UP KRITIS

Branchenspezifischer Sicherheitsstandard (B3S) für Housing, Hosting und CDN

UP KRITIS – BAK Datacenter und Hosting

Informationen zum Dokument

Versionsverlauf

Version	Datum	Geändert durch	Kommentar
01.39	12.10.2022	Wigand	Bereinigung, Barrierefreiheit

Dokumenten-Freigabe

Dokument-Version	Freigegeben von	Freigegeben am
02.01	Volker Rauscher/Sunita Saxena/Wigand	16.12.2022

Qualitätssicherung

Name	Firma	E-Mail
Ralf Wigand	Microsoft GmbH	ralf.wigand@microsoft.com

Autoren

Autoren	Firma	E-Mail
Christian Behre	SAP	Christian.Behre@SAP.com
Dietmar Bestenlehner	IBM	bestenld@de.ibm.com
Bertram Dorn	AWS	bedorn@amazon.de
Dr. Joachim Fölsch	Digital Realty	joachimf@digitalrealty.com
Gerd Giese	Akamai	ggiese@akamai.com
Lars Nadzeyka	EntServ Deutschland	Lars.Nadzeyka@dxc.com
Volker Rauscher	IONOS	Volker.Rauscher@ionos.com
Sunita Ute Saxena	Deutsche Telekom Security	S.Saxena@telekom.de
Dr. Pascal Schmidt	Equinix	Pascal.Schmidt@eu.equinix.com
David Siemering	SAP	David.Siemering@sap.com
Armin von Werner	EntServ Deutschland	Armin.vonWerner@dxc.com
Ralf Wigand	Microsoft	Ralf.Wigand@microsoft.com
Barbara Willkomm	Deutsche Telekom Security	Barbara.Willkomm@telekom.de

Verteiler

Name	Funktion
Bundesamt für Sicherheit in der Informationstechnik – Referat WG 14	
UP KRITIS – BAK Datacenter/Hosting	

Inhalt

Abbildungs- und Tabellenverzeichnis

1 Einleitung zu den Bereichen Housing und Hosting

1.1 Vorwort zu diesem Branchenstandard

Dieser Branchenspezifische Sicherheitsstandard (B3S) bildet die Vorgaben nach IT-SiG 2.0, die bis zum Zeitpunkt 27.01.2022 veröffentlichten FAQ und die gesetzlichen Bestimmungen nach § 8a Absatz 5 BSIG ab. Er umfasst die kritischen Dienstleistungen (kDL) Datenspeicherung und -verarbeitung der Branche Informationstechnik innerhalb des Sektors Informationstechnik und Telekommunikation. Der B3S beschreibt den Stand der Technik für die Bereiche Housing, Hosting und CDN. Anlagen zur Erbringung von Vertrauensdiensten gehören auch zur kDL, werden aber von diesem B3S nicht erfasst.

Hierbei ist zu beachten, dass jeder Anwender, sofern er sich für die Umsetzung dieses B3S entscheidet, die allgemeinen Anforderungen aus Kapitel 1 umsetzen muss, während die weiteren Kapitel 2 (für Housing bzw. teilweise für Hosting) und Kapitel 3 (für Hosting und CDN) unternehmensspezifisch umzusetzen sind (siehe u. a. auch Orientierungshilfe zur Angriffserkennung).

Wenn im Folgenden Text das Verb „muss“ bzw. „müssen“ verwendet wird, bedeutet dies, dass die jeweiligen Anforderungen unbedingt erfüllt werden müssen. Sie können allerdings durch gleichwertige Alternativen ersetzt werden, wobei dann die Gleichwertigkeit gezeigt werden muss.

Das Verb „soll“ bzw. „sollen“/„sollte“/„sollten“ bedeutet, dass diese Anforderungen normalerweise erfüllt werden müssen, es aber Umstände geben kann, unter denen die Umsetzung nicht angeraten ist. Die Risiken einer Nichtumsetzung müssen dann sorgfältig abgewogen und deren Akzeptanz stichhaltig begründet werden.

Das Verb „kann“ bzw. „können“/„könnte“ /„könnten“ bedeutet, dass eine Anforderung optional ist. Der Betreiber darf für sich entscheiden, ob er die Anforderung umsetzt oder nicht. Eine Betrachtung der Risiken ist jedoch auch in diesem Fall sinnvoll.

Der B3S kann auch von Betreibern angewandt werden, die nicht unter die Regulierung nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) fallen. Zur Klarstellung wird darauf hingewiesen, dass sich die Kritikalität i. S. der „Verordnung zur Bestimmung Kritischer Infrastrukturen nach der BSI-Kritisverordnung (BSI-KritisV[1])“ bezogen auf die Kritische Infrastruktur nicht auf die eventuelle Kritikalität einzelner anderer Systeme auswirkt und auch kein Ausschluss einzelner Systeme innerhalb der Kritischen Infrastruktur darstellt (keine Vererbbarkeit der Kritikalität). Die Verantwortung der Absicherung verbleibt immer bei dem Bereich, der KRITIS ist und geht nicht auf den ausgelagerten Betreiber über.

So erfordert zum Beispiel ein kritischer Service wie CDN nicht zwangsläufig einen kritischen Hosting Betreiber oder eine kritische Housing Umgebung im Sinne des BSIG und der BSI-KritisV. In diesem Fall hat der CDN-Betreiber das Hosting und Housing der für ihn relevanten Systeme und Dienstleistungen im Rahmen der Risikoanalyse und -betrachtung zu berücksichtigen.

[1] BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 6. September 2021 (BGBl. I S. 4163) geändert worden ist

Die BSI-KritisV legt anhand von branchenspezifischen Bemessungskriterien Schwellenwerte fest. Wird ein solcher Schwellenwert erreicht oder überschritten, gilt die kDL als bedeutend im Sinne des BSIG.

Dies gilt für den IKT-Sektor mit seinen beiden Dienstleistungen IT und TK genauso wie für alle anderen geregelten Sektoren. Folglich ist für die Identifizierung als Kritische Infrastruktur allein der Versorgungsgrad innerhalb der Dienstleistung selbst ausschlaggebend. Etwaige Abhängigkeiten anderer Kritischer Infrastrukturen (zum Beispiel Steuerung einer kritischen Anlage in einem ausgelagerten Colocation-RZ) sind unerheblich, sofern es sich nicht um eine gemeinsame Anlage nach Anhang 4 Teil 1 Nr. 6 der BSI-KritisV [2]) handelt. Hier muss der jeweilige KRITIS-Betreiber selbst Auflagen zum Betrieb seiner Anlage an seinen Dienstleister weitergeben und durchsetzen.

Grundsätzlich gilt bei allen Verweisen auf externe Normen und Standards in diesem Dokument, dass die jeweils gültige Fassung zu berücksichtigen ist. Bei den hier im B3S genannten nachfolgenden Verweisen auf die Anhänge der ISO/IEC 27001 wird auf die Version ISO/IEC 27001:2017 referenziert, da die ISO 27001:2022 zum Zeitpunkt der Erstellung des B3S erst kurz vorher (Oktober 2022) veröffentlicht wurde. Bei Verwendung der ISO 27001:2022 sind alle in diesem B3S genannten Anforderungen gemäß den verfügbaren Mapping-Tabellen entsprechend anzuwenden.

1.2 Anwendungsbereich dieses B3S

Der vorliegende B3S bezieht sich gemäß der BSI-KritisV sowie der KRITIS-Sektorstudie „Informationstechnik und Telekommunikation (IKT)[3] des BSI auf den Anwendungsbereich Housing, Hosting sowie CDN. In den nachfolgenden Kapiteln wird unter dem Begriff „Hosting“ auch die Variante „Hosting mit CDN“ verstanden. Dazu gehören neben den dazugehörigen Prozessen, folgende Anlagenkategorien:

Anlagenkategorie Housing:

Unter Anlage wird ein einzelnes Rechenzentrum oder verbundene bzw. Rechenzentren innerhalb eines Campus entsprechend der aktuellen BSI-KritisV verstanden[4]. Ein enger betrieblicher Zusammenhang ist unabhängig von der räumlichen Distanz der Anlagen gegeben, wenn die Anlagen:

a) mit gemeinsamen Betriebseinrichtungen oder untereinander verbunden sind,
b) einem vergleichbaren technischen Zweck dienen und
c) unter gemeinsamer Leitung oder Steuerung stehen.

[2] BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 6. September 2021 (BGBl. I S. 4163) geändert worden ist

[3] KRITIS-Sektorstudie Informationstechnik und Telekommunikation (IKT) Öffentliche Version – Revisionsstand vom 5. Februar 2015 www.bsi.bund.de/dok/12252620

[4] Darstellung der Prozesse auf Seite 8 in „Anforderungen gemäß § 8a Abs. 5 BSIG „Validierung und Darstellung eines Geltungsbereichs für Kritische Infrastrukturen der Anlagenkategorie „2.1.1 Rechenzentrum“ nach Anhang 4, Teil 3 BSI-KritisV“ Stand: 22.04.2020 www.bsi.bund.de/dok/8a5-rz

Dies gilt beispielsweise in folgenden Fällen:

- Ein Housing-Anbieter steuert oder überwacht mehrere Rechenzentren, die jeweils unterhalb des gültigen Schwellwertes liegen, über eine gemeinsame zentrale Steuerung. Diese Rechenzentren bilden eine gemeinsame Anlage unabhängig davon, ob sie gemeinsam an einem Standort oder an mehreren getrennten Standorten in Deutschland betrieben werden.
- Ein Housing-Anbieter betreibt einzelne Rechenzentren, die jeweils den Schwellwert der vertraglich vereinbarten Leistung überschreiten. Aus diesen Rechenzentren werden zeitweise (nachts, Wochenende, Feiertage) auch kleinere Rechenzentren überwacht, die während der normalen Arbeitszeiten autonom arbeiten. Dann bilden die kleineren Rechenzentren mit den ‘großen’ Rechenzentren eine gemeinsame Anlage.

In folgendem Fall bilden die Rechenzentren keine gemeinsame Anlage:

- Ein Konzern betreibt zwei Rechenzentren, eines dient für die intern vom Konzern selbst genutzten IT-Systeme, ein weiteres ist an externe Kunden vermietet. In diesem Fall liegt keine gemeinsame Anlage vor, weil der Zweck nicht gleich ist. Der Betreiber fällt mit dem extern vermieteten Rechenzentrum erst dann unter diese Regelungen der BSI-KritisV, wenn für das extern vermietete Rechenzentrum der Schwellwert der vertraglich vereinbarten Leistung überschritten wird.

Anlagenkategorie Hosting und CDN:

Während im Bereich Housing der Geltungsbereich primär die Bereitstellung der Kernkomponenten Raum, Strom, Kühlung und physischer Sicherheit und Gewährleistung derselben im Fokus hat, beinhaltet die kDL im Bereich Hosting die Bereitstellung von zusätzlicher IT-Infrastruktur an Kunden, wie beispielsweise physischer oder logischer (virtueller) Server (IaaS), bzw. im Falle der Bereitstellung von Platform as a Service (PaaS) und Software as a Service (SaaS) auch weitere darauf aufbauende Services. Zusätzlich hat ein Hosting Provider sicherzustellen, dass für ihn relevante Anforderungen aus dem Bereich Rechenzentrumsbetrieb umgesetzt sind, unabhängig davon, ob Rechenzentren von ihm selbst betrieben, oder durch Housing Anbieter bereitgestellt werden. Weitere Informationen hierzu in Kapitel 2.

Im Bereich CDN (Content Delivery Network) werden Ladezeiten verkürzt und Reaktionszeiten werden verbessert. Dies geschieht, indem geografisch verteilte Server dahingehend genutzt werden, um die Bereitstellung von Webinhalten zu beschleunigen, indem sie näher an den Ort der Nutzer („server deplyoment at the edge (of the internet)“) gebracht werden. Rechenzentren auf der ganzen Welt nutzen Caching. Dabei handelt es sich um einen Prozess, bei dem vorübergehende Kopien von Dateien gespeichert werden, damit Kunden über einen Server in ihrer Nähe mithilfe eines webfähigen Geräts oder Browsers schneller auf Internetinhalte zugreifen können[5]. Zusätzlich hat ein CDN-Betreiber sicherzustellen, dass für ihn relevante Anforderungen aus dem Bereich Rechenzentrumsbetrieb und Hosting umgesetzt sind, unabhängig davon, ob Rechenzentren bzw. Hosting von ihm selbst betrieben, oder durch Rechenzentren-/Housing-Anbieter bereitgestellt werden. Weitere Informationen hierzu in Kapitel 2.

[5] Auszug aus der Beschreibung von Akamai, siehe www.akamai.com/de/our-thinking/cdn/what-is-a-cdn

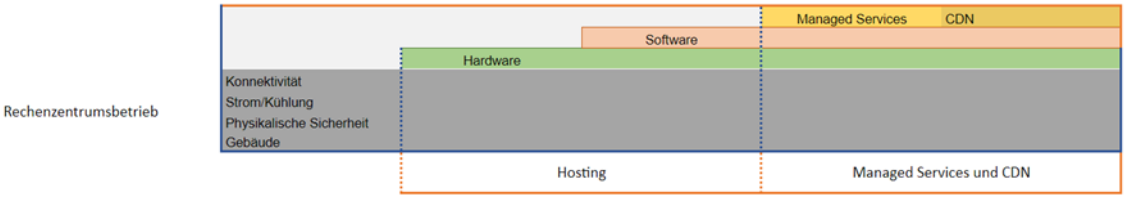

Abbildung 1: Generalistische Darstellung Housing - Hosting mit CDN

Dabei ist zwischen dem Geltungsbereich des Betreibers und dem Anwendungsbereich des B3S zu differenzieren.

Zunächst ist wichtig festzustellen, dass nur die Teile des Geschäftsbetriebs in den Geltungsbereich der Kritischen Infrastruktur fallen, die von der BSI-KritisV betroffen sind. Der Geltungsbereich der Kritischen Infrastruktur ist immer unternehmensspezifisch und muss vom jeweiligen Betreiber definiert und berücksichtigt werden. Der Anwender soll einen individuellen Geltungsbereich aus dem Anwendungsbereich des B3S herunterbrechen und auf Basis dessen seine Absicherung durchführen und begleitend dokumentieren.

Dieser B3S zielt darauf ab, diesen Geltungsbereich der Kritischen Infrastruktur für Hosting und Housing Betreiber möglichst vollständig abzudecken, dennoch muss im Rahmen der individuellen Risikobetrachtung überprüft werden, ob es Bereiche gibt, die gegebenenfalls zusätzlich zu berücksichtigen sind.

Die Überlappung des B3S mit dem Geltungsbereich der Kritischen Infrastruktur ergibt den Anwendungsbereich. Der Geltungsbereich kann unter Umständen größer als dieser Anwendungsbereich sein (siehe nachfolgende Darstellung), z. B., wenn der Betreiber mehrere unterschiedliche kDL erbringt. In diesem Fall wären ggf. weitere B3S zu anderen Sektoren erforderlich, um den Geltungsbereich voll abzudecken.

Sofern vom Anwender des Geltungsbereichs nachvollziehbar begründet, sind nicht notwendigerweise alle Aspekte dieses B3S für den ausgewiesenen Geltungsbereich relevant, beispielsweise, wenn ein Hostingbetreiber kein CDN anbietet.

Die folgende Abbildung 2 zeigt beispielhaft den *Anwendungsbereich* des B3S für ein Unternehmen als Untermenge des Geschäftsbetriebs und des Geltungsbereichs.

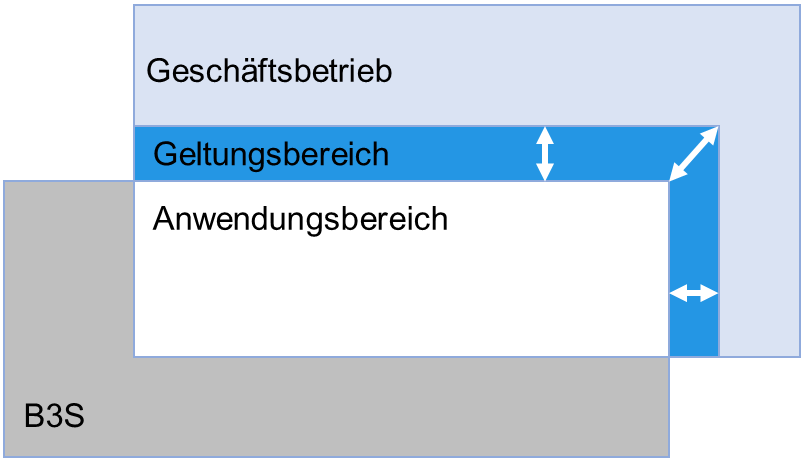

Abbildung 2: Anwendungs- und Geltungsbereich

In den Anwendungsbereich des B3S fallen auch extern erbrachte Leistungen und Kommunikationsverbindungen (siehe hierzu auch Kapitel 1.7.9).

1.3 Gesetzlicher Rahmen

Neben den Anforderungen des BSIG sind für den Bereich Housing, Hosting mit CDN allgemeine gesetzliche Vorgaben und Regelungen zu berücksichtigen, soweit sie die Erbringung der kDL beeinflussen. In Betracht kommen hier zum Beispiel Vorgaben gemäß Art. 33 EU-DSGVO, §§ 165 ff. (alt § 109) Telekommunikationsgesetz (TKG) sowie Vorgaben aus dem Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS Richtlinie)[6].

1.4 KRITIS-Schutzziele

Gemäß § 5 Absatz 1 BSI-KritisV sind kritische Dienstleistungen in der IT zu definieren als:

1. Sprach- und Datenübertragung
2. Datenspeicherung und -verarbeitung.

Im Sektor Informationstechnik und Telekommunikation sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

- den in Anhang 4 Teil 3 Spalte B der BSI-KritisV genannten Kategorien zuzuordnen sind und die für die Sprach- und Datenübertragung sowie Datenspeicherung und Datenverarbeitung in den Bereichen erforderlich sind, die in § 5 Absatz 2 und 3 BSI-KritisV genannt werden, und
- den Schwellenwert nach Anhang 4 Teil 3 Spalte D der BSI-KritisV erreichen oder überschreiten.

Die Festlegung der KRITIS-Schutzziele ist zunächst unabhängig von der benötigten IT. Der Vergleich von IT-Schutzzielen und KRITIS-Schutzzielen zeigt, dass diese im hier vorliegenden Branchenstandard nicht in allen Bereichen deckungsgleich sind.

Als IT-Schutzziel ist die allgemeine Verfügbarkeit von Rechenzentrumsleistungen mit den installierten Servern zu verstehen. KRITIS-Schutzziele sind im Housing und Hosting sowie CDN Bereich nicht nur IT-Schutzziele, beinhalten darüber hinaus auch Faktoren wie Sicherheit und Konnektivität. Siehe hierzu im Detail Kapitel 2.1.3 und 3.1.3.

Um den Schutzbedarf der in dem vorliegenden Standard betrachteten Kritischen Infrastrukturen und IT-Dienstleistungen besser zu verstehen, empfiehlt es sich, eine Trennung der Betrachtungsweise basierend auf den verschiedenen erforderlichen Strukturen und Zugangswegen vorzunehmen.

So sind einerseits die Zugangswege des Betreibers der IT-Infrastrukturen zu betrachten und zu sichern, andererseits sind ebenso die Zugriffe der Nutzer der IT-Infrastrukturen zu diesen von Bedeutung. Letztere lassen sich unter Umständen auch in verschiedene Aspekte wie Zugangswege zur Konfiguration oder Zugangswege zu den Inhalten der Dienstleistung trennen.

[6] www.bsi.bund.de/dok/9195472

1.5 Branchenspezifische Gefährdungslage

1.5.1 All-Gefahrenansatz und Relevanz von Gefährdungen

Unter „All-Gefahrenansatz“ wird verstanden, dass alle (bekannten) Gefahren gleichermaßen bewertet und dokumentiert werden. Dies ist für jeden Betreiber einer kDL verpflichtend und gilt insbesondere bei der Durchführung der Risikoanalyse. Grundlage bildet hier die Liste der elementaren Gefährdungen des BSI (siehe hierzu Anhang 4.2). Zur Orientierung können zudem die Anhänge C und D aus ISO/IEC 27005 herangezogen werden.

Im Folgenden finden sich Bedrohungsszenarien, die aus Sicht des BSI von besonderer Relevanz für die allgemeine Bedrohungslage sind. In den nachfolgenden Kapiteln Housing bzw. Hosting und CDN findet sich die jeweilige branchenspezifische Auseinandersetzung hierzu.

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

Tabelle 1: B Besonders zu berücksichtigende Bedrohungsszenarien

1.6 Risikobehandlung

1.6.1 Geeignete Behandlung aller für die kDL relevanten Risiken

Eine Risikoanalyse für die in Kapitel 1.4 genannten KRITIS Schutzziele ist unter Beachtung der in Kapitel 1.6.4 genannten Gefährdungslagen durchzuführen. Dabei können gängige Standards in der jeweils aktuell gültigen Fassung (zum Beispiel ISO/IEC 27005 oder BSI Standard 200-3) herangezogen werden. Ein Risiko gilt als abgesichert, wenn die entsprechenden technischen und organisatorischen Vorkehrungen für die kDL den Stand der Technik[7] berücksichtigen. Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die Erreichung eines allgemein hohen Schutzniveaus gesichert erscheinen lässt. Dabei soll die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert werden Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden.

[7] Stand der Technik i. S. d. Dreistufen-Theorie des BVerfG (Kalkarentscheidung) vom 8.8.1978 (BVerfGE 49, 89 [135f.])

Dies gilt in Bezug auf die betriebsrelevanten Kernprozesse und -systeme unter Berücksichtigung der KRITIS-Schutzziele und unter Berücksichtigung der Ergebnisse der Risikoanalyse.

Ziel einer Risikoanalyse ist die Identifizierung und Abschätzung von Risikobehandlungsoptionen wie: Vermeidung von Risiken, Reduzierung von Auswirkungen und Eintrittswahrscheinlichkeiten, Übertragung des Risikos (nicht möglich bei gesetzlichen Anforderungen) oder Beibehaltung (Akzeptanz). Die möglichen Behandlungsoptionen sind zu untersuchen (zum Beispiel Durchführung einer Kosten-Nutzenanalyse unter Berücksichtigung gesetzlicher und interner Anforderungen, vorzugsweise auf der Gesamtkostenanalyse über den Lebenszyklus) im Hinblick auf: Kosten, benötigte Mittel, Komplexität. Basierend auf den Behandlungsoptionen soll das Restrisiko untersucht werden. Auswirkungen und Eintrittswahrscheinlichkeit des Restrisikos sind zu untersuchen. Es ist abzuwägen, welche Gegenmaßnahmen implementiert werden. Risiken können in der Regel nur unter Berücksichtigung gesetzlicher und interne Anforderungen akzeptiert werden. Das heißt, ein Risiko muss auf ein für die kDL tragbares Maß reduziert werden. So sind Einzelfälle denkbar wie terroristische Angriffe, die grundsätzlich Restrisiken beinhalten. Diese Restrisiken sind erst dann zu akzeptieren, wenn diese durch keine weiteren Maßnahmen angemessen reduziert werden können. Andernfalls müssen Maßnahmen zum Risikotransfer eingeführt werden oder die Prozesse sind so anzupassen, dass die sich daraus resultierenden Risiken tragbar werden.

Der Umfang der erforderlichen Maßnahmen ist im Kapitel 1.6.5 detailliert beschrieben. Maßgeblich für die Behandlung relevanter Risiken ist der Anwendungsbereich dieses B3S. (siehe Kapitel 1.2)

1.6.2 Beschränkung der Behandlungsalternativen für Risiken

Eine Risikoakzeptanz ist nicht zulässig, sofern das Risiko noch angemessen reduziert werden kann. Alle für die Erbringung der kDL wesentlichen Risiken sind somit durch angemessene Maßnahmen ausreichend zu reduzieren. Eine Versicherung von Risiken ersetzt nicht die geeignete Behandlung, kann aber unter bestimmten Umständen notwendig sein.

1.6.3 Berücksichtigung von Abhängigkeiten bei der Risikoanalyse

Bei der Risikoanalyse sind alle relevanten Komponenten (siehe hierzu auch zum Beispiel Kapitel 1.2 unter **Anlagenkategorie Hosting und CDN**) zu berücksichtigen, auch wenn sie nicht unter der direkten Kontrolle des Betreibers stehen.

Für kDL relevante IT-Dienstleistungen, die von Dritten erbracht werden, müssen wirksame Verträge bzw. Dienstleistungsvereinbarungen belegbar sein, das heißt, die Verantwortung für die Umsetzung des „Stand der Technik“ verbleibt auch im Falle einer Auslagerung von Dienstleistungen beim KRITIS Betreiber. Daher sind Prüfmöglichkeiten in Abhängigkeit von der Bedeutung der jeweiligen IT-Dienstleistung als möglicher Vertragsbestandteil vorzusehen.

1.6.4 Änderung der Gefährdungslage

Die allgemeine und branchenspezifische Gefährdungslage muss mindestens durch jährliche und gegebenenfalls anlassbezogene Überprüfung, zum Beispiel im Rahmen einer Umfeldanalyse/Risikoanalyse überprüft werden. Dazu sind unter anderem die Hinweise der ENISA oder des BSI auf aktuelle Gefahrenlagen und weitere verfügbare Warnungen zu beachten.

Dabei müssen insbesondere berücksichtigt werden:

- allgemeine Bedrohungen (neu hinzugekommene Typen von Angreifern und Angriffen, intensivere Aktivität oder verbesserte Expertise oder Ressourcen von Angreifern, Neuausrichtung von Angreifern…),
- bekannt gewordene neue Schwachstellen,
- Veränderungen an der Systemarchitektur,
- anderweitige Änderungen der Exposition von für die Erbringung der kDL relevanten Informations- und Kommunikationssystemen.

1.6.5 Spezifische Maßnahmen

Gemäß § 8a Absatz 1 BSIG sind Betreiber verpflichtet, angemessene Vorkehrungen (Maßnahmen) zur Verringerung der für die kDL relevanten Risiken zu treffen.

Dabei gilt: „*Organisatorische und technische Vorkehrungen [Maßnahmen] sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht*“ (§ 8a Absatz 1 Satz 3 BSIG), siehe dazu Kapitel 1.7.

Es sind alle technischen, organisatorischen und physischen Maßnahmen anwendbar, die etwaige Risiken in geeigneter Weise reduzieren. Diese Maßnahmen sind umzusetzen und hinsichtlich ihrer Wirksamkeit zu begründen, zu dokumentieren und zu überprüfen. Dabei ist darauf zu achten, dass die zu ergreifenden Maßnahmen keine Risikoerhöhung in anderen Bereichen oder vergleichbare unerwünschte Nebeneffekte verursachen.

Gemäß § 8a Absatz 3 BSIG müssen organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit informationstechnischer Systeme, Komponenten oder Prozesse und deren Wirksamkeit im Rahmen geeigneter Audits nachgewiesen werden.

Für die Bereiche Housing, Hosting und CDN kann im Allgemeinen angenommen werden, dass die Authentizität als Integrität der Information über den Ursprung bzw., die Urheberschaft oder den Absender angesehen werden kann. Deshalb werden im Folgenden die Schutzziele Integrität und Authentizität gleichwertig behandelt. Der Betreiber der kritischen Infrastruktur muss diese Annahme für sich prüfen und gegebenenfalls die Maßnahmen zum Schutz dieser Ziele erweitern.

Eine angemessene Umsetzung der erforderlichen Maßnahmen kann durch eine ISO- oder C5-Zertifizierung unterstützt werden. So können Synergieeffekte mit bestehenden Zertifizierungen genutzt werden.

Für die Verwendung einer aktuell gültigen ISO/IEC 27001-Zertifizierung muss der Geltungsbereich und Maßnahmen geeignet sein, die jeweilige kDL ausreichend zu schützen.

So ist eine Zertifizierung der für den Betrieb der kDL relevanten IT-Systeme (siehe Kapitel 1.3) nach ISO/IEC 27001:2017[8] (auch in der Ausprägung ISO/IEC 27001:2017 auf Basis von IT-Grundschutz) grundsätzlich denkbar, wobei eine Versicherung oder Akzeptanz der Risiken über das in Kapitel 1.6.2 genannte Maß hinaus unzulässig ist.

Zur Unterstützung des Risikobehandlungsprozesses können weitere unterstützende Dokumente des BSI herangezogen werden, wie z. B.:

- IT-Grundschutz-Bausteine
- Standort-Kriterien für Rechenzentren
- RZ-Verfügbarkeitsmaßnahmen
- HV-Benchmark kompakt (als Messinstrument)

1.7 Abzudeckende Themen und Maßnahmen

Nachfolgend finden sich für alle abzudeckenden Themen solche Maßnahmen, die bei Umsetzung zur Erreichung eines angemesseneren Mindestniveaus an IT-Sicherheit geeignet sind.

Weitere Hinweise zu Maßnahmen finden sich auch in BSI-Dokument „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“[9].

1.7.1 Informations-Sicherheitsmanagement-System (ISMS)

Der Betrieb eines ISMS zum Beispiel nach ISO/IEC 27001 ist für die Absicherung der Kritischen Infrastrukturen und deren Schutzziele erforderlich. Die im ISMS definierten Prozesse und Maßnahmen müssen die in der Risikoanalyse 1.6 ermittelten Gefährdungen abdecken. Die Umsetzung der Maßnahmen und deren Wirksamkeit ist sicherzustellen.

Ein ISMS beispielsweise nach ISO/IEC 27001 ist geeignet, um die Anforderungen an ein ISMS nach § 8a Absatz 1 BSIG zu erfüllen. Wichtig dabei ist, dass der Geltungsbereich (Scope) und die Maßnahmen geeignet sind, die jeweilige Kritische Infrastruktur ausreichend zu schützen.

Die Unternehmensleitung initiiert, steuert und überwacht ein Managementsystem zur Informationssicherheit (ISMS), das sich an etablierten Standards orientiert. Bei Anwendung der ISO/IEC 2700x-Reihe muss die Erklärung zur Anwendbarkeit (Statement of Applicability) die IT-Prozesse zu Entwicklung und Betrieb der kDL umfassen.

Die hierzu eingesetzten Grundsätze, Verfahren und Maßnahmen ermöglichen eine nachvollziehbare Lenkung der folgenden Aufgaben und Aktivitäten zur dauerhaften Aufrechterhaltung der organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse zu Entwicklung und Betrieb der kDL und umfassen:

[8] Derzeit wird nachfolgend immer auf die Version ISO 27001:2017 referenziert (siehe hierzu den Hinweis in Kapitel 1.1).

[9] www.bsi.bund.de/dok/13824642

- die Planung und Durchführung des Vorhabens,
- Erfolgskontrolle beziehungsweise Überwachung der Zielerreichung und
- Beseitigung von erkannten Mängeln und Schwächen sowie kontinuierliche Verbesserung.

1.7.2 Asset Management

Ein Asset Management für die Identifikation, Klassifizierung[10] und Inventarisierung der für die kDL maßgeblichen informationstechnischen Prozesse, Systeme und Komponenten (siehe Kapitel 1.4) ist erforderlich. Ein Asset Management sollte sich mindestens an den Kriterien der ISO/IEC 27001 oder auch in der Ausprägung ISO/IEC 27001 nach IT-Grundschutz orientieren, aber es sind auch andere vergleichbare Ansätze zulässig.

1.7.3 Business Continuity Management für kDL

Für die Aufrechterhaltung der hier beschriebenen kritischen Dienstleistungen (Housing, Hosting und CDN) ist ein Business Continuity Management System (BCMS) geeignet. Dafür muss sich das BCMS an einer Norm wie zum Beispiel ISO/IEC 22301 Societal Security – Business Continuity Management Systems – Requirements oder alternativ am BSI Standard 200-4 orientieren. Dabei hat sich der PDCA Zyklus als Vorgehensmodell zur regelmäßigen Überprüfung und Verbesserung etabliert.

Es muss für die kritischen Dienstleistungen kein eigenes BCMS aufgebaut werden, wenn ein BCMS für das Unternehmen bereits besteht, dessen Geltungsbereich (Scope) die für die kDL relevanten Prozesse und Systeme umfasst.

Es ist insbesondere zu beachten:

- Die Erstellung und regelmäßige Aktualisierung eines Business Continuity Plans (BCP) zur Aufrechterhaltung der kDL entsprechend der ISO/IEC 22301
- Die Sicherstellung einer geeigneten Verzahnung des BCMs für die kDL mit dem Bereich IT-Sicherheit analog zur ISO/IEC 22301
- Die Implementierung eines Notfallmanagements in Bezug auf die Gewährleistung der kDL entsprechend der ISO/IEC 22301.

1.7.4 Technische Informationssicherheit

Für die Absicherung der Kritischen Infrastruktur ist die technische Informationssicherheit von grundlegender Bedeutung. Im Rahmen der Risikoanalyse sind dabei alle für die Kritische Infrastruktur identifizierten und relevanten Risiken entsprechend Kapitel 1.6,2.3,3.3 2.4, 3.4 und die im Kapitel 1.6.5 genannten Maßnahmenbereiche zu berücksichtigen.

[10] Klassifizierung bezieht sich auf die Kritikalität in Bezug auf die Erbringung der kDL als Ergebnis einer Risikoabschätzung.

Geeignete technische Maßnahmen sind in der ISO/IEC 27002 beschrieben und entsprechend dem Ergebnis der Risikoanalyse anzuwenden. Dabei sind die in Anhang 4.1 genannten Maßnahmen zu berücksichtigen.

Ergänzend können auch Informationen zur technischen Informationssicherheit aus dem BSI Dokument „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“ oder auch aus der TeleTrusT Handreichung „Stand der Technik in der IT-Sicherheit“ herangezogen werden.[11]

1.7.5 Personelle und organisatorische Sicherheit

Ein geeigneter Rahmen für die Behandlung der personellen und organisatorischen Sicherheit setzt sich zum Beispiel aus den folgenden Maßnahmen zusammen:

- Geeignete Auswahl von zuverlässigem und fachkundigem Personal, gegebenenfalls Sicherheitsüberprüfung oder Überprüfungen auf andere geeignete Art und Weise
- Rollenzuweisung, gegebenenfalls Festlegungen zum 4-Augen-Prinzip und ähnliches
- Identitäts- und Berechtigungsmanagement
- Festlegung notwendiger Kompetenzen (Betrieb und IT-Sicherheit)
- Notwendige / ausreichende Personalressourcen (Betrieb und IT-Sicherheit)
- Schulungen der Anwender
- Schaffung von Bewusstsein für IT-Sicherheit auf allen Ebenen (Managementebene, Geschäftsführung oder Vorstand, IT-Betrieb, Prozessverantwortlicher, Anwender)

Eine korrekte Umsetzung kann durch Einhaltung der Maßnahmen aus ISO/IEC 27001 Anhang A, Punkte A.6, A7.1, A7.2 und A.7.3 sowie A.9 erreicht werden.

1.7.6 Bauliche und physische Sicherheit

Die bauliche und physische Sicherheit (siehe hierzu auch Anhang 4.1, (Tabelle 16) spielt eine große Rolle zur Absicherung der Kritischen Infrastruktur. Entsprechende Maßnahmen sind insbesondere zu den Themenfeldern Zugangskontrolle, Notstromversorgung (USV) und Netzersatzanlagen zu treffen. Darüber hinaus sind aus einer Risikoanalyse des jeweiligen Standorts[12] und des entsprechenden Umfelds abzuleiten und ergeben sich aus einschlägigen Werken (z. B. Infrastruktur-Bausteine im IT-Grundschutz oder RZ-Verfügbarkeitsmaßnahmen des BSI[13]). Hierbei müssen insbesondere nachfolgende Aspekte berücksichtigt werden:

1. Bauliche Gegebenheiten: Bauliche Sicherheit bezüglich Fenster, Türen, Brandabschnitte, Trassenverläufe, Schutz vor Umweltereignissen, wie zum Beispiel Blitzschutz, Starkregen, Hagel.

[11] www.teletrust.de/publikationen/broschueren/stand-der-technik/

[12] siehe auch das BSI Dokument „Kriterien für die Standortwahl von Rechenzentren (RZ)“

[13] siehe BSI-Dokument „RZ-Verfügbarkeitsmaßnahmen“, www.bsi.bund.de/dok/RZ-Verfuegbarkeitsmassnahmen

2. Brandmelde- und Löschtechnik: Branderkennungssensoren (zur Brandfrühsterkennung), Brandmeldeanlage mit Aufschaltung auf die Feuerwehr, Etablierung von Abschaltfunktionen und Schadensbegrenzungsmaßnahmen.
3. Sicherheitssysteme: Zutrittskontrollanlage, mehrstufige Einbruchmeldeanlage, Kamera-Systeme, Einzäunung, Aufschaltung auf ständig besetzte Sicherheitszentrale, Schutz gegen Unbefugte und Sabotage.
4. Energieversorgung: Nach einschlägigen Normen erbrachte Installation mit Überspannungsschutz und entsprechender Notstromversorgung, zum Beispiel nach DIN EN 50600.
5. Raumlufttechnische Anlagen: Abwärme der IT-Infrastruktur und der Infrastrukturkomponenten sind durch an die jeweiligen klimatischen Gegebenheiten angepasste Kühlmechanismen gewährleistet.
6. Organisation: Sicherheitseinrichtungen werden regelmäßig geprüft, erprobt und optimiert, die regelmäßige Wartung ist durch entsprechende Pläne und Verträge sichergestellt.

Die Einhaltung der Maßnahmen aus ISO/IEC 27001:2017 Anhang A, Punkt A.11 können hier die Umsetzung unterstützen.

1.7.7 Vorfallerkennung und -bearbeitung

Betreiber Kritischer Infrastrukturen sind verpflichtet, Verantwortlichkeiten und ein Vorgehensmodell festzulegen, welche geeignet sind technische Fehler, sowie Angriffe auf die Infrastruktur zu erkennen und zu behandeln.[14]

Hierzu gehören beispielsweise folgende Maßnahmen gem. § 8a Absatz 1 und § 8b BSIG:

- Einsatz von Intrusion-Detection-Systemen (IDS) sowie Intrusion-Prevention-Systemen (IPS).
- Etablierung eines Security Incident Event Management (SIEM) Prozesses.
- Verpflichtung zur Meldung von Sicherheitsvorfällen an das BSI gemäß § 8b BSIG.
- Einsatz von qualifiziertem (internem und gegebenenfalls externem) Personal für die Bearbeitung von Sicherheitsvorfällen und eventuell notwendigen forensischen Maßnahmen (Beweissicherung, Einschaltung von Behörden).
- Dokumentation und Berichterstattung von Incidents über Sicherheitsvorfälle gemäß dem Need-to-know-Prinzip.
- Auswertung und Lernprozess („Lessons learned“).

Die ISO/IEC 27001 definiert im Anhang A, in den Punkten A 12.2. (Schutz vor Schadsoftware), A 12.4.1 (Ereignisprotokollierung), A 12.6 (Handhabung von technischen Schwachstellen) sowie A.16 (Handhabung von Informationssicherheitsvorfällen) Maßnahmen, die als Richtschnur für die Implementierung von Maßnahmen dienen können, ebenso wie die ISO/IEC 27035 (Leitfaden Störfallmanagement).

[14] siehe auch die gesetzliche Verpflichtung zur Angriffserkennung im aktuellen IT-Sicherheitsgesetz

1.7.8 Überprüfung und Übung

Um die Funktionsmäßigkeit der eingesetzten Sicherungsmaßnahmen zu überprüfen und Schwachstellen zu identifizieren, sind anlassbezogen, mindestens jedoch jährlich Überprüfungen und Übungen, bevorzugt im laufenden Betrieb oder zumindest in einer Simulations- oder Testumgebung durchzuführen (siehe auch ISO/IEC 22301).

Ferner sind anlassbezogene Prüfungen zu empfehlen, zum Beispiel aufgrund von:

- Änderungen in der Bedrohungs- oder Gefährdungslage,
- nicht zuverlässig erklärbaren Beeinträchtigungen der kDL oder der zugehörigen IT-Systeme,
- erfolgreichen oder möglicherweise erfolgreichen Angriffen,
- Änderungen an den IT- oder Kommunikationssystemen.

Darüber hinaus sind geeignete Mittel und Methoden im Rahmen von Überprüfungen und Übungen auszuwählen:

- Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen,
- Systematische Log-Auswertung,
- Interne Übungen und Systemtests,
- Übungen mit externen Partnern, insbesondere aus dem Kontext der kDL.

Außerplanmäßige Überprüfungen sind erforderlich, wenn:

- Gesetzesänderungen vorliegen, die Einfluss auf die KRITIS-Dienstleistung haben, für deren Erbringung Dienstleister einen wesentlichen Anteil beitragen.
- Neue oder veränderte Standards oder Normen Änderungen in den Vorgaben für kDL erwarten lassen.
- Neue oder bisher wenig beachtete Gefahren auftreten, die auf die kDL einen wesentlichen Einfluss haben könnten (Beispiel: Hochwasser).

Der festgestellte Änderungsbedarf ist einer Prüfung zu unterziehen, um diesen zeitgerecht und wirksam zu adressieren, zum Beispiel durch Risikominimierung, oder auch Risikominderung (Risk Mitigation). Dazu sollte im Regelfall eine Risikoanalyse zugrunde gelegt werden.

1.7.9 Lieferanten, Dienstleister und Dritte

Für den Betrieb der kDL im Bereich Housing, Hosting und CDN können für verschiedene Prozesse externe Dritte eingebunden sein.

Im Allgemeinen kann man diese unterteilen in:

1. Lieferanten bzw. Hersteller für z.B.:
    - Infrastrukturkomponenten für Elektro, Klima, Gefahrenmeldeanlagen etc.,
    - IT-Hardware,
    - Software.

2. Dienstleister, z. B.:
    - Externe Rechenzentren und technische Infrastruktur wie Netzersatzanlagen und unterbrechungsfreie Stromversorgung.
    - Wartungs- und Instandhaltungsdienste, Facility Management und Reinigungsdienste.
    - Zutrittsschutz und einschlägig geschultes bzw. erfahrenes Personal im Sicherungsdienst mit der Möglichkeit einer Einflussnahme durch Vorgaben oder einem Weisungsrecht, z. B. nach DIN 77200, sowie Monitoringsysteme wie CCTV.
3. Versorger, z. B. für:
    - Elektrizität/Energie,
    - Wasser,
    - Kraftstoffe.
4. Weitere Dritte wie z. B.:
    - Vermieter oder
    - Systemintegratoren.

Im Folgenden werden diese externen Dritten, die an sicherheitsrelevanten Stellen in Prozesse des Betreibers der kritischen Infrastruktur eingebunden sind, generell als Dienstleister bezeichnet. Alle Anforderungen gelten grundsätzlich für diese externen Dritten.

Im ersten Schritt sind diese Dienstleister für kritische Infrastrukturen sowie die Abhängigkeiten von diesen zu identifizieren und zu dokumentieren. Betreiber der Kritischen Infrastruktur sollten sicherstellen, dass sich die Leistungen ihrer Dienstleister dem aktuellen Stand der Technik orientieren. Dies könnte beispielsweise durch entsprechende vertragliche Regelungen oder Zertifizierungen erfolgen. Sie sind in gleicher Weise dafür verantwortlich, dass angemessene Vorkehrungen getroffen werden wie bei internen Prozessen. Hieraus ergeben sich vielfältige Anforderungen an die Ausgestaltung der Beziehung, insbesondere bei der Festlegung von angemessenen Sicherheitsvorkehrungen und der regelmäßigen Überprüfung durch den Betreiber. Dabei sind verpflichtend die Bereiche zu betrachten, die wesentlich für den Betrieb der kritischen Anlage sind. Zur Überprüfung von entsprechenden Nachweisen sollten Auditrechte vereinbart werden. Zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen bei Lieferanten und Herstellern sollten die „Best-Practice-Empfehlungen für Anforderungen an Lieferanten und Hersteller berücksichtigt werden[15].

Richtlinien und Anweisungen zur Sicherstellung des Schutzes von Informationen (insbesondere deren Verfügbarkeit) müssen gemäß einer IT-Informationssicherheitsrichtlinie dokumentiert, kommuniziert und bereitgestellt werden und kann zum Beispiel in Form von vertraglichen Regelungen wie durch SLAs oder AGB erfolgen.

Die Vorgaben dienen der Reduzierung von Risiken, die durch die Auslagerung von IT-Systemen entstehen können. Dabei sind mindestens die folgenden Aspekte zu berücksichtigen:

[15] www.bsi.bund.de/dok/upk-anforderungen-lieferanten

- Definition und Beschreibung von Mindest-Sicherheitsanforderungen in Bezug auf die verarbeiteten Informationen, die sich an etablierten Informationssicherheitsstandards orientieren.
- Anforderungen an das Incident- und Vulnerability-Management (insbesondere Benachrichtigungen und Kollaborationen während einer Störungsbehebung).
- Weitergabe und vertragliche Verpflichtung auf die Mindest-Sicherheitsanforderungen auch an Unterauftragnehmer, außer wenn diese nur unwesentliche Teile zu Entwicklung oder Betrieb der kDL beitragen.

Die Definition der Anforderungen ist in das Risikomanagement des KRITIS-Betreibers einzubinden und muss anlassbezogen, mindestens jedoch einmal jährlich auf ihre Angemessenheit hinüberprüft werden. Die Risikobewertung für die verschiedenen Bereiche wird in den Kapiteln Housing beziehungsweise Hosting und CDN näher beschrieben.

Verfahren zur regelmäßigen Überwachung und Überprüfung der vereinbarten Leistungen und Sicherheitsanforderungen von Dritten sind erforderlich. Die Überprüfung kann dabei analog zu folgenden Normen erfolgen:

- ISO/IEC 27001 Anhang A15 zum Thema „Lieferantenbeziehungen“.
- ISO/IEC 22301 Ziffern:
    - 8.2 (Business-Impact-Analyse und Risikobeurteilung),
    - 8.3 (Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit),
    - 9.3 (Managementbewertung).

Beispiele für konkrete Überprüfungsmaßnahmen sind Self-Assessments, Eingangsprüfungen, Sicherheitstests, Sicherheits- und Qualitätszertifikate, aber auch die Überprüfung von sicherheitsrelevanten Vorfällen, Betriebsstörungen oder Ausfällen und Unterbrechungen, die mit der Dienstleistung zusammenhängen.

1.7.10 Branchenspezifische Technik

Für die Bereiche Housing, Hosting und CDN gibt es branchenspezifische Technik für Beschaffung, Entwicklung, Einsatz, Betrieb und Wartung, die in dem jeweiligen Kapitel näher beschrieben wird.

1.7.11 Externe Informationsversorgung und Unterstützung

Die Betreiber sind verpflichtet, sich die erforderlichen Informationen zur Aufrechterhaltung und stetigen Verbesserung ihrer Sicherheitsniveaus im Allgemeinen wie auch über aktuelle Entwicklungen der für sie relevanten IT-Sicherheitslage zu beschaffen und sich zum Beispiel mit anderen Dienstleistern, dem BSI und Behörden, wie dem BKA, LKA, örtliche Feuerwehren oder dem DWD regelmäßig über die Gefahrenlage auszutauschen (analog dem Anhang 6.1 zur ISO/IEC 27001:2017 zum Thema „Kontakt mit Behörden“ und „Kontakt mit speziellen Interessensgruppen“).

2 Housing

Unter Housing wird die Unterbringung von (IT-)Hardware in einem Rechenzentrum und Zurverfügungstellung aller zum Betrieb nötigen Betriebsmittel verstanden. Bei Housing werden im Gegensatz zu Hosting keine Daten der Kunden gespeichert und/oder verarbeitet (abgesehen von Kundendaten, die im Zusammenhang mit Verträgen vorliegen). Hierbei stellt die EN 50600 eine gute Quelle für Sicherheitsanforderungen im Housing Bereich dar.

2.1 Anwendungsbereich und Schutzziele Housing

2.1.1 Anwendungsbereich Housing

Der Anwendungsbereich für Housing umfasst die Leistungen, die mit der Bereitstellung von Rechenzentrumsflächen für Kunden in Zusammenhang stehen. Das sind:

- Rechenzentrumsfläche (Gebäude bzw. Campus).
- Strom, zum Beispiel Transformatoren, Netzersatzanlagen, Generatoren, unterbrechungsfreie Stromversorgung inkl. Batterien.
- Kühlung, zum Beispiel Freikühler, adiabatische Kühler und Maßnahmen wie Kaltgang- oder Warmgangeinhausung und Optimierung der Luftzirkulation.
- Konnektivität, zum Beispiel das Anbieten von Internetanbindungen.
- Technische und organisatorische Maßnahmen zur physischen Sicherheit. Am Beispiel Zutrittsschutz bedeutet das:
    - Einsatz von Wachpersonal,
    - Einbruchmeldeanlagen (EMA),
    - Definition und Durchsetzung der Zutrittsregeln,
    - Einsatz entsprechender Systeme wie Vereinzelungsanlagen, Kartenleser und biometrische Zutrittskontrolle,
    - Videoüberwachungssystem.
- IT-Systeme zur Steuerung und Überwachung der Rechenzentren (zum Beispiel Gebäudeleittechnik).
- Brandschutz (Brandmelde- und Löschsysteme).
- Extern erbrachte Dienstleistungen wie Wartung oder Reparatur der Systeme.
- Verkabelungsinfrastruktur bis zum öffentlichen Netz (Grundstücksgrenze des Rechenzentrums).

Als Kritische Infrastruktur im Sinne der BSI-KritisV gelten Rechenzentren ab dem in der BSI-KritisV festgelegten Schwellenwert. Stand August 2021 sind dies 3,5 MW vertraglich vereinbarter Leistung. Ein Campus mit unterschiedlichen Einheiten wird für die Betrachtung des Schwellenwertes als ein Rechenzentrum im Sinne einer gemeinsamen Anlage definiert.

2.1.2 Anforderungen an die Darstellung des Geltungsbereichs und des Netzplans

Folgende Punkte sind textuell zu beschreiben und geeignet im angepassten Netzplan grafisch darzustellen[16]:

- Realisierung der Versorgung mit Strom, IT-Netz und Internet für das Housing (als Dienstleistung im Sinne des Bereichs der kDL gemäß BSI-KritisV) in der Anlage.
- Realisierung der Kühlung, insbesondere im Zusammenspiel der Kühl- und Steuerungssysteme.
- Realisierung der Betriebssicherheit, insbesondere in Bezug auf Brandvermeidung und Löschanlagen, USV und Notstromversorgung sowie Meldesysteme und technisches Monitoring.
- Realisierung der Zutritts-, Zugangs- und Zugriffssicherheit, unter Berücksichtigung der dazu erforderlichen Steuerungssysteme und Schnittstellen.
- Realisierung der Trennung der Betriebssysteme zu Kundensystemen.
- Realisierung des Kundenmanagements für das Housing, insbesondere hinsichtlich des externen IT-Zugriffs auf die Kundenmanagementsysteme und unterstützenden IT-Ressourcen sowie des Zugriffs auf Verwaltungs- und Steuerungssysteme.
- Realisierung der Mandantentrennung für das Housing, insbesondere hinsichtlich der physischen Trennung der Kundensysteme, der Zugangssicherung und der Trennung bei gemeinsam genutzten IT-Ressourcen.
- Darstellung von Schnittstellen bzw. Abhängigkeiten von Systemen untereinander sowie gegebenenfalls von ausgelagerten Teilen sofern für den Betrieb der Kritischen Infrastruktur relevant.

Zusätzliche Anforderungen bei aus mehreren Gebäuden bestehenden Anlagen (Campus)

Die Bestandteile eines Rechenzentrums können auf mehrere Gebäude oder andere Anlagenteile (zum Beispiel externe Notstrom-Generatoren) innerhalb eines Campus aufgeteilt sein. Um die verschiedenen Abstraktionsebenen nachvollziehbar darzustellen, ist zusätzlich eine kurze Beschreibung und grafische Darstellung des Campus in Form eines Anlagenplans zu empfehlen. Im Anlagenplan[17] sind die Anlagenteile und Komponenten, die den Betrieb der Kritischen Infrastruktur direkt oder indirekt unterstützen und deren Abhängigkeiten, kenntlich zu machen. Daraus muss klar erkennbar sein:

- Die Aufteilung der Funktionen auf die jeweiligen Gebäude(-teile) / Anlagenteile des Campus.
- Die gemeinsam genutzten Betriebseinrichtungen.

[16] Details auf Seite 9 in „Anforderungen gemäß § 8a Abs. 5 BSIG „Validierung und Darstellung eines Geltungsbereichs für Kritische Infrastrukturen der Anlagenkategorie „2.1.1 Rechenzentrum“ nach Anhang 4, Teil 3 BSI-KritisV“ Stand: 22.04.2020 www.bsi.bund.de/dok/8a5-rz

[17] Details auf Seiten 10, 11 in „Anforderungen gemäß § 8a Abs. 5 BSIG „Validierung und Darstellung eines Geltungsbereichs für Kritische Infrastrukturen der Anlagenkategorie „2.1.1 Rechenzentrum“ nach Anhang 4, Teil 3 BSI-KritisV“ Stand: 22.04.2020 www.bsi.bund.de/dok/8a5-rz

- Die physischen (Leitungen) Verbindungen der Gebäude(-teile)/Anlagenteile untereinander.
- Die Zuordnung der Funktionen (Zwecke) auf die jeweiligen Verbindungen. Die Darstellung soll sich auf einer höheren Abstraktionsebene als in 1.6.1 bewegen.

Ein unverbindliches Beispiel für eine grafische Darstellung ist im Folgenden enthalten.

In Abbildung 3 und Abbildung 4 sind Kundenverantwortungsbereiche und die Verantwortungsbereiche des Housing-Betreibers entsprechend der Querschnittsaufgaben - gemäß Anforderungen in § 8a Absatz 5 BSIG „Validierung und Darstellung eines Geltungsbereichs für Kritische Infrastrukturen“ der Anlagenkategorie „2.1.1 Rechenzentrum“ nach Anhang 4, Teil 3 BSI-KritisV“ - wie folgt dargestellt. Die Querschnittsaufgaben des Housing-Betreibers beinhalten unter anderem:

- Versorgung (wie bspw. Strom-, IT-Netz- und Internetversorgung),
- Kühlung,
- Betriebssicherheit sowie Zutritts-, Zugangs- und Zugriffssicherheit,
- Kunden- beziehungsweise Mandantentrennung.

Sie sind üblicherweise Bestandteil jedes einzelnen Rechenzentrums und zur Sicherstellung der kDL über Firewall vom Kundenportal abgetrennt. Dabei ist realitätsgetreu darzustellen, ob und inwiefern Querschnittsaufgaben des Rechenzentrums über das Kundenportal beeinflusst werden können. Beispielsweise könnte dargestellt werden, ob entweder nur lesend zugegriffen wird oder Aufträge über das Kundenportal erteilt werden.

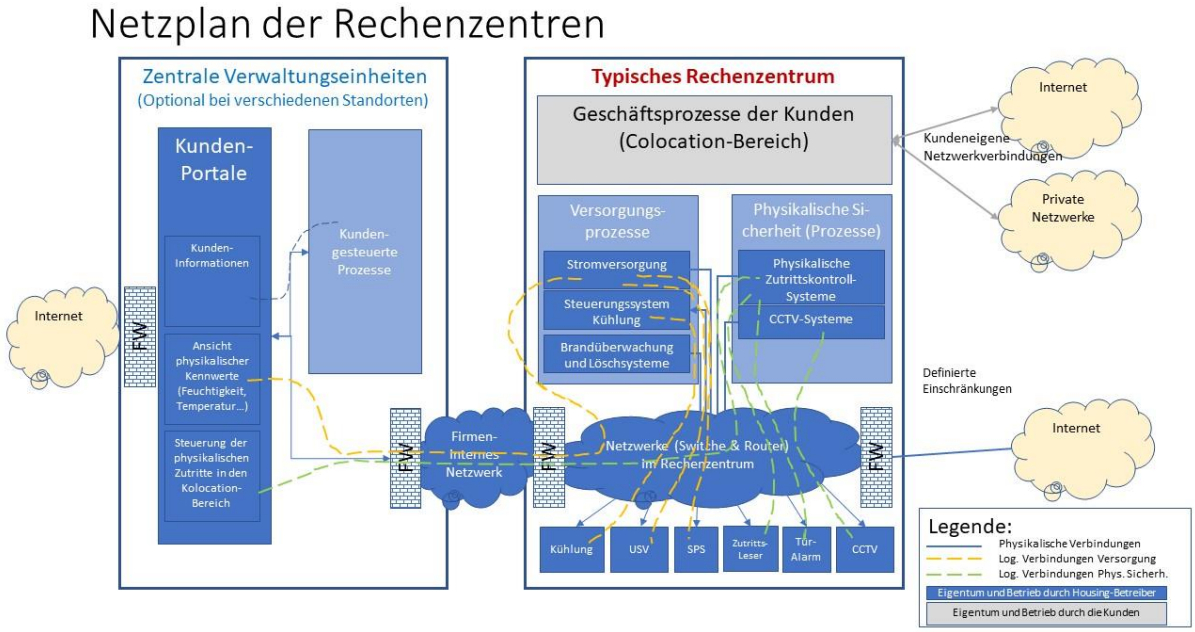

Abbildung 3: Beispiel Netzplan für Rechenzentrum

Hinweis zum Netzplan

Bei den Abbildungen handelt es sich um abstrakte Darstellung, die bei Anwendung des B3S durch den Betreiber in Form eines konkreten Netzstrukturplans weiter auszuführen sind. So sind z. B. physische Standorte, Systembezeichnungen, Schnittstellen darzustellen, um der Komplexität der eigenen Umgebung gerecht zu werden.

Zusätzliche Anforderungen bei räumlich getrennten gemeinsamen Anlagen

Im Fall einer gemeinsamen Anlage, deren Rechenzentren nicht innerhalb desselben Campus liegen, ist der Dokumentation zusätzlich eine kurze Beschreibung und grafische Darstellung der gemeinsamen Anlage in Form eines Anlagenplans hinzuzufügen. Im Anlagenplan sind die Anlagenteile und Komponenten, die den Betrieb der Kritischen Infrastruktur direkt oder indirekt unterstützen und deren Abhängigkeiten, kenntlich zu machen. Daraus muss klar erkennbar sein:

- Die geographische Verteilung der Rechenzentren.
- Die geographische Verteilung der gemeinsam genutzten Betriebseinrichtungen und deren jeweilige Funktion.
- Die physischen (Leitungen) Verbindungen der Gebäude(-teile) und Anlagenteile untereinander.
- Die Zuordnung der Funktionen (Zwecke) auf die jeweiligen Verbindungen.
- Es ist zu beschreiben, dass bzw. wie eine Mandantentrennung im Kundenmanagement gewährleistet ist.

2.1.3 Schutzziele der kDL und betriebsrelevanter Systeme Housing

Aus Schutzzielen sind für die jeweiligen Systeme die erforderlichen Schutzbedarfe zu ermitteln. Anschließend sind für die Systeme basierend auf dem Schutzbedarf Anforderungen und Maßnahmen zu definieren. Im späteren SOLL-IST-Abgleich ist zu prüfen, ob die bereits ergriffenen Maßnahmen die Schutzbedarfe sicherstellen.

Die wesentlichen KRITIS-Schutzziele im Bereich Housing sind, wie bereits im Kapitel 1.4 allgemein beschrieben:

- Sicherstellen von passenden Räumlichkeiten zum sicheren Betrieb von IT-Systemen. Dazu gehören geeignete Umgebungsbedingungen wie Temperatur und Feuchtigkeit.
- Sicherstellen einer definierten Verfügbarkeit und Qualität von Strom und Kühlung von mindestens 24 Stunden.
- Sicherstellen, dass an allen Orten im Rechenzentrum nur berechtigte Personen Zutritt haben
- Sicherstellen, dass Kunden entsprechend der vertraglichen Vereinbarung Zugang zu ihrer IT gewährt wird.

Der B3S bezieht sich auf die betriebsrelevanten IT-Systeme, die zum Betrieb der Kritischen Infrastruktur in der Anlagenkategorie „Rechenzentrum“ erforderlich sind.

Generell sind zwei Varianten an Abhängigkeiten von der GLT und die Möglichkeit einer manuellen Steuerung zu unterscheiden, auf die im nachfolgenden Kapitel 2.2 näher eingegangen wird.

Die im Folgenden genannten IT-Systeme und digitalen Steuerungssysteme sind dann relevante Anlagen, wenn deren Ausfall den Betrieb der kDL derart beeinträchtigt, dass die kDL nicht mehr in Gänze oder teilweise erbracht werden kann. Dies gilt auch für „wesentliche Bestandteile“ der Anlagen zur Erbringung der kDL im Sinne von § 93 BGB.

Nicht betriebsrelevant sind:

- IT-Systeme, deren Ausfall keine Auswirkung auf den Betrieb haben
- Netzanbindung zu den Anbietern von Datennetzen (Provider), soweit diese nicht von den betriebsrelevanten Systemen genutzt werden (zum Beispiel Internet für Office-Nutzung)
- IT-Systeme, die nicht direkt den Betrieb der kDL beeinflussen können (zum Beispiel ERP-Systeme, Office-E-Mail-Systeme)
- IT-Systeme der Kunden, einschließlich der dazu gehörenden vom Kunden oder seinen Beauftragten administrierten Netze

Netze und Netzwerkverbindungen zum Kunden sind nicht kritisch im Sinne des BSIG, da sie nicht zum originären Geschäft des Housing-Anbieters gehören und nicht gemanagt beziehungsweise überwacht werden.

Der Betreiber ist verpflichtet zu überprüfen, ob es Abweichungen beziehungsweise weitere für den Betrieb benötigte und relevante Systeme gibt.

2.2 IT-Schutzbedarfe Housing

Die IT-Schutzbedarfe leiten sich aus den IT-Schutzzielen ab.

Es muss gewährleistet sein, dass die IT-Infrastruktur zum Erbringen der Dienstleistung Datacenter/Housing durch den Anbieter entsprechend physisch abgesichert, verfügbar sowie gegen unautorisierte Benutzung oder Änderung geschützt ist. Ebenso muss der Anbieter sicherstellen, dass sein eigener Zugang und Umgang mit diesen Systemen sicher und auf entsprechenden Standards basierend durchgeführt werden, die dem jeweiligen Schutzbedarf entsprechen.

Dem gegenüber steht der Zugang, welcher dem Datacenter/Housing Kunden ermöglicht, zu seinen Systemen zu gelangen. Hier hat der Anbieter die Aufgabe, geeignete Maßnahmen zu implementieren, um diesen Zugang nur autorisiert und geschützt zur Verfügung zu stellen.

Die folgende Darstellung in Abbildung 4 zeigt diese Zusammenhänge schematisch:

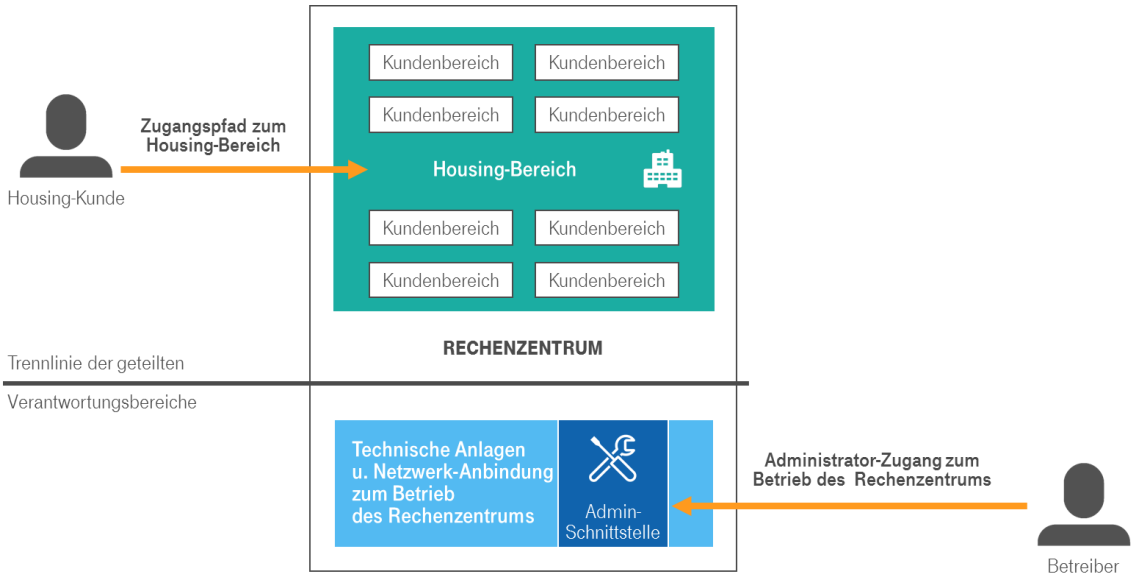

Abbildung 4: Trennung der Verantwortungsbereiche Datacenter und Housing

Abbildung 4 zeigt die Trennung der Verantwortung beim Housing. Der Betreiber der Dienstleistung Datacenter/Housing stellt den physischen Rahmen zur Verfügung, inklusive der Energieversorgung, der Klimatisierung, der Konnektivität, der Sicherheitsdienste (samt Branderkennungssystemen), der Monitoring-Systeme des Housing-Betreibers sowie der Zutrittssysteme. Der Nutzer dieses physischen Rahmens betreibt die IT-Systeme, welche in diesem Rahmen installiert werden. Der Betreiber der Dienstleistung Datacenter/Housing hat weder Einfluss auf die IT-Verfahren noch Zugriff auf die darin genutzten Daten seiner Kunden.

Der hier vorliegende Standard beschreibt daher die Sicherung der IT-Systeme zum Betrieb der rein physischen Infrastruktur Datacenter/Housing und zum anderen das Sicherstellen des Zugangs der jeweiligen Kunden zu ihren Systemen.

An folgenden zwei Varianten soll beispielhaft aufgezeigt werden, wie die Automatisierung von GLT Einfluss bei der Betrachtung auf den Schutzbedarf hat.

Variante A:

Alle wesentlichen Systeme des Rechenzentrums sind durchgängig autonom konzipiert und können auch von Hand gesteuert werden. Sie sind nicht voneinander abhängig. Daher sind diese auch ohne Gebäudeleittechnik (GLT) funktionsfähig, weil alle betrieblichen Systeme autonom und dezentral geregelt werden können.

Die Wahrscheinlichkeit eines Ausfalls der GLT ist in diesem Fall geringer als in Variante B. Das heißt, einen speziellen Schutzbedarf für Risiken, die von außen in das Rechenzentrum gelangen gibt es in diesem Fall zwar nicht durch die IT-Manipulation durch Dritte, denkbar sind jedoch Sabotagefälle z. B. durch Innentäter, die auch durch Personal nicht kompensiert werden können. Es verbleiben damit immer ein Risiko durch Innentäter, die individuell zu betrachten sind.

Variante B:

Wesentliche Teile des Rechenzentrums werden durch die GLT ohne manuelle Interaktion unmittelbar oder auch über abgesicherte Verbindungen ferngesteuert. Hier könnte das Rechenzentrum bei einem Ausfall der GLT nicht mehr beziehungsweise nur noch eingeschränkt funktionieren, weil die betrieblichen Systeme zentral gesteuert werden.

Ein Ausfall der GLT kann in diesem Fall dazu führen, dass die Funktionsfähigkeit der kDL erheblich beeinträchtigt wird. Es liegt also ein Schutzbedarf vor.

Für die betriebsrelevanten IT-Systeme werden folgende allgemeine Schutzziele analog ISO/IEC 27001 in der aktuellen Fassung definiert:

- **Vertraulichkeit**
    - Bei hohem Schutzbedarf kann die Vertraulichkeit beispielsweise durch eine 2-Faktor Authentifizierung gesteigert werden. So kann die Berechtigung besser sichergestellt werden.
- **Integrität und Authentizität**
    - Die Integrität und Authentizität der Daten innerhalb der GLT ist in Variante B von hoher Bedeutung, weil die absichtliche oder versehentliche Veränderung (Beeinträchtigung der Integrität) oder Vortäuschung (fehlende Authentizität) insbesondere von Zugangsdaten für einen Angriff ausgenutzt werden und zu einem weitgehenden Ausfall der kDL führen könnte.
- **Verfügbarkeit**
    - Je nach Aufbau des Rechenzentrums beziehungsweise je nach Implementierung der überwachenden Systeme ist die Verfügbarkeit unterschiedlich zu bewerten.

Die folgende Tabelle bewertet die Kritikalität der jeweiligen IT-Systeme für die Erbringung der kDL. Die hier beschriebene Schutzbedarfsfeststellung ist beispielhaft und dient lediglich zur Orientierung bzw. Erläuterung. Der Anwender ist in der Pflicht, die Schutzbedarfsklassen ggf. eigenständig zu definieren und die Schutzbedarfe zu erheben und zu dokumentieren. Der Anwender muss überprüfen, ob es aufgrund seiner individuellen Ausgestaltung der kDL Bereiche gibt, die einen höheren Schutzbedarf als in der Tabelle genannt haben. Dabei kann es zu Abweichungen zu den hier im B3S genannten Beispielen kommen.

- **Einstufung „normal“:**

Beispiel Schutzziel ist die Sicherstellung der Housing Einrichtung vor physikalischer Vernichtung, um die Daten von Kunden zu schützen. Hierzu gibt es zum Beispiel den Schutzbedarf „Schutz vor Brandschäden“. Eine Maßnahme hierzu ist der Einsatz von Brandmeldeanlagen, um beim Eintritt eines Feuers rechtzeitig reagieren zu können. Funktioniert die Brandmeldeanlage nicht oder nicht vollständig, ist dennoch die Erkennung eines Brandes möglich, indem mindestens zwei Verfahren zur Branderkennung eingesetzt werden. So kann zum Beispiel durch den Einsatz von Rauchmeldern und Temperaturfühlern eine Warnung sichergestellt werden, falls ein Erkennungssystem ausfällt. In diesem Fall kann entsprechend qualifiziertes, eventuell auch aus der Bereitschaft hinzugezogenes Personal grundsätzlich gewährleisten, dass der Weiterbetrieb des Housings nicht unmittelbar gefährdet wird. Zur Sicherstellung der Verfügbarkeit an Personal sind entsprechende Business Continuity Pläne vorzuhalten.

- **Einstufung „hoch“:**

Wenn zum Beispiel die Integrität eines Steuerungssystems der GLT in Variante B verletzt ist, besteht eine unmittelbare Gefahr für die Erbringung der kDL, da ein Angreifer direkt den Betrieb beeinflussen kann.

Schutzziele der betriebsrelevanten IT-Systeme	**Gebäudeleittechnik (GLT)**	**Brandmeldetechnik**	**Überwachung (Video, Bewegungsmelder)**	**Zutrittsmanagement**
Vertraulichkeit	normal	normal	normal	normal
Integrität und Authentizität	normal	normal	normal	hoch
Verfügbarkeit	normal	normal	normal	normal

Tabelle 2: Kritikalität der IT-Systeme (Housing), Variante A

Schutzziele der betriebsrelevanten IT-Systeme	**Gebäudeleittechnik (GLT)**	**Brandmeldetechnik**	**Überwachung (Video, Bewegungsmelder)**	**Zutrittsmanagement**
Vertraulichkeit	hoch	normal	normal	normal
Integrität und Authentizität	hoch	normal	normal	hoch
Verfügbarkeit	hoch	normal	normal	normal

Tabelle 3: Kritikalität der IT-Systeme (Housing), Variante B

2.3 Branchenspezifische Gefährdungslage

Der All-Gefahrenansatz (Naturereignisse, technisches beziehungsweise menschliches Versagen, Terrorismus, Kriminalität, Krieg) ist für jeden Betreiber einer kDL zugrunde zu legen. Die Risikobewertung muss regelmäßig (zum Beispiel jährlich) sowie anlassbezogen wiederholt werden.

2.3.1 Branchenspezifische Relevanz und Benennung von Szenarien

Für den Bereich Housing sind insbesondere die folgenden spezifischen Bedrohungsszenarien zu betrachten, die alle mit der physischen Sicherheit zu tun haben:

Nr.	**Maßnahme**
A 8.1	Zugangskontrolle
A 8.2	Notstromversorgung (USV)
A 8.3	Netzersatzanlagen

Tabelle 4: A 8 Bauliche/physische Sicherheit

Folgende weitere Szenarien sind zusätzlich Housing-spezifisch zu betrachten:

- Ausfall der für den Betrieb der kDL relevanten IT-Systeme (gemäß Kapitel 1.2), soweit dieser Ausfall nicht durch geeignete Redundanz-Maßnahmen aufgefangen wird.
- Cyber-Angriff auf die für den Betrieb der kDL relevanten IT-Systeme (siehe oben),
- Ausfall von Mitarbeitern, zum Beispiel durch Pandemie, Streik oder ähnliches.

Darüber hinaus könnten, sofern Auswirkungen auf die kDL möglich sind, weitere Szenarien im Housing Bereich relevant sein:

- **Zero-Day Schwachstellen:**
  - Das Ausnutzung von Zero-Day Schwachstellen kann typischerweise nicht ursächlich verhindert werden und muss daher durch andere Maßnahmen kompensiert werden (beispielsweise Grundhärtung und Überwachung von Infrastruktur und Diensten, sofern diese im Housing Bereich betroffen sind).
  - Kennung aus dem IT-Grundschutz: G 0.28, G 0.30
- **Schadsoftware in E-Mail-Anhängen:**
  - Phishing Angriffe (undifferenziert oder zielgerichtet) bedienen sich oft E-Mails als Angriffsvektor, um Schadsoftware direkt (bspw. Dokumente mit Makro-Viren) oder über Downloadlinks zur Ausführung zu bringen. Typische Abwehrmaßnahmen sind Malware-Erkennung in den E-Mail-Systemen und Mitarbeitersensibilisierung (sofern der Housing Bereich betroffen ist).
  - Kennung aus dem IT-Grundschutz: G 0.21, G 0.39, G 0.42
- **Advanced Persistent Threat (APT) Angriffe:**
  - Dies sind Cyber-Angriffe auf die für den Betrieb der kDL relevanten IT-Systeme oder aber auf IT-Systeme oder Services der kDL selbst. So kann direkt oder durch erst später folgende Angriffe (Backdoor) Schaden verursacht werden. Zur Abwehr ist eine Sicherheitsüberwachung und ein aktives Management von Sicherheitsvorfällen essenziell (sofern der Housing Bereich betroffen ist).
  - Kennung aus dem IT-Grundschutz: G 0.14, G 0.21, G 0.23, G 0.39, G 0.42, G 0.45, G 0.46
- **Ransomware:**
  - Angreifer übernehmen über Erpressungstrojaner die Kontrolle über Daten (Verschlüsselung) und Systeme (Zugriffsberechtigung). Vorbeugende Maßnahmen sind zuverlässige Datensicherungen, aktives Patchmanagement und Systemhärtung (sofern der Housing Bereich betroffen ist).
  - Kennung aus dem IT-Grundschutz: G 0.17, G 0.25, G 0.42, G 0.45, G 0.46

- **Daten-Exfiltration:**
  - Dies bezeichnet den nicht autorisierten Transfer von Daten in den Zugriffsbereich eines Angreifers. Als Gegenmaßnahmen greifen strikte logische und physische Zugriffskontrollen (sofern der Housing Bereich betroffen ist).
  - Kennung aus dem IT-Grundschutz: G 0.15, G 0.19, G 0.32, G 0.45, G 0.46

2.3.2 Benennung der Bedrohungen und Schwachstellen

Eine Risikoanalyse für die in Kapitel 2.1.3 genannten KRITIS Schutzziele ist unter Beachtung der in Kapitel 1.5, Kapitel 2.3.1 und Kapitel 2.4.2 genannten Gefährdungslage durchzuführen. Dabei können gängige Standards (zum Beispiel ISO/IEC 27005 oder BSI Standard 200-3) herangezogen werden.

Neben den in Kapitel 2.3.1 beschriebenen Angriffsszenarien wird ferner auf Kapitel 2.4.2 verwiesen.

Im Kapitel 5 (Anhang 5.1) der BSI Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG wird – beispielhaft zu den elementaren Gefährdungen[18] - der potenzielle Einfluss auf die Kritische Infrastruktur aufgezeigt und generelle Sicherheitsmaßnahmen zur Risikoreduktion gegenübergestellt. Konkrete Maßnahmen finden sich unter anderem in Industriestandards wie ISO/IEC 27001, BSI IT-Grundschutz, C5 (Cloud Computing Compliance Criteria Catalogue) und so weiter. Die genaue Bewertung und Ausgestaltung dieser Maßnahmen muss in Bezug zu den Schutzzielen der Systeme zum Betrieb der Kritischen Infrastruktur und auch der Systeme der kDL erfolgen.

Unter Gefährdung bzw. Risiko ist mindestens folgendes zu verstehen:

Gefährdung bzw. Risiko

=

Eintrittswahrscheinlichkeit x Fehlerfolge

Es gibt allerdings auch erweiterte Methoden, um Risiken zu beschreiben, die gleichermaßen verwendet werden können.

Jedes erkannte Risiko ist in seiner Bedeutung für die jeweilige Anlage zu bewerten und aufzuführen, welche Maßnahmen getroffen werden, um das Risiko auf ein akzeptables Niveau zu bringen.

[18] BSI: Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG, (Version 1.1 vom 01.09.2021, im Anhang 5.1)

2.4 Risikobehandlung Housing

Es liegt in der Verantwortung des Betreibers der kDL, anhand der elementaren Gefährdungen und ihrer dargestellten Relevanz für den Bereich Housing eine Risikobetrachtung anhand des All-Gefahrenansatzes durchzuführen. Dabei sind insbesondere die elementaren und relevanten Gefährdungen für Housing zu berücksichtigen. Dies muss unter Berücksichtigung der individuellen Assets sowie ihren Einfluss auf die kDL und der Eintrittswahrscheinlichkeit der Gefährdung erfolgen.

Die Mitigation der Risiken erfolgt durch die Auswahl und Implementierung geeigneter Maßnahmen. Neben den im oberen Teil generellen zu beachtenden Punkten gibt es für den Bereich Housing spezifische Anforderungen. Diese sind im Folgenden beschrieben.

2.4.1 Abgrenzung der zu betrachtenden Risiken

Eine Geschäftsrisikoanalyse ist nicht Bestandteil einer Gefährdungsanalyse in Bezug auf Housing-Leistungen. Aus diesem Grund hat diese nicht zu erfolgen, da die Geschäftsrisiken durch die Kunden zu betrachten sind. Bei den Risiken, die von Housing Unternehmen zu prüfen sind, handelt es sich um die Gefahren, die Einfluss auf die oben aufgeführten Schutzziele haben.

Risikogruppen an verschiedenen Beispielen:

- Technische Risiken: Zutrittssystem: mögliche Lösung durch Personaleinsatz.
- Bauliche Risiken: Infrastruktur ist veraltet. Gebäude ist so aufgebaut, dass bei einem Ausfall des Zutrittssystems sehr viel Personal benötigt wird.
- Organisatorische und personelle Risiken: Bei einem Ausfall ist sichergestellt, dass ausreichend Personal zur Verfügung steht (Stellvertreterregelung, Pandemie).
- Umfeld- und Umweltrisiken: Überschwemmung, Erdbeben, Bombenfund.

2.4.2 Risiken und Bedrohungen im Zusammenhang mit den Schutzzielen von spezifischer Technik für Housing

Es liegt in der Verantwortung des Betreibers der kDL, anhand des All-Gefahrenansatzes der elementaren Gefährdungen und ihrer dargestellten Relevanz für den Bereich Housing eine Risikobetrachtung vorzunehmen. Diese muss u. a. folgende Bestandteile berücksichtigen: betroffene Assets sowie deren Einfluss auf die kDL nebst Eintrittswahrscheinlichkeit der Gefährdung.

2.4.3 Übersicht der zu betrachtenden Risiken

Gemäß dem All-Gefahrenansatz sind alle Gefährdungen zu berücksichtigen. Im Folgenden findet sich eine Übersicht branchenspezifischer Gefährdungen. Punkte, die einer genaueren Betrachtung bedürfen, weil sie für Housing von besonderer Relevanz sind (zum Beispiel, weil es sich um typische Kundenanforderungen handelt), werden mit „X“ markiert. Sind diese Aspekte jedoch nur unter bestimmten Bedingungen relevant, wird das „X“ in Klammern gesetzt.

Nr.	KRITIS-relevante elementare Gefährdung (Risiko)	Besondere Relevanz	Erklärung Relevanz
G 0.1	Feuer	X	Physische Sicherheit
G 0.2	Ungünstige klimatische Bedingungen	X	SLA (Temperaturvorgaben)
G 0.3	Wasser	X	SLA (Physikalische Sicherheit)
G 0.4	Verschmutzung, Staub, Korrosion	X	SLA (Physikalische Sicherheit)
G 0.5	Naturkatastrophen	X	SLA (Physikalische Sicherheit)
G 0.6	Katastrophen im Umfeld	X	SLA (Physikalische Sicherheit)
G 0.7	Großereignisse im Umfeld	X	SLA (Physikalische Sicherheit)
G 0.8	Ausfall oder Störung der Stromversorgung	X	SLA (Energieversorgung)
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	(X)	Innerhalb des Gebäudes oder auf dem Campus sowie externe Kommunikationsverbindungen.
G 0.10	Ausfall oder Störung von Versorgungsnetzen	X	SLA (Energie und Kühlung)
G 0.11	Ausfall oder Störung von Dienstleistern	X	SLA (Energie und Kühlung)
G 0.12	Elektromagnetische Störstrahlung	(X)	Im Rahmen der physischen Sicherheit.
G 0.13	Abfangen kompromittierender Strahlung		
G 0.14	Ausspähen von Informationen/Spionage	(X)	Ausspähen von verschlüsselten (secure shell) Zugangsdaten oder sog. „Preshared Keys“ der Techniker.
G 0.15	Abhören		
G 0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	X	Physische Sicherheit
G 0.17	Verlust von Geräten, Datenträgern und Dokumenten	(X)	Soweit es mit fehlender Zutritts- und Zugangskontrolle zu tun hat.
G 0.18	Fehlplanung oder fehlende Anpassung		
G 0.19	Offenlegung schützenswerter Informationen	(X)	Es können Kundendaten oder Betreiberdaten von Housing Unternehmen verwaltet werden. (Beispielsweise Netzpläne, Systemversionen, Passwörter oder Zutrittsberechtigungen des Housing-Betreibers).
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle		

Nr.	KRITIS-relevante elementare Gefährdung (Risiko)	Besondere Relevanz	Erklärung Relevanz
G 0.21	Manipulation von Hard- und Software		
G 0.22	Manipulation von Informationen		
G 0.23	Unbefugtes Eindringen in IT-Systeme		
G 0.24	Zerstörung von Geräten oder Datenträgern	(X)	Geräte, soweit es sich um physische Sicherheit handelt.
G 0.25	Ausfall von Geräten oder Systemen	(X)	Soweit es SLAs Energie/ Kühlung sowie Zutritts- und Überwachungssysteme betrifft. Zu betrachten sind dabei: NEA, USV, Energieversorgung, GLT, EMA und BMA.
G 0.26	Fehlfunktion von Geräten oder Systemen		
G 0.27	Ressourcenmangel		
G 0.28	Softwareschwachstellen oder -fehler		
G 0.29	Verstoß gegen Gesetze und Regelungen		
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	(X)	Zum Beispiel durch einen Innentäter oder Dritte
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	(X)	Dies könnte im Bereich Energie/Kühlung/Zutritt relevant sein
G 0.32	Missbrauch von Berechtigungen	(X)	Nur, soweit es den Zutritt- und Zugang betrifft.
G 0.33	Personalausfall	(X)	Im Rahmen physischer Sicherheit
G 0.34	Anschlag	(X)	Im Rahmen physischer Sicherheit
G 0.35	Nötigung, Erpressung oder Korruption	(X)	Durch Dritte oder einen Innentäter möglich.
G 0.36	Identitätsdiebstahl	(X)	Nur, soweit es den Zutritt und Zugang betrifft.
G 0.37	Abstreiten von Handlungen		
G 0.38	Missbrauch personenbezogener Daten		
G 0.39	Schadprogramme		
G 0.40	Verhinderung von Diensten (DoS)		

Nr.	KRITIS-relevante elementare Gefährdung (Risiko)	Besondere Relevanz	Erklärung Relevanz
G 0.41	Sabotage	X	Im Rahmen physischer Sicherheit.
G 0.42	Social Engineering	(X)	Wenn physische Zutritte unrechtmäßig erworben werden.
G 0.43	Einspielen von Nachrichten		
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	X	Physische Sicherheit.
G 0.45	Datenverlust	(X)	Soweit es Zugangsdaten betrifft.
G 0.46	Integritätsverlust schützenswerter Informationen		
G 0.47	Schädliche Seiteneffekte IT-gestützter Angriffe		

Tabelle 5: KRITIS-relevante elementare Gefährdung (Risiko)

Für alle oben aufgeführten relevanten Gefährdungen sind Sicherheitsmaßnahmen zu beschreiben. Am Beispiel einiger Risiken wird dies im Folgenden dargestellt. Das Vorgehensmodell orientiert sich an den Industriestandards wie ISO/IEC 27001, BSI IT-Grundschutz und C5. Die genaue Bewertung und Ausgestaltung dieser Maßnahmen muss in Bezug zu den Schutzzielen der Systeme zum Betrieb der Kritischen Infrastruktur und auch der Systeme der kDL erfolgen.

Nr.	KRITIS-relevante elementare Gefährdung	Einfluss Kritische Infrastruktur	Sicherheitsmaßnahmen (beispielhaft)
G 0.1	Feuer	Bis zur kompletten Zerstörung	1. Warnmelder (Rauchmelder und Temperaturfühler) 2. Auslösung Löschvorgang 3. Information/Meldung an Feuerwehr

Nr.	KRITIS-relevante elementare Gefährdung	Einfluss Kritische Infrastruktur	Sicherheitsmaßnahmen (beispielhaft)
G 0.2	Ungünstige klimatische Bedingungen	SLAs für die Einhaltung der Temperatur in den Rechnerräumen werden mit der Folge überschritten, dass IT-Systeme schneller altern und im Extremfall ausfallen können.	1. Festlegen von Temperatur-grenzwerten. 2. Redundante Kühlungssysteme und Pläne, wenn durch besondere klimatische Bedingungen die Kühlsysteme keine ausreichende Leistung liefern können. 3. Je nach klimatischen Bedingungen sind adiabatische Kühlungen sowie Verträge mit den örtlichen Wasserwerken zur Lieferung einer garantierten Wassermenge abzuschließen. Dies ist insbesondere bei hohen Temperaturen zu empfehlen.
G 0.3	Wasser	Kann zu Aussetzern von Infrastruktur und IT führen	1. Feuchtigkeitsfühler an strategischen Stellen 2. Meldung an operatives Team
G 0.4	Verschmutzung, Staub, Korrosion	Erhöhtes Risiko des Einbringens brennbarer Materialien, erhöhte Risiken des Ausfalls der IT-Systeme, Verschmutzung der Rechner, Höherer Energieverbrauch, Reduktion der Lebensdauer	1. Verbot Einbringens brennbarer Materialien und Stauberzeuger (zum Beispiel Kartonagen) 2. Erzeugung von Unterdruck, um die Luft herauszusaugen 3. Luftfilterung
G 0.5	Naturkatastrophen	Unabsehbare Folgen bis zur kompletten Zerstörung	Bei der Planung eines Rechenzentrums sind örtliche Gegebenheiten beachten (ehemaliges Flussbett, Erdbebengebiet…)
G 0.6	Katastrophen im Umfeld	Folgen abhängig von der Katastrophe	Bei der Planung auf Umfeld achten (Abstand Tankstelle, Chemieunternehmen etc.)
G 0.7	Großereignisse im Umfeld	Hauptsächlich logistische Probleme zu erwarten	Bei der Planung auf Umfeld achten (Abstand zu Botschaften etc.)
G 0.8	Ausfall oder Störung der Stromversorgung	Ausfall sämtlicher IT-Systeme	USV, NEA (Netzersatzanlagen), ausreichende Versorgung mit Diesel, regelmäßige Ausfalltests

Nr.	KRITIS-relevante elementare Gefährdung	Einfluss Kritische Infrastruktur	Sicherheitsmaßnahmen (beispielhaft)
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	nur innerhalb des Gebäudes oder auf dem Campus	Business Continuity Plan
G 0.10	Ausfall oder Störung von Versorgungsnetzen	SLA (Energie und Kühlung)	Krisen- und Notfallmanagement, Lieferantenmanagement, Business Continuity Plan
G 0.11	Ausfall oder Störung von Dienstleistern	SLA (Energie und Kühlung)	Lieferantenmanagement, vertragliche Definition von Mindestanforderungen und Standards
G 0.12	Elektromagnetische Störstrahlung	Im Rahmen der physischen Sicherheit	Eventuell räumliche Trennung von Kommunikationskabeln und Energieverkabelung
G 0.13	Abfangen kompromittierender Strahlung	Im Rahmen der physischen Sicherheit	Physische Sicherheitsmaßnahmen
G 0.14	Ausspähen von Informationen/Spionage	Ausspähen von verschlüsselten (secure shell) Zugangsdaten der Techniker	Schutz von Informationen am Arbeitsplatz (Clean-Desk-Policy, Sichtschutz, Bildschirmsperre etc.), Sicherheitsschulungen („Security Awareness“); Zertifikatsbasierter Zugriff, Zwei-Faktor-Authentifizierung und Verbot ungeschützter Zugriffsprotokolle
G 0.15	Abhören		
G 0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	Physische Sicherheit	Physische Sicherheitsmaßnahmen, Berechtigungsmanagement
G 0.17	Verlust von Geräten, Datenträgern und Dokumenten	Soweit es mit fehlender Zutritts- und Zugangskontrolle zu tun hat	Physische Sicherheitsmaßnahmen, Berechtigungsmanagement
G 0.18	Fehlplanung oder fehlende Anpassung		
G 0.19	Offenlegung schützenswerter Informationen	Soweit es Kundendaten betrifft, die von Housing Unternehmen verwaltet werden.	Schutz von Informationen am Arbeitsplatz (Clean-Desk-Policy, Sichtschutz, Bildschirmsperre etc.), Sicherheitsschulungen („Security Awareness“).
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle		
G 0.21	Manipulation von Hard- und Software		

Nr.	KRITIS-relevante elementare Gefährdung	Einfluss Kritische Infrastruktur	Sicherheitsmaßnahmen (beispielhaft)
G 0.22	Manipulation von Informationen		
G 0.23	Unbefugtes Eindringen in IT-Systeme		
G 0.24	Zerstörung von Geräten oder Datenträgern	Geräte, soweit es die physische Sicherheit betrifft.	Erstellen eines Business Continuity Plans.
G 0.25	Ausfall von Geräten oder Systemen	Soweit es SLAs Energie/ Kühlung sowie Zutritts- und Überwachungssysteme betrifft.	Erstellen eines Business Continuity Plans und/oder Redundanz.
G 0.26	Fehlfunktion von Geräten oder Systemen		
G 0.27	Ressourcenmangel		
G 0.28	Softwareschwachstellen oder -fehler		
G 0.29	Verstoß gegen Gesetze und Regelungen		
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Zum Beispiel durch einen Innentäter oder Dritte.	Berechtigungsmanagement und Awarenesstrainings.
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Dies könnte im Bereich Energie/Kühlung/Zutritt relevant sein.	Berechtigungsmanagement und Awarenesstrainings.
G 0.32	Missbrauch von Berechtigungen	Insbesondere soweit es den Zutritt- und Zugang betrifft.	Awarenesstrainings und Definition von disziplinarischen Maßnahmen/Konsequenzen.
G 0.33	Personalausfall	Im Rahmen physischer Sicherheit.	Erstellen eines Business Continuity Plans.
G 0.34	Anschlag	Im Rahmen physischer Sicherheit.	Etablieren eines Krisen- und Incidentmanagement.
G 0.35	Nötigung, Erpressung oder Korruption	Durch Dritte oder einen Innentäter möglich.	Etablieren eines Krisen- und Incidentmanagement, Zusammenarbeit mit behördlichen Institutionen wie Polizei, Whistleblowing…
G 0.36	Identitätsdiebstahl	Insbesondere soweit es den Zutritt und Zugang betrifft.	Technische und organisatorische Maßnahmen, die einen Identitätsdiebstahl so gering wie möglich machen, Berechtigungsmanagement und Awarenesstrainings

Nr.	KRITIS-relevante elementare Gefährdung	Einfluss Kritische Infrastruktur	Sicherheitsmaßnahmen (beispielhaft)
G 0.37	Abstreiten von Handlungen		
G 0.38	Missbrauch personenbezogener Daten		
G 0.39	Schadprogramme		
G 0.40	Verhinderung von Diensten (DoS)		
G 0.41	Sabotage	Im Rahmen physischer Sicherheit	Etablieren eines Krisen- und Incidentmanagement
G 0.42	Social Engineering	Wenn physische Zutritte unrechtmäßig erworben werden	Awarenesstrainings
G 0.43	Einspielen von Nachrichten		
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	Physische Sicherheit	Physisches und logisches Zugriffs-management, Videoüberwachung, Maßnahmen für interne und externe Mitarbeiter (privilegierte Rollen und Endbenutzer). physische Sicherheitsmaßnahmen, Berechtigungsmanagement, sowie mitarbeiter-bezogene Maßnahmen (z. B. Hintergrundprüfung)
G 0.45	Datenverlust	Soweit es Zugangsdaten betrifft	Business Continuity Plan
G 0.46	Integritätsverlust schützenswerter Informationen		
G 0.47	Schädliche Seiteneffekte IT-gestützter Angriffe		

Tabelle 6: Beispiele Maßnahmen zur Risikobehandlung (Housing)

2.5 Branchenspezifische Technik Housing

Folgende Voraussetzungen sind bei der Beschaffung zu beachten (es wird hier nur der branchenspezifische Standard betrachtet, ohne Eigenentwicklung, zum Thema Eigenentwicklung siehe Ende des Abschnitts:

- Lieferanten benötigen ein entsprechendes Knowhow zu den Produkten des Herstellers
- Verfügbarkeit von Ersatzteilen

- Bei Wartungen durch Dritte ist die fachliche Kompetenz der Dienstleister sicherzustellen und darauf zu achten, dass zugesicherte Wartungsintervalle eingehalten werden.
- Reaktionszeit der Dienstleister im Instandsetzungsfall bei Bedarf vor Ort oder vertraglich festgelegte Instandsetzungszeiten oder Wiederherstellungszeiten über SLAs

Für den Bereich Housing werden die Leistungen „Gebäude“, „Energieversorgung“, „Klimatisierung“, „Zutrittsschutz“ und „Netzwerk-Anbindung“ angeboten. Deshalb sind folgende Systeme von besonderer Bedeutung (siehe auch Kapitel 2.1):

- Gebäudeleittechnik, insbesondere die digitalen Steuerungen für die Kontrolle der Infrastruktur zur Energie- und Klimaversorgung,
- Brandmeldesysteme
- Überwachungssysteme (Video-Überwachung, Einbruchmeldesysteme etc.)
- Zutrittsmanagementsysteme
- Sicherungssysteme (Firewalls, physische Trennung der Netze, Jump-Hosts etc.), mit denen sichergestellt wird, dass nur berechtigte Benutzer auf die betrieblichen Systeme zugreifen können

Die Systeme können entweder in den Überwachungszentren, in eigens gesicherten IT-Bereichen und/oder im Bereich der Infrastruktur-Systeme der Anlage installiert sein. Sie sind gegen die Systeme und Netzwerkverbindungen der Kunden einerseits und die sonstigen IT-Systeme des Anbieters andererseits abzugrenzen.

Die folgende Abbildung zeigt, wie diese Struktur grundsätzlich zu verstehen ist.

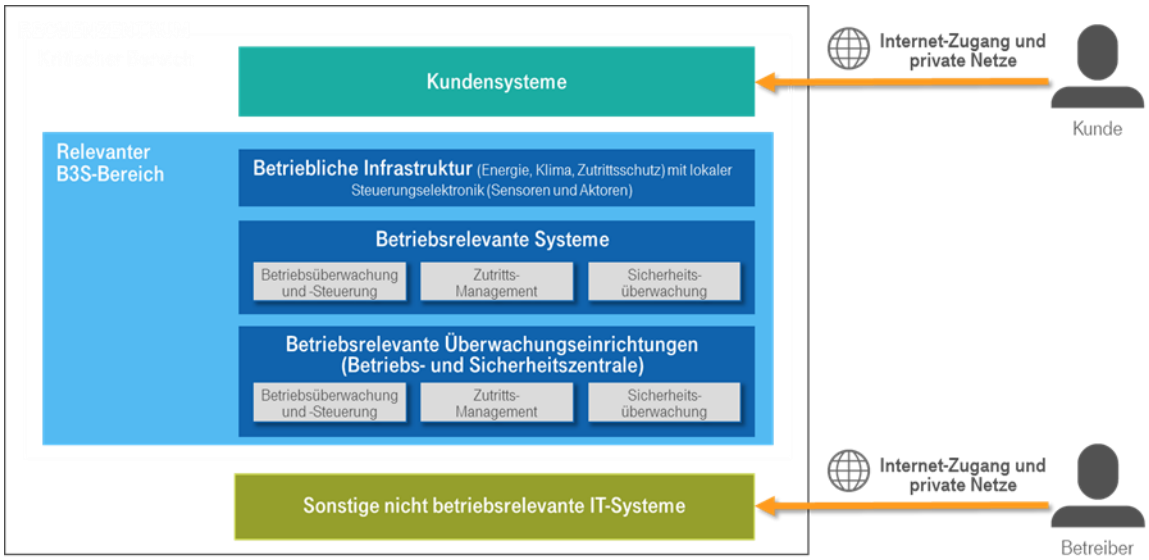

Abbildung 5: Struktur eines Rechenzentrums (Housing)

Während zu den IT-Systemen der Kunden keinerlei Verbindung besteht, kann es zwischen den betrieblich relevanten und sonstigen Systemen des Anbieters Verbindungen geben.

Auch wenn im Bereich Housing typischerweise keine Eigenentwicklung erfolgt, ist für den Fall, dass ein Anwender eigene Systeme entwickelt, entsprechende Prozesse zu definieren.

Dazu gehört beispielsweise die Fähigkeit, eigenentwickelte Systeme jederzeit anzupassen oder die Anforderung, dass die Systeme ausreichend getestet werden, bevor sie in Betrieb gehen.

2.6 Branchenspezifische Architektur und Verantwortung Housing

Der Housing Betreiber ist entsprechend den Vorgaben des IT-Sicherheitsgesetzes verantwortlich für seine kDL. Der Aufbau der IT-Systeme von Housing-Anbietern ist im Kapitel 2.5 beschrieben. Eine grundsätzliche Eigenschaft ist die vollständige Trennung der IT-Systeme der Kunden von denen des Anbieters, da diese lediglich zur Steuerung und Überwachung des RZ-Gebäudes und seiner Infrastruktur dienen. Dies ist grundsätzlich in der folgenden Abbildung dargestellt:

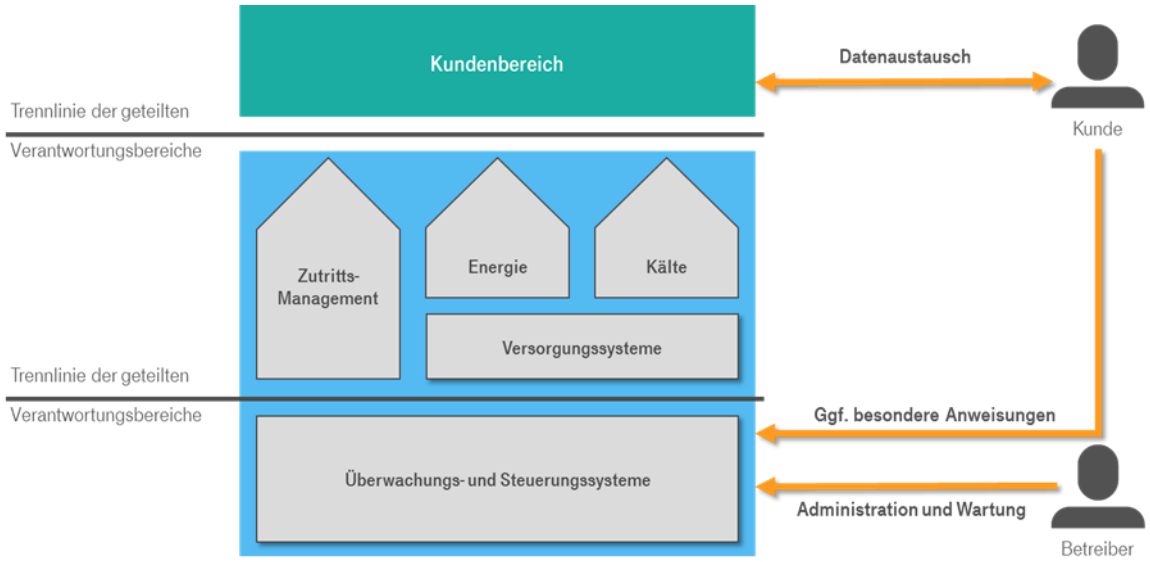

Abbildung 6: Verantwortungsbereiche Kunde / Betreiber (Housing)

Die Bereitstellung von Gebäude, Energie, Klima, Sicherheitsdiensten und Konnektivität mit der entsprechenden Verkabelung liegt in der Verantwortung des Betreibers. Ein entsprechendes Monitoring dieser Funktionen ist durch den Housing Betreiber sicherzustellen. Die dafür notwendigen IT-Systeme sind von den IT-Systemen der Kunden vollständig zu trennen und gemäß in diesem Branchenstandard dokumentierten Vorgaben zu schützen.

3 Hosting und CDN

Unter Hosting wird das Bereitstellen von IT-Infrastruktur an Kunden verstanden. Dies umfasst beispielsweise physische und logische (virtuelle) Server (IaaS), bzw. im Falle der Bereitstellung von Platform as a Service (PaaS) und Software as a Service (SaaS) auch weitere darauf aufbauende Services. Die damit abgebildeten Kundenangebote oder -dienste sind in der Regel öffentlich, können aber auf Zielgruppen beschränkt sein, wie zum Beispiel Mitarbeiter, Geschäftspartner oder Endkunden.

Ein Content Delivery Netzwerk (CDN) hat die Aufgabe, den Transport von durch einen Original-Server (Fachbegriff: Origin) zur Verfügung gestellten Web-Inhalte zu beschleunigen und für eine Ressourcenentlastung zu sorgen. Dabei stellt das CDN die erforderlichen Bandbreiten und Serverressourcen dynamisch zur Verfügung. CDNs sind typischerweise hochgradig verteilte Systeme, die durch örtliche Nähe viele Verbraucher gleichzeitig und mit niedriger Latenz versorgen können.

3.1 Anwendungsbereich und Schutzziele Hosting und CDN

3.1.1 Anwendungsbereich Hosting und CDN

Der Anwendungsbereich für Hosting und CDN umfasst die Leistungen, die mit der Bereitstellung von Hosting- und CDN-Dienstleistung für Kunden im Zusammenhang stehen. Das sind:

- Hardware und Virtualisierung
- Storage und Backup
- Netzwerkressourcen und technische Services (bspw. DNS, Zeitdienst)
- Kundenschnittstellen (bspw. Konfiguration, Datenzugriff, Überwachung und Steuerung)
- Administrationsschnittstellen (bspw. Systemkonfiguration, Überwachung und Steuerung)
- Verbraucherschnittstelle zum Abrufen von Inhalten (nur CDN)
- IT-Systeme zur Steuerung und Überwachung der kritischen Komponenten (bspw. Monitoring)
- Technische und organisatorische Maßnahmen zum Schutz der obengenannten Ressourcen, bspw.:
    - physische Sicherheit (bspw. Zutrittsschutz, Umwelteinflüsse)
    - IT-Sicherheit (bspw. Firewall, Segregation, Mandantentrennung, IDS/IPS)
    - Patch und Change-Management
    - Verfügbarkeits- und Kontinuitätsmanagement

Als Kritische Infrastruktur im Sinne der BSI-KritisV gelten Anlagen ab den in der BSI-KritisV festgelegten Schwellenwerten (die aktuelle Verordnung ist zu prüfen).

Stand August 2021 sind dies:

- Hosting-Betreiber mit Serverfarmen und einer Mindestanzahl von 10.000 physischen bzw. 15.000 virtuellen Instanzen (jeweils im Jahresdurchschnitt)
- CDN-Betreiber mit einem ausgelieferten Datenvolumen von mindestens 75.000 TByte/Jahr

Mehrere Anlagen derselben Kategorie, die durch einen betriebstechnischen Zusammenhang verbunden sind, können als gemeinsame Anlage angesehen werden, wenn die Kriterien nach BSI-KritisV Anhang 4 Teil 1 Nr. 6 zutreffen.

3.1.2 Anforderungen an die Darstellung des Geltungsbereichs

Der Netzplan sollte den Verteilungsgrad der Komponenten darstellen, insbesondere der Verteilungsgrad der Kundenschnittstelle sollte aus der grafischen Darstellung hervorgehen. Sofern es zentrale Komponenten zur Administration der Komponenten oder der Kundenschnittstelle (zum Beispiel das Erstellen und Verwalten zentraler Dateien zur Protokollierung) gibt, sollten diese auch aus der grafischen Darstellung hervorgehen.

Folgende Punkte sind textuell zu beschreiben und geeignet im angepassten Netzplan[19] grafisch darzustellen (siehe[20] auch Anhang C der Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG):

- die in das Netz eingebundenen IT-Systeme. Dazu zählen Computer (Clients und Server), Netzdrucker sowie aktive Netzkomponenten (Switches, Router, WLAN-Access Points), usw.
- die Verbindungen zwischen diesen IT-Systemen, wie LAN-Verbindungen (Ethernet), Backbone-Technik (zum Beispiel ATM), usw.
- die Außenverbindungen der IT-Systeme. Bei diesen sollte zusätzlich die Art der Verbindung gekennzeichnet sein (zum Beispiel Internet-Anbindung, DSL), usw.

Außerdem müssen relevante Systeme, Komponenten und Prozesse einschließlich deren Schnittstellen und ggf. Auslagerungen textuell beschrieben werden. Beispiele hierfür wären die Realisierung der einschlägigen ITIL-Prozesse samt Schnittstellen:

- Prozesse im Bereich Infrastruktur
    - Portfolio-, Bedarfs- und Kapazitätsmanagement
    - Patch- und Änderungsmanagement
    - Allgemeine standardisierte IT-Abläufe und -Prozesse
- Prozesse im Bereich Sicherheit
    - Richtlinien, Schulungen und Sensibilisierung
    - Physische Sicherheit und Krisenmanagement für Rechenzentren
    - Sichere Verfahren für die Entwicklung und Bereitstellung von Produkten

[19] www.bsi.bund.de/dok/10990266

[20] www.bsi.bund.de/OHNachweise

  - Sichere Verfahren für administrative Zugriffe auf Kundensysteme
  - Allgemeine Sicherheitsprozesse für den Betrieb, Client- und Endpunktsicherheit und Schutz der Cloud- und Netzwerkinfrastruktur
  - Intrusion Detection, Prävention, Überprüfung, Verwaltung und Bearbeitung von Sicherheitsvorfällen und -ereignissen,
  - Schwachstellenmanagement

- ISMS und Compliance Management
  - Betrieb und Verbesserung des ISMS
  - Einhaltung von relevanten Richtlinien und zugehörige Zertifizierungen
  - Vorbereitung und Durchführung interner und externer Audits
  - Lieferantenmanagement

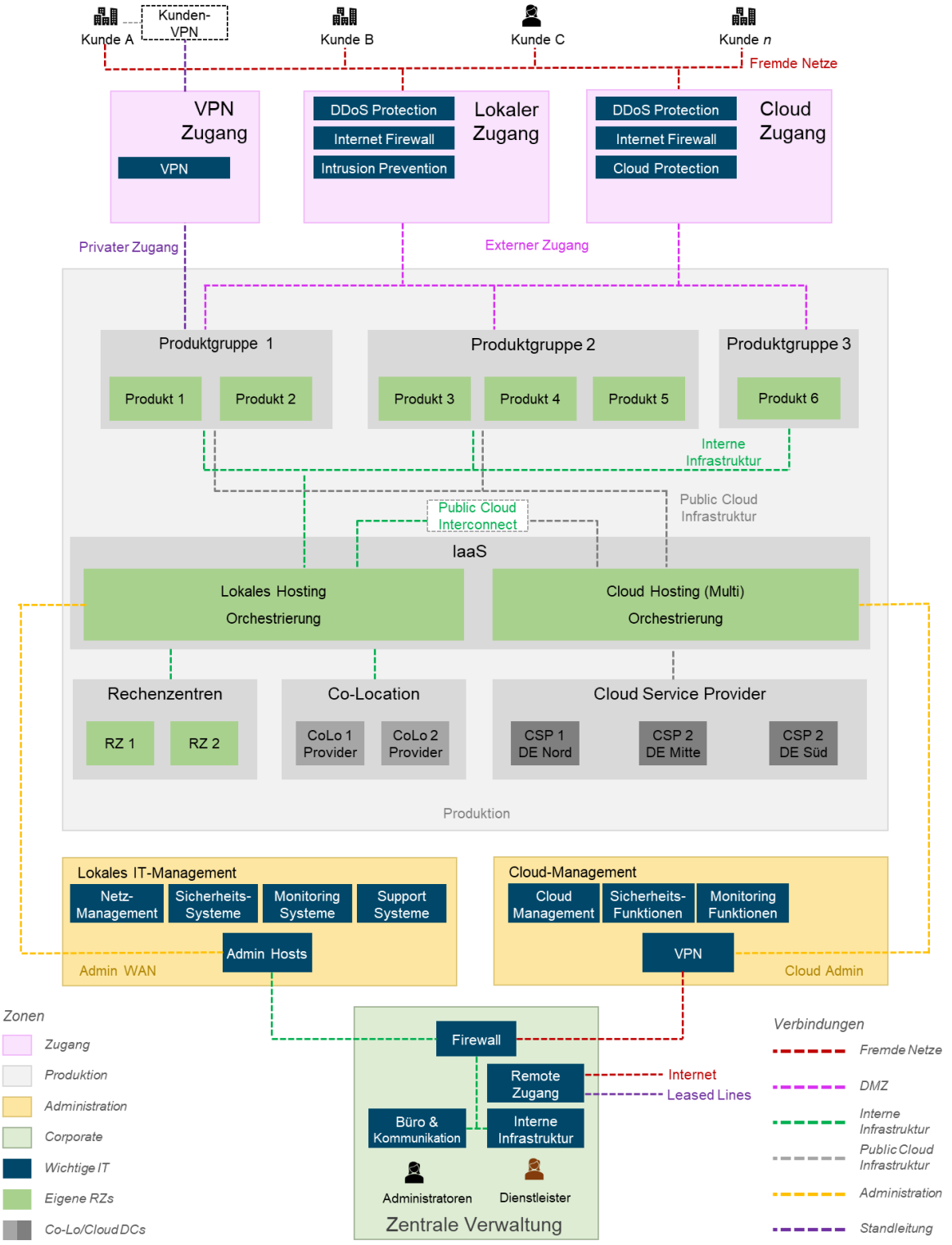

Abbildung 7: Beispiel Netzplan für eine Hosting Infrastruktur

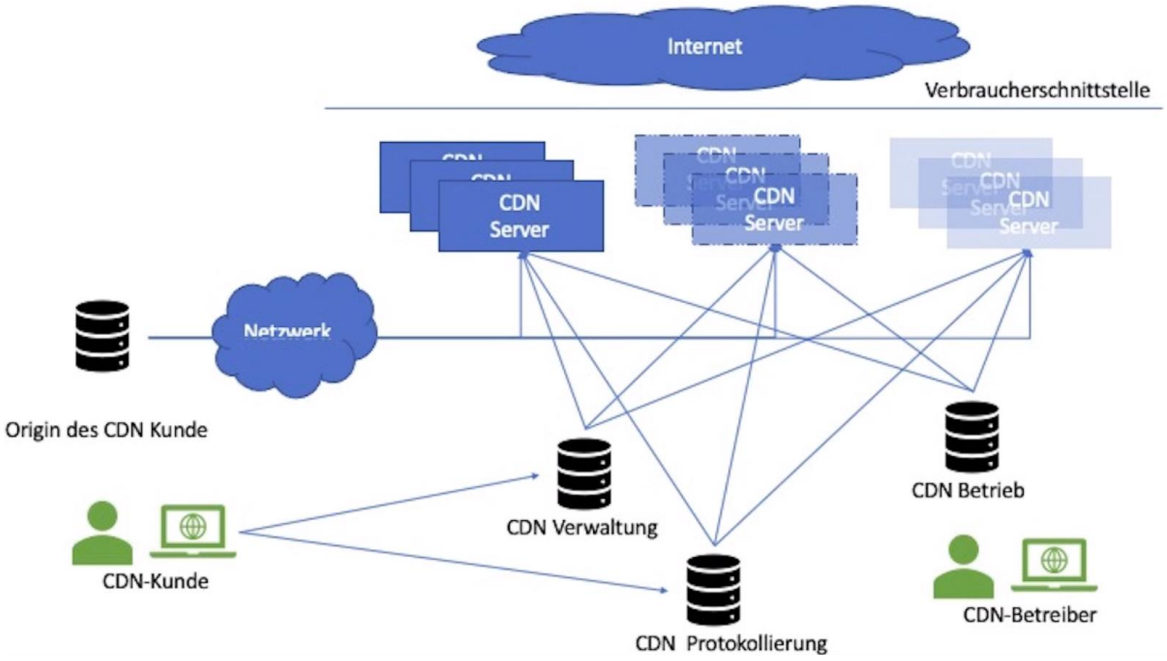

Abbildung 8: Beispiel Netzplan für eine CDN Infrastruktur

Bei beiden Abbildungen handelt es sich um abstrakte Darstellungen, die bei Anwendung des B3S durch den Betreiber in Form eines konkreten Netzstrukturplans weiter auszuführen sind. So sind z. B. physische Standorte, Systembezeichnungen, Schnittstellenbezeichnungen und ggf. Lastverteilungen detailliert darzustellen, um der Komplexität der eigenen Umgebung gerecht zu werden.

3.1.3 Schutzziele der kDL und betriebsrelevanter Systeme Hosting und CDN

Aufgabe der kDL “Hosting und CDN” ist die kontinuierliche Bereitstellung von IT-Dienstleistungen für Unternehmen, den öffentlichen Sektor und Privatpersonen.

Der B3S bezieht sich also sowohl auf die IT-Systeme, die zum Betrieb der kritischen Anlage notwendig sind, als auch auf die IT-Systeme, aus denen die Anlagen selbst bestehen. Zur Abgrenzung sei darauf hingewiesen, dass beispielsweise die „Digitalen Dienste“ nach NIS-Direktive[21] hier nicht betrachtet werden. Die enge Verbundenheit dieser Bereiche macht die Definition von gemeinsamen Schutzzielen erforderlich.

Hier äußert sich eine wichtige Besonderheit dieses Sektors „IT und Telekommunikation” und speziell des Bereichs „Hosting mit CDN”: Während wie in anderen KRITIS Sektoren (wie zum Beispiel Transport oder Energie) auch IT-Systeme zum Betrieb der kDL erforderlich sind (Netzwerk- und Managementsysteme, Monitoringsysteme), besteht die kDL selbst auch aus IT bzw. der Bereitstellung von IT Services (Dienstleistungssystemen).

[21] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, Absatz 48ff. http://data.europa.eu/eli/dir/2016/1148/oj

Damit sind die betriebsrelevanten IT-Systeme (einschließlich der davon genutzten Datennetze) alle Systeme, die vom Dienstleister zur Erbringung der kDL benutzt werden und somit als relevant für den Betrieb der Kritischen Infrastruktur betrachtet werden müssen. Alle Systeme unterliegen damit den gleichen Schutzzielen Vertraulichkeit, Integrität und Authentizität und Verfügbarkeit.

Die konkreten Schutzziele im Bereich Hosting und CDN sind:

- Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Kundeninhaltsdaten (insofern diese vom Kunden nicht selbst nach außen verfügbar gemacht werden oder durch die Natur des Dienstes nach außen verfügbar sind) sowie der Vertraulichkeit der Daten der dafür notwendigen Unterstützungssysteme (wie Netzwerk-, Management- und Monitoring-Systeme) anhand ihres Schutzbedarfes
- Sicherstellung der Verfügbarkeit der Dienstleistungssysteme gemäß SLAs mit den Kunden sowie der dafür notwendigen Verfügbarkeit von Unterstützungssystemen (wie Netzwerk-, Management- und Monitoring-Systeme)

Die Schutzbedarfe, die sich daraus ergeben, sind in der folgenden Tabelle dargestellt:

Schutzziele	**Schutzbedarfe Netzwerk- und Management-Systeme**	**Schutzbedarfe Monitoring-Systeme**	**Schutzbedarfe DL-Systeme[22]**
Vertraulichkeit	hoch/sehr hoch	hoch	hoch
Integrität und Authentizität	sehr hoch	sehr hoch	hoch
Verfügbarkeit	sehr hoch	hoch	hoch

Tabelle 7: Kritikalität der betriebsrelevanten IT-Systeme (Hosting und CDN)

Die vorstehende Tabelle bewertet die Kritikalität und damit die Schutzbedarfe der jeweiligen IT-Systeme für die Erbringung der kDL. Die in der Tabelle verwendeten Ausprägungsstufen (normal, hoch, sehr hoch) der Schutzziele orientieren sich dabei am BSI Grundschutz-Standard:

- „normal“: Die Schadensauswirkungen sind begrenzt und überschaubar.
- „hoch“: Die Schadensauswirkungen können beträchtlich sein.
- „sehr hoch“: Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Für eine erfolgreiche Umsetzung muss der Betreiber der Kritischen Infrastruktur diese Ausprägungsstufen unternehmensspezifisch definieren und dokumentieren. Nach Risikobewertung und ausführlicher Dokumentation können diese Schutzbedarfe für einzelne Systeme abweichen.

[22] Die Schutzbedarfe sind hier beispielhaft aufgeführt und unterliegen in der Praxis den vertraglich vereinbarten SLAs

Netzwerk- und Management-Systeme

- **Vertraulichkeit**
  - Der Erhalt der Vertraulichkeit ist für Netzwerk- und Management-Systeme von hoher Bedeutung. Folgen des Verlustes der Vertraulichkeit sind mögliche Datenexfiltrationen und die daraus resultierenden Angriffsvektoren.

- **Integrität und Authentizität**
  - Die Integrität und Authentizität der Daten von Netzwerk- und Management-Systemen sind von hoher bis sehr hoher Bedeutung. Beispielsweise kann die absichtliche oder versehentliche Veränderung eines Zertifikats für einen Angriff auf die kDL ausgenutzt werden.

- **Verfügbarkeit**
  - Die Verfügbarkeit von Netzwerk- und Management-Systemen ist von sehr hoher Bedeutung. Andere Systeme sind mit Ihrer Verfügbarkeit von der Verfügbarkeit dieser Systeme abhängig.

Monitoring Systeme

- **Vertraulichkeit**
  - Der Erhalt der Vertraulichkeit der Daten der Monitoring Systeme ist für die Erbringung der kDL von hoher Bedeutung. Kenntnisse über den aktuellen Status können für einen Angriff auf die kDL ausgenutzt werden und zu einer Störung der kDL führen.

- **Integrität und Authentizität**
  - Die Integrität und Authentizität der Daten in den betriebsrelevanten Monitoring Systemen ist von sehr hoher Bedeutung. Die absichtliche oder versehentliche Veränderung (Beeinträchtigung der Integrität) oder Vortäuschung (fehlende Authentizität) kann für einen Angriff auf die kDL ausgenutzt werden und zu einer Störung der kDL führen.

- **Verfügbarkeit**
  - Die Verfügbarkeit der Monitoring Systeme ist als hoch zu bewerten. Dies gilt insbesondere für unbemannte Hosting Center, die über keine 24/7 Vor-Ort-Überwachung verfügen.

Dienstleistungssysteme

- **Vertraulichkeit**
  - Der Erhalt der Vertraulichkeit ist für die Erbringung der kDL grundsätzlich von hoher Bedeutung, weil die absichtliche oder versehentliche Veröffentlichung oder unberechtigte Einsichtnahme für einen Angriff auf die kDL ausgenutzt werden und zu einer Störung der kDL führen kann.

- **Integrität und Authentizität**
  - Die Integrität und Authentizität der Daten in den betriebsrelevanten IT-Systemen sind von hoher bis sehr hoher Bedeutung. Beispielsweise kann die absichtliche oder versehentliche Veränderung (Beeinträchtigung der Integrität) oder Vortäuschung (fehlende Authentizität) für einen Angriff auf die kDL ausgenutzt werden und zu einer Störung der kDL führen.

- **Verfügbarkeit**
  - Die Kritikalität der Verfügbarkeit der Dienstleistung muss nach Sachlage betrachtet werden. Je nach Diensttyp, Verfügbarkeitsanforderungen seitens des Kunden und vereinbarter Dienstleistungs-Güte-Vereinbarung (Service-Level-Agreement - SLA) muss hier eine Bewertung angepasst werden. Zu beachten ist aber, dass die Verfügbarkeit systemabhängig mindestens den SLAs entsprechen muss.

3.2 IT-Schutzbedarfe Hosting und CDN

Die Schutzbedarfe leiten sich aus den IT-Schutzzielen ab. Es muss gewährleistet sein, dass die IT-Infrastruktur zum Erbringen der Dienstleistung Hosting mit CDN durch den Anbieter entsprechend abgesichert, verfügbar, sowie gegen unautorisierte Benutzung oder Änderung geschützt ist.

Ebenso muss der Betreiber sicherstellen, dass der Zugriff auf diese Systeme über interne und externe Schnittstellen gesichert erfolgt. Dabei müssen die dem jeweiligen Schutzbedarf entsprechenden Standards umgesetzt werden.

Die Nutzung der Hosting-Produkte ist dabei nicht Gegenstand des B3S, sondern ausschließlich die technische Anlage zum Betrieb der Hosting-Plattform.

Der Hosting Betreiber sorgt dafür, dass der Kunde den Betrieb der Gesamtplattform nicht gefährden kann. Der vorliegende Standard berücksichtigt dies durch die entsprechend umzusetzenden Kontrollen aus dem ISO/IEC 27001 Rahmenwerk für die betroffenen Bereiche.

3.3 Branchenspezifische Gefährdungslage

Der All-Gefahrenansatz (Naturereignisse, technisches beziehungsweise menschliches Versagen, Terrorismus, Kriminalität, Krieg) ist für jeden Betreiber einer kDL zugrunde zu legen. Die Risikobewertung muss regelmäßig (zum Beispiel jährlich) sowie anlassbezogen wiederholt werden.

Branchenspezifische Schwerpunkte im Bereich Hosting mit CDN werden nachfolgend beispielhaft aufgeführt.

3.3.1 Branchenspezifische Relevanz und Benennung von Szenarien

Im Bereich Hosting mit CDN sind nachfolgende Szenarien von besonderer Bedeutung. Es wird dabei jeweils auf die elementaren Gefährdungen im Kapitel 3.3.2 verwiesen.

- **Zero-Day Schwachstellen:**
  - Das Ausnutzung von Zero-Day Schwachstellen kann typischerweise nicht ursächlich verhindert werden und muss daher durch andere Maßnahmen kompensiert werden (bspw. Grundhärtung und Überwachung von Infrastruktur und Diensten).
  - G 0.28, G 0.30

- **Schadsoftware in E-Mail-Anhängen:**
  - Phishing Angriffe (undifferenziert oder zielgerichtet) bedienen sich oft E-Mails als Angriffsvektor, um Schadsoftware direkt (bspw. Dokumente mit Makro-Viren) oder über Downloadlinks zur Ausführung zu bringen. Typische Abwehrmaßnahmen sind Malware-Erkennung in den E-Mail-Systemen und Mitarbeitersensibilisierung.
  - G 0.21, G 0.39, G 0.42

- **Advanced Persistent Threat (APT) Angriffe:**
  - Dies sind Cyber-Angriffe auf die für den Betrieb der kDL relevanten IT-Systeme oder aber auf IT-Systeme oder Services der kDL selbst. So kann direkt oder durch erst später folgende Angriffe (Backdoor) Schaden verursacht werden. Zur Abwehr ist eine Sicherheitsüberwachung und ein aktives Management von Sicherheitsvorfällen essenziell.
  - G 0.14, G 0.21, G 0.23, G 0.39, G 0.42, G 0.45, G 0.46

- **Ransomware:**
  - Angreifer übernehmen über Erpressungstrojaner die Kontrolle über Daten (Verschlüsselung) und Systeme (Zugriffsberechtigung). Vorbeugende Maßnahmen sind zuverlässige Datensicherungen, aktives Patchmanagement und Systemhärtung.
  - G 0.17, G 0.25, G 0.42, G 0.45, G 0.46

- **Daten-Exfiltration:**
  - Dies bezeichnet den nicht autorisierten Transfer von Daten in den Zugriffsbereich eines externen oder internen Angreifers. Als Gegenmaßnahmen greifen strikte logische und physische Zugriffskontrollen.
  - G 0.15, G 0.19, G 0.32, G 0.45, G 0.46

- **Naturkatastrophen:**
  - Naturereignisse (Überschwemmungen, Erdbeben etc.) führen zum Ausfall der für den Betrieb der kDL relevanten IT-Systeme (gemäß Kapitel 1.2) durch physische Zerstörung. Georedundante Infrastruktur ist geeignet, die Auswirkungen auf regionale Betriebsumgebungen zu beschränken.
  - G 0.5, G 0.8, G0.9

- **Ressourcenmangel:**
  - Unzureichende Ressourcen sowie eine mangelnde Skalierung von Personal oder Infrastruktur für die Aufrechterhaltung der kDL (speziell in Zeiten von Spitzenbelastungen oder komplexen technischen Umstellungen) gefährdet den Betrieb der kDL. Eine angemessene Vorsorgeplanung beruht auf der Überwachung und Bewertung der aktuellen und geplanten Ressourcennutzung inklusive anstehender Betriebsänderungen. Dabei sind auch angemessene Kapazitäten für kritische Betriebssituationen vorzusehen.
  - G 0.18, G 0.40

3.3.2 Benennung der Bedrohungen und Schwachstellen

Im Anhang 4.2 sind die elementaren Gefährdungen gemäß BSI Orientierungshilfe[23] aufgeführt, wobei grundsätzlich gemäß des All-Gefahrenansatzes vorzugehen ist. Nachfolgend wurden die für Hosting und CDN branchentypisch besonders relevanten Gefährdungen in Bezug auf Ihren potenziellen Einfluss auf die Kritische Infrastruktur ausgewählt und beispielhafte Sicherheitsmaßnahmen zur Risikoreduktion gegenübergestellt.

Konkrete Maßnahmen finden sich unter anderem in aktuellen Industriestandards wie ISO/IEC 27001, BSI IT-Grundschutz, C5 und so weiter. Die genaue Bewertung und Ausgestaltung dieser Maßnahmen muss in Bezug zu den Schutzzielen der Systeme zum Betrieb der Kritischen Infrastruktur und auch der Systeme der kDL erfolgen.

Nr.	KRITIS-relevante elementare Gefährdung	Einfluss Kritische Infrastruktur	Sicherheitsmaßnahmen (Beispiele)
G 0.1	Feuer	Feuer kann die Kritische Infrastruktur komplett zerstören	Brandmeldeanlagen, Brandlöschanlangen, Meldesysteme zur Feuerwehr, regelmäßige Wartung dieser Anlagen
G 0.5	Naturkatastrophen	Naturkatastrophen wie z. B. Erdbeben, Überschwemmungen können zum Verlust essenzieller Ressourcen (Gebäude, Personal, Systeme) und zu physischen Schäden an Rechenzentren und deren Steuerungssystemen führen, welche zu einem Ausfall oder Zerstörung der Kritischen Infrastruktur führen können.	Physische Sicherheitsmaßnahmen, Überwachung der Umgebungs-parameter und Business Continuity Maßnahmen analog ISO/IEC 22301 für Rechenzentren und kritische Betriebsprozesse.

[23] BSI: Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG, (Version 1.0 vom 01.12.2017, Seite 24)

Nr.	KRITIS-relevante elementare Gefährdung	Einfluss Kritische Infrastruktur	Sicherheitsmaßnahmen (Beispiele)
G 0.8	Ausfall oder Störung der Stromversorgung	Der Verlust der externen Stromversorgung kann zum kompletten Ausfall von Kundensystemen, Netzwerk- und Managementsystemen oder Überwachungssystemen führen	Sicherstellung geeigneter operationaler Redundanz (z. B. Notstromversorgung, Netzersatzanlagen, redundante Stromeinspeisungen) und regelmäßiger Wartung. Ggfls. Verträge mit Dienstleistern zur Sicherstellung einer kurzfristigen Instandsetzung,
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	Der Verlust von Basisinfrastruktur und darauf aufbauender Services kann zum kompletten Ausfall von Kundensystemen, Netzwerk- und Managementsystemen oder Überwachungssystemen führen	Sicherstellung geeigneter operationaler Redundanz (z. B. sekundärer Internetzugang) und regelmäßiger Wartung. Ggf. Verträge mit Dienstleistern zur Sicherstellung einer kurzfristigen Instandsetzung,
G 0.11	Ausfall oder Störung von Dienstleistern	Die Abhängigkeit von Dienstleistern kann zu ernsten Beeinträchtigungen der Verfügbarkeit von Kundendaten und Systemen der kDL führen. Der Einfluss wird maßgeblich durch die Art der extern bezogenen spezifischen Hardware, Software oder Dienstleistung bestimmt.	Lieferantenmanagement, vertragliche Definition von Mindestanforderungen und Standards, Lieferantenrisikobetrachtungen, Regelungen für die Einbindung externer Mitarbeiter.
G 0.14	Ausspähen von Informationen (Spionage)	Das Ausspähen von Betriebsinformationen ist eine hohe Bedrohung für die Vertraulichkeit von Kundendaten und Systemen der kDL sowie von Netzwerk-, Management- und Monitoringsystemen.	Schutz von Informationen am Arbeitsplatz (Clean-Desk-Policy, Sichtschutz, Bildschirmsperre etc.), Sicherheitsschulungen („Security Awareness“), Zertifikatsbasierter Zugriff, Zwei-Faktor-Authentifizierung und Verbot ungeschützter Zugriffsprotokolle
G 0.15	Abhören	Das Abhören von Betriebsinformationen ist eine hohe Bedrohung für die Vertraulichkeit von Kundendaten und Systemen der kDL sowie von Netzwerk-, Management- und Monitoringsystemen.	Physische und logische Absicherung der Kommunikation (z. B. Abhörschutz, Verschlüsselung, Trassensicherung, Systemhärtung).

Nr.	KRITIS-relevante elementare Gefährdung	Einfluss Kritische Infrastruktur	Sicherheitsmaßnahmen (Beispiele)
G 0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	Bedrohungen durch Diebstahl (Zugangsdaten, Token) können zu schwerwiegenden Beeinträchtigungen der Vertraulichkeit, Verfügbarkeit und Integrität der kDL sowie der Netzwerk-, Management- und Überwachungssysteme führen.	Physische Sicherheitsmaßnahmen, Berechtigungsmanagement und Aufteilen kritischer Berechtigungen, sowie mitarbeiterbezogene Maßnahmen (z. B. Hintergrundprüfung).
G 0.17	Verlust von Geräten, Datenträgern und Dokumenten	Verluste von Geräten, Datenträgern und Dokumenten können zu schwerwiegenden Beeinträchtigungen der Vertraulichkeit, Verfügbarkeit und Integrität der kDL sowie der Netzwerk-, Management- und Überwachungssysteme führen.	Physische Sicherheitsmaßnahmen, Berechtigungsmanagement und Aufteilen kritischer Berechtigungen.
G 0.18	Fehlplanung oder fehlende Anpassung	Organisatorische Mängel (z. B. unklare Zuständigkeiten entlang eines Prozesses) können die Steuerung und die Bereitstellung der kDL beeinträchtigen.	Festlegung, Übung, Dokumentation und Kommunikation von Zuständigkeiten und Verantwortlichkeiten für Informationssicherheit und wesentlicher Betriebsprozesse. Sicherstellung einer ausreichenden Trennung von operativen und überwachenden Rollen und Verantwortlichkeiten. Übungen (verschiedene Szenarien mit unterschiedlichen Ursachen) zeigen erfahrungsgemäß diese Probleme am besten auf.
G 0.19	Offenlegung schützenswerter Informationen	Die Offenlegung von Betriebsinformationen ist eine hohe Bedrohung für die Vertraulichkeit von Kundendaten und Systemen der kDL, sowie von Netzwerk-, Management- und Monitoringsystemen.	Schutz von Informationen am Arbeitsplatz (Clean-Desk-Policy, Sichtschutz, Bildschirmsperre etc.), Sicherheitsschulungen („Security Awareness“)
G 0.21	Manipulation von Hard- und Software	Hacking und Manipulation kann zu signifikanter Beeinträchtigung von Vertraulichkeit, Integrität und Verfügbarkeit von Kundendaten und Systemen der kDL führen. Zusätzlich können die Steuerung und die Bereitstellung der kDL beeinträchtigt werden.	Sicherheitsmaßnahmen in den Bereichen sicheres Programmieren, automatisierte und manuelle Tests, Systemhärtung, Schwachstellenmanagement, Netzwerksicherheit, Sicherheitsüberwachung und Management von Sicherheitsvorfällen.

Nr.	KRITIS-relevante elementare Gefährdung	Einfluss Kritische Infrastruktur	Sicherheitsmaßnahmen (Beispiele)
G 0.23	Unbefugtes Eindringen in IT-Systeme	Unbefugtes Eindringen in IT-Systeme kann zu signifikanter Beeinträchtigung von Vertraulichkeit, Integrität und Verfügbarkeit von Kundendaten und Systemen der kDL führen. Zusätzlich können die Steuerung und die Bereitstellung der kDL beeinträchtigt werden.	Sicherheitsmaßnahmen in den Bereichen „Sicheres Programmieren“, automatisierte und manuelle Tests, Systemhärtung, Schwachstellenmanagement, Netzwerksicherheit, Sicherheitsüberwachung und Management von Sicherheitsvorfällen. Die Einführung eines geeigneten IDS/IPS kann sinnvoll sein.
G 0.25	Ausfall von Geräten oder Systemen	Durch technisches Versagen von Kernkomponenten kann die Verfügbarkeit der Kritischen Infrastruktur stark beeinträchtigt werden. Im Fall von Datenverlust kann es zu sehr langen Ausfallzeiten und nicht kompensierbaren Schäden kommen.	Business Impact Analyse und Kontinuitätsmanagement (Identifikation und Dokumentation von Abhängigkeiten (z. B. Single-Points-of-Failure), Prozessnotfallpläne, Incident Management), Ausprägung geeigneter technischer Redundanz, kontinuierliche Datensicherung, regelmäßige Tests. Prüfung und ggf. Verringerung von architektureller Komplexität.
G 0.28	Softwareschwachstellen oder -fehler	Schwachstellen können von Angreifern für unmittelbare oder mehrstufige, zeitversetzte Angriffe ausgenutzt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit der Kritischen Infrastruktur zu gefährden.	Asset Management und Festlegung von Schutzbedarfen für Assets, Management von Schwachstellen und Schadsoftware, Sicherheitsüberwachung und Management von Sicherheitsvorfällen.
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Identitätsmissbrauch kann zu Verlust vertraulicher Daten, Sabotage und Manipulation und, speziell in Verbindung mit administrativen Benutzern, zu signifikanten Beeinträchtigungen von Vertraulichkeit, Integrität und Verfügbarkeit von Kundendaten und Systemen der kDL führen.	Organisatorische und verhaltensbildende Maßnahmen einschließlich Definition von Richtlinien und Ausbildung. Zudem Handlungsanweisungen für die Vergabe von Passwörtern und Zugriffsrechten.

Nr.	KRITIS-relevante elementare Gefährdung	Einfluss Kritische Infrastruktur	Sicherheitsmaßnahmen (Beispiele)
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Bewusste oder unbewusste menschliche Fehlhandlungen können zu Beeinträchtigungen der Vertraulichkeit, Integrität und Verfügbarkeit der Kritischen Infrastruktur führen	Organisatorische und verhaltensbildende Maßnahmen einschließlich Definition von Richtlinien und Ausbildung bzgl. Informationssicherheit und Erkennung von Social Engineering. Mitarbeiterbezogene Maßnahmen (z. B. Hintergrundprüfung), Berechtigungsmanagement inkl. Aufteilen kritischer Berechtigungen (Vier-Augen-Prinzip).
G 0.32	Missbrauch von Berechtigungen	Die Bedrohungen durch den Missbrauch der Unternehmensinfrastruktur sind vielfältig und Missbrauch kann u. a. zu unberechtigten Zugriffen, dem Löschen oder der Veröffentlichung vertraulicher Daten, oder der Installation von Spyware oder Ransomware führen.	Berechtigungsmanagement inkl. Aufteilen von Berechtigungen, die Einfluss auf die Dienstleistung der Kritischen Infrastruktur haben, Asset Management Prozesse, und mitarbeiterbezogene Maßnahmen (z. B. Hintergrundprüfung).
G 0.39	Schadprogramme	Schadsoftware kann von Angreifern genutzt werden, um unberechtigten Zugriff zu Systemen zu erlangen, sensitive Daten zu löschen, stehlen oder manipulieren, oder um weitere Installationen von Spyware oder Ransomware vorzunehmen.	Schadsoftwaremanagement, Systemhärtung, frühe Erkennung und Management von Sicherheitsvorfällen.
G 0.40	Verhinderung von Diensten (Denial of Service)	Denial of Service Attacken können Server und Netzwerke durch eine Vielzahl von Zugriffen überfordern und so einen legitimen Zugriff auf die Systeme der kDL, sowie die Netzwerk-, Management- und Überwachungssysteme behindern.	Sicherheitsüberwachungsmaßnahmen und technische Maßnahmen wie z. B. Analyse und Filterung des Netzwerkverkehrs, sowie geeignete Redundanzen.
G 0.42	Social Engineering	Social Engineering kann dazu führen, dass Benutzer oder Administratoren unbewusst vertrauliche Daten preisgeben, Schadprogramme verbreiten oder Zugriff auf geschützte Systeme gewähren. Die Ausnutzung menschlichen Fehlverhaltens wird von Angreifern typischerweise mit weiteren Angriffsmustern kombiniert.	Organisatorische und verhaltensbildende Maßnahmen einschließlich Definition von Richtlinien und Ausbildung bzgl. Informationssicherheit und Erkennung von Social Engineering.

Nr.	KRITIS-relevante elementare Gefährdung	Einfluss Kritische Infrastruktur	Sicherheitsmaßnahmen (Beispiele)
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	Ein unbefugter Zutritt zu Gebäuden bzw. Rechenzentren ermöglicht eine Vielzahl weiterer Angriffsszenarien und kann in Folge zu einer substantiellen Beeinträchtigung von Vertraulichkeit, Integrität und Verfügbarkeit von Kundendaten und Systemen der kDL, sowie von Netzwerk-, Management- und Überwachungssystemen führen.	Physisches und logisches Zugriffsmanagement, Videoüberwachung, Maßnahmen für interne und externe Mitarbeiter (privilegierte Rollen und Endbenutzer). Physische Sicherheitsmaßnahmen, Berechtigungsmanagement, sowie mitarbeiterbezogene Maßnahmen (z. B. Hintergrundprüfung).
G 0.45	Datenverlust	Das Löschen und der Diebstahl sensitiver Daten kann zu schwerwiegenden Beeinträchtigungen der Vertraulichkeit, Verfügbarkeit und Integrität der kDL führen.	Datensicherungs- und Wiederherstellungsverfahren, Verschlüsselung, Berechtigungsmanagement, Aufteilen kritischer Berechtigungen.
G 0.46	Integritätsverlust schützenswerter Informationen	Die Integrität der schützenswerten Informationen ist durch Hacking und Manipulation, Fehlbedienung und Fehlfunktionen gefährdet und kann so zu schwerwiegenden Störungen der kDL führen.	Maßnahmen in den Bereichen sicheres Programmieren, automatisierte und manuelle Tests, Systemhärtung, Schwachstellenmanagement, Netzwerksicherheit, Sicherheitsüberwachung und Management von Sicherheitsvorfällen, sowie mitarbeiterbezogene Maßnahmen (bspw. Awareness-Schulungen).

Tabelle 8: Sicherheitsmaßnahmen zur Risikoreduktion

3.4 Risikobehandlung Hosting und CDN

Neben den im Kapitel 1.6 beschriebenen generell zu beachtenden Punkten gibt es für den Bereich Hosting und CDN spezifische Anforderungen, diese sind im Folgenden beschrieben.

3.4.1 Abgrenzung der zu betrachtenden Risiken

Bei den Risiken, die zu prüfen sind, handelt es sich um Gefahren, die Einfluss auf die in Kapitel 3.1 benannten KRITIS-Schutzziele haben.

Eine Geschäftsrisikoanalyse ist dabei kein notwendiger Bestandteil einer Risikoanalyse.

3.4.2 Risiken und Bedrohungen im Zusammenhang mit den Schutzzielen von spezifischer Technik für Hosting und CDN

Es liegt in der Verantwortung des Betreibers der kDL, anhand des Allgefahren-Ansatzes in Verbindung mit den elementaren Gefährdungen und ihrer dargestellten Relevanz für den Bereich Hosting und CDN eine Risikobetrachtung vorzunehmen. Dies muss unter Berücksichtigung der individuellen Assets (siehe 3.1.1), sowie ihrem Einfluss auf die kDL und der Eintrittswahrscheinlichkeit der Gefährdung erfolgen.

Die Minimierung der Risiken erfolgt durch die Auswahl und Implementierung geeigneter Maßnahmen, wie sie im Kapitel 3.3.2 aufgeführt werden. Die Risikominderung (Risk Mitigation) muss dabei daran ausgerichtet sein, die benannten Schutzbedarfe in Kapitel 3.1 zu erfüllen.

3.4.3 Übersicht der zu betrachtenden Risiken

Eine Übersicht der zu betrachtenden Risiken findet sich in Kapitel 3.3.2.

3.5 Branchenspezifische Technik Hosting und CDN

Wie bereits bei der Definition der Schutzziele und -bedarfe in Kapitel 3.1.3 ausgeführt, liegt die Besonderheit im Bereich Hosting und CDN darin, dass sowohl die kDL, als auch die unterstützende Technik zur Bereitstellung der kDL, aus IT-Systemen besteht.

In diesem Systemverbund stellt die Hostingplattform die branchenspezifische Technik dar, welche die Grundlage zur Erbringung der kDL ist. Als zusätzliche Komponente stellt der Hosting-Betreiber dem Kunden / Nutzer eine technische Kommandoschnittstelle und einen Zugangspfad zum Hosting-Produkt zur Verfügung. Die Sicherheit des Zugangspfades zum Hosting-Produkt als auch die Konfiguration des Hosting-Produktes liegt grundsätzlich beim Hosting-Kunden, sofern es nicht anders vereinbart wird.

Die Verfügbarkeit und Sicherheit und somit auch die Verantwortung für vom Betreiber definierte, interne und externe Schnittstellen (Kommando-Schnittstelle und Admin-Schnittstelle) liegt beim Betreiber.

Nachfolgende Abbildung zeigt diese Zusammenhänge schematisch:

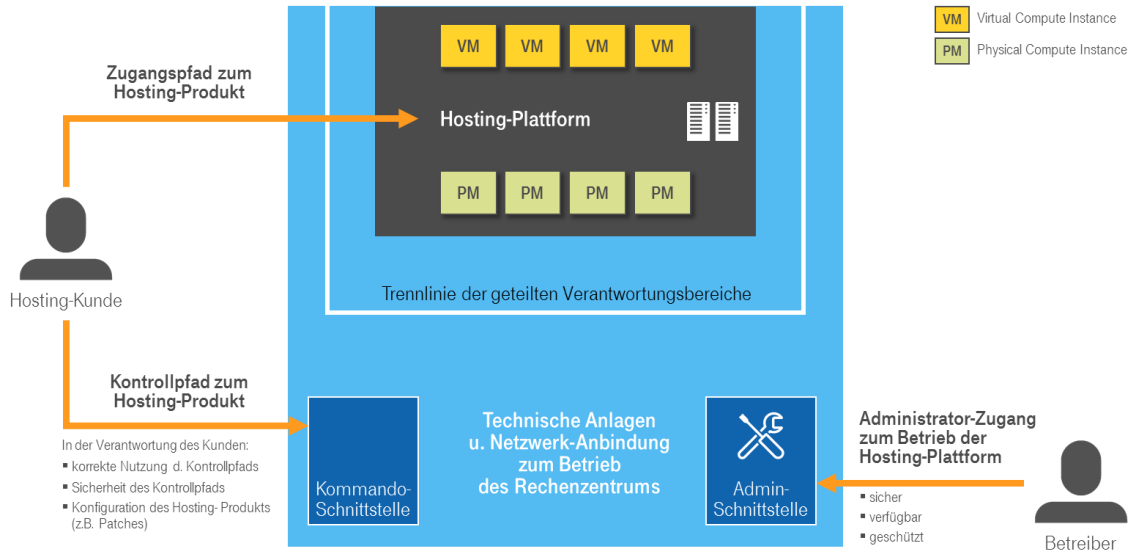

Abbildung 9: Trennung Verantwortungsbereiche im Hosting / Virtuelle Server

Die branchenspezifische Technik im Bereich Hosting und CDN besteht aus Netzwerk- und Management-Systemen, sowie zugehörigen Monitoringsystemen und ist damit Gegenstand der in Kapitel 3.1.3 ausgeführten Schutzziele und Bedarfe.

Dementsprechend müssen für die Entwicklung, den Einsatz, den Betrieb und die Wartung dieser branchenspezifischen Technik vom Betreiber IT-Sicherheitsmaßnahmen nach Stand der Technik vorgesehen werden.

Ferner müssen entsprechende Voraussetzungen bei der Beschaffung erfüllt sein:

- Lieferanten benötigen ein entsprechendes Knowhow zu den Produkten des Herstellers
- Ebenso ist auf die Verfügbarkeit von Ersatzteilen zu achten
- Sofern Wartungen an Dritte vergeben werden sollen, ist die fachliche Kompetenz der Dienstleister sicherzustellen und darauf zu achten, dass zugesicherte Wartungsintervalle eingehalten werden.
- Zusätzlich ist sicherzustellen, dass Dienstleister im Instandsetzungsfall bei Bedarf – je nach Kritikalität – kurzfristig zur Verfügung stehen.

Der Anwendungsbereich für Hosting und CDN umfasst die Leistungen, die mit der Bereitstellung von Hosting- und CDN-Dienstleistung für Kunden im Zusammenhang stehen, nicht aber Technik, die nur für den eigenen Geschäftsbetrieb oder nicht kDL bezogene Prozesse und Dienstleistungen relevant ist.

3.6 Branchenspezifische Architektur und Verantwortung Hosting und CDN

Mit IT als wesentlicher Bestandteil der kDL liegt die besondere Herausforderung für Betreiber im Bereich Hosting mit CDN in der klaren technischen und organisatorischen Trennung der verschiedenen IT-Verbünde. Dies beinhaltet sowohl die strikte Trennung der Betreiberarchitektur der gehosteten Kundenumgebungen, als auch die Separierung der Kundenumgebungen zueinander („Mandantentrennung“). Beides dient der Sicherstellung der Vertraulichkeit und Integrität der jeweiligen Umgebungen.

Je nach Art der betriebenen IT-Dienstleistungen sind unterschiedliche Trennungsmechanismen angemessen, beispielsweise:

- **Organisatorisch**: Rechte- und Rollenkonzepte, Mitarbeiteranweisungen und Verpflichtungen von Mitarbeitern
- **Technisch**: physische bzw. logische Trennung von Netzwerken und Speichersystemen inkl. Datenbanken; Trennung durch bereichsspezifische Verschlüsselung[24].

[24] Siehe auch BSI Dokument „CON.1: Kryptokonzept“

4 Anhang

4.1 Technische Informationssicherheit und bauliche oder physische Sicherheit

Nr.	Maßnahme zur Absicherung von Netzübergängen
A 1.1	Inventarisierung aller Netzzugänge
A 1.2	Netztrennung und Segmentierung, besonders im ICS-Umfeld
A 1.3	Absicherung der Fernzugriffe, Remote Access
A 1.4	Sicheres Sicherheitsgateway, Firewall
A 1.5	Härtung und sichere Basiskonfigurationen
A 1.6	Schnittstellenkontrolle, Intrusion Detection/Prevention (IDS, IPS)
A 1.7	Absicherung mobiler Netzzugänge, mobile Sicherheit, Telearbeit, ggf. BYOD
A 1.8	DDoS-Mitigation
A 1.9	Network Access Control (NAC)
A 1.10	Einsatz von Routern und VPN-Gateways

Tabelle 9: A 1 Absicherung von Netzübergängen

Nr.	Maßnahme zur sicheren Interaktion mit dem Internet
A 2.1	Browser-Virtualisierung, Exploit Protection
A 2.2	Web-Filter
A 2.3	Virtuelle Schleuse
A 2.4	Sichere Dokumentenerstellung
A 2.5	Detektionswerkzeuge für gezielte Angriffe auf Webseiten bzw. über E-Mails
A 2.6	Security Information and Event Management (SIEM)

Tabelle 10: A 2 Sichere Interaktion im Internet

Nr.	Maßnahme für sichere Software (insb. Vermeidung von offenen Sicherheitslücken)
A 3.1	Spam-Abwehr, Content Filtering
A 3.2	Toolunterstützte Inventarisierung von Hardware und Software
A 3.3	Zentrales Patch- und Änderungsmanagement, Konfigurationsmanagement
A 3.4	Schutz vor Schadsoftware
A 3.5	Softwaretest und Freigabe
A 3.6	Software Development Security (sichere Software-Entwicklung)
A 3.7	Security Operation
A 3.8	Sichere Beschaffung und Aussonderung (sicheres Löschen, Überwachung, Daten-sicherung und -wiederherstellung (Backup), Archivierung)

Tabelle 11: A 3 Sichere Software

Nr.	Maßnahme für sichere und zuverlässige Hardware
A 4.1	Sichere Beschaffung und Aussonderung
A 4.2	Geeignete Aufstellung, Schutz vor Umwelteinflüssen, Zugriffsschutz und Einsatz von Diebstahlsicherungen
A 4.3	Schutz von Schnittstellen, inkl. Verhinderung der unautorisierten Nutzung von Schnittstellen, wie z. B. integrierten Mikrofonen, Kameras, Sensoren, UMTS etc.
A 4.4	Geregelte Außerbetriebnahme
A 4.5	Redundanzen, inklusive entsprechender Lieferanten- und Wartungsvereinbarungen, und vertrauenswürdige Lieferanten- und Logistikketten sowie qualifizierte Hersteller
A 4.6	Speicher- und Tamper-Schutz
A 4.7	Patch-, Änderungs- und Konfigurationsmanagement für Firmware

Tabelle 12: A 4 Sichere und zuverlässige Hardware

Nr.	Maßnahme zur Sicheren Authentifizierung
A 5.1	Identitäts- und Rechtemanagement
A 5.2	Multifaktor-Authentisierung (Zweifaktor-Authentisierung)
A 5.3	Zugriffskontrolle (Sicheres Login)
A 5.4	Rollentrennung (Getrennte Administrator-Konten)

Tabelle 13: A 5 Sichere Authentisierung

Nr.	Maßnahme zur Verschlüsselung
A 6.1	Kryptografische Absicherung (Data in Rest, Data in Motion)
A 6.2	Cloud-Daten-Verschlüsselung (Cloud-Encryption)
A 6.3	Verschlüsselung der Kommunikationsverbindungen (z. B. Voice Encryption)
A 6.4	E-Mail-Verschlüsselung
A 6.5	Verschlüsselung der Datenträger z. B. Festplattenverschlüsselung

Tabelle 14: A 6 Verschlüsselung

Nr.	Maßnahme Sonstiges
A 7.1	Sensibilisierung und Schulungen
A 7.2	Übungen
A 7.3	Aufrechterhaltung des aktuellen Informationsstands durch Bezug von Warnungen, CERT-Meldungen, Lagebild
A 7.4	Verfügbarkeit notwendiger Ressourcen
A 7.5	Interne Audits und Penetrationstests
A 7.6	Sicherheitsstrategie und Sicherheitsleitlinie

Tabelle 15: A 7 Sonstiges

Nr.	Maßnahme Bauliche/physische Sicherheit
A 8.1	Zugangskontrolle
A 8.2	Notstromversorgung (USV)
A 8.3	Netzersatzanlagen

Tabelle 16: A 8 Bauliche/physische Sicherheit

4.2 KRITIS-relevante elementare Gefährdungen

Die nachfolgende Liste des BSI benennt alle für Betreiber Kritischer Infrastruktur relevanten elementaren 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 0.6: Katastrophen im Umfeld
- G 0.7: Großereignisse im Umfeld
- G 0.8: Ausfall oder Störung der Stromversorgung
- G 0.9: Ausfall oder Störung von Kommunikationsnetzen
- G 0.10: Ausfall oder Störung von Versorgungsnetzen
- G 0.11: Ausfall oder Störung von Dienstleistern
- G 0.12: Elektromagnetische Störstrahlung
- G 0.13: Abfangen kompromittierender Strahlung
- G 0.14: Ausspähen von Informationen/Spionage
- G 0.15: Abhören
- G 0.16: Diebstahl von Geräten, Datenträgern und Dokumenten
- G 0.17: Verlust von Geräten, Datenträgern und Dokumenten
- G 0.18: Fehlplanung oder fehlende Anpassung
- G 0.19: Offenlegung schützenswerter Informationen
- G 0.20: Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21: Manipulation von Hard- und Software
- G 0.22: Manipulation von Informationen
- G 0.23: Unbefugtes Eindringen in IT-Systeme
- G 0.24: Zerstörung von Geräten oder Datenträgern
- G 0.25: Ausfall von Geräten oder Systemen
- G 0.26: Fehlfunktion von Geräten oder Systemen
- G 0.27: Ressourcenmangel
- G 0.28: Softwareschwachstellen 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 0.33: Personalausfall
- G 0.34: Anschlag
- G 0.35: Nötigung, Erpressung oder Korruption
- G 0.36: Identitätsdiebstahl
- G 0.37: Abstreiten von Handlungen
- 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

4.3 Begriffe und Abkürzungen

Begriff/Akronym	Beschreibung
AGB	Allgemeine Geschäftsbedingungen
APT	Advanced Persistent Threat
ATM	Automated Teller Machine (Geldautomat)
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BGB	Bürgerliches Gesetzbuch
BIA	Business Impact-Analysen
BKA	Bundeskriminalamt
BMA	Brandmeldeanlage
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI Kritisverordnung)
BSIG	BSI Gesetz – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSI IT-Grundschutz	IT-Grundschutz des BSI
B3S	Branchenspezifischer Sicherheitsstandards
BYOD	Bring your own device
C5	Cloud Computing Compliance Controls Catalog
CA	Certificate Authority
CCTV	Closed Circuit Television
CDN	Content Delivery Netzwerk
DDOS	Denial-of-Service
DSL	Digital Subscriber Line
DWD	Deutscher Wetterdienst
eIDAS VO	Verordnung (EU) Nr. 910 / 2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999 / 93 / EG

EMA	Einbruchmeldeanlage
EN	Europäische Normen
ENISA	The European Union Agency for Network and Information Security
ERP-Systeme	Enterprise Resource Planning-Systeme
ETSI	European Telecommunications Standards Institute
EU-DSGVO	EU-Datenschutzgrundverordnung
FAQ	Frequently Asked Questions
GLT	Gebäudeleittechnik
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnik
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Informationstechnologie
IT-Grundschutz	IT-Grundschutz des BSI
IT-SiG	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
ITIL	Information Technology Infrastructure Library
kDL	Kritische Dienstleistung
KRITIS	Kritische Infrastrukturen
LKA	Landeskriminalamt
NEA	Netzersatzanlage
NIS Richtlinie	Richtlinie zur Netz- und Informationssicherheit
PaaS	Platform as a Service
RZ	Rechenzentrum
SaaS	Software as a Service
SIEM	Security Incident Event Management
SigG	Signatur-Gesetz

SigV	Signaturverordnung
SLA	Service Level Agreement
SSL	Secure Sockets Layer
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunications System
USV	Unterbrechungsfreie Stromversorgung
VDG	Vertrauensdienstegesetz
VPN	Virtual Private Network

4.4 Referenzverzeichnis

BSI Standard 200-3	BSI-Standard 200-3 Risikoanalyse auf Basis des IT-Grundschutz
BSI Standard 200-4	BSI-Standard 200-4 Business Continuity Management
BSI C5:2020	BSI Cloud Computing Compliance Criteria Catalogue
DIN EN 50600-1:2019	Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 1: Allgemeine Konzepte Englisch: Information technology – Data centre facilities and infrastructures – Part 1: General concepts
DIN 77200-1:2017	Sicherungsdienstleistungen – Teil 1: Allgemeine Anforderungen an Sicherheitsdienstleister
ISO/IEC 22301:2019	Security and resilience – Business continuity management systems – Requirements Übersetzung (Deutsch): Sicherheit und Resilienz – Business Continuity Management System – Anforderungen
ISO/IEC 27001:2017	Information technology – Security techniques – Information security management systems – Requirements Übersetzung (Deutsch): Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen
ISO/IEC 27002:2022	Information security, cybersecurity and privacy protection – Information security controls Übersetzung (Deutsch): Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen
ISO/IEC 27005:2018	Information technology – Security techniques Information security risk management Übersetzung (Deutsch): Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Risikomanagement
ISO/IEC 27035-1:2016	Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management Übersetzung (Deutsch): Informationstechnik - IT Sicherheitsverfahren – Informationssicherheit Störfallmanagement – Teil 1: Grundlagen des Störfallmanagements