzeichnungen
		Auftrags-verwaltung: Verwaltung von Aufträgen zur Einzelabholung von Abfällen.	**Versagen:** Ja, ein Versagen der Auftragsverwaltung kann dazu führen, dass Beschäftigte nicht wissen, wo Abfälle abgeholt werden müssen.	G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.11 Ausfall oder Störung von Dienstleistern G 0.12 Elektromagnetische Störstrahlung G 0.21 Manipulation von Hard- oder Software G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.24 Zerstörung von Geräten oder	G 0.14 Ausspähen von Informationen (Spionage) G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme	**Versagen:** Die Auswirkungen eines Versagens der Auftragsverwaltung können bspw. durch Redundante Server-Strukturen, Datensicherungen oder manuelle

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	beispielhafte Referenzmaßnahmen, die den HCE verringern können
			Manipulation: Ja, eine Manipulation der Auftragsverwaltung kann dazu führen, dass Beschäftigte nicht wissen, wo Abfälle abgeholt werden müssen. Dies führt in Konsequenz zur Nichterbringung von geplanten Sammelleistungen bzw. zur Erbringung von nicht geplanten/unnötigen Sammelleistungen führen. Die zu Erbringung von nicht geplanten bzw. unnötigen Sammelleistungen aufgebrachten Ressourcen stehen dann den geplanten Sammelleistungen nicht mehr zur Verfügung.	Datenträgern G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder Systemen G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.23 Schadprogramme 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	G 0.28 Software-Schwachstellen oder -Fehler G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.07 Mangelnde Awareness BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme 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	Ersatzprozesse bzw. durch Nutzung von Papieraufzeichnungen verringert werden. **Manipulation:** Die Auswirkungen einer Manipulation der Auftragsverwaltung können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip oder Versionskontrollen / Historisierung von Änderungen verringert werden.
Personal-planung	**HCE:** Es steht nicht genügend Personal zur Sammlung & Beförderung zur Verfügung **Beträchtlich**	**Personalplanungs-software:** Software zur Zuteilung von Personal zu Touren zur Sammlung von Abfällen in Abhängigkeit von Verfügbarkeit und Kompetenz.	**Versagen:** Ja, ein Versagen der Planungssoftware kann dazu führen, dass nicht genügend Personal zur Sammlung & Beförderung zur Verfügung steht. **Manipulation:**	G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.11 Ausfall oder Störung von Dienstleistern G 0.12 Elektromagnetische Störstrahlung G 0.21 Manipulation von Hard- oder Software G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.24 Zerstörung von Geräten oder Datenträgern	G 0.14 Ausspähen von Informationen (Spionage) G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler	**Versagen:** Dokumentation vorhandener Qualifikationen der Mitarbeitenden mit Blick auf den Einsatz qualifizierter Mitarbeitender für die

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	beispielhafte Referenzmaßnahmen, die den HCE verringern können
	Wenn nicht genug Personal verfügbar ist, um alle Touren fahren zu können, kann das zu einer Störung der Sammlung/Beförderung in einer Dauer führen, welche nicht eigenständig aufgeholt werden kann.		Nein, eine Manipulation der Personalplanungssoftware führt in der Regel nur zu Verzögerungen, aber nicht dazu, dass Touren ausfallen müssen.	G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder Systemen G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 2 Schadsoftware in E-Mail-Anhängen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.38 Missbrauch personenbezogener Daten G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.07 Mangelnde Awareness BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme 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	jeweiligen Kfz-Typen bei Eintritt HCE Zur Abmilderung der HCE-Auswirkung kann auf externes Personal zurückgegriffen werden oder der Abfall am nächsten Werktag bzw. durch andere Fahrzeuge abgeholt werden. **Manipulation:** Die Auswirkungen einer Manipulation der Personalplanungssoftware können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip oder Versionskontrollen / Historisierung von Änderungen verringert werden.
Fahrzeug-disposition	**HCE:** Es stehen nicht genügend Fahrzeuge (zeitgerecht) zur Verfügung **Begrenzt:** Wenn nicht genügend Fahrzeuge	**Dispositions-software:** Software zur Zuteilung von Fahrzeugen zu Personal bzw. Kolonnen zur Abholung von Abfällen	**Versagen:** Ja, ein Versagen der Dispositionssoftware kann dazu führen, dass nicht genügend Fahrzeuge (zeitgerecht) zur Verfügung stehen. **Manipulation:** Ja, eine Manipulation der Fahrzeugdisposition	G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.24 Zerstörung von Geräten oder Datenträgern G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder	G 0.14 Ausspähen von Informationen (Spionage) G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler	**Versagen:** Vereinbarungen mit Leihfahrzeugdienstleistern zur zeitnahen Ersatzlieferung von Fahrzeugen Schulung von Mitarbeitenden zum Einsatz auf externen Fahrzeugen

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	beispielhafte Referenzmaßnahmen, die den HCE verringern können
	(zeitgerecht) zur Verfügung stehen, kann das zu erheblichen Verzögerungen der Sammlung/Beförderung führen.		kann dazu führen, dass nicht genügend Fahrzeuge (zeitgerecht) zur Verfügung stehen.	Systemen G 0.28 Software-Schwachstellen oder -Fehler G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 2 Schadsoftware in E-Mail-Anhängen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.07 Mangelnde Awareness BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme 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	**Manipulation:** Die Auswirkungen einer Manipulation der Dispositionssoftware können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip oder Versionskontrollen / Historisierung von Änderungen verringert werden.
Sammlung und Beförderung	**HCE:** Abfälle können nicht eingesammelt werden **Beträchtlich** Wenn Abfälle nicht eingesammelt werden können, kann das zu einer	**Fahrzeug- und Tourennavigation mittels Telematiksystem:** Das Telematiksystem stellt dem Fahrpersonal Informationen über Abfallstelle, Abfallart,	**Versagen:** Ja, bei Ausfall des Telematiksystems liegen dem Fahrpersonal keine Informationen über die zu erbringenden/geplanten Sammelleistungen vor. Dies kann dazu führen, dass Abfälle nicht	G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.11 Ausfall oder Störung von Dienstleistern G 0.12 Elektromagnetische Störstrahlung G 0.21 Manipulation von Hard- oder Software G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.24 Zerstörung von Geräten oder Datenträgern G 0.25 Ausfall von Geräten oder Systemen	G 0.14 Ausspähen von Informationen (Spionage) G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	**Versagen:** Die Auswirkungen eines Versagens des Telematiksystems können bspw. Datensicherungen oder manuelle Ersatzprozesse bzw. durch Nutzung von Papieraufzeichnungen verringert werden.

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	beispielhafte Referenzmaßnahmen, die den HCE verringern können
	Störung in einer Dauer führen, welche nicht eigenständig aufgeholt werden kann.	Behältertyp, Entsorgungsanlage und Reihenfolge anhand der Auftragsdaten aus den Tourenplanungen für die Sammlung und Beförderung zur Verfügung.	eingesammelt werden können. **Manipulation:** Ja, eine Manipulation der Auftragsdaten von Telematiksystemen kann dazu führen, dass Abfälle nicht eingesammelt werden können. Die zur Erbringung von nicht geplanten bzw. unnötigen Sammelleistungen aufgebrachten Ressourcen stehen dann den geplanten Sammelleistungen nicht mehr zur Verfügung.	G 0.26 Fehlfunktion von Geräten oder Systemen G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.07 Mangelnde Awareness BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme 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	**Manipulation:** Die Auswirkungen einer Manipulation des Telematiksystems können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip oder Versionskontrollen / Historisierung von Änderungen verringert werden.
Lagerung, Zwischen-lagerung und Umladung von Abfällen	**HCE:** Abfälle können nicht (zwischen-) gelagert oder umgeladen werden **Vernachlässigbar** Der Ausfall der Planung ist unkritisch. Denn	Geringe bis keine Systemunterstützung.	n/A	n/A	n/A	n/A

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	beispielhafte Referenzmaßnahmen, die den HCE verringern können
	die Lagerungs- und Umladungskapazitäten sind in der Regel nicht knapp und es besteht auch manuell ein guter Überblick über die vorhandenen Kapazitäten.					

A.1.2 Verwertung & Beseitigung

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	Beispielhafte Referenzmaßnahmen, die den HCE verringern können
Abfallmengen-erfassung an der Annahme	**HCE:** Abfallmengen können nicht erfasst werden. **Vernachlässigbar** Fehler oder Ausbleiben der IT-gestützten Mengenerfassung haben in der Regel keine Auswirkungen auf die kDL.	**Fahrzeug-verwiegung**: Ermittlung des Gewichts von Fahrzeugen vor und nach der Entladung von Abfällen, um die abgeladene Abfallmenge zu bestimmen	**Versagen:** Nein, ein Versagen der technischen Funktion (bzw. der beteiligten Systeme) führt in der Regel nicht dazu, dass nicht mehr verwogen werden kann. Im Notfall können Daten händisch aufgenommen (im Rahmen des Eichpfads) oder nach Schätzung angenommen werden. Abfälle können auch ohne Verwiegung angenommen werden. **Manipulation:** Nein, falsche Werte bei der Verwiegung führen in der Regel lediglich zu falscher Abrechnung.	G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.12 Elektromagnetische Störstrahlung G 0.21 Manipulation von Hard- oder Software G 0.24 Zerstörung von Geräten oder Datenträgern G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder Systemen G 0.34 Anschlag G 0.39 Schadprogramme G 0.41 Sabotage G 0.44 Unbefugtes Eindringen in Räumlichkeiten G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	G 0.14 Ausspähen von Informationen (Spionage) G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten 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	**Versagen:** Bei einem Ausfall der IT-gestützten Verwiegung kann auf autarken, nicht IT basierten, Waagebetrieb (manueller Betrieb) gewechselt werden. Schulung von Mitarbeitenden zum autarken, IT unabhängigen, Betrieb **Manipulation:** Die Auswirkungen einer Manipulation der Fahrzeugverwiegung können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip oder Versionskontrollen / Historisierung von Änderungen verringert werden.

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	Beispielhafte Referenzmaßnahmen, die den HCE verringern können
Abfallvorbehandlung (u.U. mit Vorsortierung)	**HCE:** Zerstörung der Anlage **existenzbedrohend**. Eine Beschädigung von wesentlichen Anlagenkomponenten kann zu einer langfristigen Zerstörung der kritischen Anlage führen. Auswirkungen auf die Verfügbarkeit der kDL sind eher nicht realistisch.	**Bedienen und Beobachten der Anlage im Leitsystem:** Steuerung und Regelung der Abfallvorbehandlung über Speicherprogrammierbare Steuerungen (SPS) und/oder das Bedien- und Beobachtungssystem vom Leitstandsfahrer	**Versagen:** Ja, ein Versagen der Bedien- und Beobachtungsfunktion im Leitsystem kann zur Zerstörung von Anlagen führen. **Manipulation:** Ja, eine Manipulation der Bedien- und Beobachtungsfunktion im Leitsystem kann zur Zerstörung von Anlagen führen.	G 0.1 Feuer G 0.2 Ungünstige klimatische Bedingungen G 0.3 Wasser G 0.4 Verschmutzung, Staub, Korrosion G 0.5 Naturkatastrophen G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.11 Ausfall oder Störung von Dienstleistern G 0.12 Elektromagnetische Störstrahlung G 0.21 Manipulation von Hard- oder Software G 0.24 Zerstörung von Geräten oder Datenträgern G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder Systemen G 0.34 Anschlag G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.41 Sabotage G 0.44 Unbefugtes Eindringen in Räumlichkeiten G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.10 Fehlende Backups BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.22 Schadsoftware auf EWS BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	G 0.14 Ausspähen von Informationen (Spionage) G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 2 Schadsoftware in E-Mail-Anhängen	**Versagen:** Die Auswirkungen eines Versagens der Bedien- und Beobachtungsfunktion im Leitsystem können bspw. durch Sicherheitseinrichtungen oder manuelle Ersatzprozesse (z. B. Prozessbeobachtung mittels Kameras) verringert werden. **Manipulation:** Die Auswirkungen einer Manipulation der Bedien- und Beobachtungsfunktion im Leitsystem können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip, Sicherheitseinrichtungen oder physischen Zutrittskontrollen verringert werden.

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	Beispielhafte Referenzmaßnahmen, die den HCE verringern können
					B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware B 5 Daten-Exfiltration	
Lager-/ Bunkermanagement	**HCE:** Beschädigung der Anlage bspw. aufgrund eines Brands im Lager / Bunker **existenzbedrohend** Ein Brand im Bunker bzw. im Lager kann die Anlage derart beschädigen, dass diese langfristig nicht betrieben werden kann.	**Gebäude-leittechnik (GLT)** Die Gebäudeleittech-nik (GLT) ist für die Steuerung und Regelung der Kälte-/Klimatechnik zuständig.	**Versagen:** Ja, der Ausfall der Gebäudeleittechnik kann dazu führen, dass die Entstehung eines Brands bspw. durch nicht gegebene natürliche Belüftung begünstigt wird. **Manipulation:** Ja, eine Manipulation der Gebäudeleittechnik kann dazu führen, dass die Entstehung eines Brands begünstigt wird.	G 0.1 Feuer G 0.2 Ungünstige klimatische Bedingungen G 0.3 Wasser G 0.4 Verschmutzung, Staub, Korrosion G 0.5 Naturkatastrophen G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.11 Ausfall oder Störung von Dienstleistern G 0.12 Elektromagnetische Störstrahlung G 0.21 Manipulation von Hard- oder Software G 0.24 Zerstörung von Geräten oder Datenträgern G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder Systemen G 0.34 Anschlag G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.41 Sabotage G 0.44 Unbefugtes Eindringen in Räumlichkeiten G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.10 Fehlende Backups BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.22 Schadsoftware auf EWS BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	G 0.14 Ausspähen von Informationen (Spionage) G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme	**Versagen:** Die Auswirkungen eines Versagens der Gebäudeleittechnik können bspw. durch Datensicherungen, Redundanzen oder manuelle Ersatzprozesse verringert werden. **Manipulation:** Die Auswirkungen einer Manipulation der Gebäudeleittechnik können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip oder physischen Zutrittskontrollen verringert werden.
		Brand-überwachung Überwachung und Meldung von Wärme- und Rauchparametern zur Entdeckung und frühzeitigen Eindämmung von Bränden.	**Versagen:** Ja, ein Versagen der Brandüberwachung kann zur Beschädigung der Anlage aufgrund eines Brands führen. **Manipulation:** Ja, eine Manipulation der Brandüberwachung kann zur Beschädigung der Anlage aufgrund eines Brands führen.			**Versagen:** Die Auswirkungen eines Versagens der Brandüberwachung können bspw. durch Datensicherungen, Redundanzen oder manuelle Ersatzprozesse verringert werden. **Manipulation:** Die Auswirkungen einer Manipulation der Brandüberwachung können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip oder

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	Beispielhafte Referenzmaßnahmen, die den HCE verringern können
					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	physischen Zutrittskontrollen verringert werden.
		Kransteuerung und Automatisierung Die Kransteuerung und Automatisierung ist für die Ansteuerung und Überwachung des Kranprozesses zuständig.	**Versagen:** Nein, der Ausfall der Kransteuerung und Automatisierung kann keine langfristigen Anlagenschäden verursachen. **Manipulation:** Ja, eine Beschädigung des Krans durch absichtliche Fehlbedienung kann zu schweren Schäden an der Anlage führen.			**Versagen:** Die Auswirkungen eines Versagens der Kransteuerung und Automatisierung können bspw. durch Sicherheitseinrichtungen oder manuelle Ersatzprozesse verringert werden. **Manipulation:** Die Auswirkungen einer Manipulation der Kransteuerung und Automatisierung können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip, Sicherheitseinrichtungen oder physischen Zutrittskontrollen verringert werden.
		Kran-visualisierung: Die Kranvisualisierung ist für die Darstellung der Kranmeldungen, der Kranposition und für das Konfigurieren des Vollautomatikbetriebs zuständig.	**Versagen:** Nein, der Ausfall der Kranvisualisierung kann nicht zur Beschädigung der Anlage führen. **Manipulation:** Ja, eine Manipulation der Visualisierung bei Vollautomatikbetrieb kann zur Beschädigung der Anlage führen.			**Versagen:** Die Auswirkungen eines Versagens der Kransvisulaisierung können bspw. durch Sicherheitseinrichtungen oder manuelle Ersatzprozesse (z. B. Prozessbeobachtung mittels Kameras) verringert werden. **Manipulation:** Die Auswirkungen einer Manipulation der Kranvisualisierung

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	Beispielhafte Referenzmaßnahmen, die den HCE verringern können
						können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip, Sicherheitseinrichtungen oder physischen Zutrittskontrollen verringert werden.
Verbrennung	**HCE:** Erhebliche physikalische Beschädigung der Anlage **existenzbedrohend** Eine erhebliche Beschädigung der Anlage kann bspw. zu einem langfristigen Stillstand der Anlage führen.	**Bedienen und Beobachten der Anlage im Leitsystem:** Steuerung und Regelung der Verbrennung über Speicherprogram mierbare Steuerungen (SPS) und/oder das Bedien- und Beobachtungs-system vom Leitstandsfahrer	**Versagen:** Ja, sofern die Überwachung des Anlagenprozesses nicht mehr möglich ist, können keine Anpassungsmaßnahmen durchgeführt werden, was zur Beschädigung und somit zu langfristigen Stillständen der Anlage führen kann. Eine Verbrennung von Abfällen ist dann nicht mehr möglich. **Manipulation:** Ja, eine Manipulation der Steuerung und Regelung der Verbrennung kann zu einer Beschädigung und somit zu langfristigen Stillständen der Anlage führen. Eine Verbrennung von Abfällen ist dann nicht mehr möglich.	G 0.1 Feuer G 0.2 Ungünstige klimatische Bedingungen G 0.3 Wasser G 0.4 Verschmutzung, Staub, Korrosion G 0.5 Naturkatastrophen G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.11 Ausfall oder Störung von Dienstleistern G 0.12 Elektromagnetische Störstrahlung G 0.21 Manipulation von Hard- oder Software G 0.24 Zerstörung von Geräten oder Datenträgern G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder Systemen G 0.34 Anschlag G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.41 Sabotage G 0.44 Unbefugtes Eindringen in Räumlichkeiten G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.10 Fehlende Backups BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)	G 0.14 Ausspähen von Informationen (Spionage) G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk	**Versagen:** Die Auswirkungen eines Versagens der Bedien- und Beobachtungsfunktion im Leitsystem können bspw. durch Sicherheitseinrichtungen oder manuelle Ersatzprozesse (z. B. Prozessbeobachtung mittels Kameras) verringert werden. **Manipulation:** Die Auswirkungen einer Manipulation der Bedien- und Beobachtungsfunktion im Leitsystem können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip, Sicherheitseinrichtungen oder physische Zutrittskontrollen verringert werden.

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	Beispielhafte Referenzmaßnahmen, die den HCE verringern können
				BSI-ICSK.22 Schadsoftware auf EWS BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 2 Schadsoftware in E-Mail-AnhängenB 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware B 5 Daten-Exfiltration	
Sortierung	**HCE:** Erhebliche physikalische Beschädigung der Anlage **Beträchtlich** Eine Beschädigung der Anlage kann dazu führen, dass langfristig nicht mehr, ohne manuelles Sortieren, sortiert werden kann.	**Bedienung von Sortieranlagen:** z.B. Trennung von Metallen; Wegblasen von Papier;z.B. durch Einsatz von Kameras und Sensoren zum Sortieren;	**Versagen:** Ja, ein Ausfall von Sortieranlagen kann dazu führen, dass eine Sortierung nicht mehr möglich ist. **Manipulation:** Ja, eine Manipulation der Sortieranlagen kann dazu führen, dass die Anlage beschädigt wird.	G 0.1 Feuer G 0.2 Ungünstige klimatische Bedingungen G 0.3 Wasser G 0.4 Verschmutzung, Staub, Korrosion G 0.5 Naturkatastrophen G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.11 Ausfall oder Störung von Dienstleistern G 0.12 Elektromagnetische Störstrahlung G 0.21 Manipulation von Hard- oder Software G 0.24 Zerstörung von Geräten oder Datenträgern G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder Systemen G 0.34 Anschlag G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.41 Sabotage G 0.44 Unbefugtes Eindringen in Räumlichkeiten G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.10 Fehlende Backups	G 0.14 Ausspähen von Informationen (Spionage) G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen	**Versagen:** Die Auswirkungen eines Versagens der Sortieranlage können bspw. durch manuelle Ersatzprozesse (z. B. manuelle Sortieren) verringert werden. **Manipulation:** Die Auswirkungen einer Manipulation der Sortieranlagen können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip oder physische Zutrittskontrollen verringert werden.

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	Beispielhafte Referenzmaßnahmen, die den HCE verringern können
				BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.22 Schadsoftware auf EWS BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme 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	
Behandlung	**HCE:** Abfälle können bspw. aufgrund eines Brands im Lager nicht behandelt werden **Existenzbedrohend:** Ein Brand im Lager kann derart Schäden hervorrufen, dass Abfälle langfristig nicht behandelt werden können.	**Sensorik:** Sensorik zur Überwachung der Mechanisch-Biologische-Aufbereitung bzgl. Selbstentzündung	**Versagen:** Ja, Ausfälle der Sensorik bzgl. Selbstentzündung können zu Bränden führen. **Manipulation:** Ja, eine Manipulation der Sensorik kann dazu führen, dass es zu Prozessstörungen kommt. Dies kann zu Einschränkungen bis hin zum Stillstand des Betriebs führen.	G 0.1 Feuer G 0.2 Ungünstige klimatische Bedingungen G 0.3 Wasser G 0.4 Verschmutzung, Staub, Korrosion G 0.5 Naturkatastrophen G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.11 Ausfall oder Störung von Dienstleistern G 0.12 Elektromagnetische Störstrahlung G 0.21 Manipulation von Hard- oder Software G 0.24 Zerstörung von Geräten oder Datenträgern G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder Systemen G 0.34 Anschlag G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.41 Sabotage G 0.44 Unbefugtes Eindringen in Räumlichkeiten G 0.45 Datenverlust G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten	G 0.14 Ausspähen von Informationen (Spionage) G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten	**Versagen:** Die Auswirkungen eines Versagens der Sensorik können bspw. durch manuelle Ersatzprozesse (z. B. Sichtprüfungen) verringert werden. **Manipulation:** Die Auswirkungen einer Manipulation der Sensorik können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip oder physischen Zutrittskontrollen verringert werden.

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	Beispielhafte Referenzmaßnahmen, die den HCE verringern können
				BSI-ICSK.10 Fehlende Backups BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.22 Schadsoftware auf EWS BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme 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	
Rauchgas-reinigung	**HCE:** Rauchgas kann nicht mehr gereinigt werden **Beträchtlich** Ausfall der Rauchgasreinigung führt dazu, dass die Anlage nicht weiter betrieben werden kann und ein Anlagenstillstand in einer Dauer, die nicht mehr durch eigene Lagerkapazitäten abgefangen werden kann, eintritt.	**Bedienen und Beobachten der Anlage im Leitsystem:** Bedienen und Beobachten der Anlage im Leitsystem und Überwachung der Parameter und Steuerungs- und Regelungsprozesse über die SPS (z. B. Abfallmenge, -art, Luftzufuhr, Emissionen, Ammoniakzuführung, Rauchgasreinigungsumfahrung (Bypässe)).	**Versagen:** Ja, die Rauchgasreinigung kann aufgrund eines Ausfalls des Prozessleitsystems versagen, was zu einem Ausfall der Anlage führen kann. **Manipulation:** Ja, eine Manipulation im Leitsystem kann dazu führen, dass Schadstoffe in die Umwelt gelangen (bspw. weil zu wenig Ammoniak im Prozess verwendet wird) oder dass Schäden an der Anlage entstehen. Bei Überschreitung von Grenzwerten darf die Anlage nicht weiter betrieben werden (nur auf Anweisung der zuständigen Behörde). Bei Beschädigung der Anlage ist diese ggf. außer Betrieb zu nehmen, um Instandhaltungs-maßnahmen durchzuführen.	G 0.2 Ungünstige klimatische Bedingungen G 0.4 Verschmutzung, Staub, Korrosion G 0.8 Ausfall oder Störung der Stromversorgung G 0.9 Ausfall oder Störung von Kommunikationsnetzen G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.24 Zerstörung von Geräten oder Datenträgern G 0.25 Ausfall von Geräten oder Systemen G 0.26 Fehlfunktion von Geräten oder Systemen G 0.28 Software-Schwachstellen oder -Fehler G 0.39 Schadprogramme G 0.40 Verhinderung von Diensten (Denial of Service) G 0.45 Datenverlust G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten BSI-ICSK.10 Fehlende Backups	G 0.14 Ausspähen von Informationen (Spionage) G 0.18 Fehlplanung oder fehlende Anpassung G 0.19 Offenlegung schützenswerter Informationen G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle G 0.21 Manipulation von Hard- oder Software G 0.22 Manipulation von Informationen G 0.23 Unbefugtes Eindringen in IT-Systeme G 0.28 Software-Schwachstellen oder -Fehler G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.32 Missbrauch von Berechtigungen G 0.35 Nötigung, Erpressung oder Korruption G 0.36 Identitätsdiebstahl G 0.39 Schadprogramme G 0.42 Social Engineering G 0.43 Einspielen von Nachrichten G 0.46 Integritätsverlust schützenswerter Informationen BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten	**Versagen:** Die Auswirkungen eines Versagens der Bedien- und Beobachtungsfunktion im Leitsystem können bspw. durch Sicherheitseinrichtungen oder manuelle Ersatzprozesse (z. B. Prozessbeobachtung mittels Kameras) verringert werden. **Manipulation:** Die Auswirkungen einer Manipulation der Bedien- und Beobachtungsfunktion im Leitsystem können bspw. durch restriktive Berechtigungsvergabe, Vier-Augen-Prinzip, Sicherheitseinrichtungen oder physische Zutrittskontrollen verringert werden.

kDL Hauptschritt	High Consequence Events (HCE) & Bewertung	Technische Funktion	Kann Versagen oder Manipulation der Funktion zum HCE führen?	Bedrohungen und Schwachstellen, die zu einem Versagen führen können	Bedrohungen und Schwachstellen, die zu einer Manipulation führen können	Beispielhafte Referenzmaßnahmen, die den HCE verringern können
				BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten BSI-ICSK.16 Denial-of-Service-Angriffe (DoS) BSI-ICSK.23 Schadprogramme BSI-ICSK.24 Replay-Angriff B 1 Ausnutzung von Zero-Day Schwachstellen B 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware	BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk BSI-ICSK.17 Man-in-the-Middle-Angriff BSI-ICSK.18 Phishing BSI-ICSK.19 Injection-Angriffe BSI-ICSK.20 Cross-Site-Scripting BSI-ICSK.23 Schadprogramme B 1 Ausnutzung von Zero-Day Schwachstellen B 2 Schadsoftware in E-Mail-AnhängenB 3 Advanced Persistent Threat (APT)-Angriffe B 4 Ransomware B 5 Daten-Exfiltration	

A.2 Empfehlungen für Betreiber einer Kritischen Infrastruktur zur Meldung von IT-Sicherheitsvorfällen gegenüber dem BSI

Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das BSI zu melden:

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,
2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.

Eine erhebliche Beeinträchtigung der Funktionsfähigkeit ist z.B.

- ein ungeplanter Stillstand der Anlage
- eine Störung, die nicht Teil des Regelbetriebs ist und nur mit erhöhtem Aufwand bewältigt werden kann.

Es ist in jedem Fall zu berücksichtigen, dass nicht nur der Ausfall, sondern bereits die Möglichkeit des Ausfalls der kDL zur Meldung verpflichtet (vgl. § 8b Abs. 4 Nr. 2 BSIG).

A.3 Bedrohungsszenarien, elementare Gefährdungen und Schwachstellen

Im Rahmen der Sicherheit kritischer Infrastrukturen (KRITIS) ist es entscheidend, die unterschiedlichen Begriffe im Bereich der Gefährdungsanalyse klar voneinander abzugrenzen:

- **Bedrohungen** beschreiben Ereignisse oder Handlungen – absichtlich oder unabsichtlich –, die darauf abzielen oder dazu führen können, Schaden an einer kritischen Infrastruktur zu verursachen.
- **Elementare Gefährdungen** umfassen grundlegende Gefahrenquellen, die unabhängig vom Handeln eines Akteurs entstehen können, wie Naturereignisse, technische Defekte oder menschliches Versagen.
- **Schwachstellen** sind Verwundbarkeiten innerhalb von Systemen, Prozessen oder Strukturen, die es Bedrohungen ermöglichen, elementare Gefährdungen wirksam werden zu lassen.

Das Zusammenspiel dieser Faktoren bildet die Grundlage für die Risikoanalyse und das Ableiten geeigneter Schutzmaßnahmen im KRITIS-Kontext.

A.3.1 Besonders zu berücksichtigende Bedrohungsszenarien

Die folgenden Bedrohungsszenarien aus der „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG“ des BSI in der Version 1.3 vom 23.02.2024 gilt es besonders zu berücksichtigen:

Besonders zu berücksichtigende Bedrohungsszenarien (B3S Orientierungshilfe)	**Beispiele**	**Beispielhafte Referenzmaßnahmen**
B 1 Ausnutzung von Zero-Day Schwachstellen	Über eine Schwachstelle in einem Fernwartungszugang können unberechtigte Zugriffe auf interne Netze (z.B. Anlagensteuerung, Tourenplanungssoftware) erfolgen.	- Detektions- / Suchmöglichkeit auf Infektionen - Client-Isolation - Innere Sensorik (zur Detektion von IT-Angriffen) - Härtung von Verzeichnisdiensten wie z.B: dem MS Active Directory - Backup-Konzept inklusive offline Backups - Etablierung eines Patchmanagement - Netzwerksegmentierung

B 2 Schadsoftware in E-Mail-Anhängen	Mittels einer Schad-E-Mail können unberechtigte Zugriffe auf interne Netze (z.B. Anlagensteuerung, Tourenplanungssoftware) erfolgen.	- Schulung Mitarbeiter zur Erkennung von schadhaften Anhängen / E-Mails - Detektions- / Suchmöglichkeit auf Infektionen - Client-Isolation - Innere Sensorik (zur Detektion von IT-Angriffen)
B 3 Advanced Persistent Threat (APT)-Angriffe	Über APT-Angriffe können neben dem initial angegriffenen System weitere Berechtigungen für kritischere Systeme erlangt werden.	- Passwortrichtlinie - Multifaktorauthentifizierung - Detektions- / Suchmöglichkeit auf Infektionen - Client-Isolation - Innere Sensorik (zur Detektion von IT-Angriffen) - Härtung von Verzeichnisdiensten wie z.B: dem MS Active Directory - Backup-Konzept inklusive offline Backups - Etablierung eines Patchmanagement - Netzwerksegmentierung
B 4 Ransomware	Durch Einsatz von Ransomware können interne Systeme unnutzbar werden.	- Detektions- / Suchmöglichkeit auf Infektionen - Client-Isolation - Innere Sensorik (zur Detektion von IT-Angriffen) - Härtung von Verzeichnisdiensten wie z.B: dem MS Active Directory - Backup-Konzept inklusive offline Backups - Etablierung eines Patchmanagement
B 5 Daten-Exfiltration	Unberechtigt erlangte Daten können für gezielte Angriffe auf interne Systeme genutzt werden, z.B. Zugangsdaten, Netzwerkinformationen und eingesetzte Soft- und Hardware.	- Detektions- / Suchmöglichkeit auf Infektionen - Client-Isolation - Innere Sensorik (zur Detektion von IT-Angriffen) - Härtung von Verzeichnisdiensten wie z.B: dem MS Active Directory - Backup-Konzept inklusive offline Backups - Etablierung eines Patchmanagement

A.3.2 Elementare Gefährdungen

Die folgenden elementaren Gefährdungen aus dem Katalog elementarer Gefährdungen des BSI (Stand: 07.12.2020) wurden als relevant für die Branche Siedlungsabfallentsorgung ermittelt. Alle nicht aufgeführten elementare Gefährdungen sind demgegenüber in der Regel nicht in der Lage, zu einem Versagen oder einer Manipulation der branchenspezifischen technischen Funktion zu führen. Dies ist zwingendvon jedem Betreiber individuell zu überprüfen. Zur Orientierung finden sich zu jeder Gefährdung mögliche Referenzmaßnahmen aus den Kapiteln 5 bis 8.

Relevante Bedrohungen & Schwachstellen aus dem Katalog elementarer Gefährdungen	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
G 0.1 Feuer	7.5 Schutz vor physischen und umweltbedingten Bedrohungen 7.8 Platzierung und Schutz von Geräten und Betriebsmitteln
G 0.2 Ungünstige klimatische Bedingungen	5.1 Informationssicherheitspolitik und -richtlinien 5.13 Kennzeichnung von Information 5.14 Informationsübermittlung
G 0.3 Wasser	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt
G 0.4 Verschmutzung, Staub, Korrosion	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen 7.13 Instandhaltung von Geräten und Betriebsmitteln
G 0.5 Naturkatastrophen	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.5 Schutz vor physischen und umweltbedingten Bedrohungen
G 0.8 Ausfall oder Störung der Stromversorgung	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.11 Versorgungseinrichtungen 8.13 Sicherung von Information

Relevante Bedrohungen & Schwachstellen aus dem Katalog elementarer Gefährdungen	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
	8.14 Redundanz von informationsverarbeitenden Einrichtunge
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.11 Versorgungseinrichtungen 8.13 Sicherung von Information 8.14 Redundanz von informationsverarbeitenden Einrichtungen
G 0.11 Ausfall oder Störung von Dienstleistern	5.19 Informationssicherheit in Lieferantenbeziehungen 5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen 5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette 5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
G 0.12 Elektromagnetische Störstrahlung	7.5 Schutz vor physischen und umweltbedingten Bedrohungen 7.8 Platzierung und Schutz von Geräten und Betriebsmitteln
G 0.14 Ausspähen von Informationen (Spionage)	5.1 Informationssicherheitspolitik und -richtlinien 5.7 Informationen über die Bedrohungslage 5.12 Klassifizierung von Information 5.14 Informationsübermittlung 5.18 Zugangsrechte 6.1 Sicherheitsüberprüfung 6.4 Maßregelungsprozess 6.6 Vertraulichkeits- und Geheimhaltungsvereinbarungen
G 0.18 Fehlplanung oder fehlende Anpassung	5.1 Informationssicherheitspolitik und -richtlinien 5.13 Kennzeichnung von Information 5.14 Informationsübermittlung 5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit 5.37 Dokumentierte Betriebsabläufe

Relevante Bedrohungen & Schwachstellen aus dem Katalog elementarer Gefährdungen	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
G 0.19 Offenlegung schützenswerter Informationen	5.1 Informationssicherheitspolitik und -richtlinien 5.13 Kennzeichnung von Information 5.14 Informationsübermittlung 5.14 Informationsübermittlung 5.15 Zugangssteuerung 5.33 Schutz von Aufzeichnungen 6.1 Sicherheitsüberprüfung 6.2 Beschäftigungs- und Vertragsbedingungen 6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung 6.4 Maßregelungsprozess 6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung 8.13 Sicherung von Information 8.24 Verwendung von Kryptographie
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	5.1 Informationssicherheitspolitik und -richtlinien 5.13 Kennzeichnung von Information 5.14 Informationsübermittlung 5.19 Informationssicherheit in Lieferantenbeziehungen 5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen
G 0.21 Manipulation von Hard- oder Software	5.1 Informationssicherheitspolitik und -richtlinien 5.13 Kennzeichnung von Information 5.14 Informationsübermittlung 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen 7.8 Platzierung und Schutz von Geräten und Betriebsmitteln 7.9 Sicherheit von Werten außerhalb der Räumlichkeiten 7.13 Instandhaltung von Geräten und Betriebsmitteln 7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln 8.16 Überwachung von Aktivitäten

Relevante Bedrohungen & Schwachstellen aus dem Katalog elementarer Gefährdungen	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
G 0.22 Manipulation von Informationen	5.1 Informationssicherheitspolitik und -richtlinien 5.13 Kennzeichnung von Information 5.14 Informationsübermittlung 5.15 Zugangssteuerung 8.24 Verwendung von Kryptographie 8.33 Testdaten
G 0.23 Unbefugtes Eindringen in IT-Systeme	5.1 Informationssicherheitspolitik und -richtlinien 8.5 Sichere Authentisierung 8.20 Netzwerksicherheit 8.21 Sicherheit von Netzwerkdiensten 8.22 Trennung von Netzwerken
G 0.24 Zerstörung von Geräten oder Datenträgern	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen 7.6 Arbeiten in Sicherheitsbereichen
G 0.25 Ausfall von Geräten oder Systemen	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 8.14 Redundanz von informationsverarbeitenden Einrichtungen
G 0.26 Fehlfunktion von Geräten oder Systemen	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 8.15 Protokollierung
G 0.28 Software-Schwachstellen oder -Fehler	5.1 Informationssicherheitspolitik und -richtlinien 5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette 7.2 Physischer Zutritt 8.8 Handhabung von technischen Schwachstellen

Relevante Bedrohungen & Schwachstellen aus dem Katalog elementarer Gefährdungen	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
	8.15 Protokollierung 8.16 Überwachung von Aktivitäten 8.26 Anforderungen an die Anwendungssicherheit 8.29 Sicherheitsprüfung bei Entwicklung und Abnahme
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 8.2 Privilegierte Zugangsrechte 8.3 Informationszugangsbeschränkung 8.5 Sichere Authentisierung 8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 8.2 Privilegierte Zugangsrechte 8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten
G 0.32 Missbrauch von Berechtigungen	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 8.2 Privilegierte Zugangsrechte 8.3 Informationszugangsbeschränkung 8.5 Sichere Authentisierung
G 0.34 Anschlag	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen 7.5 Schutz vor physischen und umweltbedingten Bedrohungen
G 0.35 Nötigung, Erpressung oder Korruption	5.1 Informationssicherheitspolitik und -richtlinien

Relevante Bedrohungen & Schwachstellen aus dem Katalog elementarer Gefährdungen	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
	7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen
G 0.36 Identitätsdiebstahl	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen 8.2 Privilegierte Zugangsrechte 8.3 Informationszugangsbeschränkung 8.5 Sichere Authentisierung
G 0.39 Schadprogramme	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen 8.22 Trennung von Netzwerken 8.23 Webfilterung 8.13 Sicherung von Information
G 0.40 Verhinderung von Diensten (Denial of Service)	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen 8.14 Redundanz von informationsverarbeitenden Einrichtungen 8.15 Protokollierung 8.16 Überwachung von Aktivitäten 8.20 Netzwerksicherheit 8.21 Sicherheit von Netzwerkdiensten
G 0.41 Sabotage	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen 7.6 Arbeiten in Sicherheitsbereichen 7.12 Sicherheit der Verkabelung

Relevante Bedrohungen & Schwachstellen aus dem Katalog elementarer Gefährdungen	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
	7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
G 0.42 Social Engineering	5.1 Informationssicherheitspolitik und -richtlinien 5.12 Klassifizierung von Information 5.13 Kennzeichnung von Information 5.17 Authentisierungsinformationen 6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung 6.6 Vertraulichkeits- und Geheimhaltungsvereinbarungen 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen 8.3 Informationszugangsbeschränkung 8.5 Sichere Authentisierung 8.24 Verwendung von Kryptographie
G 0.43 Einspielen von Nachrichten	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen 8.15 Protokollierung 8.16 Überwachung von Aktivitäten 8.20 Netzwerksicherheit 8.21 Sicherheit von Netzwerkdiensten 8.22 Trennung von Netzwerken 8.24 Verwendung von Kryptographie
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 7.3 Sichern von Büros, Räumen und Einrichtungen
G 0.45 Datenverlust	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt

Relevante Bedrohungen & Schwachstellen aus dem Katalog elementarer Gefährdungen	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
G 0.46 Integritätsverlust schützenswerter Informationen	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 8.14 Redundanz von informationsverarbeitenden Einrichtungen 8.20 Netzwerksicherheit 8.24 Verwendung von Kryptographie
G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe	5.1 Informationssicherheitspolitik und -richtlinien 7.2 Physischer Zutritt 8.6 Kapazitätssteuerung 8.7 Schutz gegen Schadsoftware 8.13 Sicherung von Information 8.15 Protokollierung 8.16 Überwachung von Aktivitäten 8.22 Trennung von Netzwerken

A.3.3 Schwachstellen

Die folgenden Schwachstellen aus dem ICS-Security-Kompendium des BSI wurden als relevant für die Branche Siedlungsabfallentsorgung ermittelt:

Relevante Schwachstellen aus dem ICS-Security-Kompendium des BSI	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge	8.15 Protokollierung 7.2 Physischer Zutritt 8.20 Netzwerksicherheit 8.21 Sicherheit von Netzwerkdiensten 8.22 Trennung von Netzwerken
BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen	5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen 7.2 Physischer Zutritt 5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen

Relevante Schwachstellen aus dem ICS-Security-Kompendium des BSI	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
	8.8 Handhabung von technischen Schwachstellen
BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur	8.6 Kapazitätssteuerung 7.2 Physischer Zutritt
BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen	8.6 Kapazitätssteuerung 7.2 Physischer Zutritt
BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung	8.6 Kapazitätssteuerung 7.2 Physischer Zutritt
BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten	8.6 Kapazitätssteuerung 7.2 Physischer Zutritt
BSI-ICSK.10 Fehlende Backups	8.6 Kapazitätssteuerung 7.2 Physischer Zutritt
BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben	8.6 Kapazitätssteuerung 7.2 Physischer Zutritt 8.32 Änderungssteuerung 8.29 Sicherheitsprüfung bei Entwicklung und Abnahme 8.33 Testdaten
BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten	8.6 Kapazitätssteuerung 7.2 Physischer Zutritt
BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen	8.6 Kapazitätssteuerung 7.2 Physischer Zutritt 5.17 Authentisierungsinformationen 5.18 Zugangsrechte 8.2 Privilegierte Zugangsrechte

Relevante Schwachstellen aus dem ICS-Security-Kompendium des BSI	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
	8.3 Informationszugangsbeschränkung 8.5 Sichere Authentisierung
BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk	8.6 Kapazitätssteuerung 7.2 Physischer Zutritt 8.21 Sicherheit von Netzwerkdiensten 8.22 Trennung von Netzwerken
BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)	8.6 Kapazitätssteuerung 7.2 Physischer Zutritt 8.13 Sicherung von Information 8.14 Redundanz von informationsverarbeitenden Einrichtungen 8.15 Protokollierung 8.16 Überwachung von Aktivitäten 8.20 Netzwerksicherheit 8.21 Sicherheit von Netzwerkdiensten
BSI-ICSK.17 Man-in-the-Middle-Angriff	8.12 Verhinderung von Datenlecks 7.2 Physischer Zutritt 8.20 Netzwerksicherheit
BSI-ICSK.18 Phishing	5.27 Erkenntnisse aus Informationssicherheitsvorfällen 7.2 Physischer Zutritt
BSI-ICSK.19 Injection-Angriffe	8.20 Netzwerksicherheit 7.2 Physischer Zutritt 8.22 Trennung von Netzwerken 8.23 Webfilterung
BSI-ICSK.20 Cross-Site-Scripting	8.20 Netzwerksicherheit 7.2 Physischer Zutritt

Relevante Schwachstellen aus dem ICS-Security-Kompendium des BSI	Auswahl geeigneter Maßnahmen gem. Kapitel 5 bis 8
	8.22 Trennung von Netzwerken
BSI-ICSK.22 Schadsoftware auf EWS	8.7 Schutz gegen Schadsoftware 7.2 Physischer Zutritt
BSI-ICSK.23 Schadprogramme	7.10 Speichermedien 7.2 Physischer Zutritt 8.7 Schutz gegen Schadsoftware 8.22 Trennung von Netzwerken 8.23 Webfilterung
BSI-ICSK.24 Replay-Angriff	8.5 Sichere Authentisierung 7.2 Physischer Zutritt 8.21 Sicherheit von Netzwerkdiensten 8.22 Trennung von Netzwerken

A.4 Abkürzungen

B3S	Branchenspezifischer Sicherheitsstandard
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCM	Betriebliches Kontinuitätsmanagement
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
DIN	Deutsches Institut für Normung
DMZ	Demilitarisierte Zone
EE-Anlagen	Erneuerbare-Energien-Anlage
GPS	Global Positioning System
ICS	Industrial Control System
IDMZ	Industrial DMZ Infrastructure
IEC	International Electrotechnical Commission
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Information Technology, Informationstechnik
kDL	Kritische Dienstleistung
KRITIS	Kritische Infrastruktur
SaaS	Software-as-a-Service
SAE	Siedlungsabfallentsorgung
SIEM	Security Information and Event Monitoring
SPS	Speicherprogrammierbare Steuerungen
SzA	System zur Angriffserkennung
OT	Operational Technology
PbD	Personenbezogenen Daten
UP KRITIS	Unabhängige Partnerschaft KRITIS
URL	Uniform Resource Locator