Version, die zur Eignungsprüfung beim BSI eingereicht wurde, Änderungen im Rahmen des Prüfverfahrens vorbehalten.

# Branchenspezifischer Sicherheitsstandard für die Siedlungsabfallentsorgung
# B3S SAE

Nach § 8a Abs. 2 BSI-Gesetz

Stand: 05.03.2025
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

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 die 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 kritische 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 Abfallwirtschaft 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

*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 noch nicht festgestellt.*

[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

# 1 Anwendungsbereich und Adressaten des B3S

Der Anwendungsbereich dieses B3S umfasst die Siedlungsabfallentsorgung insoweit, als in der BSI-KritisV als Kritische Infrastruktur definierte Systeme oder Anlagen erfasst sind. Diese sind in den Bereichen Sammlung und Beförderung sowie Verwertung und Beseitigung definiert. Daher werden diese Bereiche in diesem B3S in den Blick genommen.

Der Branchenspezifische Sicherheitsstandard Siedlungsabfallentsorgung 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“ zur Berücksichtigung aller Gefahrenarten (zum Beispiel Naturgefahren, technologische Gefahren) im Rahmen des Risiko- und Krisenmanagements anzuwenden.

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 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.

# 2 Normative Verweise, Begriffe und Abkürzungen

## 2.1 Normative Verweise

Die folgenden zitierten Dokumente sind für die Anwendung dieses Branchenspezifischen Sicherheitsstandards für die Siedlungsabfallentsorgung erforderlich. 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).

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

**IT-Sicherheitsgesetz – IT-SiG**, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

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

**BSI-Standard 200-1**, Managementsysteme für Informationssicherheit (ISMS)

**BSI-Standard 200-2,** IT-Grundschutz-Methodik

**BSI-Standard 200-3,** Risikoanalyse auf der Basis von IT-Grundschutz

**BSI-Standard 200-4 Community Draft,** Business Continuity Management

**BSI IT-Grundschutz-Kompendium**

**BSI ICS-Security-Kompendium**

**DIN EN ISO 22301**, Sicherheit und Schutz des Gemeinwesens – Business Continuity Management System – Anforderungen

**DIN EN ISO/IEC 27001:2024**, Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen

**DIN EN ISO/IEC 27002:2024**, Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Managementsystem

**DIN ISO/IEC TR 27019,** Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Managementsystem von Steuerungssystemen der Energieversorger auf Grundlage der ISO/IEC 27002

## 2.2 Begriffe

### 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. 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 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 KritisV

Die BSI-KritisV[3] 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.[4] 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

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

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

Eine Gemeinsame Anlage ist nach Anhang 8 der BSI-KritisV, Teil 1, Nr. 4 folgendermaßen definiert: Mehrere Anlagen derselben Art, 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 in folgende Hauptschritte unterteilt:

(a) Sammlung und Beförderung
- Tourenplanung
- Personalplanung
- Fahrzeugdisposition
- Sammlung und Beförderung
- Lagerung, Zwischenlagerung und Umladen von Abfällen

(b) Verwertung und Beseitigung
- Abfallmengenerfassung an der Annahme
- Abfallvorbehandlung (u. U. mit Vorsortierung)
- Lager- und Bunkermanagement
- Verbrennung/Sortierung/Behandlung
- Rauchgasreinigung

### 2.2.6 Kritische Infrastrukturen

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? (Kontex)
- 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? (Externe)
- Wie sind die Bestandteile der Anlage vernetzt? (Netzstrukturplan)

Ausführliche Erläuterungen zur Dokumentation des Geltungsbereichs sind auf der BSI-Website veröffentlicht.[5]

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 zu der kritischen Dienstleistung. Diese muss für die Nachweiserbringung gemäß § 8a Absatz 3 BSIG anhand der vorgenannten Fragen durch die KRITIS-Betreiber ausgeprägt und detailliert werden. Ein so dokumentierter Geltungsbereich ist darüber hinaus wesentlicher Bestandteil des Managementsystems für Informationssicherheit (vgl. 3.3).

Der Geltungsbereich (Scope) umfasst alle Aspekte, die direkt zur Sicherstellung der kritischen Dienstleistungen im Sektor Siedlungsabfallentsorgung beitragen, insbesondere:

- **IT/ OT-Infrastruktur und Kommunikation** (z. B. Netzwerke, Firewalls, Gateways und Router)
- **IT/ OT für die kritische Dienstleistungen**
    - Sammlung und Beförderung
        - Dispositionssysteme
        - Flottenmanagement
        - Lagermanagement
    - Verwertung und Beseitigung
        - OT-Infrastruktur (z.B. Netztrennung)
        - Regelungs-, Steuerungs- und Leittechnik

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

        - Mengenmanagement
- **Sonstige relevante Aspekte**
    - Gebäude und Räume
    - Warten und Leitstände
    - Personal
    - Prozesse
- **Extern erbrachte Leistungen**
    - Lieferanten
    - Fernzugriff

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 oder Vertraulichkeit der für die kritischen Dienstleistungen essenziellen Systeme haben.
- Allgemeine IT-Systeme, die keine Relevanz für die kritische Dienstleistungen aufweisen (z.B. Email).
- Leistungen und Ressourcen, die unabhängig von der spezifischen kritischen Dienstleistung sind (z. B. generelle Verwaltungsprozesse).

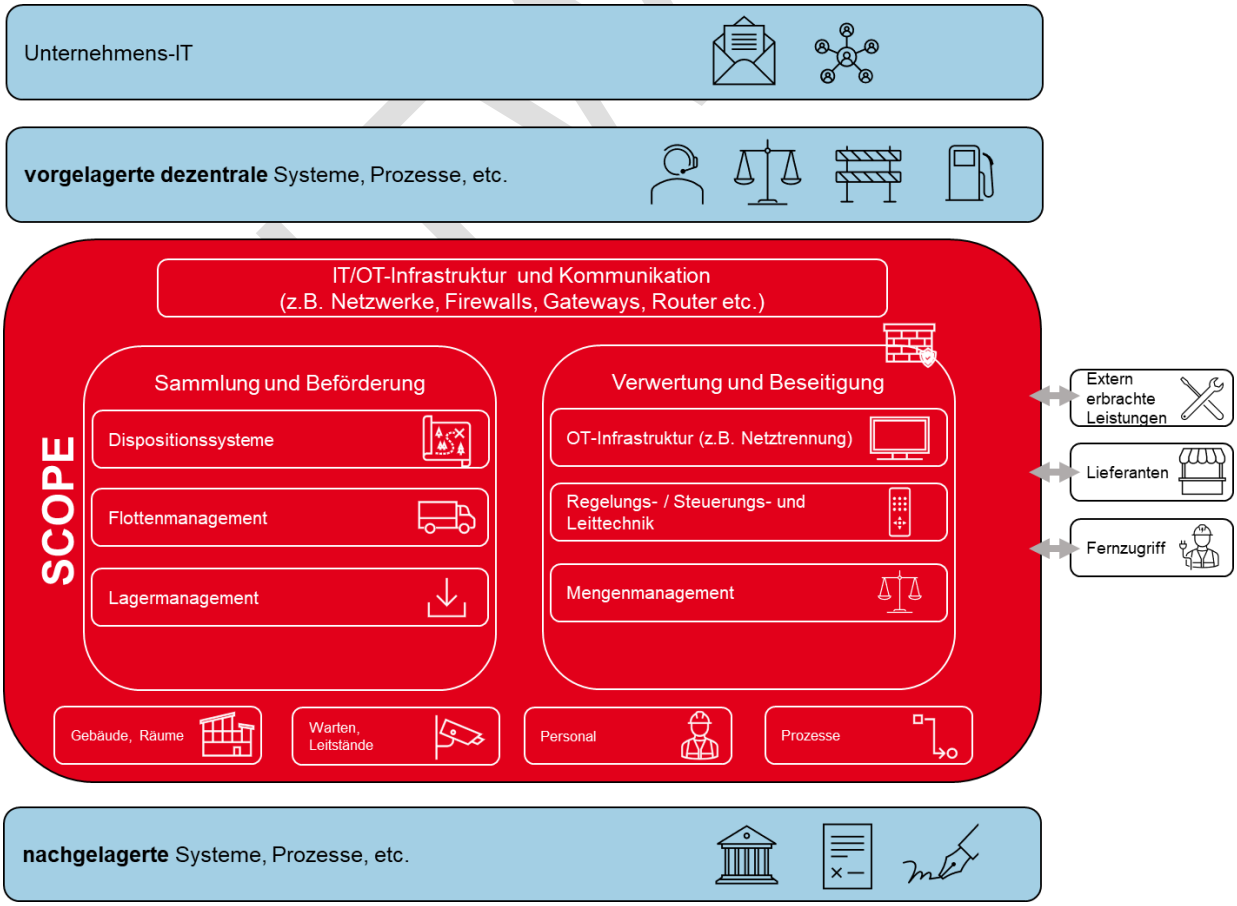


Abbildung 1: Schematische Darstellung des Geltungsbereichs

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

# 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 und Vertraulichkeit von Informationen dar, d. h. der Schutz der informationstechnischen Systeme, Komponenten, Prozesse und Daten.

Ein Informationssicherheitsmanagementsystem (ISMS) nach DIN EN ISO/IEC 27001:2024 unterscheidet organisatorische, personenbezogene, physische und technologische Maßnahmen, 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.

Mit Blick auf den Schutz der informationstechnischen Systeme, Komponenten, Prozesse und Daten im Allgemeinen und die eingesetzte Sicherheitstechnik bzw. -maßnahmen im Speziellen sollte 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. Nachweise, die im Rahmen anderer Prüfungen erbracht werden, können als Nachweisdokumente für die Betrachtung im Rahmen der BSI-KritisV herangezogen werden („mitgeltende Dokumente“). Hierbei wird jedoch nicht ihr bereits von anderer Stelle geprüfter Inhalt, sondern lediglich das Vorhandensein derartiger Nachweise überprüft.

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 branchespezifische 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 oder 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

- Ausfälle/Ausfallzeiten der informationstechnischen Systeme, Komponenten oder Prozesse vermieden werden und ein Zugriff auf die relevanten Daten im Rahmen der für die jeweilige Anlage festgelegte 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

SAE-Betreiber, die Kritische Infrastrukturen betreiben, sind zum Einsatz angemessener technischer und organisatorischer Sicherheitsvorkehrungen zum Schutz der KRITIS-Anlagen, die dem „Stand der Technik“ entsprechen, 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 als Ausfluss der Organisationsverantwortung von oben nach unten zu organisieren (Top-down-Ansatz).

Diesen Anforderungen kann zum Beispiel durch Einführung eines ISMS nach DIN EN ISO/IEC 27001:2024 Genüge getan werden. Eine formale Zertifizierung ist nach dem BSIG nicht zwingend. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen[6].

Allerdings ist für Betreiber Kritischer Infrastrukturen die Aufstellung und Einführung von Verfahren und Regeln zwingend erforderlich, um die Informationssicherheit zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Ein bestehendes zertifiziertes ISMS kann dies deutlich erleichtern.

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

[6] Weitere-führende Information-en können über https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSIG/8aBSIG_ISO27001/Fragen/01-WelcheRahmenbedingungen_ISO27001.html eingeholt werden

der Technik getroffen wurden (siehe § 8a Abs. 3 S. 1 BSIG). Dies umfasst auch den Einsatz von Systemen zur Angriffserkennung, § 8a Abs. 1a BSIG.

## 3.4 Betriebliches Kontinuitätsmanagement (BCM)

Für die Betreiber Kritischer Infrastrukturen im Sektor Siedlungsabfallentsorgung gelten aufgrund der einschlägigen gesetzlichen Regelungen (vgl. 2.1), unabhängig von den IT-Systemen, Grundanforderungen in Bezug auf die Fortsetzung des Betriebs bei Störungen. Da diese Vorgaben unabhängig von der Ursache der Störung bestehen, ist eine gesonderte Betrachtung in Bezug auf den Branchenstandard nicht erforderlich.

## 3.5 Bedrohungsanalyse für Systeme in der Siedlungsabfallentsorgung

Die Bedrohungsanalyse ist ein Teilbereich des Risikomanagements und der Risikoanalyse. Mithilfe der Bedrohungsanalyse lassen sich die verschiedenen Bedrohungen für IT-Systeme und IT-Prozesse systematisch erfassen, strukturieren und bewerten.

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

Für IT-Systeme im Sinne dieses Branchenspezifischen Sicherheitsstandards existieren eine Vielzahl möglicher Bedrohungen, die im Rahmen der Bedrohungsanalyse identifiziert, erfasst und bewertet werden müssen. Mögliche Bedrohungen sind:

- unbefugter Zugriff auf Daten
- Diebstahl oder Manipulation von Daten
- unbefugter Zugriff auf Systeme
- Störung der Verfügbarkeit von Systemen
- Manipulation von Systemen
- Angriffe durch beispielsweise Social Engineering oder Malware
- Denial of Service Angriffe
- Diebstahl von Benutzerkennungen

## 3.6 Risikoeinschätzung und-bewertung

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 Gefährdungen eingehen, die für Systeme und Anlagen bestehen, die zur Sammlung & Beförderung und zur Verwertung & Beseitigung von Siedlungsabfällen genutzt werden.

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 sollten 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.

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 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.

Gefährdungsszenarien können anhand von Gefährdungskatalogen, wie den elementaren Gefährdungen des BSI oder den Gefährdungen aus dem BSI ICS-Kompendium hergeleitet werden und haben den All-Gefahren-Ansatz abzudecken. Eine Auflistung der im Rahmen dieses Branchenspezifischen Sicherheitsstandards als relevant eingestuften Gefährdungen aus o.g. Katalogen ist Anhang A.3 zu entnehmen.

Bei der Umsetzung der Risikoanalyse wird den SAE-Betreibern empfohlen, sich am BSI-Standard 200-3[7] zu orientieren. Im Folgenden werden relevante Elemente des BSI-Standard 200-3 zu dem besseren Verständnis kurz aufgegriffen:

Im Hinblick auf die Eintrittshäufigkeit wird auf folgende Unterscheidung verwiesen:

- selten - Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten
- mittel - Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
- häufig - Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
- sehr häufig - Ereignis tritt mehrmals im Monat ein.

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.

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

| 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) |
| **Begrenzt** | erhebliche Verzögerungen der Sammlung/Beförderung; Vorfälle können eigenständig unter Einsatz externer Ressourcen (einzelne Fahrzeuge oder Arbeitskräfte) bewältigt werden | Anlagenstillstand, der durch eigene Lagerkapazitäten abgefangen werden kann |
| **Beträchtlich/ ggf. existenz-bedrohend** | Störung der Sammlung/Beförderung in einer Dauer, welche nicht eigenständig aufgeholt werden kann | Anlagenstillstand in einer Dauer, die nicht mehr durch eigene Lagerkapazitäten abgefangen werden kann - Die Abfallannahme ist nicht mehr gewährleistet |

*Tabelle 1: Einschätzung der Auswirkungen*

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

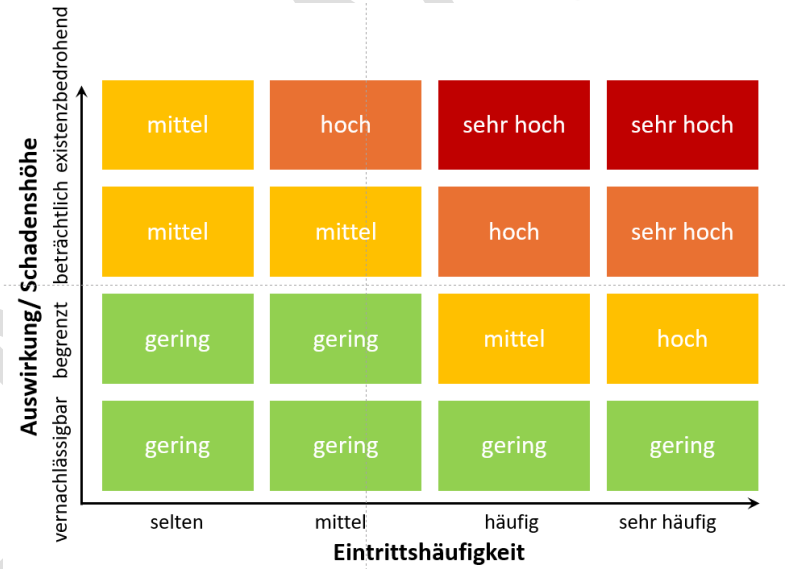


*Abbildung 2:Risikomatrix gemäß BSI-Standard 200-3*

## 3.7 Risikobehandlung

Risiken mit einer hohen oder sehr hohen Auswirkung auf die Erbringung der kritischen Dienstleistung, sind zwingend zu reduzieren.

Eine Akzeptanz oder ein Transferieren von hohen oder sehr hohen Restrisiken ist SAE-Betreibern nicht gestattet. Für geringe und mittlere Risiken ist dies jedoch möglich.

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. Das grundsätzliche Vorgehen einer Risikoanalyse kann dem BSI Standard 200-3[8] entnommen werden.

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

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



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

# 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 aus sowie in 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 in der IT zu etablieren. Aufgrund der teilweise fehlenden technischen Möglichkeiten in der OT sind hier vorallem organisatorische Maßnahmen umzusetzen.

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 zu beachten. Für die Feststellung des Reifegrads der Umsetzung kann die Definition der Umsetzungsgrade der Orientierungshilfe 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,
- bei der Implementierung einer Methode ist zu berücksichtigen, dass es keine Rückwirkung / Beeinträchtigung auf bestehende Systeme geben darf.

Dabei zu beachten sind folgende Parameter:

- Wie können Angriffe erkannt werden und wo sollte die Erkennung sinnvollerweise erfolgen?
- Gibt es abgeschottete Bereiche, wo Angriffe von innen (physisch) heraus erfolgen können und wie können diese adäquat überwacht werden?

- Wie können Angriffserkennungssysteme angelernt und konfiguriert werden, um möglichst wenige Fehlalarme (False Positives) zu erzeugen. Betriebsspezifische Situationen müssen Berücksichtigung finden, damit eine Entdeckung (z.B. Veränderung des Programms) bewertet werden kann (in der Situation „Änderung“ oder „Engineering“ -> kein Angriff; im laufenden Betrieb: Angriff).
- 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 Ersatzmaß-nahmen muss dann auf Grundlage einer Risikobetrachtung erfolgen.

## 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 Ausfluss der Organisationsverantwortung der Geschäftsführung eines Betriebs. Die Maßnahmen müssen daher in der Betriebsorganisation wirksam verankert und dokumentiert sein.

Im Folgenden werden organisatorische Anforderung 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 Einschränkungen ergänzt. Wenn die Präzisierung sich nicht direkt auf eine kritische Dienstleistung bezieht, gilt sie für alle kritische Dienstleistungen der Siedlungsabfallentsorgung. Ansonsten sind die referenzierten Anforderungen der DIN EN ISO/IEC 27002:2024 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 Informationssicherheitsrichtlinien

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.1 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.2 Informationssicherheitsrollen und-verantwortlichkeiten

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.2 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.3 Aufgabentrennung

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.3 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

Eine adäquate Aufgabentrennung hat zu erfolgen. Sollten sich widersprechende Aufgaben oder Verantwortungsbereiche nicht sauber trennen lassen, so ist in jedem Fall eine entsprechende Begründung nötig. Zudem werden in diesem Fall eine Risikoabschätzung und ggf. weitere Schutzmaßnamen erforderlich.

## 5.4 Verantwortlichkeiten der Leitung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.4 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.5 Kontakt mit Behörden

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.5 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.6 Kontakt mit speziellen Interessensgruppen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.6 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.7 Erkenntnisse über Bedrohungen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.7 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.8 Informationssicherheit im Projektmanagement

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.8 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.9 Inventar der Informationen und anderen damit verbundenen Werten

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.9 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

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

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 mindestens:

- 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. EE-Anlagen)
- Betriebsdatenerfassungssysteme
- aktive und passive Netzwerkinfrastruktur der OT

## 5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.10 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

Werte im Bereich Sammlung und Beförderung umfassen in der Regel mobile Endgeräte und Apps (. Diese kommen in der Regel auch im öffentlichen Raum zum Einsatz und benötigen daher einen Zugangsbeschränkung.

## 5.11 Rückgabe der Werte

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.11 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.12 Klassifizierung von Information

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.12 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

Informationen im Bereich Sammlung und Beförderung beziehen sich in der Regel auf Tourenplanung und Auftragsverwaltung und müssen entsprechend den Informationssicherheitsanforderungen der Organisation klassifiziert werden

## 5.13 Kennzeichnung von Information

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.13 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.14 Informationsübertragung

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.14 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

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

## 5.15 Zugangssteuerung

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.15 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

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.

## 5.16 Identitätsmanagement

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.16 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

Im Bereich Verwertung und Beseitigung gibt es Komponenten und Protokolle ohne Authentifizierung.

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.

## 5.17 Informationen zur Authentifizierung

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.17 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

Im Bereich Verwertung und Beseitigung gibt es Komponenten und Protokolle ohne Authentifizierung. Hier sind entsprechend der RisikobewertungErsatzmaßnahmen erforderlich.

## 5.18 Zugangsrechte

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.18 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.19 Informationssicherheit in Lieferantenbeziehungen

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.19 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Ergänzung:**

Im Bereich Verwertung und Beseitigung gilt es, sofern keine Alternativen zu Herstellern und Zulieferern von Steuerungs- und Leitsystemen vorhanden sind, Prozesse und Verfahren für die Pflege der

Lieferantenbeziehung sowie für den regelmäßigen Informationsaustausch bzgl. Schwachstellen festzulegen. Das Bereitstellen von Schwachstelleninformationen sollte möglichst vertraglich vereinbart werden.

## 5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.20 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Ergänzung:**

Im Bereich Verwertung und Beseitigung sollten für Zugriffe auf das Leitsystem erhöhte Anforderungen an das durch den Dienstleister eingesetzte Personal gestellt werden z. B. durch zusätzliche Anweisungen und Verpflichtungen zur Einhaltung von Informationssicherheitsmaßnahmen.

## 5.21 Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.21 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

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

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

## 5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.22 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.23 Informationssicherheit für die Nutzung von Cloud-Diensten

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.23 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.24 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.25 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.26 Reaktion auf Informationssicherheitsvorfälle

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.26 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.27 Erkenntnisse aus Informationssicherheitsvorfälle

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.27 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.28 Sammeln von Beweismaterial

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.28 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.29 Informationssicherheit bei Störungen

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.29 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

Für den Bereich Verwertung und Beseitigung 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.

## 5.30 IKT-Bereitschaft für Business Continuity

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.30 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.31 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.32 Geistiges Eigentum

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.32 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.33 Schutz von Aufzeichnungen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.33 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.34 Privatsphäre und Schutz von personenbezogenen Daten (PbD)

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.34 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.35 Unabhängige Überprüfung der Informationssicherheit

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.35 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.36 Einhaltung von Richtlinien, Vorschriften und Normen der Informationssicherheit

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.36 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 5.37 Dokumentierte Bedienabläufe

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 5.37 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

Für den Bereich Verwertung und Beseitigung 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.

Es ist branchenspezifisch nicht üblich, dass IT-Fachpersonal immer verfügbar ist. Dauerhaft besetzte Stellen (bspw. Leitwarten) sind daher zur Durchführung rudimentärer Tätigkeiten zu befähigen.

# 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 beschäftigte 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 Anforderung 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 Einschränkungen ergänzt. Wenn die Präzisierung sich nicht direkt auf eine kritische Dienstleistung bezieht, gilt sie für alle kritische Dienstleistungen der Siedlungsabfallentsorgung. Ansonsten gelten die referenzierten Anforderungen der DIN EN ISO/IEC 27002:2024.

## 6.1 Sicherheitsüberprüfung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 6.1 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 6.2 Beschäftigungs- und Vertragsbedingungen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 6.2 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 6.3 Informationssicherheitsbewusstsein,-ausbildung und-schulung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 6.3 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 6.4 Maßregelungsprozess

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 6.4 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 6.5 Verantwortlichkeiten nach Beendigung oder Änderung der Beschäftigung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 6.5 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 6.6 Vertraulichkeits- und Geheimhaltungsvereinbarungen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 6.6 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 6.7 Telearbeit

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 6.7 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 6.8 Meldung von Informationssicherheitsereignissen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 6.8 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

# 7 Physische Anforderungen

Physische Anforderung dienen zur Ableitung von praktischen nicht-virtuellen Vor-Ort Maßnahmen, die der Sicherung von Hardware und Software am jeweiligen Standort vor Zugriffen oder Zerstörung durch unbefugte Dritte dienen. Geeignete physische Maßnahmen werden im Folgenden dargestellt. Im Folgenden werden physische Anforderung 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 Einschränkungen ergänzt. Wenn die Präzisierung sich nicht direkt auf eine kritische Dienstleistung bezieht, gilt sie für alle kritische Dienstleistungen der Siedlungsabfallentsorgung. Ansonsten gelten die referenzierten Anforderungen der DIN EN ISO/IEC 27002:2024.

## 7.1 Physische Sicherheitsperimeter

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.1 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Ergänzung:**

Für den Bereich Verwertung und Beseitigung gilt es beim Schutz von Bereichen zu berücksichtigen, dass branchenüblich Teile der Betriebsgelände für betriebsfremde Personen zugänglich sind.

## 7.2 Physischer Zutritt

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.2 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 7.3 Sichern von Büros, Räumen und Einrichtungen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.3 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 7.4 Physische Sicherheitsüberwachung

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.4 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Ergänzung:**

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

## 7.5 Schutz vor physischen und umweltbedingten Bedrohungen

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.5 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

Für den Bereich Verwertung und Beseitigung 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.

## 7.6 Arbeiten in Sicherheitsbereichen

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.6 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

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 adäquate Maßnahmen getroffen werden (bspw. Betriebsfremde Personen in solchen Fällen zu Themen der Informationssicherheit unterweisen).

## 7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.7 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 7.8 Platzierung und Schutz von Geräten und Betriebsmitteln

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.8 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

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

## 7.9 Sicherheit von Werten außerhalb der Räumlichkeiten

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.9 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

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, zusätzlichen Maßnahmen zu betrachten.

## 7.10 Speichermedien

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.10 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 7.11 Versorgungseinrichtungen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.11 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 7.12 Sicherheit der Verkabelung

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.12 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

Im Bereich Verwertung und Beseitigung ist es üblich, dass Kabelwege überirdisch verlaufen.

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

- Feuer und Wärme und
- anliefernde Fahrzeuge
- Eingriffe Dritter

geschützt sind.

## 7.13 Instandhaltung von Geräten und Betriebsmitteln

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.13 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

Für den Bereich Sammlung und Beförderung sowie für den Bereich Verwertung und Beseitigung 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 abzuwägen und entsprechende Ersatzmaßnahmen zu treffen (bspw. Ersatzteilbevorratung kritischer Komponenten oder Betrieb außerhalb von herstellerseitigen Betriebsvorgaben).

## 7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 7.14 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

# 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 Einschränkungen ergänzt. Wenn die Präzisierung sich nicht direkt auf eine kritische Dienstleistung bezieht, gilt sie für alle kritische Dienstleistungen der Siedlungsabfallentsorgung. Ansonsten gelten die referenzierten Anforderungen der DIN EN ISO/IEC 27002:2024.

## 8.1 Endpunktgeräte des Benutzers

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.1 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.2 Privilegierte Zugangsrechte

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.2 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Ergänzung:**

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

## 8.3 Informationszugangsbeschränkung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.3 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.4 Zugriff auf den Quellcode

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.4 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.5 Sichere Authentifizierung

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.5 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

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 abzuwägen, entsprechende Ersatzmaßnahmen zu treffen (bspw. physischer Zutrittsschutz) und dieser Aspekt bei folgenden Neuanschaffungen zu berücksichtigen.

## 8.6 Kapazitätssteuerung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.6 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.7 Schutz gegen Schadsoftware

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.7 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

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

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

## 8.8 Handhabung von technischen Schwachstellen

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.8 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

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 abgewogen werden, ob das Einspielen von Patches Auswirkungen auf die Verfügbarkeit haben.

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

## 8.9 Konfigurationsmanagement

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.9 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.10 Löschung von Informationen

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.10 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.11 Datenmaskierung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.11 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.12 Verhinderung von Datenlecks

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.12 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.13 Sicherung von Information

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.13 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.14 Redundanz von informationsverarbeitenden Einrichtungen

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.14 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

Für den Bereich Verwertung und Beseitigung gibt es oft keine Alternativen zu Herstellern und Zulieferern, weshalb eine Redundanz auf diesem Gebiet nicht immer möglich ist. Darüber hinaus kann es aufgrund des Alters der eingesetzten Komponenten sein, dass diese keinen redundanten Aufbau unterstützen.

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

## 8.15 Protokollierung

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.15 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

Für den Bereich Verwertung und Beseitigung ist es branchenspezifisch üblich, dass eingesetzte Systeme und Komponenten bspw. aufgrund der Verwendung proprietärer Kommunikationsprotokolle nicht immer in der Lage sind, Protokolldaten 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 abzuwägen, entsprechende Ersatzmaßnahmen zu treffen und dieser Aspekt bei folgenden Neuanschaffungen zu berücksichtigen.

## 8.16 Überwachung von Aktivitäten

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.16 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.17 Uhrensynchronisation

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.17 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

Eine Uhrensynchronisation ist mandatorisch. Ist eine Uhrensynchronisierung nicht möglich, sind die damit einhergehenden Risiken abzuwägen, 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.

## 8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.18 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

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 abzuwägen, entsprechende Ersatzmaßnahmen zu treffen und dieser Aspekt bei folgenden Neuanschaffungen zu berücksichtigen.

## 8.19 Installation von Software auf Systemen im Betrieb

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.19 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.20 Netzwerksicherheit

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.20 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

Für den Bereich Verwertung und Beseitigung ist es branchenspezifisch aufgrund der Abhängigkeit von Hersteller und Dienstleister nicht immer möglich, alle Netzwerksicherheitsmaßnahmen (bspw. Härtung oder Filterung von Netzwerkverbindungen) zu ergreifen. Darüber hinaus muss der Hersteller /

Dienstleister zwingend in die Pflicht genommen werden, dass z.B. Produktverbesserungen umgesetzt werden. Zudem sollten Alternativmaßnahmen auf Grundlage einer Risiko-betrachtung geprüft werden.

In einem solchen Fall sind die damit einhergehenden Risiken abzuwägen, entsprechende Ersatzmaßnahmen (bspw. Netzwerksegmentierung gemäß Purdue Model inkl. Industrial Demilitarized Zone (IDMZ)) zu treffen und dieser Aspekt bei folgenden Neuanschaffungen zu berücksichtigen. Darüber hinaus muss auf den Hersteller / Dienstleister zwingend eingewirkt werden, dass es „Produktverbesserungen“ gibt.

## 8.21 Sicherheit von Netzwerkdiensten

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.21 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.22 Trennung von Netzwerken

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.22 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

Für den Bereich Verwertung und Beseitigung gilt, dass in einer OT-Umgebung für die IT übliche Anforderungen nicht immer umsetzbar sind. Daher kann eine Trennung von IT und OT mittels DMZ eine sinnvolle Ersatzmaßnahme sein. Die Trennung der Netzwerke kann bspw. nach dem Purdue-Modell erfolgen. Darüber hinaus könnte beispielsweise eine horizontale Segmentierung z.B. nach Verbrennungslinien erfolgen.

## 8.23 Webfilterung

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.23 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgendem Hinweis:**

Für den Bereich Verwertung und Beseitigung entfällt diese Maßnahme, sofern der Zugriff auf Websites bei Komponenten der kritischen Dienstleistung komplett unterbunden wird.

## 8.24 Verwendung von Kryptographie

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.24 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.25 Lebenszyklus einer sicheren Entwicklung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.25 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.26 Anforderungen an die Anwendungssicherheit

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.26 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.27 Sichere Systemarchitektur und technische Grundsätze

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.27 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.28 Sichere Kodierung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.28 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.29 Sicherheitsprüfung in Entwicklung und Abnahme

**Weitere Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.29 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards mit folgender Einschränkung:**

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

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

## 8.30 Ausgegliederte Entwicklung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.30 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.31 Trennung von Entwicklungs-, Prüf- und Produktionsumgebung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.31 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.32 Änderungssteuerung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.32 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.33 Testdaten

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.33 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

## 8.34 Schutz der Informationssysteme während der Überwachungsprüfung

**Keine weiteren Informationen zu DIN EN ISO/IEC 27002:2024 Kap. 8.34 für den Anwendungsbereich dieses Branchenspezifischen Sicherheitsstandards.**

# Anhänge

## A.1 Branchenspezifische Risiken

Die Vorgaben, Ausführungen und Hinweise dieses Branchenspezifischen Sicherheitsstandards basieren auf einer übergeordneten Risikoanalyse der kritischen Dienstleistungen in den Hauptschritten der Branche Siedlungsabfallentsorgung, die in Kap. 3.6 beschrieben werden.

Für jeden Hauptschritt wurde ein sogenanntes „High Consequence Event" – also das schlimmstmöglich anzunehmende Ereignis, welches im Kontext des jeweiligen kDL-Hauptschrittes eintreten könnte, definiert und anhand der in Kap. 3.6 beschriebenen Metrik zur Bestimmung der Auswirkungen eingestuft.

ACHTUNG: Bei der Einstufung der kDL-Hauptschritte 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, dessen High Consequence Event je Kategorie mindestens wie folgt bewertet wurden:

- Verwertung & Beseitigung: hoch
- Sammlung & Beförderung: mittel mit mindestens fünf Bedrohungen/ Schwachstellen

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

## A.1.1 Sammlung & Beförderung

### A.1.1.1 High Consequence Events Sammlung & Beförderung

| kDL Hauptschritt | High Consequence Events (HCE) | Einstufung HCE |
|---|---|---|
| **statische Tourenplanung** | Aufgrund der Laufzeit der statischen Tourenplanung von in der Regel ein bis zwei Jahren führt ein Ausfall der Tourenplanung in der Regel zu Effizienzverlusten. | Vernachlässigbar |
| **dynamische Tourenplanung/ Auftragsverwaltung** | Bei Ausfall oder Manipulation der Auftragsverwaltung wird die dynamische Tourenplanung gestört und erheblich verzögert. | Begrenzt |
| **Personalplanung** | Die Personalplanung dient als Rahmen für die Besetzung der Fahrzeuge. Die detaillierte Planung erfolgt dann tagesaktuell aufgrund der Anwesenheit des Personals.<br><br>Die Personalplanung kann auch eine Zuordnung von Kompetenzen enthalten (bspw. wer berechtigt ist, bestimmte Fahrzeuge zu führen).<br><br>Im schlimmsten Fall ist nicht genug Personal da, um alle Touren fahren zu können. Zur Abmilderung der HCE-Auswirkung kann auf externes Personal zurückgegriffen werden oder der Abfall am nächsten Werktag bzw. durch andere Fahrzeuge abgeholt werden. | Begrenzt |
| **Fahrzeugdisposition inkl. Fahrzeugwartung** | Ein Fehler bei den verwalteten Wartungsintervallen kann dazu führen, dass Fahrzeuge nicht im optimalen / angemessenen Zustand sind. Das hat aber nicht zwangsläufig zur Folge, dass eine signifikante Anzahl von Fahrzeugen nicht gleichzeitig zur Verfügung stehen. Da sich die anstehenden Wartungsintervalle über das Jahr und die Fahrzeuge verteilt ist ein großflächiger Ausfall des gesamten Fuhrparks unwahrscheinlich.<br>Zur Abmilderung der HCE-Auswirkung können Touren von ausgefallenen Fahrzeugen in der Regel aufgefangen werden. | Vernachlässigbar |
| **Sammlung und Beförderung** | Der Ausfall von Telematiksystemen (digitale Tourenlisten, digitale Leistungsscheine) bei statischen Touren ist in der Regel nicht kritisch, da das Wissen über die Touren weit verbreitet ist.<br><br>Bei dynamischen Touren kann es zur Nichterbringung von geplanten Sammelleistungen führen. | Begrenzt |

| | | |
|---|---|---|
| **Lagerung, Zwischenlagerung und Umladung von Abfällen** | Der Ausfall der Planung ist unkritisch. Denn die Lagerungs- und Umladungskapazitäten sind in der Regel nicht knapp und es besteht auch manuell ein guter Überblick über die vorhandenen Kapazitäten | Vernachlässigbar |

### A.1.1.2 Funktionen Sammlung & Beförderung (Versagen)

| kDL Hauptschritt | Technische Funktion | Kann ein Versagen zum HCE führen?[9] | Welche Bedrohungen und Schwachstellen können zum Versagen der Funktion führen? |
|---|---|---|---|
| **statische Tourenplanung** | Tourenplanungssoftware | Ja, ein Versagen der Tourenplanungssoftware kann zum Ausfall der Tourenplanung führen. Aufgrund der langen Laufzeiten der Tourenpläne bei der statischen Tourenplanung kann dies manuell durch vorhandene Papieraufzeichnung und durch das Erfahrungswissen der Mitarbeitenden ausgeglichen werden. | G 0.8 Ausfall oder Störung der Stromversorgung<br>G 0.9 Ausfall oder Störung von Kommunikationsnetzen<br>G 0.11 Ausfall oder Störung von Dienstleistern<br>G 0.12 Elektromagnetische Störstrahlung<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.24 Zerstörung von Geräten oder Datenträgern<br>G 0.25 Ausfall von Geräten oder Systemen<br>G 0.26 Fehlfunktion von Geräten oder Systemen<br>G 0.39 Schadprogramme<br>G 0.40 Verhinderung von Diensten (Denial of Service)<br>G 0.45 Datenverlust<br>G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe<br>BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)<br>BSI-ICSK.23 Schadprogramme |
| **dynamische Tourenplanung/ Auftragsverwaltung** | Tourenplanungssoftware | Ja, ein Versagen der Tourenplanungssoftware kann durch manuelle Prozesse (bspw. papierbasierte Planung) weniger effektiv abgefangen werden. | G 0.8 Ausfall oder Störung der Stromversorgung<br>G 0.9 Ausfall oder Störung von Kommunikationsnetzen<br>G 0.11 Ausfall oder Störung von Dienstleistern<br>G 0.12 Elektromagnetische Störstrahlung<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.24 Zerstörung von Geräten oder Datenträgern |

[9] Bezogen auf die Einstufung aus A.1.1.1 High Consequence Events Sammlung & Beförderung

| kDL Hauptschritt | Technische Funktion | Kann ein Versagen zum HCE führen?[9] | Welche Bedrohungen und Schwachstellen können zum Versagen der Funktion führen? |
|---|---|---|---|
| | | | G 0.25 Ausfall von Geräten oder Systemen<br>G 0.26 Fehlfunktion von Geräten oder Systemen<br>G 0.39 Schadprogramme<br>G 0.40 Verhinderung von Diensten (Denial of Service)<br>G 0.45 Datenverlust<br>G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe<br>BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)<br>BSI-ICSK.23 Schadprogramme |
| | Auftragsverwaltung | Ja, ein Versagen der Auftragsverwaltung kann zum HCE führen (Tourenplanung bzw. Abholung verzögert) | G 0.8 Ausfall oder Störung der Stromversorgung<br>G 0.9 Ausfall oder Störung von Kommunikationsnetzen<br>G 0.11 Ausfall oder Störung von Dienstleistern<br>G 0.12 Elektromagnetische Störstrahlung<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.24 Zerstörung von Geräten oder Datenträgern<br>G 0.25 Ausfall von Geräten oder Systemen<br>G 0.26 Fehlfunktion von Geräten oder Systemen<br>G 0.39 Schadprogramme<br>G 0.40 Verhinderung von Diensten (Denial of Service)<br>G 0.45 Datenverlust<br>G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe<br>BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)<br>BSI-ICSK.23 Schadprogramme |
| **Personalplanung** | Personalplanungssoftware | Nein, ein Versagen der Planungssoftware führt nicht zwangsweise dazu, dass Touren ausfallen müssen. Personal wird in Gruppen auf bestimmte Touren fest zugeteilt. | G 0.8 Ausfall oder Störung der Stromversorgung<br>G 0.9 Ausfall oder Störung von Kommunikationsnetzen<br>G 0.11 Ausfall oder Störung von Dienstleistern<br>G 0.12 Elektromagnetische Störstrahlung<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.24 Zerstörung von Geräten oder Datenträgern<br>G 0.25 Ausfall von Geräten oder Systemen |

| kDL Hauptschritt | Technische Funktion | Kann ein Versagen zum HCE führen?[9] | Welche Bedrohungen und Schwachstellen können zum Versagen der Funktion führen? |
|---|---|---|---|
| | | | G 0.26 Fehlfunktion von Geräten oder Systemen<br>G 0.39 Schadprogramme<br>G 0.40 Verhinderung von Diensten (Denial of Service)<br>G 0.45 Datenverlust<br>G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe<br>BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)<br>BSI-ICSK.23 Schadprogramme |
| **Fahrzeugdisposition inkl. Fahrzeugwartung** | Dispositions- und Wartungssoftware | Nein, ein Versagen der Software führt nicht zwangsweise dazu, dass Touren ausfallen müssen. Fahrzeuge werden fest zugeteilt. | G 0.8 Ausfall oder Störung der Stromversorgung<br>G 0.9 Ausfall oder Störung von Kommunikationsnetzen<br>G 0.11 Ausfall oder Störung von Dienstleistern<br>G 0.12 Elektromagnetische Störstrahlung<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.24 Zerstörung von Geräten oder Datenträgern<br>G 0.25 Ausfall von Geräten oder Systemen<br>G 0.26 Fehlfunktion von Geräten oder Systemen<br>G 0.39 Schadprogramme<br>G 0.40 Verhinderung von Diensten (Denial of Service)<br>G 0.45 Datenverlust<br>G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe<br>BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)<br>BSI-ICSK.23 Schadprogramme |
| **Sammlung und Beförderung** | Das Telematiksystem stellt dem Fahrpersonal Informationen über Abfallstelle, Abfallart, Behältertyp, Entsorgungsanlage und Reihenfolge anhand der Auftragsdaten aus den Tourenplanungen für die | Ja, bei Ausfall des Telematiksystems liegen dem Fahrpersonal keine Informationen über die zu erbringenden/geplanten Sammelleistungen vor. Dies kann zur Nichterbringung von geplanten Sammelleistungen führen. | G 0.8 Ausfall oder Störung der Stromversorgung<br>G 0.9 Ausfall oder Störung von Kommunikationsnetzen<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.24 Zerstörung von Geräten oder Datenträgern<br>G 0.25 Ausfall von Geräten oder Systemen<br>G 0.26 Fehlfunktion von Geräten oder Systemen<br>G 0.28 Software-Schwachstellen oder -Fehler |

| kDL Hauptschritt | Technische Funktion | Kann ein Versagen zum HCE führen?[9] | Welche Bedrohungen und Schwachstellen können zum Versagen der Funktion führen? |
|---|---|---|---|
| | Sammlung und Beförderung zur Verfügung. | | G 0.39 Schadprogramme<br>G 0.40 Verhinderung von Diensten (Denial of Service)<br>G 0.45 Datenverlust<br>G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe<br>BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)<br>BSI-ICSK.23 Schadprogramme |
| **Lagerung, Zwischenlagerung und Umladung von Abfällen** | Geringe bis keine Systemunterstützung. | n/A | n/A |

### A.1.1.3 Funktionen Sammlung & Beförderung (Manipulation)

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[10] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| **statische Tourenplanung** | Tourenplanungssoftware | Ja, eine Manipulation der statischen Tourenplanung kann zu zeitweisen Verzögerungen und Ineffizienzen bei der Abholung führen. Allerdings würde eine solche relativ schnell auffallen, da die Touren längerfristig Bestand haben und dadurch das eingesetzte Personal über entsprechendes Erfahrungswissen verfügt. | G 0.14 Ausspähen von Informationen (Spionage)<br>G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten<br>G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten<br>G 0.18 Fehlplanung oder fehlende Anpassung<br>G 0.19 Offenlegung schützenswerter Informationen<br>G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen<br>G 0.31 Fehlerhafte Nutzung oder Administration von |

[10] Bezogen auf die Einstufung aus A.1.1.1 High Consequence Events Sammlung & Beförderung

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[10] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | Geräten und Systemen<br>G 0.32 Missbrauch von Berechtigungen<br>G 0.35 Nötigung, Erpressung oder Korruption<br>G 0.36 Identitätsdiebstahl<br>G 0.39 Schadprogramme<br>G 0.42 Social Engineering<br>G 0.43 Einspielen von Nachrichten<br>G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen<br>BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.07 Mangelnde Awareness<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen<br>BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk<br>BSI-ICSK.17 Man-in-the-Middle-Angriff<br>BSI-ICSK.18 Phishing<br>BSI-ICSK.19 Injection-Angriffe<br>BSI-ICSK.20 Cross-Site-Scripting<br>BSI-ICSK.23 Schadprogramme |
| **dynamische Tourenplanung/ Auftragsverwaltung** | Tourenplanungssoftware | Ja, eine Manipulation der dynamischen Tourenplanung kann zur Nichterbringung von geplanten Sammelleistungen bzw. zur Erbringung von nicht geplanten/unnötigen | G 0.14 Ausspähen von Informationen (Spionage)<br>G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten<br>G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten<br>G 0.18 Fehlplanung oder fehlende Anpassung |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[10] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | Sammelleistungen führen. Die zu Erbringung von nicht geplanten bzw. unnötigen Sammelleistungen aufgebrachten Ressourcen stehen dann den geplanten Sammelleistungen nicht mehr zur Verfügung. | G 0.19 Offenlegung schützenswerter Informationen<br>G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen<br>G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen<br>G 0.32 Missbrauch von Berechtigungen<br>G 0.35 Nötigung, Erpressung oder Korruption<br>G 0.36 Identitätsdiebstahl<br>G 0.39 Schadprogramme<br>G 0.42 Social Engineering<br>G 0.43 Einspielen von Nachrichten<br>G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen<br>BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.07 Mangelnde Awareness<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen<br>BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk<br>BSI-ICSK.17 Man-in-the-Middle-Angriff |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[10] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | BSI-ICSK.18 Phishing<br>BSI-ICSK.19 Injection-Angriffe<br>BSI-ICSK.20 Cross-Site-Scripting<br>BSI-ICSK.23 Schadprogramme |
| | Auftragsverwaltung | Ja, eine Manipulation der Auftragsverwaltung kann 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. | G 0.14 Ausspähen von Informationen (Spionage)<br>G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten<br>G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten<br>G 0.18 Fehlplanung oder fehlende Anpassung<br>G 0.19 Offenlegung schützenswerter Informationen<br>G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen<br>G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen<br>G 0.32 Missbrauch von Berechtigungen<br>G 0.35 Nötigung, Erpressung oder Korruption<br>G 0.36 Identitätsdiebstahl<br>G 0.39 Schadprogramme<br>G 0.42 Social Engineering<br>G 0.43 Einspielen von Nachrichten<br>G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[10] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.07 Mangelnde Awareness<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen<br>BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk<br>BSI-ICSK.17 Man-in-the-Middle-Angriff<br>BSI-ICSK.18 Phishing<br>BSI-ICSK.19 Injection-Angriffe<br>BSI-ICSK.20 Cross-Site-Scripting<br>BSI-ICSK.23 Schadprogramme |
| **Personalplanung** | Personalplanungssoftware | Nein, eine Manipulation der Personalplanungssoftware führt in der Regel nur zu Verzögerungen, aber nicht dazu, dass Touren ausfallen müssen. | G 0.14 Ausspähen von Informationen (Spionage)<br>G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten<br>G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten<br>G 0.18 Fehlplanung oder fehlende Anpassung<br>G 0.19 Offenlegung schützenswerter Informationen<br>G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen<br>G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[10] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | G 0.32 Missbrauch von Berechtigungen<br>G 0.35 Nötigung, Erpressung oder Korruption<br>G 0.36 Identitätsdiebstahl<br>G 0.38 Missbrauch personenbezogener Daten<br>G 0.39 Schadprogramme<br>G 0.42 Social Engineering<br>G 0.43 Einspielen von Nachrichten<br>G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen<br>BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.07 Mangelnde Awareness<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen<br>BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk<br>BSI-ICSK.17 Man-in-the-Middle-Angriff<br>BSI-ICSK.18 Phishing<br>BSI-ICSK.19 Injection-Angriffe<br>BSI-ICSK.20 Cross-Site-Scripting<br>BSI-ICSK.23 Schadprogramme |
| **Fahrzeugdisposition inkl. Fahrzeugwartung** | Dispositions- und Wartungssoftware | Ja, eine Manipulation der Fahrzeugdisposition bzw. Wartungssoftware kann zum HCE führen. | G 0.14 Ausspähen von Informationen (Spionage)<br>G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten<br>G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten<br>G 0.18 Fehlplanung oder fehlende Anpassung |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[10] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | G 0.19 Offenlegung schützenswerter Informationen<br>G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen<br>G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen<br>G 0.32 Missbrauch von Berechtigungen<br>G 0.35 Nötigung, Erpressung oder Korruption<br>G 0.36 Identitätsdiebstahl<br>G 0.39 Schadprogramme<br>G 0.42 Social Engineering<br>G 0.43 Einspielen von Nachrichten<br>G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen<br>BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.07 Mangelnde Awareness<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[10] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk<br>BSI-ICSK.17 Man-in-the-Middle-Angriff<br>BSI-ICSK.18 Phishing<br>BSI-ICSK.19 Injection-Angriffe<br>BSI-ICSK.20 Cross-Site-Scripting<br>BSI-ICSK.23 Schadprogramme |
| **Sammlung und Beförderung** | Das Telematiksystem stellt dem Fahrpersonal Informationen über Abfallstelle, Abfallart, Behältertyp, Entsorgungsanlage und Reihenfolge anhand der Auftragsdaten aus den Tourenplanungen für die Sammlung und Beförderung zur Verfügung. | Ja, eine Manipulation der Auftragsdaten von Telematiksysteme kann 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. | G 0.14 Ausspähen von Informationen (Spionage)<br>G 0.18 Fehlplanung oder fehlende Anpassung<br>G 0.19 Offenlegung schützenswerter Informationen<br>G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen<br>G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen<br>G 0.32 Missbrauch von Berechtigungen<br>G 0.35 Nötigung, Erpressung oder Korruption<br>G 0.36 Identitätsdiebstahl<br>G 0.39 Schadprogramme<br>G 0.42 Social Engineering<br>G 0.43 Einspielen von Nachrichten<br>G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen<br>BSI-ICSK.05 Fehlende Überwachung der |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[10] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | unterstützenden Infrastruktur<br>BSI-ICSK.07 Mangelnde Awareness<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen<br>BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk<br>BSI-ICSK.17 Man-in-the-Middle-Angriff<br>BSI-ICSK.18 Phishing<br>BSI-ICSK.19 Injection-Angriffe<br>BSI-ICSK.20 Cross-Site-Scripting<br>BSI-ICSK.23 Schadprogramme |
| **Lagerung, Zwischenlagerung und Umladung von Abfällen** | Geringe bis keine Systemunterstützung. | n/A | n/A |

## A.1.2 Verwertung & Beseitigung

### A.1.2.1 High Conequence Events Verwertung & Beseitigung

| kDL Hauptschritt | High Consequence Events (HCE) | Einstufung HCE |
|---|---|---|
| **Abfallmengenerfassung an der Annahme** | Fehler oder Ausbleiben der IT-gestützten Mengenerfassung haben in der Regel keine Auswirkungen auf die kDL. Wenn die LKW-Schlange zu lange wird, wird auf autarken Waagebetrieb gewechselt. | Vernachlässigbar |
| **Abfallvorbehandlung (u.U. mit Vorsortierung)** | Kleinere Anlagenschäden könnten unter Umständen durch nicht herausgefilterte Störstoffe entstehen.<br><br>Auswirkungen auf die Verfügbarkeit der kDL sind eher nicht realistisch. | Vernachlässigbar |
| **Lager-/ Bunkermanagement** | Im schlimmsten Fall kann kein Material mehr der Verarbeitung (bspw. Brennstoff der Verbrennung) zugeführt werden. Der Kessel geht nach einigen Stunden aus und der Bunker füllt sich.<br>Das kann bspw. hervorgerufen werden durch:<br>• Die Umweltkonditionen im Arbeitsbereich des Kranbedieners sind nicht mehr angemessen für Menschen (bspw. durch den Ausfall der Gebäudeleittechnik und keine andere Möglichkeit der Belüftung ist gegeben).<br>• Ein Bedienen der Krananlage ist nicht mehr möglich (bspw. durch den Ausfall der Kransteuerung/ Kranautomatisierung)<br>• Ein Bedienen der Krananlage ist nur noch eingeschränkt möglich (bspw. durch Ausfall der Visualisierung).<br>• Ein großer Brand im Bereich des Müllbunkers verhindert die Mengenzuführung zur Verbrennung | Begrenzt |
| **Verbrennung / Sortierung/ Behandlung** | Beschädigung oder Stillstand der Anlage bspw. durch Manipulation oder Fehlfunktion der Steuerung oder Visualisierung (Leittechnik) | Beträchtlich |
| **Rauchgasreinigung** | Ausfall der Rauchgasreinigung führt dazu, dass die Anlage nicht weiter betrieben werden kann, weil z. B. beim Umfahren (Bypässe) der Rauchgasreinigung nachgelagerte Anlagenkomponenten Schaden durch die hohe Temperatur nehmen können. | Beträchtlich |

A.1.2.2 Funktionen Verwertung & Beseitigung (Versagen)

| kDL Hauptschritt | Technische Funktion | Kann ein Versagen zum HCE führen?[11] | Welche Bedrohungen und Schwachstellen können zum Versagen der Funktion führen? |
|---|---|---|---|
| **Abfallmengenerfassung an der Annahme** | Fahrzeugverwiegung | 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. | G 0.8 Ausfall oder Störung der Stromversorgung<br>G 0.9 Ausfall oder Störung von Kommunikationsnetzen<br>G 0.12 Elektromagnetische Störstrahlung<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.24 Zerstörung von Geräten oder Datenträgern<br>G 0.25 Ausfall von Geräten oder Systemen<br>G 0.26 Fehlfunktion von Geräten oder Systemen<br>G 0.34 Anschlag<br>G 0.39 Schadprogramme<br>G 0.41 Sabotage<br>G 0.44 Unbefugtes Eindringen in Räumlichkeiten<br>G 0.45 Datenverlust<br>G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe<br>BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten<br>BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)<br>BSI-ICSK.23 Schadprogramme |

[11] Bezogen auf die Einstufung aus A.1.2.1 High Conequence Events Verwertung & Beseitigung

| kDL Hauptschritt | Technische Funktion | Kann ein Versagen zum HCE führen?[11] | Welche Bedrohungen und Schwachstellen können zum Versagen der Funktion führen? |
|---|---|---|---|
| | | | |
| **Abfallvorbehandlung (u.U. mit Vorsortierung)** | Bedienen und Beobachten der Anlage im Leitsystem | Nein, wenn ein Bedienen und Beobachten des Leitsystems für die Abfallvorbehandlung nicht möglich ist, kann üblicherweise trotzdem der kDL Schritt Verbrennung / Sortierung/ Behandlung durchgeführt werden. Somit hat das Versagen in der Regel keine Auswirkungen im Sinne des HCE. | G 0.1 Feuer<br>G 0.2 Ungünstige klimatische Bedingungen<br>G 0.3 Wasser<br>G 0.4 Verschmutzung, Staub, Korrosion<br>G 0.5 Naturkatastrophen<br>G 0.8 Ausfall oder Störung der Stromversorgung<br>G 0.9 Ausfall oder Störung von Kommunikationsnetzen<br>G 0.11 Ausfall oder Störung von Dienstleistern<br>G 0.12 Elektromagnetische Störstrahlung<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.24 Zerstörung von Geräten oder Datenträgern<br>G 0.25 Ausfall von Geräten oder Systemen<br>G 0.26 Fehlfunktion von Geräten oder Systemen<br>G 0.34 Anschlag<br>G 0.39 Schadprogramme<br>G 0.40 Verhinderung von Diensten (Denial of Service)<br>G 0.41 Sabotage<br>G 0.44 Unbefugtes Eindringen in Räumlichkeiten<br>G 0.45 Datenverlust<br>G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe<br>BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung |

| kDL Hauptschritt | Technische Funktion | Kann ein Versagen zum HCE führen?[11] | Welche Bedrohungen und Schwachstellen können zum Versagen der Funktion führen? |
|---|---|---|---|
| | | | BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten<br>BSI-ICSK.10 Fehlende Backups<br>BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben<br>BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)<br>BSI-ICSK.22 Schadsoftware auf EWS<br>BSI-ICSK.23 Schadprogramme |
| **Lager-/ Bunkermanagement** | (1) Die Gebäudeleittechnik (GLT) ist für die Steuerung und Regelung der Kälte-/Klimatechnik zuständig.<br><br>(2) Die Kransteuerung und Automatisierung ist für die Ansteuerung und Überwachung des Kranprozesses zuständig.<br><br>(3) Die Kranvisualisierung ist für die Darstellung der Kranmeldungen, der Kranposition und für das Konfigurieren des Vollautomatikbetriebs zuständig. | (1) Nein, der Ausfall der Gebäudeleittechnik führt nicht zwangsläufig zum HCE, außer durch nicht gegebene natürliche Belüftung z.B. durch Fenster in der Krankanzel.<br><br>(2) Ja, der Ausfall der Kransteuerung und Automatisierung führt zum HCE.<br><br>(3) Ja, der Ausfall der Kranvisualisierung führt zum HCE, wenn keine lokale Bedienung des Krans mehr gegeben ist. | G 0.1 Feuer<br>G 0.2 Ungünstige klimatische Bedingungen<br>G 0.3 Wasser<br>G 0.4 Verschmutzung, Staub, Korrosion<br>G 0.5 Naturkatastrophen<br>G 0.8 Ausfall oder Störung der Stromversorgung<br>G 0.9 Ausfall oder Störung von Kommunikationsnetzen<br>G 0.11 Ausfall oder Störung von Dienstleistern<br>G 0.12 Elektromagnetische Störstrahlung<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.24 Zerstörung von Geräten oder Datenträgern<br>G 0.25 Ausfall von Geräten oder Systemen<br>G 0.26 Fehlfunktion von Geräten oder Systemen<br>G 0.34 Anschlag<br>G 0.39 Schadprogramme<br>G 0.40 Verhinderung von Diensten (Denial of Service)<br>G 0.41 Sabotage<br>G 0.44 Unbefugtes Eindringen in Räumlichkeiten<br>G 0.45 Datenverlust<br>G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe |

| kDL Hauptschritt | Technische Funktion | Kann ein Versagen zum HCE führen?[11] | Welche Bedrohungen und Schwachstellen können zum Versagen der Funktion führen? |
|---|---|---|---|
| | | | BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten<br>BSI-ICSK.10 Fehlende Backups<br>BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben<br>BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)<br>BSI-ICSK.22 Schadsoftware auf EWS<br>BSI-ICSK.23 Schadprogramme |
| **Verbrennung / Sortierung/ Behandlung** | (1) Bedienen und Beobachten der Anlage im Leitsystem (**Verbrennung**: Steuerung und Regelung der Verbrennung über Speicherprogrammierbare Steuerungen (SPS) und/oder das Bedien- und Beobachtungssystem vom Leitstandsfahrer<br><br>(2) **Sortierung:** Trennung von Metallen; Wegblasen von Papier; Kamera- und Sensoren zum Sortieren;<br><br>(3) **Behandlung:** Mechanisch-Biologische-Aufbereitung, | (1) Ja, sofern die Überwachung des Anlagenprozesses nicht mehr möglich ist, können keine Anpassungsmaßnahmen durchgeführt werden, was zur Beschädigung der Anlage führen kann.<br><br>(2) Nein, Ausfall der Sortierung führt üblicherweise dazu, dass Verbrennungskapazitäten schneller erreicht werden.<br><br>(3) Ja, Qualität der behandelten Stoffe könnte negativ | G 0.1 Feuer<br>G 0.2 Ungünstige klimatische Bedingungen<br>G 0.3 Wasser<br>G 0.4 Verschmutzung, Staub, Korrosion<br>G 0.5 Naturkatastrophen<br>G 0.8 Ausfall oder Störung der Stromversorgung<br>G 0.9 Ausfall oder Störung von Kommunikationsnetzen<br>G 0.11 Ausfall oder Störung von Dienstleistern<br>G 0.12 Elektromagnetische Störstrahlung<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.24 Zerstörung von Geräten oder Datenträgern<br>G 0.25 Ausfall von Geräten oder Systemen<br>G 0.26 Fehlfunktion von Geräten oder Systemen<br>G 0.34 Anschlag<br>G 0.39 Schadprogramme<br>G 0.40 Verhinderung von Diensten (Denial of Service)<br>G 0.41 Sabotage |

| kDL Hauptschritt | Technische Funktion | Kann ein Versagen zum HCE führen?[11] | Welche Bedrohungen und Schwachstellen können zum Versagen der Funktion führen? |
|---|---|---|---|
| | Sensorik bzgl. Selbstentzündung) | beeinflusst werden (nicht KRITIS-relevant). Lagerkapazitäten würden schneller erreicht. Ausfälle der Sensorik bzgl. Selbstentzündung können zu Bränden führen. | G 0.44 Unbefugtes Eindringen in Räumlichkeiten<br>G 0.45 Datenverlust<br>G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe<br>BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten<br>BSI-ICSK.10 Fehlende Backups<br>BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben<br>BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)<br>BSI-ICSK.22 Schadsoftware auf EWS<br>BSI-ICSK.23 Schadprogramme |
| **Rauchgasreinigung** | 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)). | Ja, die Rauchgasreinigung kann aufgrund eines Ausfalls des Prozessleitsystems versagen, was zu einem Ausfall der Anlage führen kann. | G 0.2 Ungünstige klimatische Bedingungen<br>G 0.4 Verschmutzung, Staub, Korrosion<br>G 0.8 Ausfall oder Störung der Stromversorgung<br>G 0.9 Ausfall oder Störung von Kommunikationsnetzen<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.24 Zerstörung von Geräten oder Datenträgern<br>G 0.25 Ausfall von Geräten oder Systemen<br>G 0.26 Fehlfunktion von Geräten oder Systemen<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.39 Schadprogramme<br>G 0.40 Verhinderung von Diensten (Denial of Service) |

| kDL Hauptschritt | Technische Funktion | Kann ein Versagen zum HCE führen?[11] | Welche Bedrohungen und Schwachstellen können zum Versagen der Funktion führen? |
|---|---|---|---|
| | | | G 0.45 Datenverlust<br>G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge<br>BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen<br>BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten<br>BSI-ICSK.10 Fehlende Backups<br>BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten<br>BSI-ICSK.16 Denial-of-Service-Angriffe (DoS)<br>BSI-ICSK.23 Schadprogramme<br>BSI-ICSK.24 Replay-Angriff |

### A.1.2.3 Funktionen Verwertung & Beseitigung (Manipulation)

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[12] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| **Abfallmengenerfassung an der Annahme** | Fahrzeugverwiegung mit lokaler Anbindung oder Anbindung an ERP-Systeme | Nein, falsche Werte bei der Verwiegung führen in der Regel lediglich zu falscher Abrechnung. | G 0.14 Ausspähen von Informationen (Spionage)<br>G 0.18 Fehlplanung oder fehlende Anpassung<br>G 0.19 Offenlegung schützenswerter Informationen<br>G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle<br>G 0.21 Manipulation von Hard- oder Software |

[12] Bezogen auf die Einstufung aus A.1.2.1 High Conequence Events Verwertung & Beseitigung

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[12] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen<br>G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen<br>G 0.32 Missbrauch von Berechtigungen<br>G 0.35 Nötigung, Erpressung oder Korruption<br>G 0.36 Identitätsdiebstahl<br>G 0.39 Schadprogramme<br>G 0.42 Social Engineering<br>G 0.43 Einspielen von Nachrichten<br>G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen<br>BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten<br>BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben<br>BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[12] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | |
| **Abfallvorbehandlung (u.U. mit Vorsortierung)** | Bedienen und Beobachten der Anlage im Leitsystem | Nein, eine Manipulation kann in der Regel nicht zu einem HCE führen. | G 0.14 Ausspähen von Informationen (Spionage)<br>G 0.18 Fehlplanung oder fehlende Anpassung<br>G 0.19 Offenlegung schützenswerter Informationen<br>G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen<br>G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen<br>G 0.32 Missbrauch von Berechtigungen<br>G 0.35 Nötigung, Erpressung oder Korruption<br>G 0.36 Identitätsdiebstahl<br>G 0.39 Schadprogramme<br>G 0.42 Social Engineering<br>G 0.43 Einspielen von Nachrichten<br>G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen<br>BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen<br>BSI-ICSK.08 Unzureichende Absicherung oder zu |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[12] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | weitreichende Vernetzung<br>BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten<br>BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben<br>BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten<br>BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen<br>BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk<br>BSI-ICSK.17 Man-in-the-Middle-Angriff<br>BSI-ICSK.18 Phishing<br>BSI-ICSK.19 Injection-Angriffe<br>BSI-ICSK.20 Cross-Site-Scripting<br>BSI-ICSK.23 Schadprogramme |
| **Lager-/ Bunkermanagement** | (1) Die Gebäudeleittechnik (GLT) ist für die Steuerung und Regelung der Kälte-/Klimatechnik zuständig.<br><br>(2) Die Kransteuerung und Automatisierung ist für die Ansteuerung und Überwachung des Kranprozesses zuständig.<br><br>(3) Die Kranvisualisierung ist für die Darstellung der | (1) Ja, eine Manipulation der Gebäudeleittechnik kann dazu führen, dass gesundheitsschädliche Umweltkonditionen herbeigeführt werden können.<br><br>(2) Ja, eine Beschädigung des Krans durch absichtliche Fehlbedienung kann zu schweren Schäden an der Anlage führen.<br><br>(3) Ja, eine Manipulation der Visualisierung bei | G 0.14 Ausspähen von Informationen (Spionage)<br>G 0.18 Fehlplanung oder fehlende Anpassung<br>G 0.19 Offenlegung schützenswerter Informationen<br>G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen<br>G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen<br>G 0.32 Missbrauch von Berechtigungen<br>G 0.35 Nötigung, Erpressung oder Korruption |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[12] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | Kranmeldungen, der Kranposition und für das Konfigurieren des Vollautomatikbetriebs zuständig. | Vollautomatikbetrieb kann zum HCE führen. | G 0.36 Identitätsdiebstahl<br>G 0.39 Schadprogramme<br>G 0.42 Social Engineering<br>G 0.43 Einspielen von Nachrichten<br>G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen<br>BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten<br>BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben<br>BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten<br>BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen<br>BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk<br>BSI-ICSK.17 Man-in-the-Middle-Angriff<br>BSI-ICSK.18 Phishing<br>BSI-ICSK.19 Injection-Angriffe<br>BSI-ICSK.20 Cross-Site-Scripting<br>BSI-ICSK.23 Schadprogramme |
| **Verbrennung / Sortierung/ Behandlung** | (1) Bedienen und Beobachten der Anlage | (1) Ja, eine Manipulation der Steuerung und Regelung der | G 0.14 Ausspähen von Informationen (Spionage)<br>G 0.18 Fehlplanung oder fehlende Anpassung |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[12] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | im Leitsystem (**Verbrennung**: Steuerung und Regelung der Verbrennung über Speicherprogrammierbare Steuerungen (SPS) und/oder das Bedien- und Beobachtungssystem vom Leitstandsfahrer<br><br>(2) **Sortierung:** Trennung von Metallen; Wegblasen von Papier; Kamera- und Sensoren zum Sortieren;<br><br>(3) **Behandlung:** Mechanisch-Biologische-Aufbereitung, Sensorik bzgl. Temperaturüberwachung | Verbrennung kann zu einer Beschädigung der Anlage führen.<br><br>(2) Nein, eine Manipulation der Sortierung führt in der Regel lediglich dazu, dass Verbrennungskapazitäten schneller erreicht werden.<br><br>(3) 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 0.19 Offenlegung schützenswerter Informationen<br>G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen<br>G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen<br>G 0.32 Missbrauch von Berechtigungen<br>G 0.35 Nötigung, Erpressung oder Korruption<br>G 0.36 Identitätsdiebstahl<br>G 0.39 Schadprogramme<br>G 0.42 Social Engineering<br>G 0.43 Einspielen von Nachrichten<br>G 0.46 Integritätsverlust schützenswerter Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen<br>BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten<br>BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[12] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten<br>BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen<br>BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk<br>BSI-ICSK.17 Man-in-the-Middle-Angriff<br>BSI-ICSK.18 Phishing<br>BSI-ICSK.19 Injection-Angriffe<br>BSI-ICSK.20 Cross-Site-Scripting<br>BSI-ICSK.23 Schadprogramme |
| **Rauchgasreinigung** | 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)). | 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.<br>Bei Überschreitung von Grenzwerten darf die Anlage nicht weiter betrieben werden (nur auf Anweisung der zuständigen Behörde).<br>Bei Beschädigung der Anlage ist diese ggf. außer Betrieb zu nehmen, um Instandhaltungs-maßnahmen durchzuführen. | G 0.14 Ausspähen von Informationen (Spionage)<br>G 0.18 Fehlplanung oder fehlende Anpassung<br>G 0.19 Offenlegung schützenswerter Informationen<br>G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle<br>G 0.21 Manipulation von Hard- oder Software<br>G 0.22 Manipulation von Informationen<br>G 0.23 Unbefugtes Eindringen in IT-Systeme<br>G 0.28 Software-Schwachstellen oder -Fehler<br>G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen<br>G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen<br>G 0.32 Missbrauch von Berechtigungen<br>G 0.35 Nötigung, Erpressung oder Korruption<br>G 0.36 Identitätsdiebstahl<br>G 0.39 Schadprogramme<br>G 0.42 Social Engineering<br>G 0.43 Einspielen von Nachrichten<br>G 0.46 Integritätsverlust schützenswerter |

| kDL Hauptschritt | Technische Funktion | Kann eine Manipulation zum HCE führen?[12] | Welche Bedrohungen und Schwachstellen können zur Manipulation der Funktion führen? |
|---|---|---|---|
| | | | Informationen<br>BSI-ICSK.04 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen<br>BSI-ICSK.05 Fehlende Überwachung der unterstützenden Infrastruktur<br>BSI-ICSK.06 Abhängigkeiten des ICS-Netzes von IT-Netzen<br>BSI-ICSK.08 Unzureichende Absicherung oder zu weitreichende Vernetzung<br>BSI-ICSK.09 Mangelhafte Konfigurationen von Komponenten<br>BSI-ICSK.12 Unzureichende Validierung von Eingaben und Ausgaben<br>BSI-ICSK.13 Kommunikation von Mess- und Steuerwerten<br>BSI-ICSK.14 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen<br>BSI-ICSK.15 Systematische Schwachstellensuche über das Netzwerk<br>BSI-ICSK.17 Man-in-the-Middle-Angriff<br>BSI-ICSK.18 Phishing<br>BSI-ICSK.19 Injection-Angriffe<br>BSI-ICSK.20 Cross-Site-Scripting<br>BSI-ICSK.23 Schadprogramme |

## 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 eintritt
- 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 Gefährdungskataloge

Die folgenden Gefährdungen aus dem Katalog elementarer Gefährdungen des BSI (Stand: 07.12.2020) wurden als relevant für die Branche Siedlungsabfallentsorgung ermittelt. Alle nicht aufgeführten Gefährdungen sind demgegenüber in der Regel nicht in der Lage, zu einem Versagen oder einer Manipulation der branchenspezifischen technischen Funktion zu führen.

| **Relevante elementare Gefährdungen** |
|---|
| **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 0.14 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** |

| Relevante elementare Gefährdungen |
|---|
| 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 0.30 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 0.34 Anschlag |
| G 0.35 Nötigung, Erpressung oder Korruption |
| G 0.36 Identitätsdiebstahl |
| G 0.39 Schadprogramme |
| G 0.40 Verhinderung von Diensten (Denial of Service) |
| G 0.41 Sabotage |
| G 0.42 Social Engineering |
| G 0.43 Einspielen von Nachrichten |
| G 0.44 Unbefugtes Eindringen in Räumlichkeiten |
| G 0.45 Datenverlust |
| G 0.46 Integritätsverlust schützenswerter Informationen |
| G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe |

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

| Relevante Gefährdungen aus dem ICS-Security-Kompendium des BSI |
|---|
| BSI-ICSK.03 Unvollständige Absicherung der Fernwartungszugänge |
| 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.10 Fehlende Backups |
| 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.16 Denial-of-Service-Angriffe (DoS) |

| Relevante Gefährdungen aus dem ICS-Security-Kompendium des BSI |
| --- |
| **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.22 Schadsoftware auf EWS** |
| **BSI-ICSK.23 Schadprogramme** |
| **BSI-ICSK.24 Replay-Angriff** |

## A.4 Abkürzungen

| | |
|---|---|
| B3S | Branchenspezifischer Sicherheitsstandard |
| BBK | Bundesamt für Bevölkerungsschutz und Katastrophenhilfe |
| BKM | 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 |
| DNS | Domain Name System |
| 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 | Ursprünglich: Umsetzungsplanung KRITIS, mittlerweile Eigenname |
| URL | Uniform Resource Locator |