Bundesamt
für Sicherheit in der
Informationstechnik

# 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

# Änderungshistorie

| Version | Datum | Name | Beschreibung |
|---|---|---|---|
| 0.7 | 03.03.2020 | BSI | Entwurf der Anforderungen zum Versand an betroffene Betreiber und Wirtschaftsverbände im Rahmen des Anhörungsverfahrens |
| 1.0 | 22.04.2020 | BSI | Finales Dokument nach durchgeführter Anhörung der betroffenen Betreiber und Wirtschaftsverbände |
| | | | |

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: poststelle@bsi.bund.de
Internet: https://www.bsi.bund.de

# Inhaltsverzeichnis

# 1 Zweck dieses Dokuments

Betreiber von Anlagen der Kritischen Infrastruktur gemäß der BSI-Kritisverordnung (BSI-KritisV) sind verpflichtet

„[...] *angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.* [...]“ (§ 8a Abs. 1 BSIG).

Die Erfüllung dieser Anforderungen ist mindestens alle zwei Jahre in geeigneter Weise gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachzuweisen (§ 8a Abs. 3 BSIG).

Hierzu kann das BSI

„[...] *zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen* [...] *Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.*“ (§ 8a Abs. 5 BSIG).

Mit diesem Dokument macht das BSI von der gesetzlichen Regelung des § 8a Abs. 5 BSIG Gebrauch und legt Anforderungen zur Umsetzung der Nachweisführung nach § 8a Abs. 3 BSIG hinsichtlich

- der Validierung des Geltungsbereichs der Kritischen Infrastruktur (Kapitel 2),
- der Darstellung des Geltungsbereichs in der Nachweisdokumentation (Kapitel 3)

bezogen auf den unter 1.1 genannten Anwendungsbereich fest.

## 1.1 Anwendungsbereich der Anforderungen aus diesem Dokument

Mit diesem Dokument werden Anforderungen ausschließlich für Kritische Infrastrukturen (Anlagen) der folgenden Anlagenkategorie gemäß Anhang 4 Teil 3 BSI-KritisV festgelegt:

| | | |
|---|---|---|
| **Kritische Dienstleistung:** | **2.** | **Datenspeicherung und -verarbeitung** |
| **Bereich:** | **2.1** | **Housing** |
| **Anlagenkategorie:** | **2.1.1** | **Rechenzentrum** |

Das BSI weist ausdrücklich darauf hin, dass Rechenzentren, die nicht gemäß dieser Anlagenkategorie als Kritische Infrastruktur betrieben werden, nicht den Anforderungen aus diesem Dokuments unterliegen. Dies trifft insbesondere auf rein betreiberintern genutzte Rechenzentren zu, auch dann, wenn diese zum Betrieb einer anderen Kritischen Infrastruktur des Betreibers beitragen.

## 1.2 Anwendbarkeit der Anforderungen aus diesem Dokument

Die Anforderungen aus diesem Dokument sind bei der Erstellung aller Nachweise gemäß § 8a Abs. 3 BSIG für Anlagen aus dem Anwendungsbereich einzuhalten, die **nach dem 05.05.2020** beim BSI vorgelegt werden.

# 2 Anforderung zur Validierung des Geltungsbereichs

Um eine Prüfung der Kritischen Infrastruktur zur Erstellung eines geeigneten Nachweises gem. § 8a Abs. 3 BSIG zu ermöglichen, muss der Geltungsbereich zunächst durch den Betreiber passend festgelegt werden. Im Rahmen der Nachweisprüfung muss der Geltungsbereich anschließend auf Validität geprüft werden.

Zur Überprüfung der Validität des Geltungsbereiches muss der Prüfer den beauftragten Geltungsbereich unter Berücksichtigung der realen Gegebenheiten dahingehend bewerten, ob dieser hinsichtlich

- der Anlagenteile, die zur Erbringung der kritischen Dienstleistung relevant sind,
- der informationstechnischen Systeme, Komponente und Prozesse, die für die Funktionsfähigkeit der Kritischen Infrastruktur relevant sind,
- der Schnittstellen bzw. Abhängigkeiten zwischen/von Systemen untereinander und
- der ausgelagerten, für den Betrieb der Kritischen Infrastruktur relevanten Teile

in den nachfolgenden Querschnittsaufgaben[1] vollständig ist:

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

Die genannten Querschnittsaufgaben sind nicht abschließend und vom Prüfer je nach spezifischer Situation beim Betreiber geeignet zu erweitern.

Sofern der Prüfer zu dem Ergebnis kommt, dass Teile im beauftragten Geltungsbereich fehlen, sind diese in den Geltungsbereich der Prüfung mit aufzunehmen.

1 Unter dem Begriff Querschnittsaufgaben werden in diesem Kontext Aufgaben verstanden, die sich über die gesamte Kritische Infrastruktur hinweg über alle relevanten informationstechnischen Systeme, Komponenten oder Prozesse erstrecken. Diese Aufgaben werden i.d.R keinem einzelnen Prozess zugeordnet, sondern sind in verschiedenen Ausprägungen in jedem relevanten Prozess vorhanden. Dass eine der genannten Querschnittsaufgaben bei einem Betreiber als eigener Geschäftsprozess behandelt werden kann, stellt keinen Widerspruch dar.

# 3 Anforderung an den Geltungsbereich als Bestandteil der Nachweisdokumentation

Wesentlicher Bestandteil eines geeigneten Nachweises gemäß § 8a Abs. 3 BSIG ist die **textuelle Beschreibung** sowie – wo sinnvoll bzw. erforderlich – **grafische Darstellung** des Geltungsbereichs der Kritischen Infrastruktur (Anlage), für die der Nachweis erbracht wird.

## 3.1 Anforderung an die Beschreibung und grafische Darstellung des Geltungsbereichs

**Anforderungen an die textuelle Beschreibung**

- Die Abhängigkeiten zwischen den informationstechnischen Systemen, Komponenten und Prozesse sind nachvollziehbar zu beschreiben.
- Sofern Teile der Kritischen Infrastruktur ausgelagert werden, sind diese, sowie die Abhängigkeiten der informationstechnischen Prozesse von den ausgelagerten Teilen, nachvollziehbar zu beschreiben.

**Anforderungen an die grafische Darstellung**

- Die grafische Darstellung des Geltungsbereichs muss in Form eines angepassten Netzplans erfolgen.

  Der Netzplan ist dahingehend anzupassen, dass die verschiedenen informationstechnischen Prozesse sowie die Zuordnung der (für den Betrieb der Kritischen Infrastruktur relevanten) informationstechnischen Systeme und Komponenten zu den Prozessen und Querschnittsaufgaben hervorgehen.
- Der Abstraktionsgrad für die grafische Darstellung des Geltungsbereichs muss geeignet gewählt werden. Wo sinnvoll, sind mehrere Systeme gleicher Art zusammenzufassen.
- Sofern Teile der Kritischen Infrastruktur ausgelagert werden, sind diese klar und nachvollziehbar kenntlich zu machen.

Hinweis: Ein unverbindliches Beispiel für eine grafische Darstellung ist in Anhang I – a enthalten.

**Anforderungen an die textuelle Beschreibung und grafische Darstellung**

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

- Realisierung der Versorgung mit Strom, IT-Netz und Internet für das Housing (als Dienstleistung im Sinne des Bereichs der Kritischen Dienstleistung gemäß BSI-KritisV) in der Anlage.
- Realisierung der Kühlung, insbesondere im Zusammenspiel der Kühl- und Steuerungssysteme.
- Realisierung der Betriebssicherheit, insbesondere im 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.

## 3.2 Zusätzliche Anforderungen bei aus mehreren Gebäuden bestehenden Anlagen (Campus)

Die Bestandteile eines Rechenzentrums können auf mehrere Gebäude oder andere Anlagenteile (z. B. externe Notstrom-Generatoren) innerhalb eines Campus aufgeteilt sein.

Um die verschiedenen Abstraktionsebenen nachvollziehbar darzustellen, ist in solchen Fällen der Nachweisdokumentation **zusätzlich** eine kurze Beschreibung und grafische Darstellung des Campus 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 Aufteilung der Funktionen auf die jeweiligen Gebäude(-teile)/Anlagenteile des Campus.
- Die gemeinsam genutzten Betriebseinrichtungen.
- 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 3.1 bewegen.

Hinweis: Ein unverbindliches Beispiel für eine grafische Darstellung ist in Anhang I – b enthalten.

## 3.3 Zusätzliche Anforderungen bei räumlich getrennten gemeinsamen Anlagen

Im Fall einer gemeinsamen Anlage[2], deren Rechenzentren nicht innerhalb des selben Campus liegen, ist der Nachweisdokumentation **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)/Anlagenteile untereinander.
- Die Zuordnung der Funktionen (Zwecke) auf die jeweiligen Verbindungen.

Die Darstellung soll sich auf einer höheren Abstraktionsebene als in 3.1 bzw. 3.2 bewegen. Eine zusammengefasste Darstellung von 3.2 und 3.3 ist nur dann zulässig, wenn der vollständige Informationsgehalt aus 3.2 erhalten bleibt.

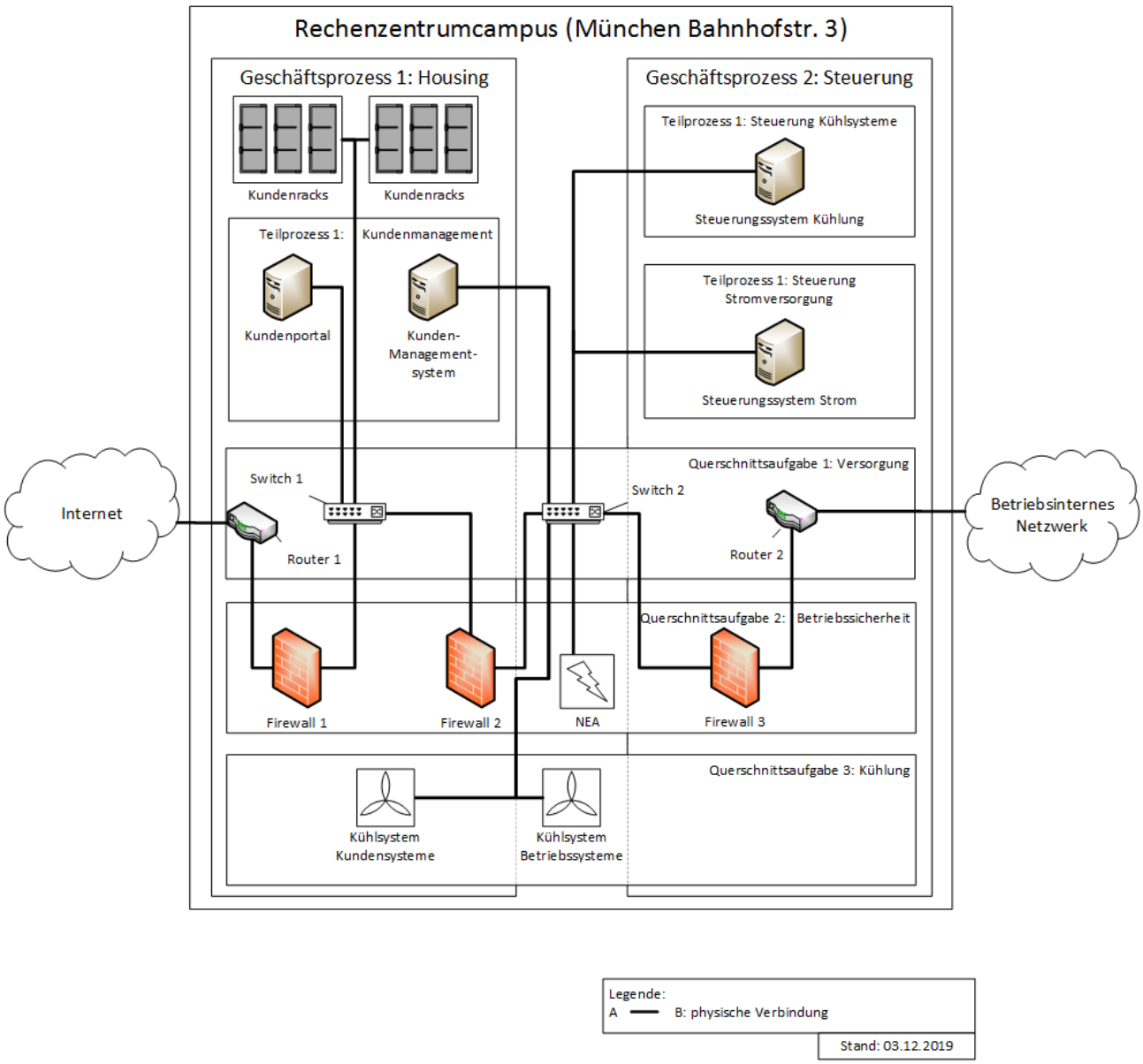
Hinweis: Ein unverbindliches Beispiel für eine grafische Darstellung ist in Anhang I - c enthalten.

2 Gemeinsame Anlage: Für die Definition einer gemeinsamen Anlage sei auf die BSI-Kritisverordnung verwiesen – siehe hierzu Anhang 4, Teil 1 Nr. 6 BSI-KritisV ( https://www.gesetze-im-internet.de/bsi-kritisv/anhang_4.html )

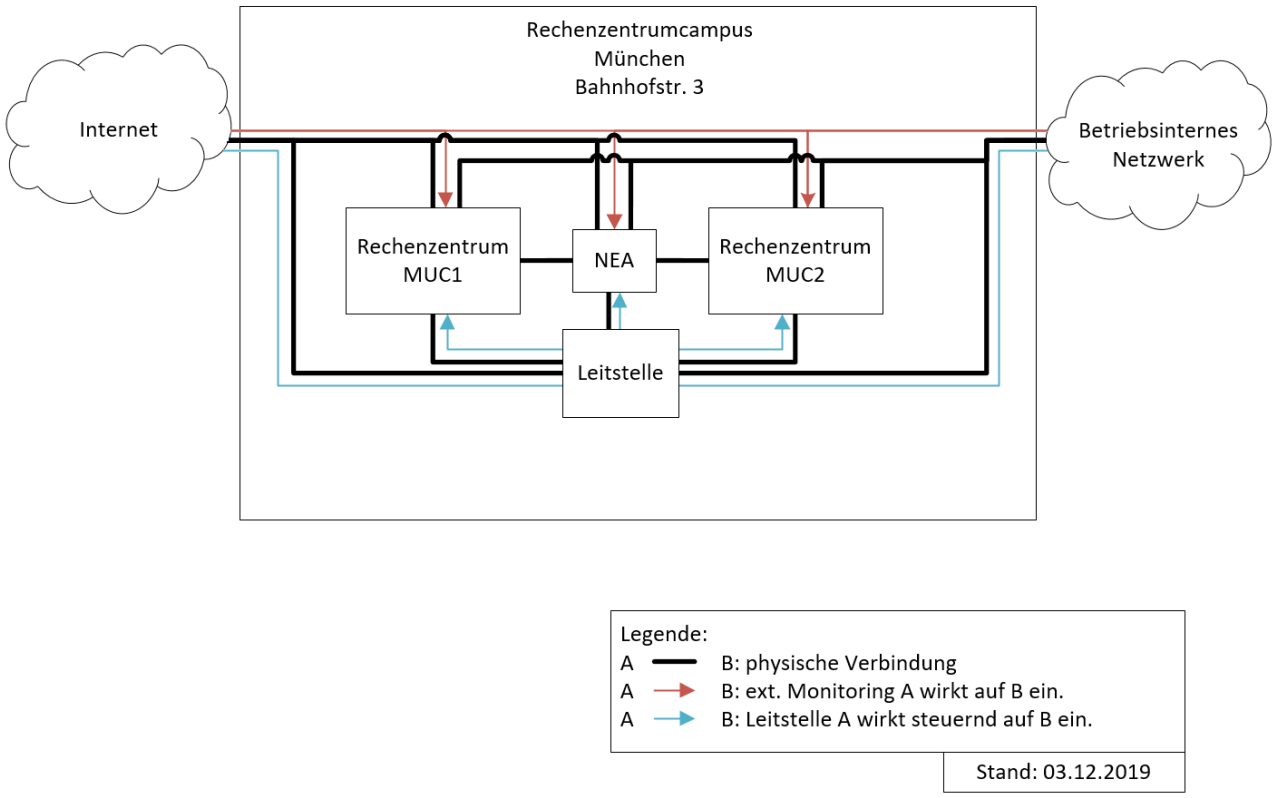
# Anhang I

Anhang I enthält einige – unverbindliche – Beispiele zur Umsetzung der Anforderungen aus Kapitel 3. Die Beispiele wurden anhand einer fiktiven Anlage erstellt und erheben keinen Anspruch auf Vollständigkeit. Eine 1:1-Anwendung dieser Beispiele in der Nachweisdokumentation, ohne Anpassung an die jeweilige Anlage, ist keinesfalls möglich!

## a) Beispiel für einen angepassten Netzplan gemäß Kapitel 3.1



# b) Beispiel für einen Anlagenplan (Campus) gemäß Kapitel 3.2



## c) Beispiel für einen Anlagenplan (räumlich getrennte gemeinsame Anlage) gemäß Kapitel 3.3