Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG

Handlungsempfehlungen für Autoren eines B3S

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.3	23.02.2024	Anpassung des regelmäßigen Gültigkeitszeitraums für B3S auf drei Jahre
1.2	11.07.2023	Hinweis auf die vom Ergebnis der Prüfung unabhängigen Gebührenpflicht von B3S in Abschnitt 2.6 ergänzt
1.1	01.09.2021	Inhaltliche Überarbeitung, u. a. • Einführung einer deutlichen Abgrenzung zwischen den Begriffen „Geltungsbereich“ und „Anwendungsbereich“ (siehe 4.1.1 für weiterführende Informationen) • Aktualisierung der Abschnitte 2.4, 2.5 und 2.6 im Hinblick auf Änderungen im Erstellungs-, Einreichungs- und Prüfprozess • Inhaltliche Überarbeitung der Abschnitte 4.2 und 4.5 • Anpassung an Aktualisierungen der „Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG“ • Aufnahme KRITIS-relevanter elementarer Gefährdungen in Anhang 5.1 • Aktualisierung der in Anhang 5.2 aufgeführten Maßnahmenkategorien • Aufnahme besonders zu berücksichtigender Bedrohungsszenarien und Maßnahmenkategorien in Anhang 5.3 • Zahlreiche redaktionelle Änderungen • Einarbeitung des Feedbacks des Themenarbeitskreises Audits und Standards des UP KRITIS
1.0	01.12.2017	Veröffentlichung der Version 1.0 der OH B3S

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6166
E-Mail: kritis.buero@bsi.bund.de
Internet: www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2024

Inhalt

1 Überblick 5
1.1 Zielsetzung und Adressatenkreis der Orientierungshilfe 5
1.2 Gesetzliche Grundlage 5
1.3 Wegweiser durch die Orientierungshilfe 5
1.4 Weiterführende Informationen 6
2 Der branchenspezifische Sicherheitsstandard (B3S) 7
2.1 Was ist ein B3S? 7
2.2 Welche Vorteile bietet ein B3S? 7
2.3 Welche Rollen gibt es bei der Erstellung eines B3S? 8
2.4 Erstellungs-, Einreichungs- und Prüfprozess 8
2.5 Vorabsichtung des Entwurfs 8
2.6 Eignungsprüfung und Bescheid der Eignungsfeststellung 9
2.7 Verwendung des Mapping-Formulars 10
2.8 Gültigkeit und Evaluierung eines B3S 10
2.9 Vertraulichkeit und Veröffentlichung 11
3 Empfehlungen zur Erstellung eines B3S 12
3.1 Struktur eines B3S und Detailtiefe 12
3.2 Einbeziehung bestehender Standards und Vorgaben 14
4 Inhaltliche Aspekte branchenspezifischer Sicherheitsstandards 15
4.1 Anwendungsbereich und Schutzziele 16
4.1.1 Anwendungsbereich 16
4.1.2 Anwendungsbereich umfasst auch extern erbrachte Leistungen 17
4.1.3 Gesetzlicher Rahmen 18
4.1.4 Schutzziele 18
4.2 Branchenspezifische Gefährdungslage 19
4.2.1 All-Gefahrenansatz 19
4.2.2 Relevanz von Gefährdungen 19
4.3 Risikomanagement 20
4.3.1 Geeignete Behandlung aller für die kDL relevanten Risiken 20
4.3.2 Beschränkung der Behandlungsalternativen für Risiken 20
4.3.3 Berücksichtigung von Abhängigkeiten bei der Risikoanalyse 20
4.3.4 Berücksichtigung der allgemeinen Gefährdungslage 20
4.3.5 Berücksichtigung der branchenspezifischen Gefährdungslage 21
4.4 Abzudeckende Themen 21
4.4.1 Informationssicherheitsmanagement-System (ISMS) 22
4.4.2 Asset Management 22

4.4.3 Continuity- und Notfallmanagement für die kDL ... 22
4.4.4 Technische Informationssicherheit ... 23
4.4.5 Personelle und organisatorische Sicherheit ... 23
4.4.6 Bauliche/physische Sicherheit ... 24
4.4.7 Vorfallserkennung und -bearbeitung ... 24
4.4.8 Überprüfung im laufenden Betrieb ... 24
4.4.9 Lieferanten, Dienstleister und Dritte ... 25
4.4.10 Branchenspezifische Technik und (Kern-)Komponenten (Beschaffung, Entwicklung, Einsatz, Betrieb und Wartung) ... 25
4.5 Anwendungshinweise für Betreiber als Anwender eines B3S ... 25
4.5.1 Behandlung der Gefährdungen und Anpassung des B3S durch Betreiber ... 25
4.5.2 Konkretisierung des Anwendungsbereichs durch die Betreiber ... 26
4.5.3 Fortschreibung und Erfahrungen der Anwender ... 26
5 Anhänge ... 27
5.1 KRITIS-relevante elementare Gefährdungen ... 27
5.2 Technische Informationssicherheit & bauliche/physische Sicherheit ... 28
5.2.1 Technische Informationssicherheit ... 28
5.2.2 Bauliche/physische Sicherheit ... 31
5.3 Besonders zu berücksichtigende Bedrohungsszenarien und Maßnahmenkategorien ... 31
5.4 Glossar ... 32

1 Überblick

1.1 Zielsetzung und Adressatenkreis der Orientierungshilfe

Die vorliegende Orientierungshilfe stellt eine Handlungshilfe für Autoren branchenspezifischer Sicherheitsstandards (B3S) dar.

In Bereichen, in denen es noch keinen B3S gibt, kann diese Orientierungshilfe eine Unterstützung für Betreiber Kritischer Infrastrukturen zur Umsetzung von § 8a Absatz 1 BSI-Gesetz (BSIG) darstellen. Betreibern bietet sie die Möglichkeit, die Kriterien für die Sicherheitsvorkehrungen der Anlagen herzuleiten, analog wie es für Autoren zur Erstellung eines B3S in dieser Orientierungshilfe beschrieben wird.

Da die von Betreibern gemäß § 8a Absatz 1 BSIG umzusetzenden Sicherheitsvorkehrungen und damit auch die von einem B3S zu gewährleistenden Anforderungen große Freiheiten in der Art der Umsetzung lassen, stellt auch diese Orientierungshilfe keine verbindliche Vorgabe dar. Vielmehr gibt sie einen qualitativen Rahmen, innerhalb dessen gleichwertige Alternativen möglich sind.

1.2 Gesetzliche Grundlage

Die rechtliche Grundlage der B3S ergibt sich aus § 8a Absatz 2 BSIG
(siehe z. B. www.gesetze-im-internet.de/bsig_2009/).

Das BSIG sieht vor, dass B3S erarbeitet werden können, die jeweils eine Möglichkeit der Erfüllung der Anforderungen an die Umsetzung von § 8a Absatz 1 BSIG (inkl. „Stand der Technik“) darstellen. B3S können von Betreibern Kritischer Infrastrukturen oder ihren Fachverbänden beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Eignungsfeststellung eingereicht werden. Eine gesetzliche Pflicht zur Erarbeitung eines B3S besteht nicht. Die Erstellung eines B3S ist für die Betreiber bzw. für die Fachverbände jedoch eine Chance, selbst aufzuzeigen, wie ein Schutz nach „Stand der Technik" in der jeweiligen Branche realisiert werden kann. Ein B3S trägt dazu bei, den Interpretationsspielraum auch im Rahmen von Prüfungen zu verringern.

Für einige Betreiber gelten spezielle gesetzliche Regelungen (z. B. Regelungen gemäß § 8d BSIG, EnWG oder TKG), die bei der Erstellung bzw. bei der Nutzung eines B3S zu beachten sind. Auf solche abweichenden Rechtsgrundlagen wird in dieser Orientierungshilfe nicht näher eingegangen.

1.3 Wegweiser durch die Orientierungshilfe

Kapitel 1 der Orientierungshilfe beschreibt die Zielsetzung dieses Dokuments und die gesetzlichen Grundlagen. Kapitel 2 gibt eine Einführung in branchenspezifische Sicherheitsstandards, eine Begriffserläuterung (Abschnitt 2.1), die typischen Vorteile eines B3S für die Betreiber (Abschnitt 2.2) und die bei Erstellung und Anwendung wesentlichen Rollen (Abschnitt 2.3).

Der Einreichungs-, Bewertungs- und Prüfprozess wird in den Abschnitten 2.4 bis 2.9 beschrieben. Außerhalb des formalen Prozesses der Eignungsprüfung empfiehlt das BSI, bereits frühzeitig Kontakt mit dem BSI aufzunehmen, um bereits in möglichst frühen Phasen ein gemeinsames Verständnis zum Vorhaben aufzubauen und einen direkten Austausch zu pflegen. Offene Fragen können so geklärt werden, bevor unnötiger Aufwand entsteht.

Die bisherige Erfahrung in der Erstellung von B3S zeigt, dass vor allem der Einstieg und die Wahl eines geeigneten Vorgehens für die Autoren eine Hürde darstellen. Kapitel 3 gibt daher Empfehlungen zur Erstellung eines B3S. Hierdurch sollen u. a. Aufwände für Korrekturen im Erstellungsprozess und für spätere Fortschreibungen verringert werden. Der damit verbundene Abstimmungsprozess zwischen Autoren und BSI wird so erleichtert.

Kapitel 4 listet typische Themen auf, die von einem B3S behandelt werden sollten. Analog zur in Abschnitt 3.1 empfohlenen Struktur eines B3S beginnen die Themenfelder mit allgemeinen, grundlegenden Inhalten, die eher direkt von den Autoren im B3S definiert werden können (Abschnitte 4.1 bis 4.3). Die Themenfelder in Abschnitt 4.4 befassen sich hingegen mit konkreteren Themen, für die im B3S Maßnahmen oder die Ableitung von Maßnahmen konkret beschrieben werden sollte. Ferner sind Anwendungshinweise zur Umsetzung des B3S beim Betreiber (Abschnitt 4.5) vorgesehen.

Kapitel 5 enthält Anhänge zur vorliegenden Orientierungshilfe. Diese umfassen insbesondere Listen zu KRITIS-relevanten elementaren Gefährdungen (Abschnitt 5.1), typischen Maßnahmenkategorien (Abschnitt 5.2) und besonders zu berücksichtigende Bedrohungsszenarien und Maßnahmenkategorien (Abschnitt 5.3). Sie können von den Autoren eines B3S zur Identifikation der in ihrem Anwendungsbereich (siehe Abschnitt 4.1.1 für die Definition dieses Begriffs) relevanten konkreten Bedrohungen, Schwachstellen und Maßnahmen herangezogen werden. Der Anhang enthält auch ein Glossar (Abschnitt 5.4).

1.4 Weiterführende Informationen

Zur Orientierungshilfe gehören als ausgegliederte Dokumente das „Mapping-Formular zur Orientierungshilfe B3S“, eine Fragen-Antwort-Liste (FAQ) mit weitergehenden Erläuterungen zu wiederkehrenden Fragen und ein Formular zur Einreichung eines B3S beim BSI (siehe www.bsi.bund.de/kritis-downloads). Mit Hilfe des Mapping-Formulars können die Autoren eines B3S relevante Zusatzinformationen für die Bewertung des B3S liefern – beispielsweise über die Inhalte des B3S hinausgehende Erklärungen, wie die Inhalte hergeleitet wurden oder warum diese geeignet sind, um den Stand der Technik widerzuspiegeln (siehe Abschnitt 2.7).

2 Der branchenspezifische Sicherheitsstandard (B3S)

2.1 Was ist ein B3S?

Ein B3S ist typischerweise kein von einer Normungsorganisation wie DIN oder ISO erstellter Standard. Er soll ein Konzept sein, das von Branchenvertretern gemeinsam definiert wurde, um geeignete Sicherheitsanforderungen bzw. Sicherheitsvorkehrungen zur Erfüllung des § 8a Absatz 1 BSIG für einen festgelegten Anwendungsbereich (siehe Abschnitt 4.1.1 für die Definition dieses Begriffs) zusammenzustellen.

Es ist durchaus möglich, dass es in einer Branche mehrere B3S gibt, die sich z. B. durch den Anwendungsbereich oder spezifische Anforderungen in speziellen Umgebungen oder Lagen unterscheiden.

Eine gesetzliche Pflicht zur Erarbeitung eines solchen B3S besteht nicht. Auch müssen KRITIS-Betreiber einen B3S nicht zwingend anwenden, auch wenn für ihre Branche ein solcher vorliegt. Es bleibt jedem Betreiber überlassen, einen B3S anzuwenden, diesen auf seine individuellen Gegebenheiten anzupassen oder ggf. angemessen zu ergänzen. In der Gesamtschau müssen die umgesetzten Einzelmaßnahmen immer angemessen und wirkungsvoll sein. Es bleibt die Pflicht des Betreibers, dies sicherzustellen.

2.2 Welche Vorteile bietet ein B3S?

Ein B3S gemäß § 8a Absatz 2 BSIG gibt Betreibern Kritischer Infrastrukturen und ihren Branchenverbänden die Möglichkeit, die zur Erfüllung von § 8a Absatz 1 BSIG erforderlichen Vorkehrungen innerhalb ihres Bereiches aufzuzeigen. Dies hat für die Betreiber wesentliche Vorteile:

1. Durch die Eignungsprüfung wird die Interpretation der Autoren des B3S vom BSI auf Eignung zur Erfüllung von § 8a Absatz 1 BSIG geprüft. Die Anwender eines B3S gewinnen Sicherheit bzgl. der Interpretation der abstrakten Begriffe des BSIG wie „angemessen“, „geeignet“ und „Stand der Technik“. Diese sind unter anderem vom Schutzbedarf und der Gefährdungslage der jeweiligen Branche sowie von der in den Anlagen der Kritischen Infrastruktur verwendeten Technik abhängig.
2. Ein B3S gibt den Anwendern Hilfestellungen in der Umsetzung von § 8a Absatz 1 BSIG. Insbesondere erleichtert er den Anwendern die Identifikation geeigneter Vorkehrungen und hilft, eine geeignete Methodik zur Umsetzung zu finden. Angemessene Maßnahmen sollen durch den B3S einfacher zu finden sein.
3. Ein B3S berücksichtigt branchenspezifische Anforderungen. Insbesondere können Best Practices der jeweiligen Branche definiert werden, um bei der Umsetzung durch eine effiziente Integration in etablierte Techniken und Vorgehensweisen zugleich Wirtschaftlichkeit und Wirksamkeit zu steigern. Außerdem gibt ein B3S für die gesetzlich geforderten Nachweise der Umsetzung von § 8a Absatz 1 BSIG die Möglichkeit, die Kriterien der „Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG“ entsprechend branchenüblicher Prüfungen, Audits oder Zertifizierungen zu präzisieren und damit effizient und wirtschaftlich zu gestalten. Die „Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG“ ist auf der Website des BSI veröffentlicht: www.bsi.bund.de/OHNachweise
4. Sind B3S entsprechend detailliert, können sie ggf. auch für die Erstellung einer Prüfgrundlage zur Erbringung von Nachweisen gemäß § 8a Absatz 3 BSIG herangezogen werden, da ein B3S, dessen Eignung durch das BSI offiziell festgestellt wurde, den Stand der Technik in der Branche konkretisiert. Ob und in welchem Umfang dies geschieht, liegt allerdings im Ermessen des Prüfers.

Hinweis: *Die vorliegende Orientierungshilfe soll die Erstellung solcher B3S begleiten. Im Sinne einer Handlungshilfe handelt es sich hierbei nicht um harte Vorgaben, sondern um einen qualitativen Rahmen. Gleichwertige Alternativen zu der beschriebenen Vorgehensweise und den Kriterien sind möglich. Entsprechend sind im Folgenden die Begriffe „sollen“, „können“ und „sollten“ synonym zu verstehen.*

2.3 Welche Rollen gibt es bei der Erstellung eines B3S?

An der Erstellung und Anwendung eines B3S sind verschiedene Rollen beteiligt, die für ein einheitliches Verständnis hier definiert werden. Die Rollen schließen sich gegenseitig nicht aus, eine Person kann mehrere Rollen zugleich wahrnehmen.

Die **Autoren** eines B3S sind die Personen, die den Text des B3S verfassen und somit die Inhalte gestalten. Beispielsweise können die Autoren Mitglieder eines BAK (Branchenarbeitskreis des UP KRITIS) sein oder auch Mitarbeiter eines von der einreichenden Stelle beauftragten Dienstleisters. Im Gegensatz zur einreichenden Stelle dürfen als Autoren auch Personen mitwirken, die nicht zur Beantragung einer Eignungsprüfung gemäß § 8a Absatz 2 BSIG berechtigt sind.

Die **einreichende Stelle** ist ein Betreiber, ein Zusammenschluss mehrerer Betreiber oder ein Branchenverband, die gemäß § 8a Absatz 2 BSIG berechtigt sind, eine Eignungsprüfung eines B3S beim BSI zu beantragen.

Da an einem B3S in der Regel mehrere Autoren mitwirken, wird von der einreichenden Stelle ein **Ansprechpartner B3S** benannt, der den Kontakt zum BSI hält und während der Eignungsprüfung für Rückfragen verfügbar ist. Dies kann auch eine Person sein, die selbst nicht zur Beantragung einer Eignungsprüfung gemäß § 8a Absatz 2 BSIG berechtigt ist.

Der **Anwender** ist der Nutzer des fertig erstellten B3S. In der Regel handelt es sich hierbei um den Betreiber einer Kritischen Infrastruktur, der einen B3S zur Umsetzung von § 8a Absatz 1 BSIG anwendet. Ein Anwender kann auch mehrere B3S anwenden, beispielsweise wenn der Anwendungsbereich der B3S jeweils nur einen Teil seiner Anlagen umfasst.

Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** prüft auf Antrag die Eignung eines B3S zur Umsetzung der Anforderungen gemäß § 8a Absatz 1 BSIG. Bei Bedarf kann das BSI auch während der Erstellung eines B3S die Autoren bzw. die einreichende Stelle unterstützen, z. B. durch Workshops. Im Rahmen der Eignungsprüfung durch das BSI erfolgt nach § 8a Absatz 2 BSIG eine Abstimmung mit dem **Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)** und mit den zuständigen Aufsichtsbehörden.

2.4 Erstellungs-, Einreichungs- und Prüfprozess

Der Prozess zur Erstellung, Einreichung und Prüfung eines B3S besteht im Allgemeinen aus

- Gesprächen und Workshops der Autoren,
- unverbindlichen Vorgesprächen und Workshops mit dem BSI,
- einer Vorabsichtung von Zwischenergebnissen durch das BSI,
- einer verbindlichen Einreichung des finalen B3S beim BSI und
- einer verbindlichen Eignungsprüfung durch das BSI mit abschließendem Bescheid.

Die verbindliche Einreichung ist Ausgangspunkt der Eignungsprüfung. Die Schritte vor der verbindlichen Einreichung sind optional. Sie dienen dazu, einen frühzeitigen Austausch zwischen BSI und Autoren bzw. einreichender Stelle aufzubauen und ein gemeinsames, zielgerichtetes Verständnis des Vorhabens zu gewinnen.

Bei Fragen zur Erstellung eines B3S können mit dem BSI Gespräche oder Workshops durch eine formlose E-Mail an kritische.infrastrukturen@bsi.bund.de vereinbart werden.

2.5 Vorabsichtung des Entwurfs

Damit bereits frühzeitig ein gemeinsames Verständnis zwischen Betreibern, ihren Verbänden und dem BSI sowie ggf. den Aufsichtsbehörden hergestellt werden kann, bietet das BSI eine Vorabsichtung eines B3S auf dessen Eignung an.

Die Arbeiten an den unterschiedlichen Teilen des B3S können sich überlappen, wobei die Fertigstellung eines Teils entsprechend Abschnitt 3.1 einen typischen Anlass für eine Vorabsichtung bietet. Der B3S kann während der Vorabsichtung bereits weiter verbessert werden.

Durch Vorgespräche mit dem BSI bzw. durch eine Vorabsichtung kann die Branche ein Zwischenergebnis bzgl. der Eignung des erarbeiteten B3S erhalten, natürlich nur auf Grundlage der vorgelegten Informationen und unter Vorbehalt zusätzlicher Erkenntnisse aus weiteren Prüfungen sowie der im Rahmen der eigentlichen Eignungsprüfung notwendigen Abstimmung mit anderen Behörden. Diese Möglichkeit, sich frühzeitig zum Nachbesserungsbedarf auszutauschen, hat sich als positiv für alle Beteiligten erwiesen.

Bei Zustimmung der einreichenden Stelle können die Teilergebnisse auch schon an die anderen zu beteiligenden Behörden zur Vorabinformation weitergegeben werden, so dass die spätere, eigentliche Eignungsprüfung erheblich beschleunigt werden kann.

Im Gegensatz zu allgemeinen Diskussionen und Workshops werden in einer Vorabsichtung relativ stabile Versionen des B3S oder einzelner Kapitel tiefgehender und durch alle zuständigen Fachreferate des BSI begutachtet. Die Bewertung durch das BSI ist weiterhin unverbindlich. Allerdings bekommen die Autoren hierbei eine frühe Rückmeldung.

2.6 Eignungsprüfung und Bescheid der Eignungsfeststellung

Wurde ein B3S fertiggestellt, kann dieser mit Hilfe eines Formulars beim BSI zur Prüfung seiner Eignung gemäß § 8a Absatz 2 BSIG eingereicht werden. Das Formular umfasst die notwendigen Metadaten für die Beantragung der Eignungsprüfung sowie eine Checkliste zu formalen Informationen über das Dokument. Zusätzlich zu dem Antragsformular sollte das Mapping-Formular (siehe Abschnitt 2.7) ausgefüllt und eingereicht werden.

Die Eignungsprüfung eines B3S durch das BSI ist kostenpflichtig. Diese Kosten werden auf Basis der Zeit bemessen, die für die Durchführung der Eignungsprüfung von BSI-Mitarbeitern aufgewendet werden musste. Das Antragsformular sollte daher möglichst vollständig und widerspruchsfrei ausgefüllt werden, um Nachfragen und damit die Bearbeitungszeit zu minimieren. Sollte der Antrag zurückgezogen werden oder das Verfahren der Prüfung aus anderen Gründen abgebrochen werden, fallen Kosten im Rahmen der bis zu diesem Zeitpunkt entstandenen Aufwände an.

Das BSI prüft anhand der eingereichten Unterlagen, ob diese geeignet sind, die Anforderungen gemäß § 8a Absatz 1 BSIG innerhalb des vom B3S definierten Anwendungsbereichs und in Bezug auf die branchenspezifische Gefährdungslage und die Risikobetrachtung zu erfüllen. Die Prüfung der Eignung erfolgt in Abstimmung mit dem BBK und den zuständigen Aufsichtsbehörden.

Grundsätzlich sind zur Gewährleistung der Anforderungen gemäß § 8a Absatz 1 BSIG die Teile „Anwendungsbereich, Gefährdungs- und Risikoanalyse“ und „Sicherheitsanforderungen nach Stand der Technik und Vorgehensweisen“ (siehe Abschnitt 3.1) eines B3S erforderlich. Daraus folgt, dass ein Dokument, welches nur einen der beiden Teile beinhaltet, zwar bei der Umsetzung von § 8a Absatz 1 BSIG unterstützen kann, im Allgemeinen aber noch keinen kompletten B3S darstellt.

Eventuelle Ausführungen im B3S über die Nachweisbarkeit der Umsetzung (Prüfungen) im Sinne von § 8a Absatz 3 BSIG sind zur Eignungsfeststellung nicht erforderlich. Im Rahmen der Eignungsprüfung kann das BSI diesen Teil ggf. sichten und kommentieren, bezieht diesen aber nicht in die Eignungsfeststellung ein.

Die Eignungsprüfung kann zu dem Ergebnis kommen, dass die Eignung eines B3S durch das BSI festgestellt wurde (positives Ergebnis) oder dass die Eignung durch das BSI nicht festgestellt werden konnte (negatives Ergebnis). In beiden Fällen versendet das BSI einen Bescheid an die einreichende Stelle.

Gründe für eine Nichtanerkennung der Eignung können zum Beispiel ein zu hoher Abstraktionsgrad oder zu viele implizite Annahmen sein.

Beispiel: *Bei einer Einreichung in der ohne weitere Ausführungen nur auf den BSI IT-Grundschutz oder ISO/IEC 27001 verwiesen wird, könnte die Eignung als B3S durch das BSI nicht festgestellt werden (negatives Ergebnis).*

Das Ergebnis der Eignungsprüfung wird – ggf. unter Auflagen oder Einschränkungen – der einreichenden Stelle durch einen Bescheid zugestellt. Bei Mängeln am B3S versucht das BSI, bereits im Rahmen des Prüfprozesses bzw. bei der Vorabsichtung in Zusammenarbeit mit den Autoren eine Korrektur herbeizuführen.

2.7 Verwendung des Mapping-Formulars

Neben dem Antragsformular ist für die Eignungsprüfung die Verwendung eines Mapping-Formulars vorgesehen (www.bsi.bund.de/dok/b3s-mapping). Diese hilft dabei, die Eignung eines B3S eindeutig und ohne großen Aufwand nachvollziehbar zu machen. Hier können die Autoren für jedes Kriterium der Orientierungshilfe angeben, durch welchen Abschnitt des B3S dieses erfüllt wurde. Durch eine Kurzbeschreibung der Umsetzung soll dargelegt werden, wie das jeweilige Kriterium im B3S geeignet umgesetzt wurde bzw. erklärt werden, warum ein Kriterium innerhalb des Anwendungsbereichs des B3S nicht berücksichtigt werden muss oder wie es durch eine gleichwertige Alternative ersetzt wird.

Durch das sorgfältige Ausfüllen des Mapping-Formulars durch die B3S-Autoren können Missverständnisse und Nachfragen seitens des BSI während der Eignungsfeststellung vermieden werden. Andernfalls kann es schwierig sein, grundsätzlich geeignete Vorkehrungen mangels Nachvollziehbarkeit angemessen zu bewerten. Dadurch kann die Bewertung durch zusätzlichen Prüfaufwand erheblich länger dauern oder es können zusätzliche Gespräche notwendig werden, insbesondere, wenn weitere Aufsichtsbehörden eingebunden sind.

Das Mapping-Formular kann später auch Anwendern des B3S helfen, die Aussagen des B3S nachzuvollziehen und so auf geänderte Rahmenbedingungen besser zu reagieren.

2.8 Gültigkeit und Evaluierung eines B3S

Das BSI stellt die Eignung eines B3S im Allgemeinen für drei Jahre fest, danach ist dieser für eine fortbestehende Aussage über seine Eignung dem BSI erneut vorzulegen. Wenn Änderungen abzusehen sind, die eine frühere Prüfung sinnvoll erscheinen lassen, kann der Eignungszeitraum beispielsweise auf zwei Jahre verkürzt werden.

Ein B3S kann auch nach Ablauf des Eignungszeitraums weiter genutzt werden, er wird nicht „unzulässig“, aber die Aussage des BSI über seine Eignung erlischt. Die Gültigkeit ist im Allgemeinen auf drei Jahre begrenzt, da über einen längeren Zeitraum die Gefahr wächst, dass sich die Gefährdungslage, die Prozesse einer Kritischen Infrastruktur oder die Wirksamkeit von Maßnahmen zu stark ändern, um die getroffene Aussage über eine Eignung fortbestehen zu lassen. Auf der anderen Seite würde ein kürzerer Zeitraum den Autoren nicht genug Gelegenheit für eine Evaluierung und Fortschreibung des B3S lassen. Nach Ablauf des Eignungszeitraums (und bei Bedarf auch schon früher) kann der fortgeschriebene B3S dem BSI erneut zur Eignungsprüfung vorgelegt werden. Dabei ist unerheblich, ob lediglich kleinere oder auch größere Änderungen vorgenommen wurden. Grundsätzlich könnte sogar der gleiche B3S erneut zur Eignungsprüfung eingereicht werden, wenn keine Änderungen erforderlich waren.

Generell sollten die Anwender die aktuelle Version eines B3S verwenden. Fortschreibungen eines B3S können auch schon vor Ablauf der Eignungsfeststellung erneut beim BSI eingereicht werden, z. B. wenn dieser aufgrund geänderter Gefahrenlage oder neuer Maßnahmen nach Stand der Technik geändert wurde und die einreichende Stelle eine erneute Eignungsfeststellung wünscht.

Wird ein B3S erneut eingereicht, findet ein erneutes Prüfungsverfahren der Eignung nach den aktuellen Regeln und Maßgaben statt.

2.9 Vertraulichkeit und Veröffentlichung

Die Rechte am B3S bleiben von der Eignungsprüfung unangetastet: Der B3S bleibt Eigentum des ursprünglichen Eigentümers (im Allgemeinen der einreichenden Stelle). Entsprechend kann der Eigentümer darüber entscheiden, ob und wo der B3S veröffentlicht wird und wie die Konditionen zum Bezug des B3S sind. Das BSI bietet an, auf den BSI-Webseiten einen Link auf eine Webseite zum B3S zu veröffentlichen oder bei einer Veröffentlichung zu unterstützen.

Eine Liste der bereits in Arbeit befindlichen bzw. veröffentlichten B3S ist auf der Website des BSI veröffentlicht: www.bsi.bund.de/b3s.

Die Tatsache, dass sich ein B3S in einer Eignungsprüfung befindet oder bereits eine Eignungsfeststellung erhalten hat, ist im Allgemeinen öffentlich. Eine Weitergabe des B3S innerhalb des BSI, an das BBK und an die zuständigen Aufsichtsbehörden ist im Rahmen der Eignungsprüfung immer erforderlich und erfolgt unter Wahrung der vereinbarten Vertraulichkeitsstufen.

3 Empfehlungen zur Erstellung eines B3S

Das nachfolgende Kapitel gibt Empfehlungen zur Erstellung und Strukturierung eines B3S. Hierzu wurden die bisherigen Erfahrungen des BSI und von Autoren bei der Erstellung eines B3S zusammengefasst. Die Vorschläge sollen Autoren den Einstieg bei der Erstellung erleichtern.

Die Erarbeitung eines B3S erfolgt typischerweise in den Branchenarbeitskreisen (BAK) des UP KRITIS oder vergleichbaren Gremien. Der UP KRITIS als etablierte Kooperationsplattform zwischen Betreibern und Staat stellt hierfür die entsprechenden Strukturen zur Abstimmung unter Experten der jeweiligen Branchen und zuständigen Behörden zur Verfügung. Eine Liste der Branchenarbeitskreise finden Sie auf der BSI-Website: www.bsi.bund.de/dok/upk-bak

Hinweis: *Bitte beachten Sie als Autor eines B3S:*

- *Haben Sie immer im Hinterkopf, dass diese Orientierungshilfe keine Pflichtvorgabe ist, sondern die Autoren bei der Erstellung eines B3S unterstützen soll.*
- *Schwerpunkte können durchaus unterschiedlich – insbesondere branchenspezifisch – sein.*
- *Falls bestimmte Maßnahmen von einem KRITIS-Betreiber anders umgesetzt werden als im B3S beschrieben, ist dies möglich, sollte aber nachvollziehbar begründet sein. Dieser Umstand sollte in jedem B3S adressiert werden.*
- *Eigene Beispiele machen den B3S anschaulicher.*
- *Denken Sie daran, Ihre wesentlichen Diskussionspunkte und die Entscheidungen, die Sie bei der Erstellung des B3S getroffen haben, nachvollziehbar zu dokumentieren, um den Anwendern des B3S die Entscheidungsprozesse transparent und den B3S leichter anwendbar zu machen.*
- *Nehmen Sie sich ausreichend Zeit für die Beschreibung des Anwendungsbereichs des B3S, seiner Schnittstellen und Abgrenzungen. Ein gutes Beispiel für eine für den Anwender hilfreiche Beschreibung des Anwendungsbereichs ist im „B3S für die Verteilung von Fernwärme“ enthalten. Die aktuelle Version dieses B3S ist verfügbar unter www.bsi.bund.de/b3s.*
- *Generieren Sie einen Mehrwert für die Anwender durch eine konkrete Herausstellung der branchenspezifischen Anforderungen.*
- *Konkretisieren Sie die Sicherheitsanforderungen so gut wie möglich. Nutzen Sie Referenzen auf Maßnahmen aus anderen Regelwerken, z. B. dem BSI IT-Grundschutz, um die Erstellung und Anwendung des B3S zu vereinfachen, indem auf in der Branche übliche Maßnahmen zurückgegriffen wird.*

3.1 Struktur eines B3S und Detailtiefe

Grundsätzlich steht es den Autoren eines B3S frei, die Struktur des B3S selbst zu gestalten. Die im Folgenden beschriebene Struktur hat sich aber in den bisher erarbeiteten B3S bewährt und sollte daher als Grundlage gewählt werden. Darüber hinaus haben die im Folgenden beschriebenen einzelnen Bereiche bzw. Teile eines B3S jeweils einen unterschiedlichen Detaillierungsgrad und umfassen unterschiedliche Aspekte, was die spätere Fortschreibung des B3S vereinfacht.

Teil 1: Anwendungsbereich, Gefährdungs- und Risikoanalyse

- Anwendungsbereich und Schutzziele (Abschnitt 4.1)
  - Anwendungsbereich (Abschnitt 4.1.1)
  - extern erbrachte Leistungen (Abschnitt 4.1.2)
  - gesetzlicher Rahmen (Abschnitt 4.1.3)
  - Schutzziele (Abschnitt 4.1.4)

- Branchenspezifische Gefährdungslage (Abschnitt 4.2)
  - All-Gefahrenansatz (Abschnitt 4.2.1)
  - Branchenspezifische Relevanz von Bedrohungen und Schwachstellen (Abschnitt 4.2.2)
- Risikomanagement (Abschnitt 4.3)
  - Geeignete Behandlung aller für die kritische Dienstleistung relevanten Risiken (Abschnitt 4.3.1)
  - Beschränkung der Behandlungsalternativen für Risiken (Abschnitt 4.3.2)
  - Berücksichtigung von Abhängigkeiten bei den Risikoanalysemethoden (Abschnitt 4.3.3)
  - Berücksichtigung der allgemeinen Gefährdungslage (Abschnitt 4.3.4)
  - Berücksichtigung der branchenspezifischen Gefährdungslage (Abschnitt 4.3.5)

Teil 2: Sicherheitsanforderungen nach Stand der Technik und Vorgehensweisen

- Abzudeckende Themen (Abschnitt 4.4)
- Anwendungshinweise für Betreiber als Anwender eines B3S (Abschnitt 4.5)
  - Behandlung der Gefährdungen und Anpassung des B3S durch Betreiber (Abschnitt 4.5.1)
  - Konkretisierung des Anwendungsbereichs durch die Betreiber (Abschnitt 4.5.2)
  - Fortschreibung und Erfahrungen der Anwender (Abschnitt 4.5.3)

Im Einzelnen beschreiben die Teile typischerweise folgende Themen:

Teil 1 behandelt überwiegend branchenspezifische, branchenübergreifende und wenig detaillierte Aspekte wie den Anwendungsbereich, Schutzziele/ Schutzbedarf oder besondere Rahmenbedingungen der Branche. Hier werden die typischen Geschäftsprozesse der kritischen Dienstleistung beschrieben und der durch § 8a BSIG zu berücksichtigende Bereich von anderen Bereichen der Institution abgegrenzt. Die Abgrenzung der Bereiche innerhalb und außerhalb des Anwendungsbereichs des B3S müssen durch eine erklärende, abstrakte, grafische Darstellung der Systeme, Komponenten und Prozesse für einen typischen Informationsverbund dargestellt werden. Insbesondere müssen hierbei die Schnittstellen zwischen den Bereichen, die innerhalb und außerhalb des Anwendungsbereichs des B3S liegen, abgebildet werden. Des Weiteren muss eine Modellierung der wesentlichen Prozesse im Anwendungsbereich vorhanden sein. Im Vergleich zu konkreten Maßnahmen bleiben Angaben in diesem Teil über einen längeren Zeitraum konstant.

Teil 2 beschreibt die Anforderungen zum Schutz der Kritischen Infrastruktur in höherem Detaillierungsgrad. Er ist anwenderorientiert und konkret. In den konkreten Vorkehrungen zum Schutz der Kritischen Infrastruktur (Abschnitt 4.5 dieser Orientierungshilfe) erreicht der B3S eine höhere Detailtiefe als die ersten Abschnitte aus Teil 1.

Als Orientierung für diese höhere Detailtiefe können branchenspezifische Dokumente dienen, wie etwa

- BSI IT-Grundschutz-Editionen,
- IEC 62443 (Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme),
- ISO/IEC 27019 (Informationssicherheitsmaßnahmen für die Energieversorgung),
- vergleichbare technische Regelsetzungen.

Hierdurch kann der B3S einer höheren Dynamik unterliegen, so dass in Teil 2 im Vergleich zu Teil 1 mit häufigerem Fortschreibungsbedarf zu rechnen ist. Daher sollte bereits bei der Erstellung eine Vorgehensweise zur kontinuierlichen Anpassung des B3S durch die Autoren bzw. Betreiber festgelegt werden (siehe Abschnitt 4.5.3).

3.2 Einbeziehung bestehender Standards und Vorgaben

Anstelle einer Duplizierung von Inhalten aus anderen Standards kann auf geeignete Dokumente (d. h. auf konkrete Teile bzw. Abschnitte) verwiesen werden. Beispielsweise können in einem B3S Anforderungen definiert werden, während zur konkreten Umsetzung auf Maßnahmen in entsprechenden externen Dokumenten verwiesen wird. Ein globaler Verweis auf die Anwendung einer Norm oder eines Standards ist nicht hilfreich und sollte daher vermieden werden. Des Weiteren müssen nicht öffentliche Standards, auf die im B3S verwiesen wird, dem BSI bei der Prüfung des B3S mit vorgelegt werden, soweit sie zur korrekten Anwendung des B3S erforderlich sind.

Regularien und Vorgaben der jeweiligen Branche, die die IT-Sicherheit betreffen, sind in einem B3S so zu erläutern, dass ein nachvollziehbares und anwendbares Gesamtdokument entsteht, das die Betreiber bei der Umsetzung von § 8a Absatz 1 BSIG unterstützt.

Es ist auch möglich, einen B3S als Ergänzungsdokument zu einem bestehenden Standard zu erstellen. Gängige ISMS-Regelwerke wie ISO/IEC 27001 oder IT-Grundschutz sind praxiserprobt und behandeln einen Großteil der auch in dieser Orientierungshilfe erläuterten Sicherheitsanforderungen. Allerdings werden in diesen weder branchenspezifische Besonderheiten noch der Schutz Kritischer Infrastrukturen berücksichtigt.

Die FAQ auf der BSI-Website enthalten weitere Informationen hierzu:

- Nutzung eines bestehenden ISO 27001-Zertifikats als Bestandteil eines Nachweises gemäß § 8a Absatz 3 BSIG
- Nutzung eines bestehenden C5-Testates als Bestandteil eines Nachweises gemäß § 8a Absatz 3 BSIG

Insbesondere bietet ISO/IEC 27009 „Sector-specific application of ISO/IEC 27001 – Requirements“ die Möglichkeit, einen auf ISO/IEC 27001 basierenden Branchenstandard zu definieren. Ein solcher Branchenstandard kann gezielt als B3S mit den Besonderheiten Kritischer Infrastrukturen unter Berücksichtigung des deutschen Rechts erstellt werden. Alternativ können auch Teile eines B3S in ein ergänzendes Dokument ausgelagert und beide Dokumente in Kombination als B3S beim BSI eingereicht werden. Letzteres bietet sich insbesondere an, falls beabsichtigt ist, den Branchenstandard auch als deutsche DIN-Norm oder ggf. als EN- oder ISO-Norm (beispielsweise im Rahmen der europäischen Harmonisierung) fortzuentwickeln.

Analoges gilt auch für Ergänzungsdokumente zu anderen bestehenden Standards oder vergleichbare regulatorische Werke.

4 Inhaltliche Aspekte branchenspezifischer Sicherheitsstandards

Das nachfolgende Kapitel beschreibt, welche inhaltlichen Aspekte ein B3S mindestens behandeln sollte, um die Erfüllung der Anforderungen nach § 8a Absatz 1 BSIG zu gewährleisten und um eine Eignungsfeststellung des BSI erreichen zu können. Es ist zulässig, in einem B3S einzelne Anforderungen durch gleichwertige Alternativen zu ersetzen oder sogar nicht zu berücksichtigen. Dies sollte aber im Mapping-Formular nachvollziehbar begründet werden (siehe Abschnitt 2.7).

Ziel eines B3S ist die Konkretisierung des Stands der Technik für eine bestimmte Branche oder Teile davon. Daher sollten B3S möglichst detailliert sein und konkrete Maßnahmen und Vorgehensweisen nennen, die zur Erhöhung der IT-Sicherheit zu ergreifen sind. Der Detaillierungsgrad der Erläuterungen in einem B3S sollte sich danach richten, wie groß die Gemeinsamkeiten unter den betroffenen Betreibern sind. Grundsätzlich können Betreiber aus einem B3S mit einem hohen Detaillierungsgrad einen größeren Nutzen ziehen. Das BSI rät von der Einreichung von Entwürfen ab, deren Ausführungen nur unwesentlich über das Niveau der ISO/IEC 27001 hinausgehen, da der Prüfaufwand hoch und der Mehrwert für die Betreiber einer Branche minimal ist.

Die FAQ auf der BSI-Website enthalten weitere Informationen hierzu:
Nutzung eines bestehenden ISO 27001-Zertifikats als Bestandteil eines Nachweises gemäß § 8a Absatz 3 BSIG

Ein B3S legt die Themenfelder fest, die aufgrund der Schutzziele, der Gefährdungsanalyse und der Risikobetrachtung für die Branche, insbesondere für die Gewährleistung der kritischen Dienstleistung (kDL), besonders relevant sind und begründet dies, um den Anwendern die Auswahl der Sicherheitsanforderungen transparent zu machen. Die Anwender erhalten so einen ersten Überblick über die relevanten und wichtigsten Sicherheitsthemen, die umzusetzen sind. Diese Auswahl sollte daher nachvollziehbar begründet sein.

Gemäß § 8a Absatz 1 BSIG sind Betreiber verpflichtet, angemessene Vorkehrungen (Maßnahmen) zu treffen, um die für die kDL relevanten Risiken zu verringern. Dabei gilt: „Organisatorische und technische Vorkehrungen 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). Hierzu sollte im B3S dargelegt werden, wie diese Abschätzung in der Branche durchgeführt werden kann.

Ein B3S unterstützt bei der Auswahl geeigneter Maßnahmen. Eine gute Grundlage können Verweise auf Vorkehrungen und Maßnahmen nach den branchenüblichen „Best Practices“ sein. Ein B3S zeigt bei Bedarf deren Grenzen auf, beispielsweise, wenn der zur Gewährleistung der Anforderungen an die kDL notwendige informationstechnische Schutz allein durch branchenübliche Maßnahmen nicht sichergestellt wird, und schlägt – soweit möglich – ergänzende Vorkehrungen und Maßnahmen vor. Damit die Anwender befähigt sind, wirksame Entscheidungen zu treffen, soll der Zusammenhang zwischen Risikoidentifizierung und den vorgeschlagenen Maßnahmen angemessen dargestellt werden. Anwender müssen hiernach insbesondere zur Anpassung an die eigenen Gegebenheiten befähigt und angehalten werden, diese Zusammenhänge für die eigenen Risiken und Maßnahmen abzubilden.

Im Folgenden werden Themenfelder benannt, die ein B3S mindestens behandeln sollte.

4.1 Anwendungsbereich und Schutzziele

4.1.1 Anwendungsbereich

Eine wesentliche Voraussetzung für die Eignung eines B3S ist die deutliche Benennung und Beschreibung des Anwendungsbereichs. Nur dadurch können die weiteren Ausführungen im B3S nachvollziehbar sein. Sowohl für die Eignungsprüfung als auch für die spätere Anwendung muss also unmissverständlich sein, auf welche Bereiche der B3S angewendet werden kann, welche Bereiche nicht Gegenstand des B3S sind und damit von den Betreibern in Eigenleistung berücksichtigt werden müssen und welche Abhängigkeiten zwischen diesen Bereichen bestehen. Dies gewinnt insbesondere an Bedeutung, wenn ein B3S nur Teile einer kDL oder Anlagenkategorie umfasst oder wenn – z. B. aufgrund heterogener Strukturen in einer Branche – Teile nicht betrachtet wurden.

Hinweis: *Mit dem Begriff „Anwendungsbereich“ wird in dieser Orientierungshilfe der Informationsverbund – mit seinen IT-Systemen, Komponenten und Prozessen – bezeichnet, welcher im B3S adressiert wird. In der Regel unterscheidet sich dieser vom Geltungsbereich des Nachweises. Daher wird dieser in der „Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG“ zur besseren Unterscheidbarkeit auch genauso, nämlich als „Geltungsbereich des Nachweises“, bezeichnet.*

Die Beschreibung des Geltungsbereiches des Nachweises bei einem konkreten KRITIS-Betreiber muss erfahrungsgemäß deutlich mehr Informationen umfassen als die des Anwendungsbereiches, z. B. in Form von Netzplänen oder Prozessdiagrammen.

Die bisherigen Erfahrungen in diesem Kontext zeigen, dass die deutliche Abgrenzung dieser beiden Begriffe – welche sich in ihrer Verwendung und Bedeutung (im Hinblick auf die Detailtiefe) unterscheiden – zur Vermeidung von Missverständnissen sehr wichtig ist.
Das BSI empfiehlt allen im KRITIS-Kontext beteiligten Rollen, zur besseren Verständlichkeit dieser Namenskonvention zu folgen. Weiterführende Informationen zum „Geltungsbereich“ sind in der „Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG“ enthalten.

Zur vollständigen Benennung des Anwendungsbereichs eines B3S gehört eine Beschreibung der für die Erbringung der kritischen Dienstleistung wesentlichen Prozesse und maßgeblichen Infrastrukturen. Hierzu muss der Anwendungsbereich sowohl durch textuelle Beschreibungen als auch durch grafische Darstellungen der Systeme, Komponenten, Prozesse sowie ihrer Schnittstellen und möglichen Auslagerungen (z. B. an Rechenzentren) für einen typischen Informationsverbund erläutert bzw. abgebildet werden. Hierbei müssen die textuellen Beschreibungen und die grafischen Darstellungen aufeinander abgestimmt sein und demselben Abstraktionsgrad entsprechen.

Im B3S sollte möglichst eindeutig gezeigt werden, welche Bereiche innerhalb des Anwendungsbereichs des B3S liegen, welche nicht und welche (organisatorischen oder technischen) Schnittstellen dazwischen liegen. Ergänzend hierzu ist eine Modellierung der in der Branche üblichen Geschäftsprozesse oder eine Modellierung wesentlicher Prozesse hilfreich.

Der Anwendungsbereich eines B3S kann z. B. die kDL, eine Anlagenkategorie oder nur Teile davon umfassen, wie besondere Typen von Systemen, Komponenten und Prozessen. In der Regel umfasst er eine kDL oder Anlagenkategorie und die zu ihrer Erbringung notwendigen Systeme, Komponenten und Prozesse. Es müssen auch Systeme, Komponenten und Prozesse betrachtet werden, die diese direkt oder indirekt unterstützen oder von denen die kDL abhängig ist und bei deren Ausfall es zu einer Störung der kDL kommen könnte. Dieser Aspekt gilt sowohl für Standard- (bzw. Office-) IT als auch für branchenspezifische Technik, sofern diese für die kDL relevant ist. Alle externen Kommunikationsverbindungen z. B. zu externen Dienstleistern oder anderen IT-Netzen usw. sind ebenfalls zu erfassen.

Ist es nicht möglich, eine einheitliche Darstellung zur Erbringung der kDL in der Branche zu finden, sollte der Anwendungsbereich so gewählt werden, dass dies möglich ist. Alternativ müssen die unterschiedlichen in der Branche üblichen Realisierungsmöglichkeiten differenziert betrachtet werden, z. B. durch die Darstellung einer „einfachen“ Anlage und einer „komplexen“ Anlage. Eine Beschreibung unterschiedlicher Szenarien ist oft hilfreich. Der Anwendungsbereich sollte so groß gewählt werden, dass der B3S für möglichst viele Betreiber anwendbar ist, aber auch klein genug, damit noch präzise Aussagen zum darin beschriebenen „gemeinsamen Nenner“ möglich sind.

Die Autoren des B3S sollten eine möglichst detaillierte und präzise Beschreibung des Anwendungsbereichs wählen. Denn die bisherigen Erfahrungen zeigen, dass bei einer höheren Detailtiefe in der Beschreibung die Umsetzung der Sicherheitsanforderungen bzw. Sicherheitsvorkehrungen im B3S durch die Betreiber deutlich einfacher ist.

Gleichzeitig bietet es sich aber an, zusätzlich im B3S eine vereinfachte Darstellung des Anwendungsbereichs abzubilden. Dadurch kann der Anwendungsbereich in den verschiedenen Detailtiefen unter Berücksichtigung der differenzierten Sichtweisen (z. B. Prozess- und Systemebene) übersichtlich dargestellt werden. Des Weiteren können dadurch potenzielle Anwender schnellstmöglich entscheiden, ob der vorliegende B3S für die eigene Anlage anwendbar ist.

Da der festgelegte Anwendungsbereich die Basis für alle im folgenden beschriebenen Punkte darstellt, sollten die Definition und Abgrenzung des Anwendungsbereichs besonders sorgfältig erfolgen. Das BSI bietet in diesem Zusammenhang den B3S-Autoren an, diese Abgrenzung im Rahmen gemeinsamer Gespräche und Workshops zu erarbeiten. Erfahrungsgemäß ist es sinnvoll, diese Möglichkeit bereits in einem frühen Stadium der Entstehung des B3S wahrzunehmen.

4.1.2 Anwendungsbereich umfasst auch extern erbrachte Leistungen

Ein B3S berücksichtigt in geeigneter Weise, wie das notwendige informationstechnische Sicherheitsniveau auch dort sichergestellt werden kann, wo für die Aufrechterhaltung der kDL relevante Teile im Auftrag des Betreibers durch Dritte betrieben werden. Betreiber sind bei externen Prozessen in gleicher Weise dafür verantwortlich, dass angemessene Vorkehrungen getroffen werden, wie bei internen Prozessen. Hieraus ergeben sich vielfältige Anforderungen an die Ausgestaltung der Beziehung zwischen Betreiber und Dienstleister, insbesondere bei der Festlegung von angemessenen Sicherheitsvorkehrungen und der regelmäßigen Überprüfung durch den Betreiber. Es sind alle externen Schnittstellen und Kommunikationsverbindungen zu berücksichtigen, beispielsweise zu

- externen Rechenzentren,
- ausgelagerten Prozessen,
- externen Dienstleistern, Partnerunternehmen etc.,
- Kunden, Versorgungsempfängern etc.,
- Dritten, die Wartungsaufgaben wahrnehmen,
- Versorgungs-Dienstleistern (Energie, Wasser, ...),
- externen Firmen mit Zutritt (Sicherungsdienst, Facility Management, Reinigungsdienst, ...).

sowie ggf. weitere Abhängigkeiten. Hilfreich für die Darstellung der Dienstleistung könnte das UP-KRITIS-Papier „Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen“ des Themenarbeitskreises „Anforderungen an Lieferanten und Hersteller“ sein: www.bsi.bund.de/dok/upk-anforderungen-lieferanten.

Hinweis: *Die Aufnahme einer Schnittstelle oder eines anderen Schutzobjekts in den Anwendungsbereich führt nicht in jedem Fall dazu, dass zusätzliche Sicherheitsvorkehrungen erforderlich sind. Dies klärt sich erst später, z. B. durch eine Schutzbedarfsfeststellung oder eine Risikoanalyse.*

4.1.3 Gesetzlicher Rahmen

In einem B3S sollten neben den Vorgaben gemäß § 8a BSIG auch allgemeine gesetzliche Vorgaben oder branchenspezifische Vorgaben und Regelungen aufgeführt werden, soweit sie die Erbringung der kDL beeinflussen bzw. mit ihr in Wechselwirkung stehen.

Es könnte beispielsweise herausgestellt werden, ob andere gesetzliche Vorgaben den Vorgaben nach § 8a BSIG entgegenstehen, diesen entsprechen, sie unterstützen oder die möglichen Maßnahmen einschränken. Insbesondere ist festzulegen, wie mit widersprüchlichen Anforderungen umzugehen ist. Beispielsweise können gesetzliche Anforderungen an die Vertraulichkeit von Daten zu Einschränkungen in den zur Steigerung der Verfügbarkeit möglichen Maßnahmen führen.

Soweit sinnvoll könnte auch explizit darauf verwiesen werden, wenn die Einhaltung bestimmter gesetzlicher Vorgaben nicht Gegenstand des B3S ist.

Beispiele:

- *Aufgrund des Medizinproduktegesetzes (MPG) sind Veränderungen an Medizinprodukten nicht zulässig. Folglich können ansonsten übliche Maßnahmen wie regelmäßige Patches und Updates nicht angewendet werden – auch wenn diese dem Stand der Technik entsprechen. Diese einschränkende gesetzliche Vorgabe wird bei den weiteren Ausführungen des B3S berücksichtigt.*
- *Anforderungen an elektronische Signaturen gemäß Vertrauensdienstegesetz (VDG) sind für die Aufrechterhaltung der kDL nicht von Bedeutung und werden daher im Kontext des B3S nicht betrachtet.*

4.1.4 Schutzziele

Die Schutzziele sollten von den Autoren in einem B3S nachvollziehbar definiert werden. Diese werden von den Anwendern benötigt, um im Rahmen der Schutzbedarfsfeststellung und der Risikoanalyse auf Ebene der Systeme, Komponenten und Prozesse konkretisierte Aussagen herzuleiten.

KRITIS-Schutzziele (Schutzziele der kDL)

Im Fokus der zum Schutz Kritischer Infrastrukturen geforderten Sicherheitsvorkehrungen steht die Sicherung der Versorgung der Bevölkerung mit der kDL zur Vermeidung von Versorgungsengpässen sowie die Gewährleistung der öffentlichen Sicherheit. Dies kann sich mit unternehmerischen Zielsetzungen weitgehend decken, ist zunächst aber eine andere, auf die Auswirkungen für die Bevölkerung gerichtete Betrachtung.

Die KRITIS-Schutzziele beschreiben, welche Anforderungen an die qualitative und quantitative Versorgung mit der kDL („Mindestqualität“) gestellt werden. Die Frage, was unter einer Beeinträchtigung oder einem Versorgungsengpass zu verstehen ist und welche Konsequenzen sich daraus für die KRITIS-Schutzziele ergeben, ist stark branchenabhängig. Es kann auch sinnvoll sein, nach unterschiedlichen Situationen zu differenzieren. Die Beschreibungen sollten insbesondere Normallagen, aber auch besondere Lagen geeignet widerspiegeln (Situationen im Regelbetrieb oder mit erhöhten Anforderungen, Störungen, Krisen, Großschadenslagen, ...). Die Festlegung der KRITIS-Schutzziele ist zunächst unabhängig von der hierfür benötigten IT.

Beispiele (fiktiv):

- *Im Bereich Fernwärme wurde als KRITIS-Schutzziel festgestellt, dass in den Haushalten ankommendes Heizwasser eine Vorlauftemperatur von mindestens XXX ° Celsius haben muss. Eine geringere Vorlauftemperatur würde keine ausreichende Erwärmung des Wohnbereichs gewährleisten und dies würde als Störung empfunden werden. Eine Temperatur unter YYY ° Celsius wird als Versorgungsengpass betrachtet. Um dies zu erreichen, darf eine Unterbrechung der Pumpleistungen nicht länger als Z Stunden andauern. Bei niedrigen Außentemperaturen (z. B. Winter) wurde ein verschärfter Wert definiert.*

- *Im Bereich der Luftfahrt wurde als KRITIS-Schutzziel festgestellt, dass die Funktionsfähigkeit der Kontrollen des Flughafens IMMER gegeben sein muss, um zu gewährleisten, dass keine unkontrollierten Personen in den Sicherheitsbereich oder unbefugte Personen in den luftseitigen Bereich des Flughafens gelangen. Sollte dies geschehen, so hätte dies zur Folge, dass der Flugverkehr zumindest teilweise eingestellt werden muss und somit die Aufrechterhaltung der kDL nicht mehr gewährleistet ist.*

Hierbei sollten insbesondere branchen- oder anlagenspezifische Schutzziele berücksichtigt werden. Diese können zum Beispiel Anforderungen an ein besonderes branchenspezifisches Steuerungssystem, branchentypische Leitzentralen, spezifische Regelungsprozesse oder andere branchenspezifische Besonderheiten sein.

Ableitung des KRITIS-IT-Schutzbedarfs aus den KRITIS-Schutzzielen

Für die für einen störungsfreien Betrieb der kDL erforderlichen IT-Systeme, Komponenten und Prozesse soll hinsichtlich der kDL und unter Berücksichtigung der KRITIS-Schutzziele der KRITIS-IT-Schutzbedarf hergeleitet werden. Dabei sollten Störungen oder Störungsklassen der Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität (VIVA, IT-Schutzziele) behandelt werden.

Hinweis: *Der KRITIS-IT-Schutzbedarf kann vom herkömmlichen IT-Schutzbedarf abweichen, da die in den KRITIS-Schutzzielen ermittelten Anforderungen hier im Vordergrund stehen.*

Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit müssen bei der Ermittlung des Schutzbedarfs betrachtet werden, um die gesetzlichen Anforderungen zu erfüllen. Es ist aber zulässig, dies über eine andere Einteilung der IT-Schutzziele zu erreichen.

Dabei kann die Gewichtung der IT-Schutzbedarfe für verschiedene Bereiche der Kritischen Infrastruktur unterschiedlich ausfallen. Beispielsweise könnte ein industrielles Steuerungssystem (ICS) einer Anlage einen höheren Schutzbedarf bzgl. Integrität der Steuerdaten haben, eine zugehörige Leitwarte verstärkten Schutzbedarf in Vertraulichkeit und Authentizität. Im B3S muss eine quantitative Definition der Schutzbedarfsklassen, nach der diese Gewichtung des IT-Schutzbedarfe erfolgt, angegeben sein.

4.2 Branchenspezifische Gefährdungslage

4.2.1 All-Gefahrenansatz

Ein B3S regelt ausdrücklich die Behandlung aller möglichen Gefährdungen und Schwachstellen (All-Gefahrenansatz) der maßgeblichen IT-Systeme, Komponenten oder Prozesse. Hierzu sollte die Liste der KRITIS-relevanten elementaren Gefährdungen aus Abschnitt 5.1 zugrunde gelegt und ggf. um erforderliche ergänzende Gefährdungen erweitert werden. Des Weiteren sollten die in Anhang 5.3 aufgelisteten Bedrohungsszenarien, die aus Sicht des BSI von besonderer Relevanz für die allgemeine Bedrohungslage sind, berücksichtigt werden. Es können auch aus anderen Quellen geeignete ergänzende Gefährdungen hinzugenommen werden, sofern diese für den Anwendungsbereich des B3S relevant sind. Im B3S sollte die hierdurch entstandene Liste aller möglichen Gefährdungen und Schwachstellen explizit benannt werden.

4.2.2 Relevanz von Gefährdungen

In einem B3S wird die Relevanz der Gefährdungen innerhalb des Anwendungsbereichs im Hinblick auf die Gewährleistung der kDL von den Autoren bewertet. Dafür sind alle Gefährdungen, die Auswirkung auf die Erbringung der kDL haben könnten, nachvollziehbar herauszustellen. Hierzu sind alle in Abschnitt 4.2.1 ermittelten möglichen Gefährdungen und Schwachstellen zu betrachten, zu bewerten und zu gewichten. Die durch diese Bewertung und Gewichtung entstandene Liste der für den Anwendungsbereich des B3S relevanten Gefährdungen sollte im B3S explizit benannt werden.

4.3 Risikomanagement

4.3.1 Geeignete Behandlung aller für die kDL relevanten Risiken

Ein B3S setzt einen Rahmen für das Risikomanagement, durch den für die kDL relevante Risiken ausreichend verringert werden. Ein B3S beschreibt insbesondere geeignete Methoden

- für die Identifizierung der für die kDL relevanten Risiken und für deren geeignete Klassifizierung,
- für die Identifizierung geeigneter Maßnahmen, um diese Risiken entsprechend ihrer Klassifizierung zu reduzieren sowie
- zur Integration des Informationssicherheitsrisikomanagements in übergeordnete ganzheitliche Konzepte, z. B. Risiko- und Krisenmanagement.

Geeignete Risikoanalysemethoden sind z. B. in ISO/IEC 27005 oder dem BSI-Standard 200-3 beschrieben.

Innerhalb eines B3S können Risiken im Allgemeinen nur global betrachtet werden. Folglich ersetzt dies nicht die individuelle Risikoanalyse des Betreibers, sondern liefert hierfür Eingangsinformationen.

Die Autoren sollten sich zusätzlich die Frage stellen, wie stark sich die jeweilige Gefährdung auf die Erbringung einer kDL auswirken kann.

Um die identifizierten Risiken zu reduzieren, muss der Anwender geeignete Maßnahmen auswählen. Der Anwender muss durch den B3S in die Lage versetzt werden, die Auswahl an geeigneten Maßnahmen nachzuvollziehen und an die eigenen Gegebenheiten anzupassen. Daher muss der B3S die Zusammenhänge zwischen den Risiken und der Auswahl der geeigneten Maßnahmen darstellen bspw. in Form einer Mapping-Tabelle. Diese Tabelle kann dann vom Anwender angepasst werden, um auch individuelle Risiken mit entsprechenden Maßnahmen zu reduzieren.

4.3.2 Beschränkung der Behandlungsalternativen für Risiken

Ein B3S beschreibt, welche Grenzen dem Risikomanagement für eine kDL bei der Auswahl der Behandlungsalternativen im Sinne des BSIG gesetzt sind. Der B3S erläutert dabei explizit die Einschränkungen der Optionen gegenüber allgemeinen Risikomanagementansätzen.

Der B3S stellt klar, dass bzgl. relevanter Risiken für die kDL eine eigenständige dauerhafte Risikoakzeptanz durch den Betreiber in der Regel keine zulässige Option im Sinne des BSIG ist. Ähnliches gilt für die Übertragung von Risiken, insbesondere durch Versicherung. Durch eine Versicherung wird bei Schadenseintritt zwar der betriebswirtschaftliche Schaden des Betreibers verringert, die Auswirkungen in Bezug auf Versorgungsengpässe bleiben aber unverändert. Ggf. weist der B3S darauf hin, in welchem Rahmen eine Risikoakzeptanz aufgrund regulatorischer Vorgaben oder expliziter Beschränkung der Anforderungen an die Qualität oder Quantität der kDL denkbar ist.

Der B3S stellt klar, dass bei einer Aufgabenübertragung an Externe durch Outsourcing o. Ä. die volle Verantwortung für das Risikomanagement inklusive einer geeigneten Risikobehandlung beim Betreiber verbleibt (siehe auch Abschnitt 4.1.2).

4.3.3 Berücksichtigung von Abhängigkeiten bei der Risikoanalyse

In einem B3S sind Abhängigkeiten zwischen den eigenen IT-Systemen der Betreiber und IT-Systemen Dritter zu berücksichtigen, z. B. Auswirkungen von Störungen verbundener IT-Systeme anderer Betreiber/Dritter auf die eigenen IT-Systeme.

4.3.4 Berücksichtigung der allgemeinen Gefährdungslage

In einem B3S ist die allgemeine Gefährdungslage sowie deren potentielle Fortentwicklung zu berücksichtigen und zu beschreiben.

Bei der Weiterentwicklung der Gefährdungslage müssen insbesondere berücksichtigt werden:

- allgemeine Bedrohungen (neu hinzugekommene Typen von Schadensauslösern, Angreifern und Angriffen, intensivere Aktivität oder verbesserte Expertise/Ressourcen von Angreifern, Neuausrichtung von Angreifern, ...),
- bekannt gewordene neue Schwachstellen,
- neue Schwachstellen durch Veränderungen an der Systemarchitektur des Betreibers.

Hier können geeignete Informationsquellen zur Erkennung solcher Änderungen der Gefährdungslage benannt werden.

4.3.5 Berücksichtigung der branchenspezifischen Gefährdungslage

Die in einem B3S beschriebene Vorgehensweise erfordert die Berücksichtigung und geeignete Behandlung der branchenspezifischen Gefährdungslage (Bedrohungen und Schwachstellen) inklusive deren Änderungen.

Idealerweise sollte beschrieben werden, wie und wo ein Betreiber sich regelmäßig über die aktuelle branchenspezifische Gefährdungslage informieren kann.

4.4 Abzudeckende Themen

In einem B3S müssen zumindest die nachfolgend genannten Themenfelder behandelt werden. Die Autoren des B3S sind in der Pflicht, zu prüfen, ob noch weitere Themenfelder behandelt werden müssen. Insbesondere sollten die Themen unter „Technische Informationssicherheit“ (Abschnitt 5.2.1) mit herangezogen und um noch fehlende branchenspezifische Aspekte ergänzt werden.

Die folgenden abzudeckenden Themenfelder eines B3S entsprechen dem Anhang E aus der „Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG“:

- Informations-Sicherheits-Management-System (ISMS) (Abschnitt 4.4.1)
- Asset Management (Abschnitt 4.4.2)
- Continuity- und Notfallmanagement für die kDL (Abschnitt 4.4.3)
- Technische Informationssicherheit (Abschnitt 4.4.4)
- Personelle und organisatorische Sicherheit (Abschnitt 4.4.5)
- Bauliche/physische Sicherheit (Abschnitt 4.4.6)
- Vorfallserkennung und -bearbeitung (Abschnitt 4.4.7)
- Überprüfung im laufenden Betrieb (Abschnitt 4.4.8)
- Lieferanten, Dienstleister und Dritte (Abschnitt 4.4.9)
- Branchenspezifische Technik und (Kern-)Komponenten (Abschnitt 4.4.10).

Der jeweilige Anspruch an die Behandlung der einzelnen Themenfelder hängt von den Anforderungen an die kDL und der Art ihrer technischen und informationstechnischen Infrastruktur ab und leitet sich aus den Sicherheitszielen, der Bedrohungs- und Risikolage der Branche ab. Für einen positiven Ausgang der Eignungsprüfung eines B3S müssen allerdings zu jedem einzelnen dieser Themenfelder Maßnahmen angegeben werden, die vom Anwender zu ergreifen sind, um ein angemessenes Mindestniveau an IT-Sicherheit zu erreichen.

Vor dem Hintergrund der besonderen Relevanz für die allgemeine Bedrohungslage ist zusätzlich eine Auseinandersetzung mit den unter Abschnitt 5.3 aufgelisteten besonders zu betrachtenden Maßnahmenkategorien erforderlich.

In diesem Teil hat der B3S einen deutlich tieferen Detaillierungsgrad als in den ersten Abschnitten, um den Betreibern möglichst konkrete Umsetzungshinweise zu den Sicherheitsthemen und zu den Sicherheitsanforderungen zu geben.

Zur Vermeidung von Redundanzen wird empfohlen, auf bestehende veröffentlichte Sicherheitsempfehlungen, Anforderungen aus dem IT-Grundschutz oder technische Hinweise zu verweisen. Da sich sowohl die Gefährdungslage als auch die technischen Möglichkeiten teilweise rasant weiterentwickeln, unterliegt dieser Abschnitt im Allgemeinen einem höheren und intensiveren Revisionsbedarf als der übrige B3S.

Die Herleitung der Maßnahmen im B3S sollte für die Anwender nachvollziehbar sein. Hierdurch kann ein Anwender erkennen, ob Annahmen aufgrund anderer Rahmenbedingungen oder einer Änderung seit Erstellung des B3S nicht mehr zutreffen und somit auch eine Anpassung seiner Umsetzung erforderlich ist. Dazu muss der Anwender insbesondere befähigt werden, die Maßnahmen den zuvor identifizierten Risiken zuzuordnen.

Hinweis: *Auch, wenn verschiedene Managementsysteme in der Orientierungshilfe gesondert beschrieben werden, können diese durch ein gemeinsames/integriertes Managementsystem umgesetzt werden. Beispielsweise kann Risikomanagement Teil des Informationssicherheitsmanagements sein oder auch das ISMS Teil des Risikomanagements, Notfallmanagement kann Teil des Business Continuity Management sein. Funktional sollen aber alle Bereiche abgebildet werden.*

4.4.1 Informationssicherheitsmanagement-System (ISMS)

Ein ISMS ist die Grundlage für einen alle Aspekte der kDL umfassenden sicheren Betrieb. Ein B3S beschreibt, wie mithilfe eines ISMS ein geeigneter Rahmen für die nachhaltige und angemessene Behandlung aller relevanten Themenfelder zur Umsetzung der Anforderungen nach § 8a Absatz 1 BSIG gesetzt wird.

Dies kann unter anderem durch die Einführung und den Betrieb eines ISMS beispielsweise auf Grundlage des BSI IT-Grundschutzes, der ISO/IEC 27001, der NIST SP 800 oder im ICS-Umfeld gemäß IEC 62443 erfolgen.

Informationssicherheit ist dabei als kontinuierlicher Prozess zu etablieren.

In einem B3S wird außerdem dargelegt, wie und woher sich die Anwender die erforderlichen Informationen zur Aufrechterhaltung und stetigen Verbesserung ihres Sicherheitsniveaus sowie über aktuelle Entwicklungen der für sie relevanten IT-Sicherheitslage beschaffen können. Feste/zwingende Vorgaben sind nicht notwendig, aber die Anwender sollten auf Grundlage der Hinweise im B3S zuverlässig einen für ihren konkreten Informationsbedarf geeigneten Ansatz finden können.

4.4.2 Asset Management

Ein B3S muss einen geeigneten Rahmen für die Identifikation, Klassifizierung, Inventarisierung und Auswertung der für die kDL maßgeblichen informationstechnischen Prozesse, Systeme und Komponenten setzen. Es sollten typische Systeme und Konfigurationen, die zum Einsatz kommen, beschrieben werden. Insbesondere müssen in einem B3S die besonders geschäftskritischen Assets des Anwendungsbereichs B3S hervorgehoben werden.

4.4.3 Continuity- und Notfallmanagement für die kDL

Ein B3S beschreibt, wie mithilfe eines Continuity Managements die Aufrechterhaltung der kDL und deren Mindestqualität (entsprechend der jeweiligen KRITIS-Schutzziele) gewährleistet werden können. Dafür können zum Beispiel folgende Maßnahmen zum Einsatz kommen:

- Plan zur Aufrechterhaltung der kDL („Continuity Plan“ für die kDL),
- Sicherstellung einer geeigneten Verzahnung des Continuity Managements für die kDL mit dem Bereich Informationssicherheit,

- Impact-Analysen, z. B. Business Impact Analyse (BIA),
- Analysen in Bezug auf Komponenten, deren Ausfall den Ausfall der gesamten Anlage auslösen kann („Single Point of Failure“),
- Entwicklung von Kontinuitäts- und Wiederanlaufstrategien.

In einem B3S sollte dargelegt werden, durch welche Prinzipien die kDL bestmöglich gegen vorsätzlich oder unbeabsichtigt herbeigeführte Fehlfunktionen resistent gehalten wird. Hier kann zum Beispiel auch auf eine Konzeption zur Verfügbarkeit der kDL in außergewöhnlichen Lagen oder bei Beeinträchtigungen anderer Kritischer Infrastrukturen verwiesen werden (Beispiel: Massive Störungen des Internets).

Soweit nicht-informationstechnische Infrastrukturen die Robustheit und Resilienz der kDL im oben genannten Sinne beeinflussen (steigern oder verringern), sollten diese aufgeführt werden.

Ein B3S sollte zudem einen geeigneten Rahmen setzen für die Etablierung eines geeigneten Notfallmanagements (in Bezug auf die Gewährleistung der kDL). Grundlage hierfür können z. B. BSI-Standard 200-4 „Business Continuity Management” oder ISO 22301 – „Societal Security – Business continuity management systems – Requirements“ und ISO 22313 – „Societal Security – Business continuity management systems – Guidance“ sein.

Das „Verletzlichkeitsparadoxon“ besagt: Je besser etwas funktioniert, desto gravierender sind die Folgen bei einem Dennoch-Ausfall. Somit kann trotz einer hohen Versorgungssicherheit eine hohe Verletzlichkeit bestehen. Insbesondere bei einer hohen Verfügbarkeit nehmen sowohl das Vertrauen in die jeweilige kDL und damit die Abhängigkeit von deren Funktionieren zu, während zugleich die Kompetenz im Umgang mit besonderen Situationen mangels Erfahrung und Routine sinkt. Um diesem Effekt entgegenzuwirken, sollten Vorgehensweisen zur Bewältigung seltener oder besonders folgenreicher Ereignisse geübt werden. Beispiele hierfür können sein:

- Interne Übungen und Systemtests,
- Übungen mit externen Partnern, insbesondere aus dem Kontext der kDL,
- Übungen im Rahmen des Notfallmanagements,
- Kommunikationsübungen,
- Planübungen, Krisenübungen, Training seltener Ereignisse, ...

4.4.4 Technische Informationssicherheit

Zum Thema „Technische Informationssicherheit" greift ein B3S zumindest die im Anhang „Technische Informationssicherheit“ (Abschnitt 5.2.1) aufgeführten Maßnahmenkategorien auf und beschreibt deren spezifische Relevanz im Kontext des B3S.

Hinweis: Die Maßnahmenkategorien der technischen Informationssicherheit in Abschnitt 5.2.1 sind nicht abschließend aufgelistet und stellen lediglich eine Übersicht, keine konkreten Maßnahmen dar.

Soweit für die Erfüllung der Anforderungen nach § 8a Absatz 1 BSIG Maßnahmen (Vorkehrungen) aus weiteren Bereichen der technischen Informationssicherheit notwendig sind, sind diese ebenfalls geeignet zu behandeln. Sind im Anhang genannte Maßnahmenkategorien im Kontext des B3S nicht relevant, so sollte auch dies dargelegt werden. Dies dient unter anderem den Anwendern des B3S zur Orientierung. Der B3S sollte festlegen, dass Maßnahmen zur technischen Informationssicherheit identifiziert und umgesetzt werden, wo dies für die Gewährleistung der kDL notwendig ist.

4.4.5 Personelle und organisatorische Sicherheit

Ein B3S setzt einen geeigneten Rahmen für die Behandlung der personellen und organisatorischen Sicherheit, zum Beispiel auf Basis folgender Maßnahmen:

- geeignete Auswahl von Personal, gegebenenfalls Sicherheitsüberprüfung,

- Rollenzuweisung, gegebenenfalls Festlegungen z. B. zum Vieraugenprinzip oder Funktionstrennung,
- Identitäts- und Berechtigungsmanagement,
- Festlegung notwendiger Kompetenzen (Betrieb und IT-Sicherheit),
- Notwendige/ausreichende Personalressourcen (Betrieb und IT-Sicherheit),
- Schulungen des Personals (Betrieb und IT-Sicherheit),
- Schaffung von Verständnis (Awareness) für IT-Sicherheit auf allen Ebenen (Vorstand, IT-Betrieb, Prozessverantwortliche, ..., Mitarbeiter)

4.4.6 Bauliche/physische Sicherheit

Ferner setzt ein B3S einen geeigneten Rahmen für die bauliche und physische Sicherheit, die zum sicheren Betrieb einer kDL notwendig ist. Bei der Realisierung der baulichen und physischen Sicherheit sind insbesondere die Schutzziele der kDL (beispielsweise für den Schutz vor unberechtigtem Zutritt bei nicht dauerhaft besetzten Umschaltstationen oder anderen unbesetzten Standorten) und die Maßnahmenkategorien aus Abschnitt 5.2.2 zu berücksichtigen.

4.4.7 Vorfallserkennung und -bearbeitung

Ein B3S setzt einen geeigneten Rahmen für die Vorfallserkennung und -bearbeitung in seinem Anwendungsbereich, beispielsweise zu:

- Detektion von Angriffen,
- Detektion von sonstigen IT-Vorfällen oder -Störungen (und Unterscheidung von Angriffen),
- Einsatz von Intrusion-Detection- und Intrusion-Prevention-Systemen (IDS und IPS),
- Reaktion auf Angriffe,
- Reaktion auf sonstige IT-Vorfälle/Störungen und zur
- Forensik (Hilfe zur Abwägung zwischen Schadensbegrenzung und Wiederherstellung der kDL einerseits und Beweissicherung, Einschaltung von Behörden und Experten andererseits).

Des Weiteren adressiert ein B3S die Umsetzung der Meldepflicht (gemäß § 8b BSIG) durch die Betreiber im Hinblick auf Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse. Ein B3S enthält Vorschläge zur Umsetzung des vom BSI vorgegebenen Meldeprozesses in der Organisation der Betreiber.

4.4.8 Überprüfung im laufenden Betrieb

Ein B3S setzt einen geeigneten Rahmen für Überprüfungen im laufenden Betrieb (z. B. Penetrationstests, spezifische Audits, Wirksamkeitsprüfung, Revisionen, (technische) Prüfungen etc. in Teilbereichen), auch außerhalb des von § 8a Absatz 3 BSIG vorgegebenen Prüfzyklus und Prüfumfangs. Beispiele hierfür sind:

- Anlassbezogene Prüfungen, z. B. aufgrund von:
  - Änderungen der Bedrohungs- oder Gefährdungslage,
  - nicht zuverlässig erklärbaren Beeinträchtigungen der kDL oder der zugehörigen IT-Systeme,
  - erfolgreichen oder möglicherweise erfolgreichen Angriffen oder
  - Änderungen an den IT- oder Kommunikationssystemen.
- Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen
- Systematische Log-Auswertungen
- Penetrationstests, ggf. in Testumgebungen

4.4.9 Lieferanten, Dienstleister und Dritte

Ein B3S muss einen geeigneten Rahmen für den Umgang mit Lieferanten, Dienstleistern und sonstigen Dritten beschreiben (beispielsweise in Form von Regeln und Richtlinien), damit die Anwender in der Lage sind, geeignete Vorkehrungen zu treffen (z. B. in Form von vertraglichen Regelungen gegenüber Dritten oder durch Monitoring von extern erbrachten Dienstleistungen),

- wenn sie IT-Komponenten oder IT-Systeme von Lieferanten beziehen (z. B. Eingangsprüfungen, Sicherheitstests),
- um externe Dienstleister sicher in den Betrieb der kDL oder die Wartung von Systemen oder Komponenten einzubinden und
- um eigene Leistungen geeignet an Externe auszulagern.

Hierzu zählen insbesondere Cloud-Dienste jedes Service-Modells, wie Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) oder andere (XaaS). Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen sind unter folgendem Link veröffentlicht: www.bsi.bund.de/dok/upk-anforderungen-lieferanten .

4.4.10 Branchenspezifische Technik und (Kern-)Komponenten (Beschaffung, Entwicklung, Einsatz, Betrieb und Wartung)

Im Gegensatz zur Standard-IT, für deren Absicherung häufig zahlreiche Standard-IT-Sicherheitsmaßnahmen existieren, ist dies für branchenspezifische Technik nicht im gleichen Maße der Fall. Diese spielt in vielen Sektoren jedoch die entscheidende Rolle bei der Erbringung der kDL. Ein B3S geht daher insbesondere auch auf branchenspezifische Informationstechnik und sonstige branchenspezifische Technik ein, die durch IT gesteuert wird.

Des Weiteren müssen in einem B3S die besonders geschäftskritischen (Kern-)Komponenten des Anwendungsbereichs identifiziert werden. Solche Komponenten zeichnen sich dadurch aus, dass deren Diebstahl, Zerstörung oder Kompromittierung eine erhebliche Störung bzw. sogar einen Ausfall der kDL bedeuten würde. Ein B3S sollte daher einen geeigneten Rahmen setzen für die Beschaffung, die Entwicklung, den Einsatz, den Betrieb und die Wartung dieser (Kern-)Komponenten.

In einem B3S wird zudem dargelegt, welchen besonderen Bedrohungen diese branchenspezifische Technik und diese (Kern-)Komponenten ausgesetzt sind, welche besonderen (z. B. architektur- oder einsatzbedingten) Verwundbarkeiten vorhanden sind und wie auf diese Gefährdungen reagiert werden muss.

Außerdem können typische Schwachstellen branchenspezifischer Technik wie fehlende oder ungenügende Trennung von den Office-Netzen, fehlende Verschlüsselung oder die unzureichende Sicherheit bei (Fern)-Wartungen sowie Industriellen Steuerungssystemen (Industrial Control Systems, ICS) bei der Betrachtung berücksichtigt werden.

Hinweis: *Es ist dabei ausdrücklich nicht gemeint, dass hier konkrete Schwachstelleninformationen einzelner Geräte oder Implementationen offengelegt werden sollen. Der Vertraulichkeitsgrad der Angaben sollte entsprechend dem späteren Empfängerkreis des B3S gewählt sein. Ggf. können auch Detailinformationen in ein Dokument ausgelagert werden, das einen höheren Vertraulichkeitsgrad hat.*

4.5 Anwendungshinweise für Betreiber als Anwender eines B3S

Folgende an die Anwender gerichteten Hinweise sollten in einem B3S enthalten sein:

4.5.1 Behandlung der Gefährdungen und Anpassung des B3S durch Betreiber

Ein B3S beschreibt generisch, wie ein Betreiber einer Kritischen Infrastruktur aus der jeweiligen Zielgruppe des B3S geeignete Maßnahmen nach Stand der Technik identifizieren und umsetzen kann. Insbesondere setzt ein B3S einen Rahmen für die Behandlung der in Abschnitt 4.2.2 ermittelten relevanten Gefährdungen.

Sofern es möglich ist, sollten geeignete Anforderungen oder Vorgehensweisen angegeben werden, mit denen die Anwender des B3S den konkreten Gefährdungen begegnen können. Sollten für einzelne Gefährdungen keine geeigneten Anforderungen oder Vorgehensweisen angegeben werden können, muss im B3S explizit erwähnt werden, dass solche Gefährdungen zusätzlich im Rahmen der Risikoanalyse von den Anwendern des B3S behandelt werden müssen.

Hinweis: Da die Bezeichnungen der in Abschnitt 5.1 aufgelisteten Gefährdungen der Liste der elementaren Gefährdungen aus dem IT-Grundschutz-Kompendium entnommen sind, können die Kreuzreferenztabellen in den Bausteinen des IT-Grundschutz-Kompendiums herangezogen werden, um geeignete Anforderungen zu identifizieren.

Ein Betreiber sollte die Vorgaben eines B3S sinngemäß auf seine konkreten Anlagen anpassen. Er kann ggf. Maßnahmen weglassen, falls bei ihm keine diesbezüglichen Risiken bestehen. Er sollte aber auch zusätzliche Maßnahmen umsetzen, um ein angemessenes Schutzniveau sicherzustellen, auch wenn diese über die im B3S genannten mindestens zu ergreifenden Maßnahmen hinausgehen.

4.5.2 Konkretisierung des Anwendungsbereichs durch die Betreiber

In Abschnitt 4.1.1 dieser Orientierungshilfe wird von den Autoren eine Beschreibung des im B3S adressierten Informationsverbunds gefordert. Diese Modellierung wird als „Anwendungsbereich“ bezeichnet. Darüber hinaus muss in einem B3S zudem deutlich gemacht werden, dass dieser Anwendungsbereich im Hinblick auf die eigene Informationsinfrastruktur beim Betreiber zu konkretisieren ist, damit darauf aufbauend auch der Geltungsbereich des Nachweises festgelegt werden kann. Es ist im B3S auf geeignete Weise hervorzuheben, dass hierzu eine Replikation des Anwendungsbereichs des B3S allein nicht ausreichend ist.

4.5.3 Fortschreibung und Erfahrungen der Anwender

Jeder Anwender eines B3S sollte die Möglichkeit haben, Themen und Maßnahmen zum Stand der Technik weiterzuentwickeln, indem er seine Erfahrungen und Kenntnisse mit in die Fortentwicklung des B3S einfließen lässt. Wie die Kommentierungsprozesse definiert sind, d. h., wie und an wen Änderungsvorschläge gemeldet werden können, sollte im B3S transparent werden.

5 Anhänge

Die in Anhang 5.1 aufgelisteten KRITIS-relevanten elementaren Gefährdungen sind dem IT-Grundschutz-Kompendium entnommen worden. Die in Anhang 5.2 aufgeführten Maßnahmenkategorien zur Technischen Informationssicherheit und baulichen/physischen Sicherheit basieren auf Expertenmeinungen. Wie in den Abschnitten 4.2.1 und 4.4.4 dargestellt, handelt es sich hierbei um Kategorien, deren konkrete Inhalte durch den B3S oder durch die Betreiber konkretisiert werden müssen. In Anhang 5.3 sind Bedrohungsszenarien aufgelistet, die aus Sicht des BSI von besonderer Relevanz für die allgemeine Bedrohungslage sind, sowie vor diesem Hintergrund besonders zu berücksichtigende Maßnahmenkategorien. Die Listen sind nicht abschließend und ersetzen nicht, dass der B3S oder der Betreiber ggf. zusätzlich erforderliche Themen berücksichtigt. Wie in Abschnitt 4.2.1 dargestellt, können auch andere, vergleichbare Kategorien verwendet werden.

Letztlich ist in Anhang 5.4 ein Glossar zu finden.

5.1 KRITIS-relevante elementare Gefährdungen

Die folgende Liste basiert auf den „elementaren Gefährdungen“ aus dem IT-Grundschutz-Kompendium. Hier sind diejenigen elementaren Gefährdungen aus dem IT-Grundschutz-Kompendium enthalten, die aus Sicht des BSI für die Erbringung der kDL einer Kritischen Infrastruktur relevant sind.

Kennung aus dem IT-Grundschutz	KRITIS-relevante elementare Gefährdung
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

Kennung aus dem IT-Grundschutz	KRITIS-relevante elementare Gefährdung
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

5.2 Technische Informationssicherheit & bauliche/physische Sicherheit

5.2.1 Technische Informationssicherheit

A 1 Absicherung von Netzübergängen

Kennung	Maßnahme
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

A 2 Sichere Interaktion im Internet

Kennung	Maßnahme
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)

A 3 Sichere Software (insbesondere Vermeidung von offenen Sicherheitslücken)

Kennung	Maßnahme
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 Operations
A 3.8	Sichere Beschaffung und Aussonderung (sicheres Löschen, Überwachung, Datensicherung und -wiederherstellung (Backup), Archivierung)

A 4 Sichere und zuverlässige Hardware

Kennung	Maßnahme
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

A 5 Sichere Authentisierung

Kennung	Maßnahme
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)

A 6 Verschlüsselung

Kennung	Maßnahme
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

A 7 Sonstiges

Kennung	Maßnahme
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

5.2.2 Bauliche/physische Sicherheit

A 8 Bauliche/physische Sicherheit

Kennung	Maßnahme
A 8.1	Zugangskontrolle
A 8.2	Notstromversorgung (USV)
A 8.3	Netzersatzanlagen

5.3 Besonders zu berücksichtigende Bedrohungsszenarien und Maßnahmenkategorien

Im Zuge der Lagebewertung hat das BSI verschiedene Bedrohungsszenarien als besonders relevant für die allgemeine Gefährdungslage identifiziert. Auf die nachfolgenden weist das BSI hier explizit hin.

B Besonders zu berücksichtigende Bedrohungsszenarien

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

Weitere für den Anwendungsbereich relevante Bedrohungsszenarien sollten ergänzt oder angepasst werden.

Ein B3S sollte vor dem Hintergrund dieser spezifischen Bedrohungsszenarien zusätzlich zu den an anderer Stelle erwähnten Anforderungen eine gezielte Betrachtung mit entsprechenden Maßnahmenkategorien beinhalten. Hier zu den oben aufgeführten Bedrohungsszenarien Beispiele für passende Maßnahmenkategorien:

A 9 Besonders zu betrachtende Maßnahmenkategorien

Kennung	Maßnahme
A 9.1	Detektions- / Suchmöglichkeiten auf Infektionen
A 9.2	Innere Sensorik (zur Detektion von IT-Angriffen)
A 9.3	Client-Isolation
A 9.4	Härtung von Verzeichnisdiensten wie bspw. dem Microsoft Active Directory
A 9.5	Backup-Konzept inklusive Offline-Backups

Die Liste soll den Anwendern keinesfalls den Eindruck vermitteln, die besonders zu betrachtenden Maßnahmenkategorien allein böten einen ausreichenden Schutz in den zu berücksichtigenden Bedrohungsszenarien. Sie bedürfen vor dem Hintergrund dieser Szenarien allerdings besonderer Aufmerksamkeit.

5.4 Glossar

Das Glossar definiert zentrale Begriffe des B3S.

Begriff	Definition
Angemessen (im Sinne des BSIG)	Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.
Anlage	Kritische Infrastruktur gemäß Definition der BSI-KritisV).
Ansprechpartner B3S	Von der einreichenden Stelle benannte Person, die den Kontakt zum BSI hält und während der Eignungsprüfung für Rückfragen verfügbar ist. Dies kann auch eine Person sein, die selbst nicht zur Beantragung einer Eignungsprüfung gemäß § 8a Absatz 2 BSIG berechtigt ist.
Anwender	Nutzer des fertig erstellten B3S. In der Regel handelt es sich hierbei um den Betreiber einer Kritischen Infrastruktur, der den B3S zur Umsetzung von § 8a BSIG anwendet. Ein Anwender kann auch mehrere B3S anwenden, beispielsweise wenn der Anwendungsbereich der B3S jeweils nur einen Teil seiner Anlagen umfasst.
Anwendungsbereich	Bereich, den ein B3S abdeckt (siehe 4.1.1).
Autoren des B3S	Personen, die den Text des B3S verfassen und somit die Inhalte gestalten. Beispielsweise können die Autoren Mitglieder eines BAK sein oder auch ein von der einreichenden Stelle beauftragter Dienstleister. Im Gegensatz zur einreichenden Stelle dürfen auch Personen als Autoren mitwirken, die nicht zur Beantragung einer Eignungsprüfung gemäß § 8a Absatz 2 BSIG berechtigt sind.
Branchenspezifischer Sicherheitsstandard (B3S)	Gemäß § 8a Absatz 2 BSIG haben Betreiber Kritischer Infrastrukturen und ihre Branchenverbände die Möglichkeit, branchenspezifische Sicherheitsstandards (B3S) zur Gewährleistung der Anforderungen gem. § 8a Absatz 1 BSIG vorzuschlagen.
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG oder kurz BSI-Kritis-Verordnung.
Einreichende Stelle	Betreiber oder Branchenverband, die eine Eignungsprüfung beim BSI beantragen und gemäß § 8a Absatz 2 BSIG berechtigt sind, einen B3S vorzuschlagen.
Geeignet (im Sinne des BSIG)	Organisatorische und technische Vorkehrungen sind geeignet, wenn der damit verfolgte Zweck erfüllt ist.
KRITIS-Betreiber	Institution, die eine Kritische Infrastruktur nach § 2 Absatz 2 BSIG sowie § 1 Absatz 2 BSI-KritisV betreibt.
Kritische Dienstleistung (kDL)	Kritische Dienstleistungen sind für die Bevölkerung wichtige, teils lebenswichtige Güter und Dienstleistungen. Bei einer Beeinträchtigung dieser kritischen Dienstleistungen würden erhebliche Versorgungsengpässe, Störungen der öffentlichen Sicherheit oder vergleichbare dramatische Folgen eintreten. Die BSI-KritisV enthält neben der Definition der kDL eine Auflistung der kDL nach KRITIS-Sektoren.
Kritische Infrastruktur	Siehe Definition im BSIG bzw. Konkretisierung in der BSI-KritisV.

Begriff	Definition
Maßnahmen, Sicherheitsvorkehrungen, Sicherheitsanforderungen	Die gemäß § 8a Absatz 1 BSIG umzusetzenden angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von informationstechnischen Systemen, Komponenten oder Prozessen. Zu diesen Vorkehrungen gehören auch infrastrukturelle und personelle Maßnahmen. Besonders kritische Prozesse bedürfen besonderer Sicherheitsmaßnahmen. Je nach „gemeinsamem Nenner“ einer Branche kann die Ausgestaltung in einem B3S auf sehr unterschiedlichem Abstraktionsgrad erfolgen. Teilweise können konkrete Maßnahmen definiert werden, teilweise können nur Sicherheitsanforderungen oder Vorgehensweisen benannt werden. Die Begriffe werden in dieser Orientierungshilfe darum synonym verwendet.
Nachweis	Die Gesamtheit der Nachweisdokumente bildet den Nachweis.
Stand der Technik	Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt.