Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Zur Dokumentation des Geltungsbereiches bei KRITIS-Betreibern

Erfahrungen aus den Nachweisen gemäß § 8a Absatz 3 BSIG – Hilfestellung und Beispiel zur Dokumentation des Geltungsbereiches bei KRITIS-Betreibern

Änderungshistorie

Version	*Datum*	*Beschreibung*
2.0	15.08.2024	Anpassungen an die aktualisierten Anforderungen nach § 8a Absatz 5 BSIG (GAiN 2.0“)
1.0	27.06.2022	Initiale Veröffentlichung

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6166
E-Mail: kritische.infrastrukturen@bsi.bund.de
Internet: www.bsi.bund.de

Inhalt

1 Einleitung

Bei der Dokumentation des Geltungsbereiches handelt es sich um eines der wichtigsten initialen Dokumente für die Betrachtung der Informationssicherheit in Kritischen Infrastrukturen (KRITIS). Über den Geltungsbereich legen Betreiber die Grenzen der einzelnen KRITIS-Anlagen in ihrem Betrieb fest. In einer Dokumentation des Geltungsbereiches beschreiben sie diese Grenzen, ebenso wie die Funktionen und Prozesse der einzelnen KRITIS-Anlagen und legen so dar, welcher Teil der eigenen Informationstechnik für den Betrieb der KRITIS-Anlage notwendig und von anderer IT hinreichend getrennt ist. Abgeschlossen wird die Dokumentation eines Geltungsbereiches durch eine Behandlung von externen Beteiligten und Schnittstellen in der Anlage.

Aus den Erfahrungen der Nachweisprüfungen Kritischer Infrastrukturen der letzten Jahre im Rahmen des § 8a Absatz 3 BSIG zeigt sich, dass vor allem ein passendes Abstraktionsniveau für die grafische Darstellung und textuelle Beschreibung des Geltungsbereiches bei KRITIS-Betreibern für eine effektive Vorbereitung und Durchführung der Nachweisprüfungen unentbehrlich ist. Aus diesen Erfahrungen haben wir Empfehlungen für die Dokumentation des Geltungsbereiches abgeleitet und in diesem Artikel zusammengestellt.

Im Rahmen der Nachweiserbringung nach § 8a Absatz 3 BSIG spielen der Geltungsbereich und seine Dokumentation für mindestens drei Adressatenkreise eine wichtige Rolle:

1. Der KRITIS-Betreiber legt mit dem Geltungsbereich normativ innerhalb seines Betriebs die Grenzen der KRITIS-Anlage und ihrer IT fest. Durch eine vollständige Dokumentation des Geltungsbereiches schafft er über diese Grenzen Klarheit. Dies ist für die Vorbereitung der Prüfung zur Nachweiserstellung, aber auch bereits im Hinblick auf die zu treffenden Maßnahmen innerbetrieblich wichtig.
2. KRITIS-Prüfende nehmen die Dokumentation des Geltungsbereiches als Grundlage für die Prüfung zur Nachweiserstellung und die zu prüfenden Komponenten. Die Dokumentation des Geltungsbereiches wird als eines der ersten Dokumente im Rahmen einer Prüfung geprüft. Der darin beschriebene Geltungsbereich muss die KRITIS-Anlage korrekt und vollständig wiedergeben, sowie für Dritte nachvollziehbar beschreiben.
3. Für das BSI beschreibt die Dokumentation des Geltungsbereiches zusammengefasst die KRITIS-Anlage, für die Nachweise eingereicht werden. Die Funktionsweise, Prozesse und Erklärung der Grenzen der KRITIS-Anlage müssen verständlich erklärt werden, damit nachvollzogen werden kann, dass die Anforderungen des § 8a Absatz 1 BSIG für die gesamte zu betrachtende IT erfüllt sind.

Die folgenden Ausführungen erläutern unsere Erfahrungen mit Geltungsbereichen am Beispiel des fiktiven Unternehmens Tanklager GmbH Hamburg (TAGH), das als KRITIS-Betreiber in der Mineralöl-Branche eine KRITIS-Anlage Tanklager am Standort Hamburg betreibt. Im Anhang des Artikels befindet sich die beispielhafte Dokumentation des Geltungsbereiches, inkl. eines Netzstrukturplans der TAGH.

In der Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG (15.08.2024, V1.3) hat das BSI elf Anforderungen an die Dokumentation des Geltungsbereiches (G) und elf zusätzliche Anforderungen an die Darstellung des Geltungsbereiches durch einen Netzstrukturplan (N) definiert. Der vorliegende Artikel strukturiert diese Anforderungen (G01-13 und N01-10) in thematisch zusammenhängende Abschnitte und erklärt deren Umsetzung anhand der beiden angehängten Beispieldokumente der TAGH.

Die Struktur des Artikels, die Beschreibungen und die Beispieldokumente sollen als Anhaltspunkt dienen, nicht als normative Festlegung. Betreiber müssen für die Dokumentation ihres Geltungsbereiches ein passendes Abstraktionsniveau finden und Aufteilung und Inhalte den eigenen Gegebenheiten anpassen. Bestimmte Betreiber unterliegen nach § 8a Absatz 5 BSIG separaten Regeln und Anforderungen an die Dokumentation des Geltungsbereiches und Netzstrukturplans[1]. Das BSI hat im August 2024 weitere verpflichtende Vorgaben nach § 8a Absatz 5 BSIG erlassen; KRITIS-Betreiber und –Verbände wurden im Prozess beteiligt. Die Dokumentation des Geltungsbereiches muss auf Deutsch verfasst werden.

[1] Anforderungen an die Nachweisführung bei der Anlagenkategorie „Rechenzentrum“

2 Kontext

Welchen Zweck verfolgt der Betreiber und welche Rolle hat hierbei die KRITIS-Anlage?

Der erste Abschnitt der Dokumentation des Geltungsbereiches beschreibt den Kontext des Betreibers und der gemeldeten KRITIS-Anlage. Ziel der Ausführungen im Kontext ist eine kurze und prägnante Zusammenfassung der Geschäftstätigkeit des Betreibers und eine Einordnung der Anlage in den KRITIS-Kontext von Sektor, Branche und kritischer Dienstleistung (kDL). Die konkrete Anlagenkategorie sollte in diesem Abschnitt mit allen ihren Merkmalen und Bereichen, in der Form wie diese Eigenschaften in der Anlage beim Betreiber vorzufinden sind, dargestellt werden.

Im Beispiel der TAGH werden im ersten Abschnitt „Kontext“ der Branchen-Hintergrund (Mineralöl und Logistik) und Unternehmensgegenstand der TAGH beschrieben und die über den Schwellenwerten liegende KRITIS-Anlage Tanklager Hamburg definiert, die eine kritische Dienstleistung erbringt (G02). Der Geltungsbereich im Unternehmen sowie eine Einordnung der Assets und das Sicherheitsmanagement werden hier ebenfalls kurz umrissen (G06).

Bei der TAGH wird die KRITIS-Anlage selbst in einem zweiten, separaten Abschnitt „Anlagenbeschreibung“ näher beschrieben und definiert (G01). Hierzu zählen eine Einordnung der Betriebsstätten (Umschlagsanlagen, Produkte) und Umgebung (Industrie- und Hafengebiet Hamburg) sowie eine konkrete Festlegung der einzelnen Anlagenteile, die zur KRITIS-Anlage Tanklager Hamburg gehören.

Die folgenden Anforderungen werden vorrangig durch die Darstellung im Abschnitt Kontext erfüllt:

G01 Die Anlage ist erkennbar und nachvollziehbar beschrieben.

G02 Die vom Betreiber erbrachten Teile der kDL sind erkennbar und nachvollziehbar beschrieben.

G06 Alle Teile der KRITIS gehen aus dem eingereichten Geltungsbereich hervor.

3 Prozesse

Welche Abläufe bestimmen den Betrieb der KRITIS-Anlage?

Der Abschnitt Prozesse beschreibt die prinzipielle Funktion der KRITIS-Anlage samt ihren funktionalen Prozessen im Geltungsbereich. Ziel der Ausführungen ist eine Auflistung der zur Anlage gehörigen Prozesse, die für den Betrieb der Anlage und die Erbringung der kritischen Dienstleistung im Geltungsbereich zwingend notwendig sind (G04):

1. Die Prozessschritte, die den tatsächlichen Betrieb bzw. die Versorgung der Bevölkerung durch die KRITIS-Anlage gewährleisten, sollten klar definiert sein. Im Beispiel der TAGH sind dies im dritten Abschnitt „Prozesse“ die drei primären Prozessschritte Einlagerung, Lagerbetrieb und Auslagerung im Tanklager.
2. Prozesse, die den eigentlichen Betrieb im Geltungsbereich unterstützen und die für die Erbringung der kritischen Dienstleistung zwingend erforderlich sind, sollten ebenfalls aufgelistet werden. Im Beispiel der TAGH sind dies unter anderem der Prozess Betrieb und der Prozess kommerzielle Abwicklung.

Diese Prozesse sind im weiteren Verlauf auch für die Zuordnung der Informationstechnologie notwendig, eine zusätzliche übersichtliche grafische Visualisierung als Blockdiagramm bietet sich bei komplexeren Anlagen an. Ebenso muss eine mögliche Aufteilung der KRITIS-Anlage oder des Betriebs auf mehrere Standorte beschrieben werden, einschließlich standortspezifischer und übergreifender Prozesse. Im Beispiel der TAGH weist die Anlage selbst nur einen Standort auf.

Abgeschlossen werden sollte die Darstellung der Prozesse mit einer Abgrenzung von Betriebsteilen, Standorten und Prozessen, die nicht relevant und somit nicht Teil des Geltungsbereiches sind. Hierzu können beispielsweise Prozesse wie der Betrieb der Zentrale, der Verwaltung oder anderer Anlagen zählen, auch wenn diese auf demselben Gelände ablaufen, sofern eine klare Abgrenzung zur KRITIS-Anlage möglich ist (G07). Für eine solche Abgrenzung ist insbesondere eine Trennung bzw. Segmentierung auf der Ebene der IT erforderlich. Andernfalls müssen solche Betriebsteile trotz fehlender funktionaler Relevanz für die KRITIS-Anlage mit in den Geltungsbereich aufgenommen werden.

Die folgenden Anforderungen werden vorrangig im Abschnitt Prozesse erfüllt:

G04 Alle für die kDL maßgeblichen Prozesse sind erfasst.

G07 Die Grenzen des Geltungsbereiches sind klar erkennbar.

4 Informationstechnik

Wozu dient die IT?

Nach der betrieblichen und prozessualen Dokumentation des Geltungsbereiches der KRITIS-Anlage beschreibt der Abschnitt Informationstechnik die für den Betrieb der KRITIS-Anlage zur Erbringung der kritischen Dienstleistung wichtigen IT-Systeme. Ziel der Ausführungen ist eine trennscharfe Dokumentation der Gesamtheit der Informationstechnik und ihrer Rolle in der KRITIS-Anlage.

Diese umfasst alle IT- und OT-Systeme, -Komponenten und, wenn notwendig, -Applikationen, auf welche die KRITIS-Anlage maßgeblich angewiesen ist. Zur besseren Dokumentation und Handhabung in der Prüfung bietet sich eine schriftliche Fixierung der Kriterien an, nach denen diese Systeme für den Geltungsbereich ausgewählt und abgegrenzt werden, wie z. B. eine Bewertung der Kritikalität durch Business Continuity Management (BCM) oder IT Service Continuity Management (ITSCM).

Im Beispiel der TAGH werden im vierten Abschnitt „Informationstechnik“ zunächst die Verbindungen zur Zentrale und eine Lokalisierung der IT-Systeme am Standort der KRITIS-Anlage beschrieben. Anschließend werden alle IT-Systeme aufgelistet, die für den Betrieb des Tanklagers maßgeblich sind (G05).

In der abschließenden Tabelle im vierten Abschnitt listet die TAGH die zur KRITIS-Anlage gehörenden IT-Systeme gesammelt auf und ordnet sie den einzelnen betrieblichen Prozessen der Anlage zu (G11). Die TAGH nutzt diese Zuordnung zu Prozessen als Kriterium zur Auswahl der maßgeblichen IT-Systeme.

Die folgenden Anforderungen werden vorrangig im Abschnitt Informationstechnik erfüllt:

G05 Alle für die kDL maßgeblichen Systeme, Komponenten und ggf. Applikationen sind erfasst.

G11 Der Geltungsbereich ermöglicht eine Zuordnung zwischen Prozessen und zugehörigen notwendigen Systemen, Komponenten und ggf. Applikationen.

5 Schnittstellen

Welche Zugriffe erfolgen über die Grenzen des Geltungsbereiches hinweg?

Aufbauend auf der Dokumentation der Informationstechnik beschreibt der Abschnitt Schnittstellen die externen Zugänge, Schnittstellen und Abhängigkeiten der KRITIS-Anlage. Damit soll dargelegt werden, welche externen Parteien Zugriff auf die KRITIS-Anlage, z. B. zum Betrieb oder zur Wartung, haben und welche Schnittstellen auch von internem Personal beim Zugriff von außen genutzt werden, z B. für Remote-Arbeit. Im Beispiel der TAGH werden Teile der Anlage aus der Ferne durch eine Fremdfirma gewartet, die über einen externen Zugang durch die DMZ zugreift (G08).

Ebenso werden in diesem Abschnitt Abhängigkeiten zu außerhalb des Geltungsbereiches der KRITIS-Anlage liegenden Prozessen und Informationstechnik beschrieben, die für den Betrieb der KRITIS-Anlage wichtig sind. Dies umfasst Verbindungen und Abhängigkeiten zu weiteren Betriebsteilen des Betreibers – im Beispiel der TAGH die Verbindung zur Zentrale, dort aber bereits im vorigen Abschnitt Informationstechnik beschrieben.

Die folgenden Anforderungen werden vorrangig im Abschnitt Schnittstellen erfüllt:

G08 Die Schnittstellen zu außerhalb des Geltungsbereich liegenden Prozessen, Systemen, Komponenten und ggf. Applikationen sind erkennbar und nachvollziehbar beschrieben.

6 Externe

Welche Rolle spielen Externe?

Neben externen Zugriffen und Abhängigkeiten der KRITIS-Anlage macht die Dokumentation des Geltungsbereiches klar kenntlich, welche Teile der KRITIS-Anlage, inklusive Informations- und Kommunikationstechnik, von Dritten betrieben werden. Der Abschnitt Externe listet dazu die Teile der KRITIS-Anlage, Prozesse und IT-Systeme auf, die von Dienstleistern und weiteren Unternehmen erbracht oder betrieben werden (G10).

Beispiele dafür sind IT-Provider, Cloud-Provider und Hersteller, die bestimmte IT-Systeme und Verfahren betreiben, die für den Betrieb der KRITIS-Anlage und ihrer Prozesse maßgeblich sind. Bei der TAGH ist dies ein Kontrollsystem für Waren, das durch eine externe Firma betrieben wird und dessen Informationen durch die TAGH verarbeitet werden. Im Beispiel wird diese Firma aus Gründen der Übersichtlichkeit schon im vorigen Abschnitt Schnittstellen behandelt.

Die folgenden Anforderungen werden vorrangig im Abschnitt Externe erfüllt:

G10 Durch Dritte betriebene Teile der KRITIS sind erkennbar und nachvollziehbar beschrieben.

7 Netzstrukturplan

Wie sind die Bestandteile der Anlage vernetzt?

Zur Dokumentation eines Geltungsbereiches gehört ein Netzstrukturplan, der die grundlegenden Zusammenhänge in der KRITIS-Anlage mit Blick auf das IT-Netz zusammenfasst. Der Netzstrukturplan ist üblicherweise ein eigenständiges Dokument, das den Geltungsbereich samt IT-Systemen und Verbindungen übersichtlich grafisch darstellt (G12). Insbesondere die Informationen aus dem Abschnitt Informationstechnik sollten hier aufgegriffen und in einen Zusammenhang gestellt werden. Die Strukturierung nach Räumen oder Standorten (physische Aufteilung) hat sich dabei in vielen Anwendungsbeispielen als zielführend erwiesen. Andere Darstellungsformen als eine Strukturierung nach bspw. Räumen sind zulässig und ggf. hilfreich, sofern sie der Nachvollziehbarkeit und der Übersicht dienlich sind. Der Netzstrukturplan muss dabei kein vollwertiges, umfangreiches Netzdiagramm darstellen, sondern soll die Anlage passend abstrahiert und verständlich beschreiben (N03).

Im Beispiel der TAGH stellt der grafische Netzstrukturplan das Tanklager Hamburg mit seinen Anlagenteilen, Verbindungen und IT-Systemen übersichtlich und passend abstrahiert dar und verwendet dazu funktionale Blöcke zur Unterteilung der Anlage, Piktogramme für IT-Systeme und farbige Linien für Netzwerkverbindungen. Aus der Darstellung der Netz- bzw. Funktionsbereiche und der Netzwerkverbindungen wird ersichtlich, an welchen Stellen Netze getrennt oder separiert wurden (N11).

Die IT-Systeme und Prozesse sind im Beispiel zu mehreren funktionalen Blöcken für den Betrieb der Anlage zusammengefasst und die IT-Systeme sind den einzelnen Komponenten und Prozessen der Anlage zugeordnet. Nicht eingezeichnet sind detaillierte interne Informationen wie IP-Adressen, Hostnamen, Ports oder vergleichbare vertrauliche Informationen.

Der Geltungsbereich der KRITIS-Anlage sollte im Netzstrukturplan separat abgegrenzt und hervorgehoben werden – im Beispiel der TAGH grau unterlegt – (N01). Zudem sollten die wichtigsten maßgeblichen IT-Systeme aus den zuvor beschriebenen Abschnitten zur Dokumentation des Geltungsbereiches eingezeichnet werden (N02). Wurden IT-Systeme in der bisherigen Dokumentation des Geltungsbereiches aus Gründen der Komplexität und Übersichtlichkeit zusammengefasst oder gruppiert, kann diese Zusammenfassung oder Gruppierung hier ebenfalls verwendet werden. Es ist jedoch zu beachten, dass die Zusammenfassung oder Gruppierung über die Grenzen der verschiedenen Dokumente hinweg einheitlich erfolgt.

Im Beispiel sind Verbindungen nach außen im oberen Teil des Netzstrukturplans eingezeichnet. So beinhaltet der Netzstrukturplan eine Verbindung über das VPN zur Zentrale und eine Verbindung über die DMZ in das Internet (N05) sowie einen permanenten Wartungszugriff durch eine externe Firma, ebenfalls über das Internet (N06). Der Einsatz und die Anbindung der Systeme zur Angriffserkennung erfolgt am Beispiel der TAGH an einem zentralen Ort. Die relevanten IT-Komponenten sind in diesem Fall direkt verbunden (N12).

Falls eine Anlage auf mehrere Standorte verteilt ist, müssen im Netzstrukturplan sowohl die Aufteilung auf Standorte als auch deren IT-Anbindungen an Netzwerke kenntlich gemacht werden (N07, N08). Das Tanklager der TAGH befindet sich nur an einem Ort, die Verbindung zur Zentrale (außerhalb des Geltungsbereiches) ist jedoch eingezeichnet. Werden Dienstleistungen, IT-Systeme oder Teile vom Betrieb der Anlage an Dienstleister ausgelagert, muss dies ebenfalls im Netzstrukturplan eingezeichnet werden (N09). Bei der TAGH waren neben der Fernwartung keine Auslagerungen darzustellen.

Der Netzstrukturplan sollte verwendete Symbole, Farben und Linien in einer Legende beschreiben. Im Beispiel der TAGH erfolgt dies links in der Grafik (N10). Eine Einführung und Erklärung der funktionalen Bezeichnungen muss bei entsprechender Komplexität in einem eigenen Abschnitt innerhalb der textuellen Beschreibung des Geltungsbereiches hinzugefügt werden, um das Verständnis für den Netzstrukturplan zu erleichtern (G13). Im Beispiel der TAGH wurde aufgrund der wenigen und einfachen funktionalen Bezeichnungen darauf verzichtet.

Die folgenden Anforderungen werden durch den Netzstrukturplan und die notwendigen schriftlichen Ergänzungen erfüllt:

G12 Der Geltungsbereich ist in einem Netzstrukturplan dargestellt.

G13 Zum Verständnis notwendige schriftliche Ergänzungen zum Netzstrukturplan wurden vorgenommen.

N01 Der Netzstrukturplan bietet einen Überblick über den Geltungsbereich.

N02 Alle maßgeblichen Systeme, Komponenten und ggf. Applikationen sind dargestellt.

N03 Das Abstraktionsniveau ist passend gewählt worden.

N05 Alle Kommunikationsschnittstellen nach außen sind dargestellt.

N06 Wartungsschnittstellen sind abgebildet, sofern sie dauerhaft freigeschaltet sind.

N07 Der Netzstrukturplan gibt eine ggf. existierende Aufteilung in Standorte wieder.

N08 Die IT-Anbindungen verschiedener Standorte zueinander sind dargestellt.

N09 Ausgelagerte Dienstleistungen sind dargestellt.

N10 Funktionale Bezeichnungen und Legenden liegen nötigenfalls vor und sind verständlich.

N11 Aus dem Netzstrukturplan ist ersichtlich, an welchen Stellen Netze getrennt oder separiert wurden.

N12 Im Netzstrukturplan ist ersichtlich, welche Netzabschnitte und KRITIS-relevanten IT-Komponenten (Server, Router, Firewalls etc.) durch Systeme zur Angriffserkennung überwacht werden. Bereiche, die nicht überwacht werden, sind gekennzeichnet.

8 Abschließende Worte

Was zeigt die Erfahrung?

Zum Schluss dieser Ausführungen möchten wir unterstreichen, welche wichtige Rolle eine übersichtliche und vollständige Dokumentation des Geltungsbereiches in der erfolgreichen Nachweiserstellung spielt. Er gibt der Vorbereitung und Durchführung der tatsächlichen Prüfung zur Nachweiserstellung und der Nachweiserbringung an das BSI den grundlegenden Rahmen und dient dabei als Erklärung und Festlegung zugleich.

Unsere Erfahrungen zeigen, dass insbesondere die Beschreibung und Abbildung von Schnittstellen und ausgelagerten Dienstleistungen besonderer Sorgfalt bedürfen. Eine einheitliche Darstellung im Netzstrukturplan schafft Konsistenz und macht ihn damit nachvollziehbar. Gleiches gilt für die textuelle Beschreibung oder sonstige Darstellung in der Dokumentation des Geltungsbereiches, denn auch hier hilft eine konsistente und einheitliche Darstellung dabei, Schnittstellen und ausgelagerte Dienstleistungen einzuordnen und einfacher im Kontext des Nachweises bewerten zu können. So können die Nachfragen zu eingereichten Nachweisunterlagen auf ein Minimum reduziert werden.

Zusätzlich wollen wir noch folgende Empfehlungen und Beobachtungen neben den beschriebenen Ansätzen zur Erfüllung der eigentlichen Anforderungen an die Dokumentation von Geltungsbereichen teilen, die bei der Erstellung hilfreich sein könnten:

Als Abschluss der Dokumentation des Geltungsbereiches oder als Anhang bietet sich eine Tabelle mit allen Anforderungen aus der Orientierungshilfe zu Nachweisen des BSI an, in welcher jeder Anforderung der passende Abschnitt oder der passende Unterabschnitt der eigenen Dokumentation des Geltungsbereiches zugeordnet ist. Damit kann bei der Erstellung der Dokumentation des Geltungsbereiches eine erste eigene Qualitätssicherung erfolgen.

Bei der Erstellung der Dokumentation des Geltungsbereiches empfehlen wir, stets den Fokus darauf zu legen, **dass die Dokumentation des Geltungsbereiches es einem unabhängigen Dritten möglich machen sollte, die KRITIS-Anlage und ihre Versorgungsfunktion, Informationstechnik und Grenzen nachvollziehen zu können**. Die Dokumentation des Geltungsbereiches legt für die Prüfung zur Nachweiserstellung Grenzen fest, die so klar wie möglich dargestellt werden sollten. Das erlaubt allen Beteiligten eine Konzentration auf die Kritische Infrastruktur selbst.

Anhang A: Beispiel zur Dokumentation eines Geltungsbereiches – textuelle Beschreibung

Geltungsbereich des Tanklager Hamburg der Tanklager GmbH Hamburg

1. Kontext

Die Tanklager GmbH Hamburg (TAGH) ist als Unternehmen in der Mineralöl- und Logistikbranche tätig. Unternehmensgegenstand sind die Lagerung und der Umschlag von Mineralölprodukten und anderen flüssigen Umschlaggütern für Dritte in Tanklagern.

Aufgrund der am Standort Hamburg umgeschlagenen Mengen ist das Tanklager eine KRI¬TIS nach BSIG. Die KRITIS-Anlage Tanklager Hamburg erbringt im Sektor Energie der kritische Dienstleistung Kraftstoff- und Heizölversorgung in der Betriebsstätte Hamburg.

Alle Assets, die für die Prozesse der Auslagerung, Einlagerung und Lagerhaltung im Tanklager erforderlich sind, werden vom Informationssicherheitsmanagementsystem (ISMS) der TAGH erfasst. Ein Fokus liegt hier insbesondere auf den Leit- und Steuerungssystemen, da diese zur Aufrechterhaltung der Verladebereitschaft besonders wichtig sind. Der Geltungsbereich beinhaltet daher den Betrieb der Informations-, Kommunikations- und Prozessleitsysteme zur Sicherstellung der Verlade- und Umschlagsfähigkeit von Mineralölprodukten.

Die zentrale Verwaltung und weitere Betriebsstätten der Tanklager GmbH Hamburg befinden sich ebenfalls in Hamburg. Da sie zur Erbringung der kritischen Dienstleistung nicht notwendig sind und gegenüber der KRITIS-Anlage klar abgegrenzt werden können, sind sie nicht Teil des Geltungsbereiches.

2. Anlagenbeschreibung

Die TAGH betreibt unter dem Namen Tanklager Hamburg eine KRITIS-Anlage des Typs Erdöl- und Erdölproduktenlager im Sinne der BSI-KritisV.

Das Tanklager befindet sich im Industrie- und Hafengebiet der Stadt Hamburg. Im Tankraum können über einen Anschluss für Schiffe und Kesselwagen flüssige Umschlagsgüter eingelagert werden. Die Auslagerung erfolgt über einen Anschluss auf Tankwagen und Binnenschiffe.

Das Unternehmen betreibt Umschlagsanlagen für die Abfertigung von:

- Tankwagen
- Kesselwagen
- Binnenschiffen

Gesamte Nutzkapazität: 157.000 m³ Tankvolumen

Umschlagprodukte:

- Heizöl extra leicht
- Dieselkraftstoff
- Ottokraftstoff

Das Tanklager Hamburg besteht aus den folgenden Einheiten:

- Tankwagen-Füllbühnen I und II
- Bürogebäude

- Messwarte
- Lagerhalle
- 8 Tanks mit Schwimmdach für Benzine und Mitteldestillate
- 5 Zylindertanks
- 4 Tankwagen-Füllspuren
- 2 Kesselwagen-Füllstellen für Mitteldestillate Pumpenhaus für Feuerlöschung
- Ladesteiger mit 2 Verladearmen

3. Prozesse

Die Betriebsstätte Tanklager Hamburg wird zur Lagerung und für den Umschlag von Mineralölprodukten genutzt. Dabei werden durch die TAGH die Hauptprozessschritte Einlagerung, Lagerbetrieb und Auslagerung in der Anlage durchgeführt:

Einlagerung entspricht der Entladung der Ware aus dem Transportmittel und dem Einpumpen in Lagertanks. Im Lagerbetrieb werden der Bestand verwaltet und die technische Verfügbarkeit gewährleistet. Die Auslagerung beinhaltet die Bereitstellung und Verladung der Ware für den Abtransport durch die Tankwagen, Kesselwagen und Schiffe.

Unterstützend begleitet werden diese Prozesse vom Betrieb, der kommerziellen Abwicklung und den Services der IT und OT.

Weitere Prozesse und die Verwaltung in der Zentrale der Firma TAGH sind nicht Teil der gemeldeten Anlage.

Kategorie	*Prozess*
Hauptprozess	Einlagerung
Hauptprozess	Lagerbetrieb
Hauptprozess	Auslagerung
Unterstützungsprozess	Betrieb
Unterstützungsprozess	Kommerzielle Abwicklung
Unterstützungsprozess	Services der IT und OT

4. Informationstechnik

Die Informationstechnik für die Anlage Tanklager Hamburg befindet sich ausschließlich auf dem Gelände der Betriebsstätte. Der Standort ist via VDSL-Verbindung durch eine DMZ mit dem Internet verbunden; der Zugriff der Fernwartung erfolgt ebenfalls über die DMZ. Über ein VPN besteht eine Verbindung mit der Zentrale der TAGH.

Die folgenden Systeme werden lokal am Standort innerhalb des Büro- und Produktionsnetzes betrieben:

- Für die Verladesteuerung wird eine eigene Software „MusterTsoft“ verwendet. Diese beinhaltet auch alle relevanten Stammdaten und kommuniziert über BeiSpielO-Schnittstellen mit der Mess- und Fördertechnik.
- Die Mess- und Fördertechnik ist über Relais mit der Automatisierungstechnik verbunden.
- Die Messtechnik ist von der Firma MusterM3ss und fungiert als eichrechtliche Messstrecke.
- Um die Aufbewahrung von Urbelegen zu gewährleisten, wird ein BeiSpielU-System, ebenfalls von der Firma MusterM3ss, verwendet.

Im Netz sind weitere Steuerungs- und Regelungskomponenten eingebunden, so auch eine Vapor Recovery Unit (VRU) der Firma BeispielT3K zur Dampfrückgewinnung. Für die weitere Tanklagerautomatisierung wurde Technik der Firma MusterH3R installiert.

Um Tankstände zu ermitteln, wurde ein Tankradarsystem (MusterVisT) installiert. Darüber hinaus sind lagespezifische Daten über die Office-IT auf physischen Systemen im Standort hinterlegt.

Zur besseren Übersichtlichkeit sind die einzelnen Systeme im Folgenden den jeweiligen betrieblichen Prozessen der Anlage **Tanklager Hamburg** zugeordnet.

System	*Systemtyp*	*Prozess*
MusterVisT	Bedienarbeitsplatz	Kommerzielle Abwicklung
Mu5terXC	Fernwirkgerät	Kommerzielle Abwicklung, Services der IT und OT
BeiSpielO	Server	Betrieb
MusterTsoft	Bedienarbeitsplatz	Kommerzielle Abwicklung
BeiSpielU	Server	Kommerzielle Abwicklung
Anlagenterminal	Zähler	Betrieb, kommerzielle Abwicklung, Services der IT und OT
MusterH3R IM 511-1 PN	Gateway	Betrieb
BeispielH3R UT 100SP	Fernwirkgerät	Betrieb
T1 Vapor Recovery Unit	Speicherprogrammierbare Steuerung	Betrieb
Router	Kommunikationskomponente	Betrieb, kommerzielle Abwicklung, Services der IT und OT
Aktoren	Feldgeräte	Betrieb

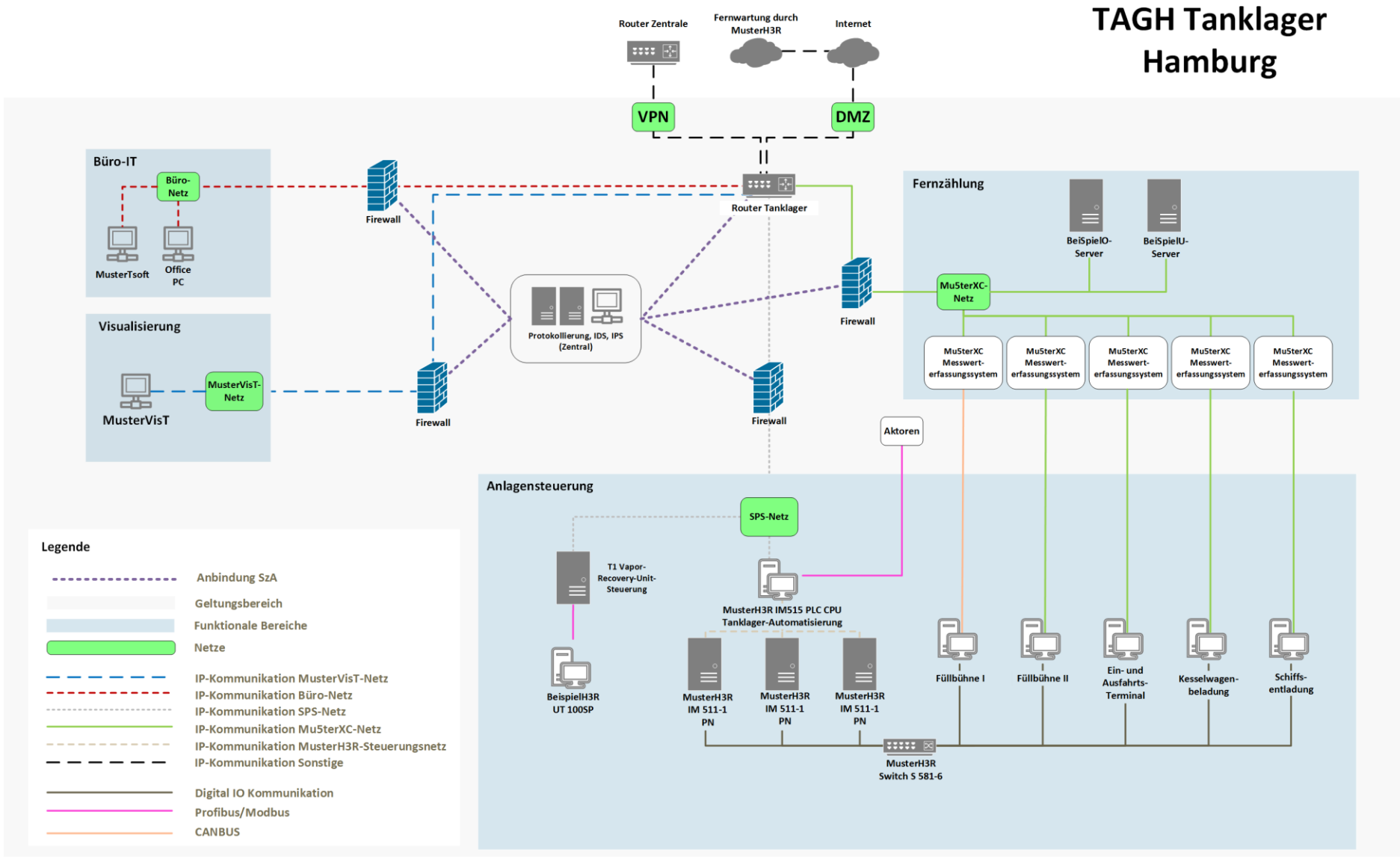
5. Schnittstellen

Die Wartung der MusterH3R-Systeme zur Tanklagerautomatisierung erfolgt über eine Fernwartungsschnittstelle. Der Zugriff erfolgt über die DMZ und ist mit der Firma MusterH3R über einen Wartungsvertrag abgesichert. Über diese Schnittstelle greifen Mitarbeitende der Firma MusterH3R unter Einhaltung festgelegter Sicherheitsanforderungen auf die Systeme zu und führen den Prozess Wartung durch.

Das IT-gestützte Beförderungs- und Kontrollsystem für verbrauchsteuerpflichtige Waren (EMCS) wird von dem Dienstleister MusterDi3N GmbH betrieben. Es ist zur Bereitstellung der kritischen Dienstleistung nicht notwendig und daher nicht im Geltungsbereich enthalten. Meldungen des EMCS werden vom Serviceprovider als externe Dienstleistung zur Verfügung gestellt und von der Zentrale der TAGH verarbeitet.

Weitere Schnittstellen oder von Externen erbrachte Teile der kritischen Dienstleistung bestehen nicht.

Anhang B: Beispiel zur Dokumentation eines Geltungsbereiches – Netzstrukturplan



Anhang C: Liste der Anforderungen

Geltungsbereich

G01 Die Anlage ist erkennbar und nachvollziehbar beschrieben.

G02 Die vom Betreiber erbrachten Teile der kDL sind erkennbar und nachvollziehbar beschrieben.

G03 Entfällt

G04 Alle für die kDL maßgeblichen Prozesse sind erfasst.

G05 Alle für die kDL maßgeblichen Systeme, Komponenten und ggf. Applikationen sind erfasst.

G06 Alle Teile der KRITIS gehen aus dem eingereichten Geltungsbereich hervor.

G07 Die Grenzen des Geltungsbereiches sind klar erkennbar.

G08 Die Schnittstellen zu außerhalb des Geltungsbereich liegenden Prozessen, Systemen, Komponenten und ggf. Applikationen sind erkennbar und nachvollziehbar beschrieben.

G09 Entfällt.

G10 Durch Dritte betriebene Teile der KRITIS sind erkennbar und nachvollziehbar beschrieben.

G11 Der Geltungsbereich ermöglicht eine Zuordnung zwischen Prozessen und zugehörigen notwendigen Systemen, Komponenten und ggf. Applikationen.

G12 Der Geltungsbereich ist in einem Netzstrukturplan dargestellt.

G13 Zum Verständnis notwendige schriftliche Ergänzungen zum Netzstrukturplan wurden vorgenommen.

Netzstrukturplan

N01 Der Netzstrukturplan bietet einen Überblick über den Geltungsbereich.

N02 Alle maßgeblichen Systeme, Komponenten und ggf. Applikationen sind dargestellt.

N03 Das Abstraktionsniveau ist passend gewählt worden.

N04 Entfällt.

N05 Alle Kommunikationsschnittstellen nach außen sind dargestellt.

N06 Wartungsschnittstellen sind abgebildet, sofern sie dauerhaft freigeschaltet sind.

N07 Der Netzstrukturplan gibt eine ggf. existierende Aufteilung in Standorte wieder.

N08 Die IT-Anbindungen verschiedener Standorte zueinander sind dargestellt.

N09 Ausgelagerte Dienstleistungen sind dargestellt.

N10 Funktionale Bezeichnungen und Legenden liegen nötigenfalls vor und sind verständlich.

N11 Aus dem Netzstrukturplan ist ersichtlich, an welchen Stellen Netze getrennt oder separiert wurden.

N12 Im Netzstrukturplan ist ersichtlich, welche Netzabschnitte und KRITIS-relevanten IT-Komponenten (Server, Router, Firewalls etc.) durch Systeme zur Angriffserkennung überwacht werden. Bereiche, die nicht überwacht werden, sind gekennzeichnet.