



BSIG, Sektore
BSI-Kritis-V
Schwellenwer
Fristen, B3S
Prüfverfahren
Formulare



KRITIS

Anforderungen, Pflichten, Nachweisprüfung

Zur
aktuellen
BSI-Kritis-V

- ▶ Sicher durch die Nachweisprüfung nach dem BSIG
- ▶ Hintergründe und Fachwissen zum BSI-Gesetz für IT-Verantwortliche und Auditoren
- ▶ Prüfverfahrenskompetenz erwerben

Jacqueline Naumann

Wie Ihnen dieses Buch helfen kann – und was es nicht ist

In diesem Buch geht es um die regelmäßig wiederkehrenden Nachweisprüfungen für Kritische Infrastrukturen aller Sektoren, aber auch um *Unternehmen im besonderen öffentlichen Interesse* (UBIs). Mit dem IT-Sicherheitsgesetz aus dem Jahr 2015 verabschiedete der Bundestag einige neue Pflichten für systemrelevante Organisationen. Neben dem Aufbau von Schutzvorkehrungen gehört deren Nachweis gegenüber dem BSI zu den größten Herausforderungen, denen sich diese Organisationen stellen müssen.

Seit 2018 führe ich Nachweisprüfungen sowie Schulungen zum Erwerb der notwendigen Prüfverfahrenskompetenz durch. Seitdem spezifizierten sich die Anforderungen an Nachweisprüfungen immer heftiger.

Für dieses Buch studierte ich mehr als einhundert Quellen. Von diesen wählte ich siebenundsechzig für Sie aus und gebe deren relevantesten Inhalte im Buch wieder. An vielen Stellen versuche ich, Ihnen die Anforderungen an Nachweisprüfungen auch durch Abbildungen oder Tabellen visuell darzustellen. Dort, wo es mir möglich war, stelle ich zusätzlich elektronische Dateien als Begleitmaterial zum Buch bereit. Dabei sammelte ich zweiundfünfzig Dokumente für Sie.

Zugriff auf diese Dateien haben Sie immer dann, wenn Sie einen Infokasten, wie den folgenden mit dem Hinweis zum Begleitmaterial vorfinden. Die von mir zusammengestellten Begleitmaterialien stammen beispielsweise vom Bund, vom BMI, vom BSI, von der Bundesnetzagentur, vom UP KRITIS oder auch von mir in Form von Vorlagen. Die Namen fast aller Dokumente beginnen mit dem Ausgabejahr und dem Monat. Nur selten fand ich lediglich eine Jahreszahl.

Hinweis zum Begleitmaterial

Das BSI-Errichtungsgesetz vom Dezember 1990 finden Sie im Dokument:

- 1990-12_BSI-Errichtungsgesetz



Ich habe für Sie interessante Stellen aus den Gesetzen und Regulatorien der Begleitmaterialien herausgepickt und zitiere diese. Sie müssten die Gesetzestexte somit nicht vollständig im Original lesen, da ich auf alle relevanten Stellen im Buch eingehe.

Die Zitate sind vor allem für Trainer interessant, um die Hintergründe genauer erläutern und Aussagen mit Quellen belegen zu können.

Außerdem streute ich für angehende Nachweisprüfer etwa achtzig potenzielle Prüfungsfragen in die Abschnitte ein. Wenn Sie eine Zertifizierung im Seminar »Zusätzliche Prüfverfahrenskompetenz nach dem BSIG« anstreben, können Sie Ihr Wissen im Buch testen.

Die potenziellen Prüfungsfragen erkennen Sie an Infokästen, wie dem nachfolgend gezeigten. Die Nummer der Frage entspricht dem Kapitel und einer laufenden Nummer. Ihre Lösungen können Sie im Abschnitt 15.2, »Überprüfung Ihrer Antworten«, kontrollieren. Beachten Sie bitte: Bei einer BSI-Prüfung können immer eine, mehrere oder alle Antworten richtig sein und eine Frage gilt nur dann als korrekt beantwortet, wenn Sie alle richtigen Antworten ausgewählt haben.



F-01-1: Das IT-Sicherheitsgesetz ist ...

- a) ein europäisches Gesetz
- b) ein Artikelgesetz
- c) ein Gesetz des Landes
- d) ein Gesetz des Umweltministeriums

Während ich das Manuskript zum Buch schrieb, konnte ich an vielen Stellen geplante Änderungen im Prüfungs- und Nachweisprozess für den Zeitraum ab Oktober 2024 wahrnehmen. Deshalb veränderte ich mir bekannte Prüfungsfragen bereits für die Zukunft, indem ich zum Beispiel Paragraphen aus den Fragen löschte oder neue Sektoren hinzufügte. Wie alt oder neu Prüfungsfragen bei einer BSI-Personenzertifizierung dann sind, vermag ich allerdings nicht zu beurteilen.

An einigen Stellen gebe ich zusätzliche Hinweise zu Anforderungen, auf die Sie achten müssen. Hinweise erkennen Sie an Infokästen in folgendem Format.



Nachweisdokument KI / KI*

Vergessen Sie nicht den Stempel der Organisation.

Konkrete Umsetzungsmöglichkeiten für Krankenhäuser, IT-Sicherheitsstandards oder BaFin-Anforderungen werde ich in diesem Buch nicht behandeln.

Was gibt es stattdessen?

Sie erhalten die Anforderungen und Pflichten für KRITIS-Betreiber und alle relevanten Aspekte rund um die Nachweisprüfung nach dem BSIG.

Als ich das Buch schrieb, war mein Ziel, ein zentrales Werk zum Thema Nachweisprüfungen zu schaffen. Ich hoffe, dass mir dies geglückt ist und dass ich Sie mit diesem Handbuch gut unterstützen kann, damit Sie Ihre nächste Nachweisprüfung reibungslos überstehen.

Sehen wir uns im folgenden Abschnitt gemeinsam den Aufbau dieses Buches an.

Der Weg durch das Buch

Dieser Abschnitt soll Ihnen zeigen, wie Sie sich in diesem Buch zurechtfinden.

Das Buch ist in fünf Hauptthemen unterteilt und umfasst insgesamt sechzehn Kapitel. Den ersten Schwerpunkt des Buches legte ich auf die gesetzlichen Anforderungen für unsere Nachweisprüfungen und auf die Einführung von Begriffen und Regelwerken.

Als ich an diesem Buch arbeitete, entwickelte sich nach und nach ein Prozessverständnis, das ich als *doppelten Reformprozess für Kritische Infrastrukturen* bezeichne und Ihnen in Abbildung 1 zeige.

Anhand dieses Reformprozesses kann ich Ihnen gut erklären, welche Dinge es für Kritische Infrastrukturen und KRITIS-Betreiber bereits gibt und wo wir uns befinden.

Im ersten Teil des Buches starte ich auf der linken Seite von Abbildung 1, die ich *öffentlichen Reformprozess* nenne. Dort beginnt jeder Verbesserungskreislauf mit Artikelgesetzen, deren Paragraphen in Gesetze überführt werden und durch Verordnungen ihre Macht entfalten.

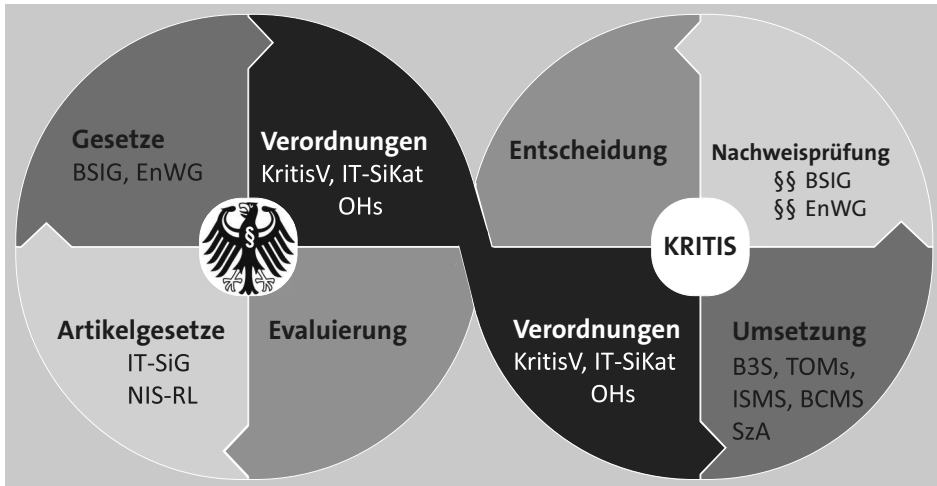


Abbildung 1 Doppelter Reformprozess für Kritische Infrastrukturen

Diese Kraft der Verordnungen schwappt hinüber in den *wirtschaftlichen Verbesserungskreislauf*, fordert von den Sektoren die unterschiedlichsten Umsetzungen und mündet in regelmäßige Nachweisprüfungen. Mein Ziel ist es, diesen fast letzten Aspekt im doppelten Reformprozess erfolgreich beenden zu können.

Sie erkennen: Anschließend müssen Entscheidungen getroffen werden, die bis in die öffentlichen Verbesserungen durch Evaluierungen führen können. Jeder Reformpro-

zess kann für sich allein kontinuierlich verbessert werden. Doch neue Verordnungen zwingen die Wirtschaft zum Handeln, und Ergebnisse aus Nachweisprüfungen führen zu Entscheidungen auf Wirtschafts- und öffentlicher Seite.

Zu **Teil I**, »Gesetzliche Anforderungen und Begriffe im KRITIS-Umfeld«, gehören die ersten drei Kapitel.

Kapitel 1, »Geschichtliche Hintergründe zur Nachweisprüfung«, beginnt mit einem Rückblick auf die letzten fast fünfunddreißig Jahre. Ich beginne mit der Gründung des BSI, in der ich den späteren offiziellen Start aller Nachweisprüfungen für KRITIS-Betreiber in Deutschland sehe.

In **Kapitel 2**, »Die Kritisverordnung«, erläutere ich die Begriffe rund um Kritische Infrastrukturen und die BSI-Kritisverordnung. Die Kritisverordnung legt für Sie als Betreiber den Grundstein, um zu bestimmen, ob Sie als Kritische Infrastruktur gelten und Nachweise beim Bundesamt für Sicherheit in der Informationstechnik (BSI) einreichen müssen oder nicht.

Kapitel 3, »Die IT-Sicherheitskataloge (IT-SiKat) für den Sektor Energie«, rückt für Betreiber und Prüfer im Sektor Energie die IT-Sicherheitskataloge und deren Verwendung in den Fokus. Mit diesem Kapitel endet der Rückblick und somit der erste Teil des Buches.

Den zweiten Schwerpunkt des Buches lege ich auf die Bedeutung und Verantwortung des BSI. Auch dieser **Teil II** des Buches umfasst drei Kapitel:

In **Kapitel 4**, »Die Unterstützung durch das BSI«, können Sie sich einen Überblick über die Aufgaben des BSI verschaffen. Ich stütze mich dabei auf die öffentlich zugänglichen Informationen und begrenze die Schwerpunkte auf eine Analyse der Sicherheitslage in Deutschland und die Warnung der Betreiber. Bei der Auswahl dieser Themen habe ich diejenigen Paragraphen aus dem BSI-Gesetz (BSIG) stärker gewichtet, die Aufgaben für das BSI definieren. Natürlich ist dies nur ein kleiner Ausschnitt aus den BSI-Aufgaben.

Nachdem das BSI drei *Orientierungshilfen* (OH) für Betreiber und Prüfer veröffentlichte, erläutere ich diese in **Kapitel 5**, »Die Orientierungshilfen (OH) des BSI«, um Ihnen Hilfestellungen und Orientierung im Nachweisprozess zu geben.

Das BSIG gibt dem BSI die Befugnisse, Vorgaben für die Art und Weise von Nachweisprüfungen zu definieren. In **Kapitel 6**, »Vorgaben an die Art und Weise von Nachweisprüfungen«, bereitete ich diese Vorgaben in Form von Dokumenten und Vorlagen für Sie auf, um Ihnen die Vorbereitung und Durchführung von Nachweisprüfungen zu vereinfachen. In diesem Kapitel beschäftigen wir uns auch mit den *grundsätzlichen Anforderungen im Nachweisprozess* (GAiN). Mit dem sechsten Kapitel endet der zweite Teil des Buches.

Den dritten Schwerpunkt des Buches lege ich auf die Pflichten und Möglichkeiten der KRITIS-Betreiber. Dieser **Teil III**, »Pflichten und Möglichkeiten des KRITIS-Betreibers«, umfasst zwei Kapitel.

In **Kapitel 7**, »Ihre Pflichten als KRITIS-Betreiber«, zeige ich Ihnen, welche Aufgaben auf Sie als Betreiber einer kritischen Infrastruktur zukommen. Wir sehen uns in diesem Kapitel beispielsweise die Bestimmung des Geltungsbereiches, das Risikomanagement, die *Systeme zur Angriffserkennung* und die *Gemeinsame übergeordnete Ansprechstelle* (GÜAS) genauer an.

Weil die Möglichkeit besteht, als Betreiber auch an einem *Branchenspezifischen Sicherheitsstandard* (B3S) mitzuwirken und diesen durch das BSI bestätigen zu lassen, zeige ich Ihnen in **Kapitel 8**, »Einen branchenspezifischen Sicherheitsstandard (B3S) veröffentlichen«, wie ein B3S erstellt werden könnte und welche Schritte nötig sind, um ihn als offizielle Prüfgrundlage beim Betreiber einsetzen zu können. Mit dem achten Kapitel endet Teil III des Buches.

Kommen wir nun zum vierten Themenschwerpunkt des Buches, der eigentlichen Nachweisprüfung nach dem BSIG. **Teil IV**, »Die Nachweisprüfung gemäß § 8a Abs. 3 BSIG«, umfasst fünf Kapitel.

In **Kapitel 9**, »Planung der Nachweisprüfung durch den Betreiber«, gehe ich auf die Planung einer Nachweisprüfung durch die KRITIS-Betreiber ein, und in **Kapitel 10**, »Vorarbeiten für die Nachweisprüfung durch Prüfer«, zeige ich Ihnen, welche Schritte vor einer Nachweisprüfung durch die Prüfstelle umgesetzt werden müssen.

Zu diesen Vorarbeiten gehören beispielsweise die Auswahl und Definition einer Prüfgrundlage, die Bestimmung der notwendigen Prüfer-Kompetenzen, die Prüfplanung nach GAI-N, die Auswahl von Stichproben und die Berücksichtigung von externen Dienstleistern.

Sind dann alle Vorarbeiten abgeschlossen, kann die Durchführung der Prüfung beginnen. Diese erläutere ich Ihnen in **Kapitel 11**, »Die Nachweisprüfung durchführen«. Zur Prüfdurchführung gehören beispielsweise Remote Audits, die unterschiedlichen Prüfmethoden, die Berücksichtigung bestehender ISO/IEC 27001-Zertifikate, die Prüfung branchenspezifischer Maßnahmen und des Notfallmanagements (BCMS). Auch die Aktualität der Nachweisdokumente besprechen wir im elften Kapitel.

In **Kapitel 12**, »Nacharbeiten nach der Nachweisprüfung«, geht es um die Arbeiten, die Prüfer und Betreiber nach einer abgeschlossenen Nachweisprüfung erledigen müssen. Die Nacharbeiten beginnen für Prüfer mit der Bewertung der ISMS- und BCMS-Reifegrade sowie mit den SZA-Umsetzungsgraden.

Zu den Nacharbeiten für Betreiber gehören die Umsetzungsplanung für Maßnahmen und die Selbsterklärung für die AWV-UBI (Außenwirtschaftsverordnung-UBI, UBI 1).

Zuletzt erkläre ich in diesem Kapitel, wie Betreiber die Nachweise an das BSI übermitteln oder wie die Zertifizierungsstellen ihre Nachweise an die Bundesnetzagentur (BNetzA) weiterleiten.

In **Kapitel 13**, »Prüfung der eingereichten Nachweise durch das BSI«, zeige ich Ihnen, was Sie als Betreiber nach Einreichung Ihrer Unterlagen vom BSI möglicherweise noch an Eskalationen, Nachforderungen oder Sonderprüfungen erwarten dürfen. Auch auf Bußgelder kommen wir in diesem Kapitel zu sprechen.

Der **Teil IV** des Buches endet mit dem dreizehnten Kapitel und somit mit dem Abschluss der Nachweisprüfung.

Im fünften und letzten Teil des Buches lege ich den Schwerpunkt auf Erfahrungen aus der Praxis und wie Sie als zukünftige Nachweisprüfer in die Praxis hineinfinden. **Teil V**, »Aus der Praxis – in die Praxis«, umfasst drei Kapitel.

In **Kapitel 14**, »Untersuchung zu Umfang und Komplexität der Nachweisprüfung«, zeige ich Ihnen die Ergebnisse aus meiner Untersuchung zur Komplexität von Nachweisprüfungen im Sommer 2023. Dieses Kapitel beginnt mit einem Vergleich der BSI-Studie vom Winter/Frühjahr 2023 zur Umsetzung der IT-Sicherheitsgesetze mit den Ergebnissen meiner Studie.

Anschließend habe ich für alle, die zukünftig selbst Nachweisprüfungen durchführen möchten und den Kompetenznachweis dafür benötigen, in **Kapitel 15** die Prüfung zur »Zusätzlichen Prüfverfahrenskompetenz nach dem BSIG« in den Mittelpunkt gestellt. In diesem Kapitel erfahren Sie, wie die Prüfung abläuft, und können Ihre Ergebnisse testen, die Sie während der Lektüre dieses Buches anhand der potenziellen Prüfungsfragen gesammelt haben.

Am Ende des Buches ziehe ich in **Kapitel 16** ein Fazit und möchte Ihnen noch einige Ausblicke auf aktuelle Entwicklungen geben.

Kapitel 2

Die Kritisverordnung

Hat Rubik's Cube 'nen tief'ren Sinn, mal wird gruppiert, dann liquidiert? Ganz ähnlich sieht's für KRITIS aus, nach Diensten sind sie strukturiert. Die Ordnung finden ist hier Ziel, nach Strom, IT und selbst Verkehr. Betreibern scheint's leicht abgedreht. Verordnung heißt die Lösung hier.

Können Sie sich an dieser Stelle noch an Abbildung 1.4 im ersten Kapitel erinnern? Die Abbildung zeigte uns die ersten beiden Kritisverordnungen aus den Jahren 2016 und 2017 und stellte den Startpunkt für die Meldung einer Kontaktstelle und die Nachweispflicht dar.

In diesem Kapitel möchte ich nicht mehr auf diese alten, bereits ersetzten Rechtsverordnungen eingehen, sondern auf die derzeit aktuelle Kritisverordnung (13) vom 23. Februar 2023.

Hinweis zum Begleitmaterial

Die Kritisverordnung vom 23. Februar 2023 finden Sie im Dokument:

► 2023-02_BSI-KritisV



In den folgenden Abschnitten zeige ich Ihnen Hintergründe zur Erarbeitung und zum Aufbau dieser Kritisverordnung.

2.1 Kritische Infrastrukturen

Logischerweise gelten nicht alle Organisationen in Deutschland als Betreiber kritischer Infrastrukturen. Um sich zu ihnen zählen zu können, muss ein Unternehmen essenzielle Dienstleistungen oder Produkte für unsere Bevölkerung gewinnen, herstellen, bereitstellen, verarbeiten oder vertreiben.

Die Fokussierung auf bestimmte Organisationen geschah in einem längeren Entscheidungsprozess, den ich Ihnen in Kapitel 1 aufgezeigt habe. Die Frage, die dabei geklärt werden musste, lautete: Was benötigt unsere Gesellschaft – und damit jeder Einzelne von uns – mit besonders hoher Priorität?

Daraus entstand die Konzentration auf Unternehmen, die genau dieses von uns benötigte Angebot liefern können. Für diese Unternehmen entstand die Bezeichnung *Kritische Infrastruktur*. Früher lag diese Entscheidung bei den Betreibern. Sie regulierten die Zusammenarbeit mit anderen Institutionen weitestgehend selbst.

Wenn wir darüber nachdenken, welche Produkte oder Dienstleistungen für uns unentbehrlich geworden sind, werden wir erkennen, dass mindestens die Kernthemen Stromversorgung, Computer und Internet, Ernährung, Gesundheit, Trinkwasser oder Bargeld für uns relevant sind, aber noch weitere, die im ersten Augenblick gar nicht so wichtig erscheinen. Aber auch diese *kritischen Dienstleistungen (kDL)* sollen uns möglichst ununterbrochen zur Verfügung stehen.

Diese von uns benötigten Dienstleistungen wurden schwerpunktmäßig zu *Sektoren* zusammengefasst, und für jeden Sektor wurden die Anlagen bestimmt, die zur Gewinnung, Erzeugung, Verarbeitung, Bereitstellung oder Verteilung vonnöten sind.

Um als Betreiber nun erkennen zu können, ob das eigene Unternehmen zu den KRITIS-Betreibern zählt, können wir die Kritisverordnung zu Hilfe nehmen. Wie das funktioniert, möchte ich Ihnen in den nächsten Abschnitten dieses Kapitels erläutern.

Testen Sie zum Schluss dieses Abschnitts noch Ihr Wissen:



F-02-1: Auf welche Art und Weise wurde vor dem Erlass der BSI-Kritisverordnung Kritische Infrastrukturen definiert?

- a) Das BSI hat den Betreibern Kritischer Infrastrukturen ein entsprechendes Zertifikat ausgestellt.
- b) Es gab ein System der Selbstregulierung im Rahmen der öffentlich-privaten Partnerschaft von Wirtschaft und Staat im UP KRITIS.
- c) Die Einschätzung, ob Infrastrukturen als kritisch anzusehen sind, lag beim Betreiber.
- d) Die Betreiber wurden per Rechtsverordnung zu Betreibern Kritischer Infrastrukturen erklärt.

2.2 Die Erarbeitung der Kritisverordnung

In diesem Abschnitt erfahren Sie, welche Institutionen an der Erarbeitung der Kritisverordnung beteiligt waren. Dieses Hintergrundwissen ist für diejenigen von Interesse, die eine Prüfung zur *Zusätzlichen Prüfverfahrenskompetenz* ablegen wollen.

An der Erarbeitung der letzten Kritisverordnung waren beteiligt:

- ▶ das Bundesministerium des Inneren (BMI),
- ▶ die Kreise der UP KRITIS sowie
- ▶ Aufsichtsbehörden.

Außerdem mitgewirkt haben:

- ▶ das Bundesministerium für Wirtschaft und Klimaschutz (BMWK),
- ▶ das Bundesministerium der Finanzen (BMF),
- ▶ das Bundesministerium der Justiz (BMJ),
- ▶ das Bundesministerium für Arbeit und Soziales (BMAS),
- ▶ das Bundesministerium für Ernährung und Landwirtschaft (BMEL),
- ▶ das Bundesministerium für Verkehr und digitale Infrastruktur (BMDV),
- ▶ das Bundesministerium für Gesundheit (BMG) und
- ▶ das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMVU).

Während ich diesen Abschnitt schrieb, überprüfte ich die Abkürzungen der Bundesministerien immer mal wieder und stellte dabei fest, dass sich einige Bezeichnungen seit Februar 2023 weiterentwickelten. Sie können dies selbst in der Eingangsformel auf der ersten Seite der Kritisverordnung überprüfen.

Anhand der großen Gruppe von Beteiligten können Sie erkennen, wie umfangreich die Erarbeitung der Kritisverordnung gewesen sein muss.

F-02-2: Wer war an der Erstellung der BSI-Kritisverordnung beteiligt?

- a) das Bundesministerium des Inneren (BMI) und weitere Bundesministerien
- b) Aufsichtsbehörden
- c) die Wirtschaft im Rahmen der UP KRITIS
- d) das europäische Parlament



In Abbildung 2.1 sehen Sie grafisch dargestellt, welche Bundesministerien und andere Gruppen an der Erarbeitung der letzten Kritisverordnung mitgewirkt haben. Wir finden die Autoren, wie oben schon erwähnt, in der Eingangsformel der Kritisverordnung.

Im nächsten Abschnitt möchte ich auf die Begriffe eingehen, die in der Kritisverordnung verwendet werden.

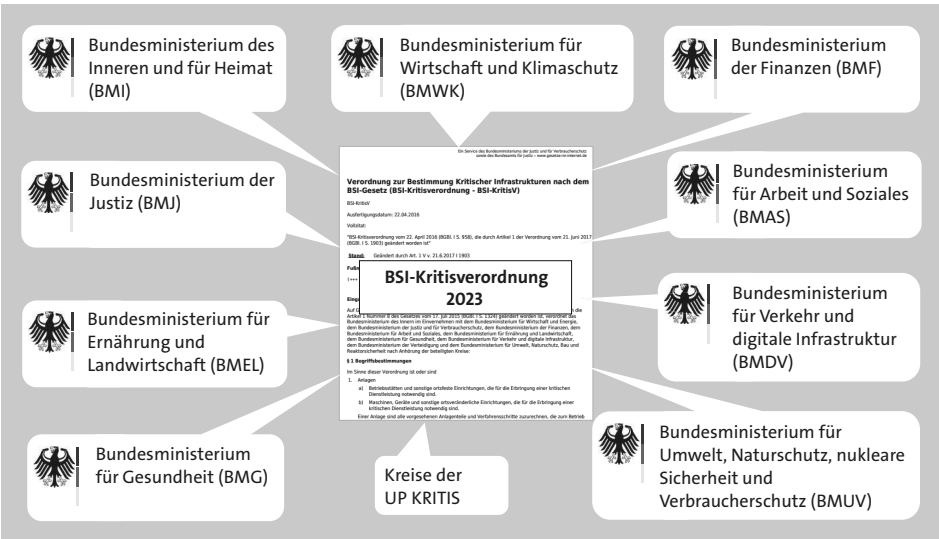


Abbildung 2.1 Die BSI-Kritisverordnung von 2023 wurde durch das Bundesministerium des Inneren (BMI) in Zusammenarbeit mit anderen Bundesministerien und den Kreisen der UP KRITIS erarbeitet.

2.3 Begriffe und Definitionen

Die Kritisverordnung (13) besitzt eine zweiteilige Struktur aus Paragrafen und Anhängen.

Im § 1 Abs. 1 der Kritisverordnung finden wir die Definitionen für die Begriffe *Anlage*, *Betreiber*, *Kritische Dienstleistung*, *Versorgungsgrad* und *Schwellenwert*.

In Abbildung 2.2 zeige ich Ihnen die Definitionen für *Anlage* und *Betreiber*.



BSI Kritisverordnung
23.02.2023

§ 1 (1)

Begriffsbestimmungen

1) Anlagen

- a) Betriebsstätten und sonstige **ortsfeste** Einrichtungen,
- b) Maschinen, Geräte und sonstige **ortsveränderliche** Einrichtung oder
- c) Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind.

2) Betreiber

Eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.

Abbildung 2.2 Begriffsbestimmung zu »Anlagen« und »Betreiber« (KritisV, 02.2023)

In Abbildung 2.3 zeige ich Ihnen die Definitionen für die *kritische Dienstleistung* und für den *Versorgungsgrad*. Ein Ausfall von kritischen Dienstleistungen kann zu erheblichen Beeinträchtigungen und zu sozialen Unruhen führen.

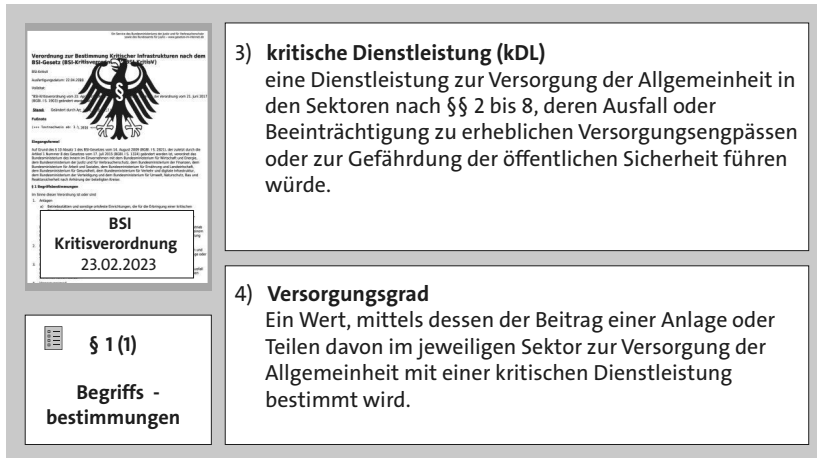


Abbildung 2.3 Begriffsbestimmung zu »kritische Dienstleistung« und »Versorgungsgrad« (KritisV, 02.2023)

Zuletzt finden wir den Begriff *Schwellenwert* im § 1, dessen Definition ich Ihnen in Abbildung 2.4 zeigen möchte.

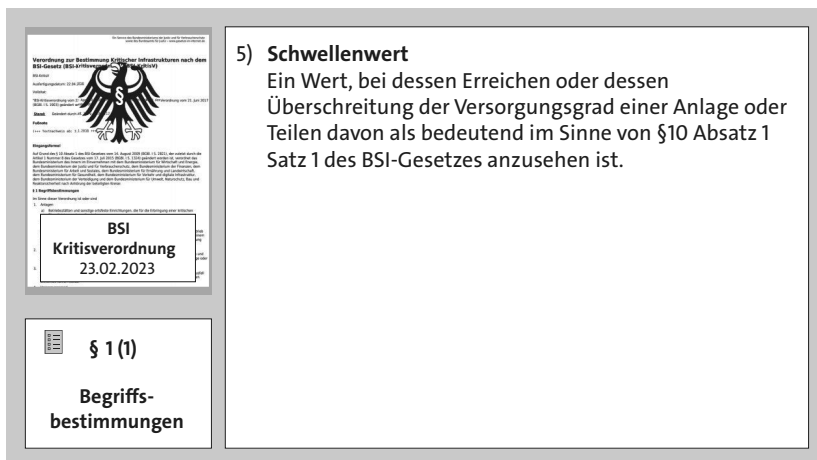


Abbildung 2.4 Begriffsbestimmung »Schwellenwert« (KritisV, 02.2023)

Diese Begriffe werden in der Kritisverordnung verwendet und müssen oft auch in Zertifizierungsprüfungen zur Prüfverfahrenskompetenz bekannt sein.

Als ich selbst die Personenzertifizierung zum Nachweisprüfer im Spätsommer 2018 ablegte und zu Paragrafen der Kritisverordnung gefragt wurde, dachte ich mir: »Ver-

dammt, um welche Paragraphen geht es hier eigentlich?« Mich hatten bis dahin nur die Anhänge interessiert.



F-02-3: Was beinhalten die Paragraphen der BSI-Kritisverordnung?

- a) Berechnungsformeln
- b) Anlagenkategorien
- c) Meldepflichten
- d) Begriffsbestimmungen

Ich war überrascht, in der Prüfung zu konkreten Paragraphen befragt zu werden. Bis dahin ging ich davon aus, ich könnte jederzeit alles nachschlagen. Doch diese Prüfung findet als Closed-Book-Verfahren statt, was bedeutet, dass keine zusätzlichen Unterlagen oder Hilfsmittel erlaubt sind.

Testen Sie also Ihr Wissen:



F-02-4: Welche Begriffe bestimmt § 1 der BSI-Kritisverordnung?

- a) Versorgungsgrad
- b) Anlagen
- c) Betreiber
- d) kritische Dienstleistung

In Abbildung 2.5 zeige ich Ihnen die §§ 2 bis 8 der Kritisverordnung, in denen die kritischen Sektoren und ihre Dienstleistungen definiert sind.

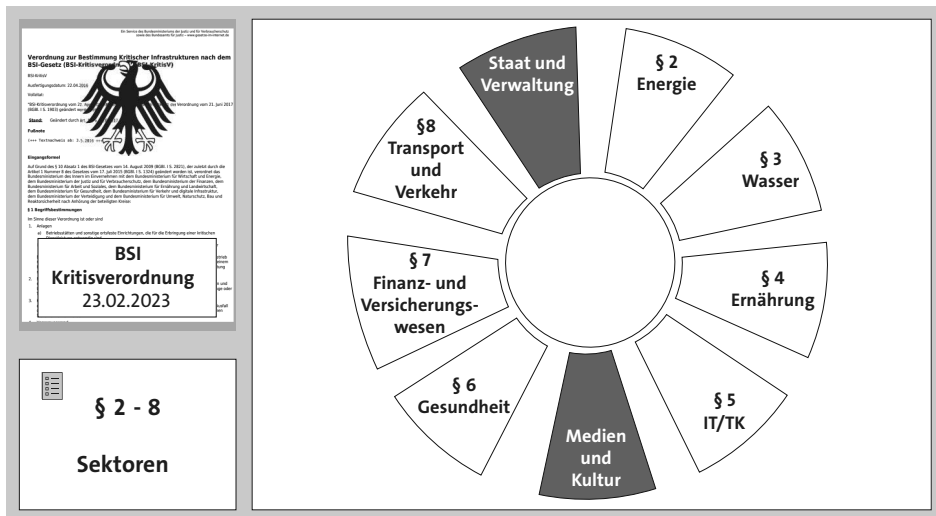


Abbildung 2.5 Sektoren nach der KritisV vom 23.02.2023

Sie sehen: 2023 gab es keine Paragraphen für die Sektoren »öffentliche Verwaltung« und »Medien und Kultur«.

Dieser Sektorkreis stammt aus dem Jahr 2018 und vom BSI und wird in einigen Schulungen noch zur Darstellung eingesetzt. In ihm fehlt auch der Sektor »Siedlungsabfallentsorgung«. Zukünftig wird der Sektorkreis durch die Sektormauer des BSI ersetzt, die ich Ihnen in Abschnitt 2.4 in Abbildung 2.6 zeigen werde.

Wir können an beinahe allen denkbaren Orten auf *kritische Dienstleistungen* stoßen. Welche dazu zählen und in welchen Sektoren diese zu finden sind, zeige ich Ihnen im nächsten Abschnitt.

2.4 Sektoren nach dem BSIg

In diesem Abschnitt kommen wir nun endlich zu den spannenden Sektoren, in die sich Betreiber einsortieren müssen. Wie ich Ihnen im letzten Abschnitt gezeigt habe, finden Sie die Definitionen für die kritischen Dienstleistungen der einzelnen Sektoren in den **§§ 2 bis 8 der Kritisverordnung** (13).

Im UP KRITIS-Flyer auf der BSI-Seite (4) erhalten wir eine Antwort darauf, weshalb nicht alle Sektoren, obwohl sie relevant sind, unter das BSIg fallen:

»Neun der zehn Sektoren Kritischer Infrastrukturen wurden im UP KRITIS behandelt. Der zehnte Sektor ›Staat und Verwaltung‹ wird durch Sicherheitsaktivitäten auf Bundes-, Länder- oder Kommunalebene geregelt.« (4)

Später zeigte sich, dass auch der Sektor »Medien und Kultur« auf Länderebene geregelt wird und nicht durch das BSI-Gesetz.

F-02-5: Der Sektor »Medien & Kultur« wird nicht durch die BSI-Kritisverordnung geregelt, weil ...

- a) ... dieser Sektor im BSI-Gesetz geregelt wird.
- b) ... dieser Sektor bei der Bundesnetzagentur geregelt wird.
- c) ... dieser Sektor bei der Internetagentur geregelt wird.
- d) ... dieser Sektor im Wesentlichen durch Landesgesetzgebung oder andere Rechtsnormen geregelt wird.

Im aktuellen BSI-Gesetz finden wir nun auch den Sektor *Siedlungsabfallentsorgung* und die *Unternehmen im besonderen öffentlichen Interesse* (UBIs). Wie oben schon erwähnt, könnten die UBIs ab Oktober 2024 durch *besonders wichtige und wichtige Einrichtungen* möglicherweise ersetzt werden.

In Abbildung 2.6 zeige ich Ihnen die sogenannte *Sektormauer*. Diese Abbildung stellte mir das BSI im Mai 2023 freundlicherweise zur Verfügung. Wir können den neuen



Sektor *Siedlungsabfallentsorgung* rechts oben erkennen, aber auch die Sektoren *Staat und Verwaltung* (hier »Öffentliche Verwaltung«) sowie *Medien und Kultur* sind gleichwertig dargestellt. Möglicherweise ist diese Darstellung bereits auf die erwartete NIS-2-Umstellung zurückzuführen, denn wie Sie in Abschnitt 1.5, »Die NIS-2-Richtlinie«, sehen konnten, werden bald noch weitere kritische Sektoren betroffen sein.

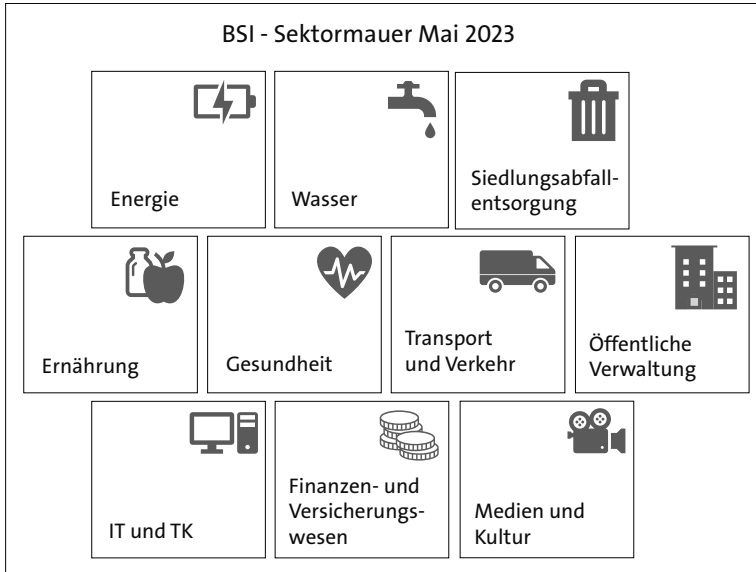


Abbildung 2.6 Die Sektormauer des BSI vom Mai 2023

Für zukünftige Nachweisprüfer oder auch als Berater für einen KRITIS-Betreiber ist es wichtig, die Sektoren der Kritisverordnung zu kennen.



F-02-6: Welche Sektoren der Kritischen Infrastrukturen werden im BSIG definiert?

- a) Gesundheit
- b) Staat und Verwaltung
- c) Genehmigungsinhaber nach Atomgesetz
- d) Energie

In den folgenden Unterabschnitten gehe ich auf die Versorgungsaspekte der einzelnen Sektoren ein. Wir starten mit dem Sektor Energie.

2.4.1 Der Sektor Energie

Für den *Sektor Energie* möchte ich Ihnen an dieser Stelle die relevanten Dienstleistungen aus **§ 2 der Kritisverordnung** (13) in Abbildung 2.7 zeigen.

**Verordnung zur Bestimmung kritischer Infrastrukturen nach dem
BSIG-Gesetz (KritiV-Verordnung) vom 02.02.2023**

**BSI
KritiV-Verordnung
23.02.2023**

§ 2 (1)

**Sektor
Energie**

(1)
Wegen ihrer besonderen Bedeutung für das Funktionieren
des Gemeinwesens sind im Sektor Energie kritische
Dienstleistungen...

- 1) die Versorgung der Allgemeinheit mit Elektrizität
(**Stromversorgung**);
- 2) die Versorgung der Allgemeinheit mit Gas
(**Gasversorgung**);
- 3) die Versorgung der Allgemeinheit mit Kraftstoff und
Heizöl (**Kraftstoff- und Heizölversorgung**);
- 4) die Versorgung der Allgemeinheit mit Fernwärme
(**Fernwärmeversorgung**).

Abbildung 2.7 Kritische Dienstleistungen in § 2 »Sektor Energie« (KritiV, 02.2023)

Zusammengefasst können wir feststellen: Stromversorgung, Gasversorgung, Kraftstoff- und Heizölversorgung sowie Fernwärme sind im Sektor Energie von hoher Bedeutung.

In Abbildung 2.8 zeige ich Ihnen ein Umspannwerk. Von rechts sehen Sie die Hochspannungsleitungen, die mit 110 kV freischwingend ankommen. In dem Generator, der rechts neben dem Trafobaus steht, wird der Strom herunterwandelt.



Abbildung 2.8 Ansicht eines Umspannwerkes vom Hochspannungsnetz zum Mittelspannungsnetz

In Abbildung 2.9 zeige ich Ihnen eine Gasverdichtungsanlage. Hier wird Gas, das einen zu niedrigen Druck besitzt, verdichtet, um mit höherem Druck weitergeleitet werden zu können.



Abbildung 2.9 Ansicht einer Gasverdichtungsstation

In Abbildung 2.10 sehen Sie ein Heizkraftwerk zur Wärmegewinnung. Für mich als Prüferin sind Audits bei Energieversorgern jedes Mal ein spannendes Erlebnis.



Abbildung 2.10 Ansicht eines Heizkraftwerkes

Der nächste Abschnitt gilt dem Sektor Wasser.

2.4.2 Der Sektor Wasser

Für den *Sektor Wasser* sind die relevanten Dienstleistungen in der Kritisverordnung (13) in § 3 aufgelistet, den ich Ihnen in Abbildung 2.11 zeigen möchte.

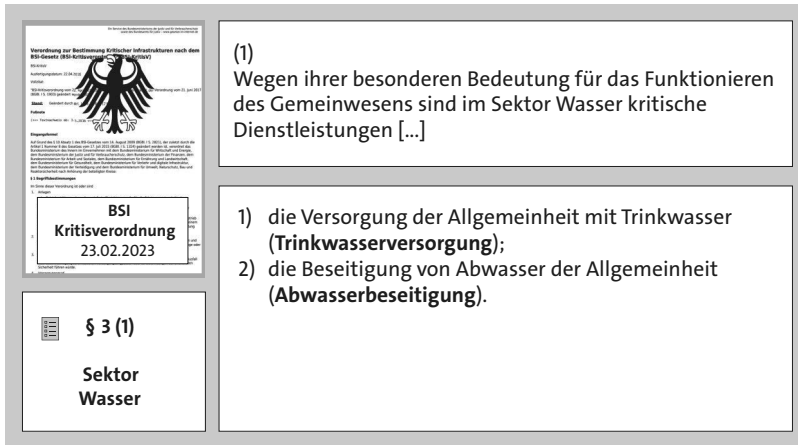


Abbildung 2.11 Kritische Dienstleistungen in § 3 »Sektor Wasser« (KritisV, 02.2023)

In Abbildung 2.12 sehen Sie einen künstlerisch gestalteten Trinkwasserhochbehälter. Er dient uns als Trinkwasserspeicher.



Abbildung 2.12 Ansicht eines Trinkwasserhochbehälters, auch als Wasserspeicherreservoir bezeichnet

In Abbildung 2.13 sehen Sie links eine Wasserpumpe, die in einer Pumpstation steht. Solche Pumpen erzeugen ordentlich Geräusche. Pumpstationen zählen zur Kanalisation.

Rechts in der Abbildung sehen Sie ein Klärwerk von oben. Die Siedlungsentwässerung ist der Abwasserbeseitigung zugeordnet.



Abbildung 2.13 Trinkwasserpumpe in einer Pumpstation; Draufsicht auf eine Kläranlage

In Abbildung 2.14 blicken wir über eine Kläranlage. Es gibt Monate, in denen eine Kläranlage spektakuläre Düfte verströmt, was den Besuch nicht immer angenehm macht. Nebenbei möchte ich erwähnen, dass KRITIS-Betreiber im Sektor Wasser während eines Audits gern selbst erzeugtes Trinkwasser anbieten.



Abbildung 2.14 Ansicht einer Kläranlage zur Reinigung von Abwasser

Fehlendes Trinkwasser oder nicht abgeführtes Schmutzwasser würden definitiv zu sozialen Unruhen führen, weshalb dieser Sektor im Jahr 2018 mit einer der ersten Sektoren war, die zu einer Nachweisprüfung verpflichtet wurden.

Der nächste Abschnitt gilt dem Sektor Ernährung.

2.4.3 Der Sektor Ernährung

Für den *Sektor Ernährung* möchte ich Ihnen in Abbildung 2.15 seine Definition als kritische Dienstleistung in § 4 der Kritisverordnung (13) zeigen.

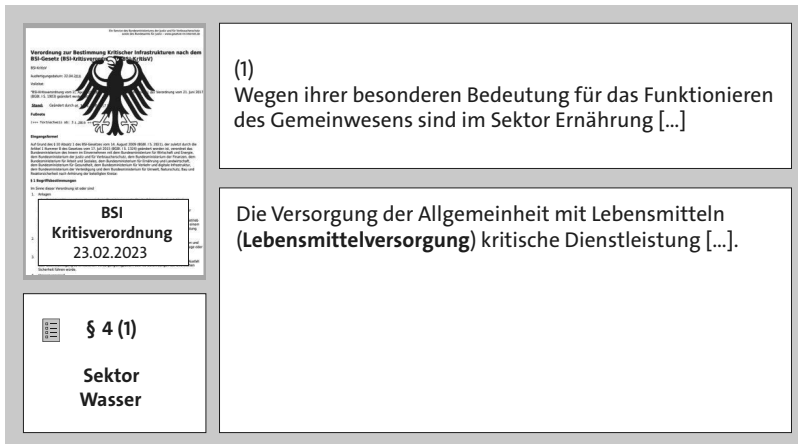


Abbildung 2.15 Kritische Dienstleistung in § 4 »Sektor Ernährung« (KritisV, 02.2023)

Die Lebensmittelversorgung gilt allgemein als wichtig für uns. Die Versorgung umfasst dabei die Lebensmittelherstellung und -behandlung sowie den Lebensmittelhandel.

In Abbildung 2.16 sehen Sie einen Bereich mit Kühltruhen in einem Einkaufsmarkt. Nebenbei angemerkt: Auch dieser ist von Strom abhängig, um die Lebensmittel zu kühlen.



Abbildung 2.16 Ansicht eines Kühlbereichs im Lebensmittelhandel

Der folgende Abschnitt ist dem Sektor IT und TK gewidmet.

2.4.4 Sektor Informationstechnik und Telekommunikation

Für den *Sektor Informationstechnik und Telekommunikation* sind in § 5 der Kritisverordnung (13) die relevanten Dienstleistungen aufgelistet, die ich Ihnen in Abbildung 2.17 zeigen möchte.

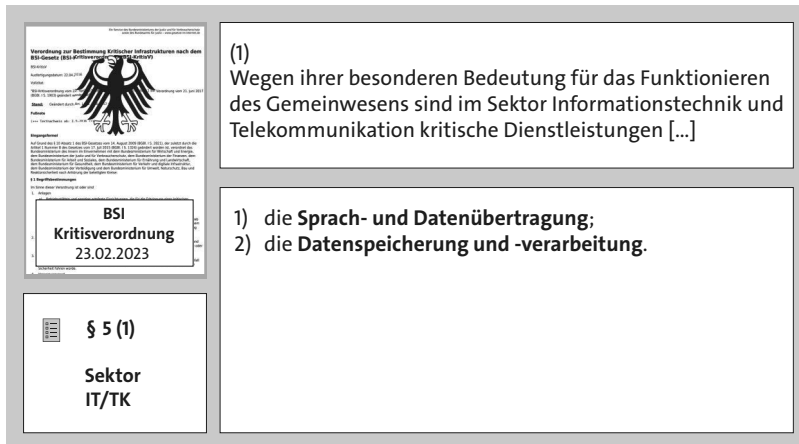


Abbildung 2.17 Kritische Dienstleistungen in § 5 »Sektor Informationstechnik und Telekommunikation« (KritisV, 02.2023)

Wer hätte vor über fünfunddreißig Jahren geahnt, dass die Sprach- und Datenübertragung sowie die Datenspeicherung und Datenverarbeitung aus unserem Leben nicht mehr wegzudenken sein würden? Sie gehören eindeutig zu unseren kritischen Dienstleistungen, deren Ausfall wir als Bürgerinnen und Bürger unter keinen Umständen akzeptieren würden.

Im nächsten Abschnitt befassen wir uns mit dem Sektor Gesundheit.

2.4.5 Sektor Gesundheit

In diesem Abschnitt sehen wir uns die relevanten Dienstleistungen für den *Sektor Gesundheit* an. Die vier Schwerpunktthemen aus § 6 der Kritisverordnung zeige ich Ihnen in Abbildung 2.18.

Im Gesundheitssektor sind die stationäre medizinische Versorgung, lebenserhaltende Medizinprodukte oder auch Arzneimittel und Bluttransfusionen von hoher Bedeutung. Wie wichtig auch die Dienstleistung der Labore ist, wurde uns während der Corona-Pandemie verdeutlicht.

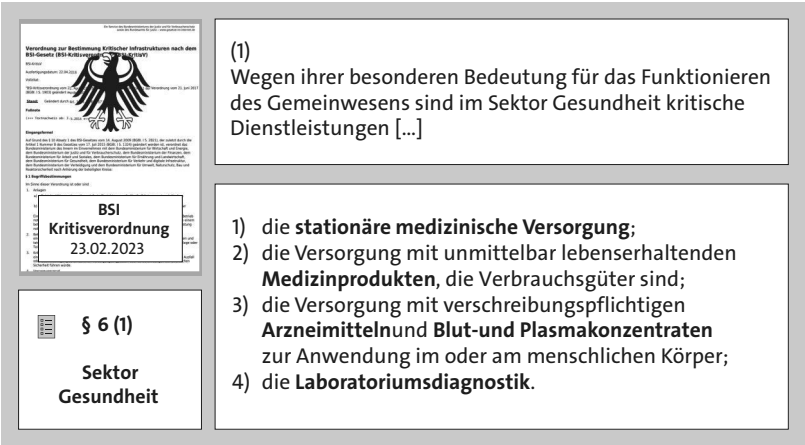


Abbildung 2.18 Kritische Dienstleistungen in § 6 »Sektor Gesundheit« (KritisV, 02.2023)

Wie wir gerade feststellen konnten, gehören Krankenhäuser zu den kritischen Infrastrukturen. In Abbildung 2.19 zeige ich Ihnen ein Frauen-, Kinder- und Geburtsklinikum.



Abbildung 2.19 Ansicht eines Frauen-, Kinder- und Geburtsklinikums

In Abbildung 2.20 sehen Sie eine Apotheke, die sich an der Versorgung mit verschreibungspflichtigen Arzneimitteln beteiligt.

Im nächsten Abschnitt stelle ich den Sektor Finanz- und Versicherungswesen vor.



Abbildung 2.20 Ansicht einer Apotheke zur Versorgung mit verschreibungspflichtigen Arzneimitteln

2.4.6 Sektor Finanz- und Versicherungswesen

Für den *Sektor Finanz- und Versicherungswesen* sind in § 7 der Kritisverordnung die relevanten Dienstleistungen aufgelistet, die ich Ihnen in Abbildung 2.21 zeigen möchte.

Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (Kritisverordnung - KritisV) 23.02.2023	(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Finanz- und Versicherungswesen kritische Dienstleistungen [...]
§ 7 (1) Sektor Finanz- und Versicherungswesen	1) die Bargeldversorgung; 2) der kartengestützte Zahlungsverkehr; 3) der konventionelle Zahlungsverkehr; 4) der Handel mit Wertpapieren und Derivaten sowie die Verrechnung und die Abwicklung von Wertpapier- und Derivatgeschäften; 5) Versicherungsdienstleistungen und Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitssuchende.

Abbildung 2.21 Kritische Dienstleistungen in § 7 »Sektor Finanz- und Versicherungswesen« (KritisV, 02.2023)

Auch fehlende Finanzen oder Versicherungsleistungen können zu sozialen Unruhen führen und müssen uns deshalb permanent bereitgestellt werden.

Stellen Sie sich vor, Versicherungsleistungen würden im Notfall nicht zeitnah ausbezahlt. In Abbildung 2.22 zeige ich Ihnen den Eingang zu einem Standort der Deutschen Rentenversicherung.



Abbildung 2.22 Eingang zu einem Standort der Deutschen Rentenversicherung

In Abbildung 2.23 sehen Sie einen Eingang zur Agentur für Arbeit und zum JobCenter. Auch die Grundsicherung für Arbeitssuchende ist eine kritische Dienstleistung, weil das fehlende Auszahlen dieser Gelder zu Unfrieden führen könnte.



Abbildung 2.23 Eingang zur Agentur für Arbeit als Anlaufstelle für Arbeitssuchende

Bevor ich in den nächsten Unterabschnitt zum Sektor Transport und Verkehr wechsle, biete ich Ihnen eine Prüfungsfrage an, mit der Sie Ihr aktuelles Sektorenwissen testen können.



F-02-7: Welche Sektoren der Kritischen Infrastrukturen werden im BSIG definiert?

- a) Automobilindustrie
- b) Medien und Kultur
- c) Wasser
- d) Finanz- und Versicherungswesen

Die kritischen Dienstleistungen im Sektor Transport und Verkehr sehen wir uns im folgenden Abschnitt an.

2.4.7 Sektor Transport und Verkehr

§ 8 der Kritisverordnung definiert die relevante Dienstleistung für den *Sektor Transport und Verkehr*, die ich Ihnen in Abbildung 2.24 zeigen möchte.

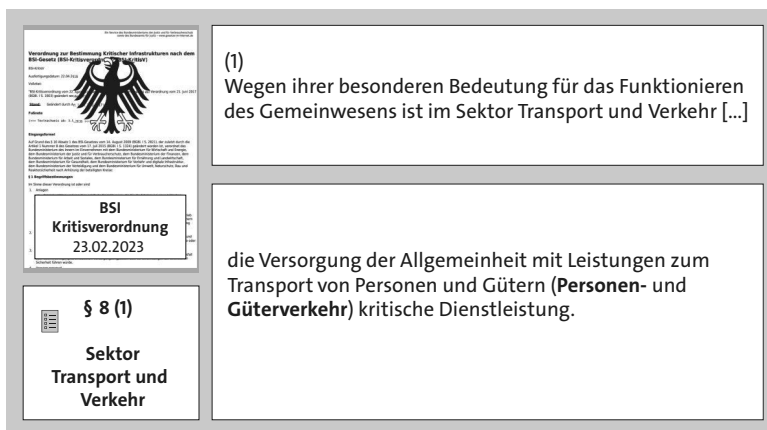


Abbildung 2.24 Kritische Dienstleistungen in § 8 »Sektor Transport und Verkehr« (KritisV, 02.2023)

In Abbildung 2.25 zeige ich Ihnen Anlagen für den Infrastrukturbetrieb eines Flughafens. Hier zählen die Passagiere pro Jahr: Sobald an einem Flughafen zwanzig Millionen Passagiere abgefertigt werden, gehört ein Flughafen zur Kritischen Infrastruktur.

In Abbildung 2.26 sehen Sie das Schienennetz vor einem Bahnhof. Auch Schienen gelten als kritische Anlage, weil über sie die kritische Dienstleistung des Personen- und Gütertransports erbracht wird.

Resümierend können wir feststellen, dass sogar der Transport von Personen und Gütern im Notfall zu Komplikationen führen könnte, wenn dieser Transport nicht reibungslos abläuft.



Abbildung 2.25 Infrastrukturbetrieb eines Flughafens zur Beförderung von Passagieren



Abbildung 2.26 Eisenbahnschiennetz zum Personen- und Gütertransport

Im letzten Unterabschnitt zu den Sektoren gehe ich auf den neuen Sektor der Siedlungsabfallentsorgung ein.

2.4.8 Sektor Siedlungsabfallentsorgung

Für den *Sektor Siedlungsabfallentsorgung* gab es in der Kritisverordnung vom Februar 2023 noch keine eigene Definition, keine Anlagenkategorien und keine Schwellenwerte. Ich gehe aber davon aus, dass es in der zukünftigen Kritisverordnung einen eigenen Abschnitt zu ihm geben wird.

Was können wir erwarten?

Es geht um die Beseitigung von Abfällen durch die Müllentsorgungsunternehmen und im Speziellen um Fahrzeuge, Müllsortierungs- und Müllverbrennungsanlagen.

Mein Kollege Daniel Jedecke von HiSolutions hat mir freundlicherweise die Tabelle 2.1 von OpenKritis zur Verfügung gestellt. In dieser Tabelle sehen Sie wahrscheinliche Versorgungsbereiche, Dienstleistungen und Anlagen für die Siedlungsabfallentsorgung, die in der nächsten Kritisverordnung erwähnt werden. Bis Dezember 2023 kamen diese bereits bei zwei Versorgern bei Nachweisprüfungen zum Einsatz.

Bereich	Definition kritische Dienstleistung	Mögliche Anlagen
Sammlung	Einsammeln von Abfällen, einschließlich deren vorläufiger Sortierung und vorläufiger Lagerung zum Zweck der Beförderung zu einer Abfallbehandlungsanlage.	Steuerung und Tourenplanung der Müllabfuhr; Sortieranlage, Abfallbehandlungsanlage
Verwertung	Verfahren, als dessen Hauptergebnis die Abfälle innerhalb der Anlage oder in der weiteren Wirtschaft einem sinnvollen Zweck zugeführt werden, indem sie entweder andere Materialien ersetzen, die sonst zur Erfüllung einer bestimmten Funktion verwendet worden wären, oder indem die Abfälle so vorbereitet werden, dass sie diese Funktion erfüllen.	Verbrennungsanlage, Müllverbrennungsanlage
	Möglicherweise auch die stoffliche Verwertung mit der Vorbereitung zur Wiederverwendung, das Recycling und die Verfüllung.	Recyclinghof, Wertstoffhof
Beseitigung	Verfahren, das keine Verwertung ist, auch wenn das Verfahren zur Nebenfolge hat, dass Stoffe oder Energie zurückgewonnen werden.	Deponien; Anlagen zur Behandlung, Verpressung und Verbrennung

Tabelle 2.1 Der »Sektor Siedlungsabfallentsorgung«, mögliche Anlagen und Dienstleistungen (Stand: November 2023, Quelle: OpenKritis)

Ein mögliches Schadensszenario wurde mir vor einigen Jahren von einem Stadtreinigungsunternehmen erläutert. Das Szenario hat überhaupt nichts mit der Entsorgung zu tun, wohl aber mit den Müllfahrzeugen.

Das besagte Unternehmen hatte eine Risikobewertung durchgeführt und festgestellt, dass das Risiko eines Müllautodiebstahls bisher nicht in Betracht gezogen worden

war. Bei der Risikoidentifikation stellten die Kollegen allerdings fest, dass ein Diebstahl gar nicht so abwegig sei: Bis zur Betrachtung möglicher Schwachstellen wurden die Fahrzeugschlüssel nämlich am Schicht- beziehungsweise am Tagesende auf dem Fahrersitz abgelegt, sodass am Folgetag ein anderer Kollege reibungslos mit dem Müllfahrzeug zu seiner Schicht abfahren konnte.

Nach dem Terroranschlag auf dem Berliner Weihnachtsmarkt, der im Jahr 2016 mit einem gestohlenen LKW durchgeführt wurde, änderte das Stadtreinigungsunternehmen sein Vorgehen mit den Fahrzeugschlüsseln. Seither ist es dort verboten, die Müllfahrzeuge am Schichtende unverschlossen abzustellen.

Nach diesen Erläuterungen zu den Sektoren der Kritisverordnung möchte ich im nächsten Abschnitt mit Ihnen auf Anlagenkategorien eingehen.

2.5 Anlagenkategorien für kritische Dienstleistungen

Die Zuordnung zu einem kritischen Sektor fällt Betreibern in der Regel leicht. Schwierigkeiten können dann entstehen, wenn zwei Sektoren scheinbar passen. Das kann zum Beispiel bei Krankenversicherungen vorkommen, die sich dem Sektor *Gesundheit* und gleichzeitig dem Sektor *Finanz- und Versicherungswesen* zugehörig fühlen. Oder bei Betreibern von Tankstellen, die sich den Sektoren *Transport und Verkehr* und *Energie* zuordnen möchten.

Um hier eine Hilfestellung zu erhalten, können wir in der Kritisverordnung (13) den Begriff *Anlagen* betrachten. Die Begriffsdefinition für Anlagen habe ich Ihnen in Abbildung 2.2 (in Abschnitt 2.3, »Begriffe und Definitionen«) gezeigt.

Außerdem finden wir in **§ 1 Abs. 2** der Kritisverordnung für eine Anlage und ihre Betreiber zusätzliche Bestimmungen, die ich Ihnen stark gekürzt in Abbildung 2.27 zeigen möchte.



BSI
Kritisverordnung
23.02.2023

§ 1 (2)
Begriffs-
bestimmungen

Zur Erbringung derselben kritischen Dienstleistung:

- umfasst eine Anlage alle **Anlagenteile** und **Verfahrensschritte** sowie **Nebeneinrichtungen**, die in einem **betrieblichen Zusammenhang** stehen;
- Mehrere Anlagen **derselben Kategorie**, die durch einen **betriebstechnischen Zusammenhang verbunden** sind, gelten als **gemeinsame Anlage**;
- **Jeder** für sich ist für die Erfüllung der Pflichten als Betreiber **verantwortlich**, auch wenn **zwei oder mehr Personen** gemeinsam die Anlage betreiben.

Abbildung 2.27 Begriffsbestimmung zu »Anlagen« und »Betreibern« (KritisV, 02.2023)

Sie können in dieser Zusammenfassung sehen, unter welchen Bedingungen eine Anlage als *gemeinsame Anlage* zählt und wer für eine Anlage verantwortlich ist, wenn mehrere Personen eine Anlage betreiben. Dies finde ich wichtig für die spätere Definition des Geltungsbereiches einer Kritischen Infrastruktur.

Die kritischen Anlagen werden in *Anlagenkategorien* geclustert.

Jeder Sektor besitzt seine eigenen Anlagenkategorien, die wir in den derzeit sieben Anhängen der Kritisverordnung finden.

Falls Sie als Betreiber nicht sofort feststellen können, zu welchem Sektor Sie gehören, müssen Sie in die Anhänge der Kritisverordnung schauen, um zu prüfen, welchem Sektor Ihre Anlagen zugeordnet sind. Wir wechseln deshalb im nächsten Abschnitt zu den Anhängen der Kritisverordnung.

2.6 Anhänge zu den Sektoren

In der Kritisverordnung vom Februar 2023 (13) finden wir nach den Paragraphen sieben Anhänge, die jeweils für einen Sektor gelten und stets drei Teile besitzen.

Die Inhalte dieser Anhänge gliedern sich jeweils in:

- *Teil 1 – Grundsätze und Fristen*
- *Teil 2 – Berechnungsformeln zur Ermittlung der Schwellenwerte*
- *Teil 3 – Anlagenkategorien und Schwellenwerte*

In Abbildung 2.28 zeige ich Ihnen die Anhänge 1 bis 7 für die Sektoren sowie die drei Teile, die jeder Anhang besitzt.

Anhang 1	Sektor Energie	Teil 1 Grundsätze und Fristen
Anhang 2	Sektor Wasser	
Anhang 3	Sektor Ernährung	
Anhang 4	Sektor Informationstechnik und Telekommunikation	Teil 2 Berechnungsformeln zur Ermittlung der Schwellenwerte
Anhang 5	Sektor Gesundheit	
Anhang 6	Sektor Finanz- und Versicherungswesen	Teil 3 Anlagenkategorien und Schwellenwerte
Anhang 7	Sektor Transport und Verkehr	

Abbildung 2.28 Übersicht über die Anhänge der Kritisverordnung und die drei Teile, in die sie jeweils gegliedert sind

Die Anhänge sind in der gleichen Reihenfolge wie die Paragraphen angeordnet.

Für den Sektor *Energie* finden Sie die Konkretisierung im Kapitel 1 der Kritisverordnung.

Die Inhalte der Anhänge möchte ich gern mit Ihnen in den drei folgenden Unterabschnitten beleuchten.

2.6.1 Teil 1 – Grundsätze und Fristen (Kritische Anlagen)

Wir betrachten jetzt den ersten Teil eines beliebigen Anhangs der Kritisverordnung. Wir erinnern uns: Jeder Anhang ist einem Sektor gewidmet.

Der erste Teil dient uns dazu, zu erkennen, ob unsere Anlagen, die eine kritische Dienstleistung erbringen, zu diesem Sektor gehören.

Anlagen sind zur Gewinnung, zur Erzeugung, zur Aufbereitung, zum Transport, zur Verteilung, zur Steuerung oder zur Überwachung von kritischen Dienstleistungen notwendig.

Um zu identifizieren, ob eine unserer Anlagen relevant ist, wurden diese Anlagen in Kategorien eingeteilt, und diese finden wir im ersten Teil der Anhänge.

Nicht jede einzelne Anlage ist kritisch. Sie ist es nur dann, wenn sie für eine kritische Dienstleistung einen festgelegten Schwellenwert überschreitet.

In Abbildung 2.29 zeige ich Ihnen einen kleinen Einblick in Anlagenkategorien. Für jeden Sektor nenne ich bewusst nur zwei Kategorien, um die Lesbarkeit nicht zu gefährden.

Beispiele für Anlagenkategorien		
Sektoren	Beispiel 1	Beispiel 2
Energie	Stromverteilnetz	Tankstellennetz
Wasser	Leitzentrale	Kläranlage
Ernährung	Anlage oder System zur Herstellung von Lebensmitteln	Anlage oder System zum Inverkehrbringen von Lebensmitteln
IT/TK	Rechenzentrum (Housing)	Serverfarm (Hosting)
Gesundheit	Krankenhaus	Labor
Finanz-/Versicherungswesen	Autorisierungssystem	Kontoführungssystem
Transport und Verkehr	Infrastrukturbetrieb eines Flugplatzes	Verkehrssteuerungs- und Leitsystem

Abbildung 2.29 Anlagenkategorien-Beispiele (KritisV, 2023)

Wenn Sie als Betreiber kritische Dienstleistungen erbringen und sich unsicher sind, ob Sie eine gesetzliche Nachweisprüfung durchführen müssen, prüfen Sie bitte die Anlagenkategorien für Ihren Sektor in der aktuellen Kritisverordnung. Möglicherweise ist Ihre Anlage nicht aufgelistet; dann müssen Sie derzeit keinen Nachweis gegenüber dem BSI erbringen.

Falls Sie jedoch eine Ihrer Anlagen in Teil 1 entdeckt haben, sollten Sie prüfen, ob die von Ihnen erbrachte Versorgungsmenge bereits systemrelevant ist und den festgelegten Schwellenwert in Teil 3 erreicht oder übersteigt.

Jeder Sektor besitzt andere Fristen zur Ermittlung seines Versorgungsgrades. Diese Fristen finden Sie in Teil 1 eines jeden Sektor-Anhangs.

Zur Verdeutlichung zeige ich beispielhaft die Fristen für den Sektor Energie in Abbildung 2.30.

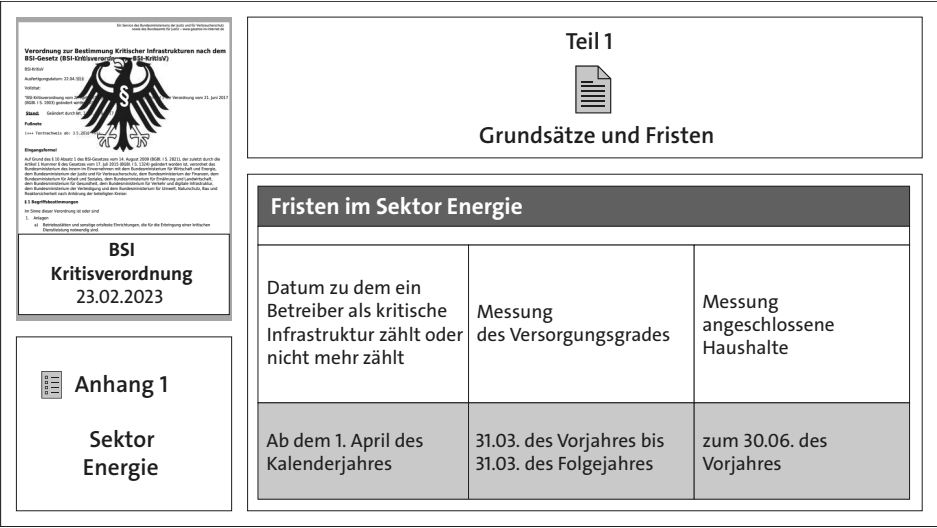


Abbildung 2.30 Fristen zur Messung des Versorgungsgrades im Sektor Energie für KRITIS-Betreiber

Für jeden Sektor gelten eigene Fristen, weshalb ich darauf verzichten möchte, alle Fristen zum Ermitteln der Versorgungsgrade hier aufzulisten.

In Teil 2 der Anhänge finden wir die Berechnungsformeln, die ich Ihnen im folgenden Abschnitt erläutern möchte.

2.6.2 Teil 2 – Berechnungsformeln für die kritische Dienstleistung

In diesem Abschnitt sehen wir uns die Berechnungsformeln an, die zur Definition der Schwellenwerte eingesetzt wurden.

Diese Formeln sind für Betreiber, aber auch für Nachweisprüfer relevant. Wir finden sie jeweils im zweiten Teil der Sektor-Anhänge in der Kritisverordnung.

Mit Stand Dezember 2023 lässt sich sagen: Wenn Sie 500.000 Bürger mit Ihrer Dienstleistung versorgen, dann gehören Ihre Anlagen mit hoher Wahrscheinlichkeit zu den kritischen Infrastrukturen und Sie sind ein KRITIS-Betreiber.

Diese Anzahl an versorgten Personen hat sich seit 2016 noch nicht geändert. Im gesamten Jahr 2023 wurde allerdings oft über die Änderung dieser Bezugsgröße durch die NIS-2-Richtlinie gesprochen.

Für Sie bedeutet das: Falls Sie bisher kein KRITIS-Betreiber waren, müssen Sie bei der Veröffentlichung jeder neuen Kritisverordnung im zweiten Teil Ihres Sektor-Anhangs prüfen, ob die Regelung mit den 500.000 Bürgern erhalten geblieben ist oder ob Sie eventuell trotz weniger versorgter Bürger plötzlich auch zu den kritischen Infrastrukturen gezählt werden.

Aber sehen wir uns zuallererst an, was diese Anzahl an Personen bedeutet. Um sich die Zahl besser vorstellen zu können, sollten Sie sich die Städte in Tabelle 2.2 ansehen und mit der Einwohnerzahl Ihres Kreises vergleichen. Die Versorgungsdienstleister dieser Städte sind meistens auch KRITIS-Betreiber.

Platz	Stadt	Einwohnerzahl
1	Berlin	3.664.088
2	Hamburg	1.852.478
3	München	1.488.202
4	Köln	1.083.498
5	Frankfurt am Main	764.104
6	Stuttgart	630.305
7	Düsseldorf	620.523
8	Leipzig	597.493
9	Dortmund	587.696
10	Essen	582.415
11	Bremen	566.573
12	Dresden	556.227

Tabelle 2.2 Einwohnerzahlen großer Städte
(Quelle: Statistisches Bundesamt, 08.05.2023)

Platz	Stadt	Einwohnerzahl
13	Hannover	534.49
14	Nürnberg	515.543
15	Duisburg	495.885

Tabelle 2.2 Einwohnerzahlen großer Städte
(Quelle: Statistisches Bundesamt, 08.05.2023) (Forts.)

Ein Betreiber, der eine Stadt von der Größe Dresdens, Nürnbergs oder Hannovers von ihrem Abwasser befreit, wäre somit bereits ein KRITIS-Betreiber im Sektor Wasser.

Damit Sie verstehen, wie die *Schwellenwerte* ermittelt wurden, habe ich Ihnen in Abbildung 2.31 die Grundlagen dargestellt.

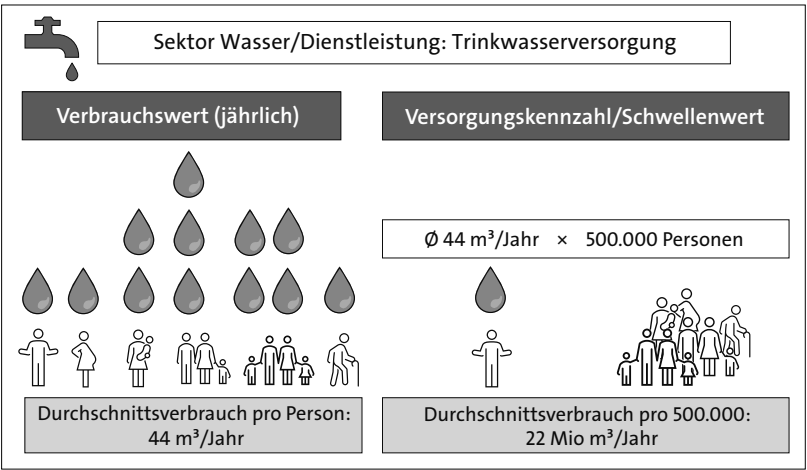


Abbildung 2.31 Darstellung der Berechnungsformel für 500.000 Personen für die kritische Dienstleistung Trinkwasser

Wir starten mit der Auswahl im Sektor Wasser und wählen als Dienstleistung die Trinkwasserversorgung aus. Anschließend wird statistisch ermittelt, wie hoch der Trinkwasserverbrauch für einen Bürger in zwölf Monaten ist. In unserem Beispiel haben wir den Verbrauch von vierundvierzig Kubikmetern Trinkwasser. Das sind 44.000 Ein-Liter-Flaschen Wasser für nur eine Person pro Jahr.

Diese Menge wurde anschließend mit 500.000 Personen multipliziert. Der Gesamtverbrauchswert für 500.000 Menschen ergab 22 Millionen Kubikmeter Trinkwasser, und so entstanden die Schwellenwerte. Es müssen also keine einzelnen Bürger gezählt werden, sondern der Verbrauchswert an Dienstleistungen und Produkten eines Betreibers. Diesen Schwellenwert sehen wir uns gleich im folgenden Abschnitt an.

Die folgende Prüfungsfrage entspricht in etwa einer Frage, die seit 2018 in Prüfungen gestellt wurde.

F-02-8: Was ist die grundlegende Zielgröße für die Berechnung von Schwellenwerten?



- a) das Volumen, mit dem die Bewohner im Einzugsgebiet einer Industrieanlage versorgt werden müssen
- b) der Verbrauchswert einer Gruppe von 500.000 Personen
- c) der Energiebedarf einer Anlage multipliziert mit 500.000
- d) der Anzahl aller Haushalte einer Stadt oder Gemeinde, geteilt durch die Anzahl der zu versorgenden Haushalte

Sie wissen jetzt, wie Sie selbst die Schwellenwerte berechnen und wo Sie nach Neuerungen suchen können. Dazu noch eine Frage:

F-02-9: Wo befindet sich die Berechnungsformel für kritische Anlagen?



- a) In Teil 2 der Anhänge der Kritisverordnung
- b) im IT-Sicherheitsgesetz
- c) im BSI-Gesetz
- d) Es gibt keine Berechnungsformel. Kritische Anlagen wurden per Gesetz zu kritischen Anlagen.

Wenn Sie ein *Energieversorgungsnetz* betreiben, spielen die Schwellenwerte bei der Nachweispflicht jedoch keine Rolle: Alle Energieversorger erhielten im November 2022 ein Schreiben mit der Aufforderung, bis zum 1. Mai 2023 »Systeme zur Angriffserkennung« nachzuweisen. Das Schreiben können Sie sich in Abschnitt 12.2.3, »Fristen für Betreiber«, in Abbildung 12.15 ansehen.

Dies führte zu einiger Verwirrung bei Netzbetreibern, da viele der Meinung waren, einen geringeren Versorgungsgrad zu besitzen, als die Kritisverordnung vorgibt. Das Anschreiben weist jedoch auf die Unerheblichkeit der Schwellenwerte für Netzbetreiber hin. Auf Anfrage bei der BNetzA erhielt ich im November 2023 auch eine schriftliche Bestätigung, dass alle Netzbetreiber betroffen seien.

Im Zuge der Überführung von NIS-2 in deutsche Gesetze hörte ich im Laufe des Jahres 2023 oft die Vermutung, die Schwellenwerte seien nach dessen Umsetzung für alle Sektoren irrelevant. Sollte das tatsächlich zutreffen, verschwinden vielleicht die Berechnungsformeln aus zukünftigen Kritisverordnungen, wodurch plötzlich viele kleine Versorger nachweispflichtig würden.

Falls Sie das Buch zu einer Zeit lesen, in der es keine Berechnungsformeln mehr gibt, bitte ich Sie, diesen Abschnitt als historischen Rückblick zu betrachten. Bis Oktober

2024 gelten die Formeln aber definitiv mindestens noch, und Betreiber, die im Jahr 2023 zu den Kritischen Infrastrukturen gehörten, werden auch zukünftig dazu zählen und Nachweise erbringen müssen.

Die Ergebnisse dieser Berechnungen finden Sie in den Anhängen der Kritisverordnung jeweils in Teil 3. Diesen stelle ich Ihnen im folgenden Abschnitt vor.

2.6.3 Teil 3 – Anlagenkategorien und Schwellenwerte

Nachdem wir in **Teil 2** der Sektoren-Anhänge in der Kritisverordnung die Berechnungsformeln kennengelernt haben, wechseln wir in den **Teil 3**, um die Anlagen zu finden, die für unsere Produkt- oder Dienstleistungserbringung benötigt werden.

Für das Beispiel zum Sektor *Wasser* sehen Sie in Abbildung 2.32 die Anlagen zur *Trinkwasserversorgung*. Diese sind die *Gewinnungsanlage*, das *Wasserwerk*, das *Wasserverteilungssystem* und die *Leitzentrale*.

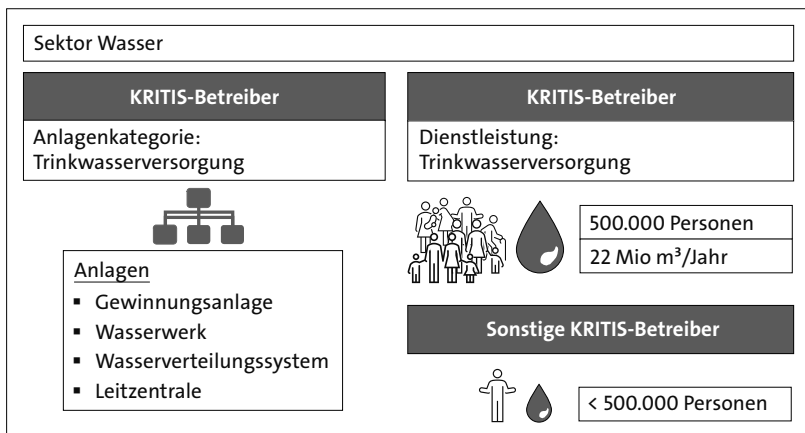


Abbildung 2.32 Anlagen und Schwellenwerte für die kritische Dienstleistung Trinkwasserversorgung

Leben im Einzugsgebiet eines Betreibers mindestens 500.000 Personen egal welchen Alters oder verarbeitet der Betreiber 22 Millionen Kubikmeter Trinkwasser, dann zählt er zu den KRITIS-Betreibern und ist nachweispflichtig gemäß BSIG.

Alle anderen Betreiber, die eine Trinkwasserversorgung bereitstellen, jedoch weniger als 500.000 Personen versorgen, gehören zu den *sonstigen* KRITIS-Betreibern und sind bisher nicht nachweispflichtig.

Zwei weitere Beispiele, die ich Ihnen zeigen möchte, stammen aus dem Kapitel 7 für den Sektor *Transport und Verkehr*.

Das erste Beispiel betrifft den *Personentransport* im öffentlichen Personennahverkehr (ÖPNV). Hier werden die Fahrgäste für ein Jahr gezählt. Betreiber, die mehr als

125 Millionen Fahrgäste im Jahr transportieren, gehören zu den KRITIS-Betreibern. Die Anlagen und Schwellenwerte für den Personentransport können Sie in Abbildung 2.33 sehen. Die Abkürzung ÖSPV steht für »Öffentlicher Straßenpersonenverkehr«.

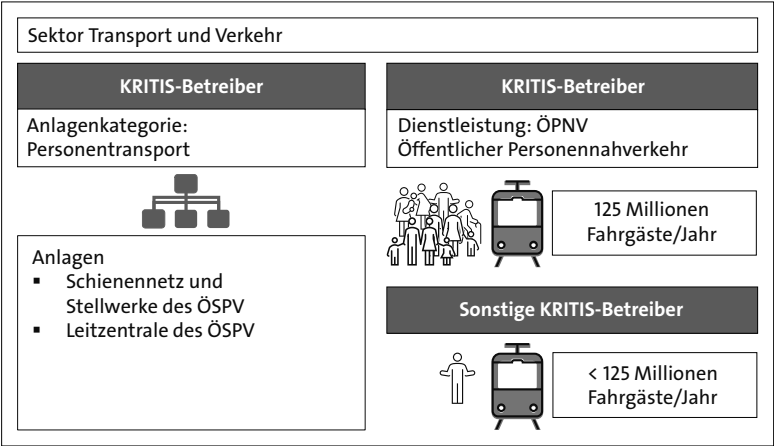


Abbildung 2.33 Anlagen und Schwellenwerte für den Personentransport

Beim zweiten Beispiel handelt es sich um Dienstleistungen im *Straßenverkehr*.

Wenn ein KRITIS-Betreiber die *Verkehrssteuerungs- und Leitsysteme* oder ein *intelligentes Verkehrssystem* verantwortet und dabei 500.000 Einwohner beziehungsweise angeschlossene Nutzer im Versorgungsgebiet versorgt, dann gehört er zu den KRITIS-Betreibern. Die Anlagen und Schwellenwerte für den Straßenverkehr können Sie in Abbildung 2.34 sehen.

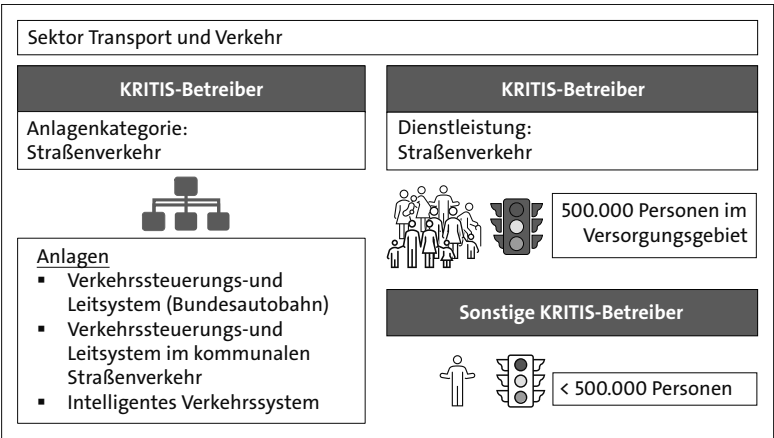


Abbildung 2.34 Anlagen und Schwellenwerte für den Straßenverkehr

Die Bundesautobahnen werden auf Bundesebene verantwortet.

Teil 3 der Anhänge in der Kritisverordnung ist meiner Meinung nach der spannendste Teil der in den Anhängen. Hier können Sie als Betreiber überprüfen, ob Ihre Anlage überhaupt als KRITIS-relevant aufgelistet ist, welche Einheit das Bemessungskriterium für diese Anlage ist und wie hoch der Schwellenwert liegt, ab dem Ihre Anlage zur Nachweisprüfung verpflichtet ist.

Die Darstellung in Teil 3 ist tabellarisch und gliedert sich in vier Spalten.



Die vier Spalten in Teil 3 der Kritisverordnung

- ▶ In Spalte A finden wir eine laufende Nummer, die der kritischen Dienstleistung zugeordnet ist.
- ▶ In Spalte B sehen wir die Anlagenkategorien, die in Teil 1 erläutert wurden.
- ▶ In Spalte C ist das Bemessungskriterium formuliert, und
- ▶ in Spalte D können wir den Schwellenwert ablesen.

Ich möchte Ihnen anschließend den Tabellenaufbau von *Teil 3* an zwei Beispielen zeigen: Tabelle 2.3 stellt die Gliederung für die Trinkwasserversorgung und die Abwasserbeseitigung dar.

In Abbildung 2.32 hatte ich Ihnen die vier möglichen Anlagen für die Trinkwasserversorgung aufgelistet. Die erste *Anlagenkategorie* war die *Gewinnungsanlage*, die wir in der Tabelle der Nummer 1.1.1 zugeordnet in Spalte B wiederfinden.

Als *Bemessungskriterium* (das erkennen wir in Spalte C) ist die *gewonnene Wassermenge* in Millionen Kubikmeter berücksichtigt.

Der *Schwellenwert* in Spalte D zeigt 22 Millionen an. Diese Wassermenge ist der Grenzwert, ab dem eine Anlage als KRITIS-relevant gilt und ihr Betreiber nachweispflichtig ist.

Würde Ihre Gewinnungsanlage weniger als 22 Millionen Kubikmeter Wasser gewinnen, wäre sie nicht nachweispflichtig und Sie als Betreiber müssten keinen Nachweis nach dem BSIG erbringen.

In der folgenden Prüfungsfrage können Sie Ihr Wissen zu Kritischen Infrastrukturen testen.



F-02-10: Warum war die Art und Weise der Definition Kritischer Infrastrukturen vor dem Erlass der BSI-Kritisverordnung problematisch?

- a) Die vorherige Verordnung verstieß gegen EU-Recht.
- b) Es war nicht sichergestellt, dass ein gleichwertiges und hinreichendes Schutzniveau erreicht wird.

- c) Die IT-Systeme der Betreiber Kritischer Infrastrukturen waren nicht gegen IT-Angriffe geschützt.
- d) Die bisherige Art und Weise war regulativ und musste geändert werden.

Als zweites Beispiel in Tabelle 2.3 dient jetzt die *Anlagenkategorie* Kanalisation mit der zugeordneten Nummer 2.1.2.

Das *Bemessungskriterium* sind die *angeschlossenen Einwohner*. Es wird dabei gezählt, wie viele Einwohner an die Kanalisation angeschlossen sind. Der *Schwellenwert* liegt bei 500.000 Einwohnern. Besitzt eine Kanalisation so viele angeschlossene Einwohner, gilt sie als KRITIS-relevant, und Sie als Betreiber müssen eine Nachweisprüfung für Ihre Anlage durchführen lassen.

Sind weniger Einwohner angeschlossen, ist die Kanalisation nicht nachweispflichtig.

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	Trinkwasserversorgung		
1.1	Gewinnung		
1.1.1	Gewinnungs-anlage	Gewonnene Wassermenge in Millionen m ³ /Jahr	22
2	Abwasserbeseitigung		
2.1	Siedlungsentwässerung		
2.1.2	Kanalisation	Angeschlossene Einwohner	500 000

Tabelle 2.3 Auszug aus Teil 3 »Anlagenkategorien und Schwellenwerte«

Jeder Teil 3 in den Anhängen der Kritisverordnung hat diese tabellarische Struktur, in der Sie sich schnell zurechtfinden werden. Dazu noch eine Prüfungsfrage:

F-02-11: Bei der fachlichen Erstellung der BSI-Kritisverordnung hat sich das Kernteam den folgenden Themenfeldern gewidmet:

- a) Exportkontrollen
- b) Produktionsgrenzen
- c) Schwellenwerten
- d) Anlagenkategorien



Ab wann ein KRITIS-Betreiber seine Anlagen an- und wieder abmelden kann, habe ich in Abschnitt 12.2.3, »Fristen für Betreiber«, für Sie zusammengefasst.

Wenn wir die Schwellenwerte aus der Kritisverordnung von 2017 mit denen aus den Jahren 2021 und 2023 vergleichen, erkennen wir, dass im Sektor Energie die Durchschnittsverbrauchswerte von Bürgern um fast das Vierfache gesunken sind. Somit sind seit 2021 mehr KRITIS-Betreiber im Energiesektor zu finden als in der ersten Nachweisrunde.

Schauen wir uns die Schwellenwerte in der alten Kritisverordnung aus dem Jahr 2017 und in der Verordnung aus dem Jahr 2023 genauer an, stellen wir fest, dass die Stromerzeugungsanlagen im Jahr 2023 mit einem geringeren Schwellenwert bereits als KRITIS-Betreiber definiert sind. Aber wie oben bereits erwähnt wurde, sind *alle* Betreiber eines Energieversorgungsnetzes nachweispflichtig.



F-02-12: Wo kann ein Betreiber überprüfen, ob seine Anlage als kritische Anlage gilt?

- a) in Teil 3 des Anhangs seines Sektors in der Kritisverordnung
- b) im BSI-Gesetz
- c) in der Orientierungshilfe B35
- d) Er wird durch das BSI dazu bestimmt.

Nicht alle Betreiber fallen unter das BSIG. Es gibt Betreiber, die unter andere Gesetze fallen. Diese Aspekte möchte ich mit Ihnen im folgenden Abschnitt betrachten.

2.7 Welche Betreiber fallen unter das BSIG?

Ob Sie als Betreiber unter die Nachweispflicht nach dem BSIG fallen, können Sie relativ einfach kontrollieren: Sie schlagen Ihren Sektor in der Kritisverordnung nach und prüfen, ob Ihre Dienstleistung aufgelistet wurde.

Sobald Sie Ihre Anlage in der Kritisverordnung in einem Teil 3 wiederfinden und Ihre Anlage außerdem den Schwellenwert erreicht, sind Sie ein KRITIS-Betreiber.



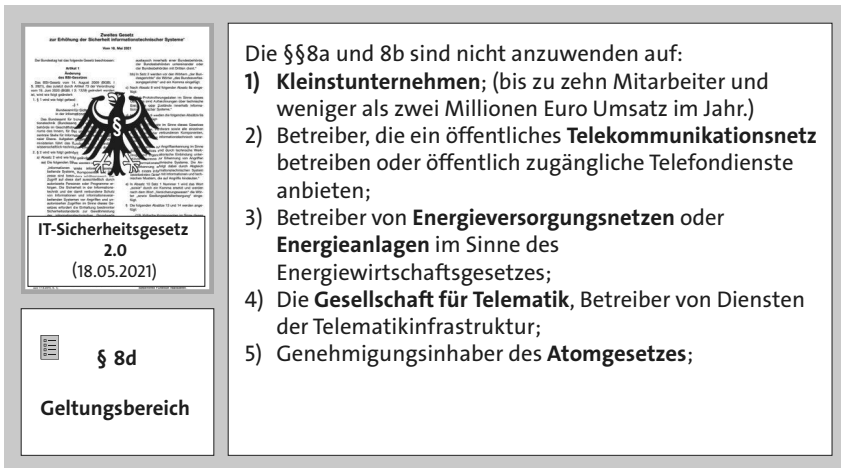
F-02-13: Welche Leitfragen lagen der methodischen Bewertung, wer Betreiber Kritischer Infrastrukturen ist, zugrunde?

- a) Welche Anlagen werden für die Erbringung kritischer Dienstleistungen benötigt?
- b) Ab welchem Schwellenwert ist die Anlage für die kritische Dienstleistung kritisch?
- c) Welche Betreiber gehören zu den oberen zehn Prozent bei der Größe der Belegschaft?
- d) Welche Betreiber können zusätzliche Überprüfungen finanziell bewältigen?

Aber es gilt noch weitere Eigenschaften zu erfüllen, um als KRITIS-Betreiber tatsächlich nachweispflichtig nach dem BSIG zu sein.

Im BSI-Gesetz finden wir die Betreiber, die anderen Gesetzen unterliegen oder zu klein, also Kleinstunternehmen sind. In Abbildung 2.35 zeige ich Ihnen gekürzt diese Betreiber. Wir sehen zum Beispiel Kleinstunternehmen, Betreiber im Sektor Energie oder Genehmigungsinhaber des Atomgesetzes.

Unter *Kleinstunternehmen* verstehen wir Unternehmen, die nur bis zu zehn Mitarbeiter haben und weniger als 2.000.000 € Umsatz im Jahr erwirtschaften. Für die hier gezeigten Betreiber galt im Dezember 2023 keine Verpflichtung, eine vollumfängliche Nachweisprüfung gegenüber dem BSI nachzuweisen. Für den Sektor *Energie* wurde meiner Meinung nach mit der Nachweispflicht über SzA dieser Anwendungsbereich etwas aufgeweicht.



Die §§8a und 8b sind nicht anzuwenden auf:

- 1) **Kleinstunternehmen**; (bis zu zehn Mitarbeiter und weniger als zwei Millionen Euro Umsatz im Jahr.)
- 2) Betreiber, die ein öffentliches **Telekommunikationsnetz** betreiben oder öffentlich zugängliche Telefondienste anbieten;
- 3) Betreiber von **Energieversorgungsnetzen** oder **Energieanlagen** im Sinne des Energiewirtschaftsgesetzes;
- 4) Die **Gesellschaft für Telematik**, Betreiber von Diensten der Telematikinfrastruktur;
- 5) Genehmigungsinhaber des **Atomgesetzes**;

IT-Sicherheitsgesetz 2.0 (18.05.2021)

§ 8d

Geltungsbereich

Abbildung 2.35 Anwendungsbereich nach § 8d BSIG (2021)

Außer den Kleinstunternehmen haben Betreiber von Anlagen, die in Abbildung 2.35 aufgelistet sind, meist strengere oder zumindest vergleichbare Nachweispflichten.

F-02-14: Für welche Betreiber gelten nach dem BSIG Sonderregelungen?

- a) Betreiber von Energieversorgungsnetzen oder Energieanlagen
- b) Die Gesellschaft für Telematik
- c) Genehmigung nach dem Atomgesetz
- d) für Betreiber in der Lebensmittelproduktion

Den nächsten Abschnitt habe ich den *wichtigen Einrichtungen* oder den *Unternehmen im besonderen öffentlichen Interesse* gewidmet.



2.8 Unternehmen im besonderen öffentlichen Interesse (UBIs)

In diesem Abschnitt möchte ich auf die Unternehmen eingehen, die derzeit noch vor ihrer ersten Nachweisprüfung stehen und für die bisher eine Selbsterklärung ausreicht.

Nicht nur Betreiber kritischer Infrastrukturen müssen einen Nachweis über ihre umgesetzten Maßnahmen einreichen, sondern mit der Änderung des BSI-Gesetzes im Jahr 2021 auch *Unternehmen*, die *im besonderen öffentlichen Interesse* stehen. Umgangssprachlich werden diese Unternehmen als *UBIs* bezeichnet. In der NIS-2-Richtlinie werden die UBIs nun als *besonders wichtige Einrichtungen* oder *wichtige Einrichtungen* bezeichnet. Im Buch bleibe ich dennoch bei der Abkürzung UBI, da die BSI-Prozesse und Selbsterklärungen diese Abkürzung im Dezember 2023 einsetzten.

Auf der BSI-Webseite (14) sind drei Kategorien von UBIs analog zum BSIG definiert, die ich Ihnen in Abbildung 2.36 zeigen möchte. In Abbildung 1.41 sahen Sie dazu bereits die Definition von UBIs im IT-Sicherheitsgesetz 2.0.

UBI 1	Hersteller/Entwickler nach Außenwirtschaftsverordnung (AWV), im Bereich Waffen, Munition und Rüstungsmaterial oder im Bereich von Produkten mit IT-Sicherheitsfunktionen	UBI 1 AWV-UBI
UBI 2	sind die nach ihrer inländischen Wertschöpfung größten Unternehmen Deutschlands sowie wesentliche Zulieferer für diese Unternehmen.	UBI 2 Wertschöpfungs-UBI
UBI 3	sind Betreiber »eines Betriebsbereiches der oberen Klasse im Sinne der Störfall-Verordnung« oder Betreiber, die »nach der Störfall-Verordnung« gleichgestellt sind	UBI 3 Störfall-UBI

Abbildung 2.36 Die drei Kategorien für »Unternehmen im besonderen öffentlichen Interesse« nach § 2 Abs. 14 Nummer 1 bis 3 BSIG

Die Pflichten, die UBIs einhalten müssen, habe ich Ihnen in Abbildung 1.46 gezeigt. Die Pflicht zur Selbsterklärung gegenüber dem BSI gilt derzeit für die AWV-UBIs.

Das Formular zur Selbsterklärung für diese UBIs sehen wir uns in Abschnitt 6.4.9, »Selbsterklärung für AWV-UBI (UBI 1)«, genauer an. Dieses steht Ihnen auf der BSI-Seite seit November 2022 als Vorlage (15) zur Verfügung.

Hinweis zum Begleitmaterial

Die Selbsterklärung zur IT-Sicherheit für Unternehmen im besonderen öffentlichen Interesse für UBI 1 vom November 2022 finden Sie im Dokument:

- 2022-11_BSI_Selbsterklaerung_UBI



Mit dieser kurzen Vorstellung von »Unternehmen im besonderen öffentlichen Interesse« beziehungsweise »besonders wichtigen und wichtigen Einrichtungen« ist das Kapitel zur Kritisverordnung beendet. In Kapitel 3 sehen wir uns die IT-Sicherheitskataloge für den Sektor Energie genauer an.

Inhalt

Materialien zum Buch	13
Einleitung	15
Wie Ihnen dieses Buch helfen kann – und was es nicht ist	17
Der Weg durch das Buch	19
Danksagung	23

TEIL I Gesetzliche Anforderungen und Begriffe im KRITIS-Umfeld

1	Geschichtliche Hintergründe zur Nachweisprüfung	29
1.1	UP KRITIS	42
1.2	Das IT-Sicherheitsgesetz von 2015	47
1.2.1	Änderungen im BSIG	49
1.2.2	Änderungen im Energiewirtschaftsgesetz (EnWG)	58
1.3	Das Gesetz zur Umsetzung der NIS-Richtlinie	60
1.4	Das IT-Sicherheitsgesetz 2.0	64
1.4.1	Änderungen im BSIG	64
1.4.2	Änderungen im EnWG	70
1.5	Die NIS-2-Richtlinie	72
1.6	Das BSI-Gesetz (BSIG)	75
2	Die Kritisverordnung	81
2.1	Kritische Infrastrukturen	81
2.2	Die Erarbeitung der Kritisverordnung	82
2.3	Begriffe und Definitionen	84
2.4	Sektoren nach dem BSIG	87
2.4.1	Der Sektor Energie	88
2.4.2	Der Sektor Wasser	90

2.4.3	Der Sektor Ernährung	93
2.4.4	Sektor Informationstechnik und Telekommunikation	94
2.4.5	Sektor Gesundheit	94
2.4.6	Sektor Finanz- und Versicherungswesen	96
2.4.7	Sektor Transport und Verkehr	98
2.4.8	Sektor Siedlungsabfallentsorgung	99
2.5	Anlagenkategorien für kritische Dienstleistungen	101
2.6	Anhänge zu den Sektoren	102
2.6.1	Teil 1 – Grundsätze und Fristen (Kritische Anlagen)	103
2.6.2	Teil 2 – Berechnungsformeln für die kritische Dienstleistung	104
2.6.3	Teil 3 – Anlagenkategorien und Schwellenwerte	108
2.7	Welche Betreiber fallen unter das BSIG?	112
2.8	Unternehmen im besonderen öffentlichen Interesse (UBIs)	114

3 Die IT-Sicherheitskataloge (IT-SiKat) für den Sektor Energie 117

3.1	Die Bundesnetzagentur (BNetzA)	119
3.2	Das Energiewirtschaftsgesetz (EnWG)	120
3.3	Die IT-Sicherheitskataloge	122
3.3.1	Der IT-Sicherheitskatalog für Strom- und Gasnetze (2015)	123
3.3.2	Der IT-Sicherheitskatalog für Energieanlagen (2018)	126
3.4	Die ISO/IEC 27019 – Steuerungssysteme der Energieversorgung	130
3.4.1	Fazit zu Teil 1 des Buches	133

TEIL II Bedeutung und Verantwortung des BSI für Kritische Infrastrukturen

4 Die Unterstützung durch das BSI 137

4.1	Die Gewährleistungsverantwortung gegenüber der Bevölkerung	143
4.2	Die Meldestelle für Informationssicherheitsvorfälle	144

4.3	Erstellung von Lagebildern und Weiterleitung von Information an die KRITIS-Betreiber	145
4.3.1	Die E-Mail-Verkehrsstatistik	147
4.3.2	Die Malware-Statistik	149
4.4	Informations- und Meldeflüsse nach dem BSIG	152
4.4.1	Cyber-Sicherheitswarnungen	153
4.4.2	CERT-Bund Meldungen	154
4.4.3	Die Allianz für Cyber-Sicherheit (ACS)	155
4.4.4	Konferenzen mit BSI-Beteiligung	156

5 Die Orientierungshilfen (OH) des BSI 159

5.1	OH zum Aufbau eines branchenspezifischen Sicherheitsstandards (B3S)	159
5.2	OH zu Systemen zur Angriffserkennung (SzA)	161
5.3	OH zu Nachweisen (für Prüfer)	163

6 Vorgaben an die Art und Weise von Nachweisprüfungen 169

6.1	Registrierung als KRITIS-Betreiber	171
6.2	Das Melde- und Informationsportal (MIP)	171
6.2.1	Schritt 1: Die Institutions-ID	172
6.2.2	Schritt 2: Die Institutionsverwalter-ID	172
6.2.3	Schritt 3: Für die Meldestelle KRITIS registrieren	173
6.2.4	Schritt 4: Sektor und Anlagenkategorie eintragen	173
6.2.5	Schritt 5: Meldeberechtigte ergänzen	173
6.2.6	Token	174
6.2.7	Sanitarisierung	174
6.2.8	Die Aufgaben der Meldeberechtigten	174
6.3	Der Nachweisprozess	176
6.4	Die Vorgabedokumente im Nachweisprozess	177
6.4.1	Grundsätzliche Anforderungen im Nachweisprozess (GAiN)	177
6.4.2	Das Nachweisdokument KI für KRITIS-Betreiber	181
6.4.3	Der Prüfplan als Excel-Vorlage für Auditoren	182
6.4.4	Das Nachweisdokument P für Prüfer	184

6.4.5	Die Nachweisdokumente KI* / P* für Prüfungen im Sektor Energie	187
6.4.6	Selbsterklärung der prüfenden Stelle	189
6.4.7	Selbsterklärung zur zusätzlichen Prüfverfahrenskompetenz	190
6.4.8	Erklärung zur Unabhängigkeit	191
6.4.9	Selbsterklärung für AWW-UBI (UBI 1)	192
6.4.10	Die Mängelliste als Excel-Vorlage für Auditoren	194

TEIL III Pflichten und Möglichkeiten des KRITIS-Betreibers

7 Ihre Pflichten als KRITIS-Betreiber 199

7.1	Der Geltungsbereich für die kritische Dienstleistung	200
7.1.1	Den KRITIS-Geltungsbereich eingrenzen	201
7.1.2	Den Netzstrukturplan erstellen	203
7.1.3	Ein zu kleiner Geltungsbereich	205
7.1.4	Ein zu großer Geltungsbereich	206
7.1.5	Der Geltungsbereich umfasst die kritische Dienstleistung	208
7.1.6	Gruppierung von Objekten im Netzstrukturplan	210
7.2	Organisatorische und technische Vorkehrungen zur Vermeidung von Störungen	210
7.2.1	Berücksichtigung des All-Gefahrenansatzes	211
7.2.2	Eingeschränkte Risikoakzeptanz	212
7.2.3	Maßnahmen nach dem Stand der Technik	213
7.2.4	Umsetzung aller risikomindernden Maßnahmen	214
7.3	Systeme zur Angriffserkennung (SzA)	215
7.3.1	Die Umsetzungsempfehlungen des BSI zu SzA	216
7.3.2	Praktisches Umsetzungsbeispiel IRMA®	219
7.3.3	Besonderheiten des Energie-Sektors	221
7.4	Interne Audits	222
7.5	Melden von Informationssicherheitsvorfällen, Störungen und Ausfällen	223
7.6	Gemeinsame übergeordnete Ansprechstelle (GÜAS)	224

8 Einen branchenspezifischen Sicherheitsstandard (B3S) veröffentlichen 227

8.1	Aufbau eines B3S mithilfe der OH B3S	227
8.2	Einen B3S beim BSI einreichen	232
8.3	Eignungsfeststellung des BSI	235
8.4	Aktuell veröffentlichte B3S	236
8.5	Vorteile und Nachteile vorhandener B3S	238

TEIL IV Die Nachweisprüfung gemäß § 8a Abs. 3 BSIG

9 Planung der Nachweisprüfung durch den Betreiber 241

9.1	Auswahl einer Prüfstelle	241
9.2	Anforderungen an eine prüfende Stelle	242
9.3	Eignung als prüfende Stelle	243

10 Vorarbeiten für die Nachweisprüfung durch Prüfer 247

10.1	Welche Prüfgrundlagen können wir einsetzen?	248
10.1.1	Ein passender B3S als Prüfgrundlage	250
10.1.2	Klassische Standards als Prüfgrundlage	251
10.1.3	Cloud Computing Compliance Criteria Catalogue – C5:2020	252
10.1.4	Die »Konkretisierten Anforderungen« als Prüfgrundlage	253
10.1.5	Die Orientierungshilfe B3S als Prüfgrundlage	254
10.1.6	Der IT-Sicherheitskatalog als Prüfgrundlage	256
10.2	Kompetenzbereiche und Aufteilung im Prüftteam	257
10.3	Fachexperten auswählen und einsetzen	258
10.4	Die Prüfungsplanung durch die Prüfstelle	260
10.4.1	Abstimmung im Vorfeld	260
10.4.2	Einen Prüfplan entwerfen	260
10.4.3	Die Excel-Vorlage des BSI zum Prüfplan	261

10.5 Auswahl von Stichproben	264
10.6 Berücksichtigung externer Dienstleister	266
10.7 Die Mängelkategorien des BSI	267

11 Die Nachweisprüfung durchführen 271

11.1 Audit von Managementsystemen nach der ISO 19011	272
11.1.1 Das Eröffnungsgespräch	273
11.2 Arbeitsschutz für Auditoren	275
11.3 Remote-Audits	277
11.3.1 Welche Risiken können sich bei einem Remote-Audit ergeben?	277
11.3.2 Themen für Remote-Audits	278
11.4 Mögliche Prüfmethoden	282
11.5 Verwendung bestehender Zertifikate	283
11.6 Prüfung der branchenspezifischen Maßnahmen	287
11.7 Prüfung des BCMS	291
11.7.1 Organisation zum BCMS	293
11.7.2 Vorbereitung und Durchführung von Notfallübungen	294
11.7.3 Wartungen, Inspektionen und Wiederherstellung	296
11.8 Aktualität der BSI-Formulare und OHs beim Prüfteam	297

12 Nacharbeiten nach der Nachweisprüfung 301

12.1 Aufgaben des Prüfers	302
12.1.1 Bewertung des ISMS-Reifegrades	302
12.1.2 Bewertung des BCMS-Reifegrades	303
12.1.3 Bewertung des SzA-Umsetzungsgrades	304
12.1.4 Die Mängelliste dokumentieren	310
12.1.5 Übermittlung der Auditdokumentation an den Betreiber	315
12.2 Aufgaben des Betreibers	316
12.2.1 Nachverfolgung und Überwachung der geplanten Maßnahmen	317
12.2.2 Selbsterklärung der AWW-UBI (UBI 1)	317
12.2.3 Fristen für Betreiber	319
12.2.4 Übergabe der Nachweise an das BSI	324
12.2.5 Übergabe der Nachweise im Energie-Sektor	325

13 Prüfung der eingereichten Nachweise durch das BSI 329

13.1	Nachforderung von Dokumenten	329
13.2	Eskalation bei Unvollständigkeit	331
13.3	Sonderprüfungen nach dem BSIG	332
13.4	Nachprüfung wegen zu kleinem Geltungsbereich	333
13.5	Bußgelder	334

TEIL V Aus der Praxis – in die Praxis

14 Untersuchung zu Umfang und Komplexität der Nachweisprüfung 341

14.1	Die BSI-Studie zur Umsetzung der IT-Sicherheitsgesetze	342
14.2	Studie zu Nachweisprüfungen nach BSIG	344
14.2.1	Durchführung der Umfrage	345
14.2.2	Ziele der Umfrage	345
14.2.3	Statistische Auswertung und Ergebnisse	347
14.2.4	Fazit der Ergebnisse	372

15 Zusätzliche Prüfverfahrenskompetenz nach dem BSIG 377

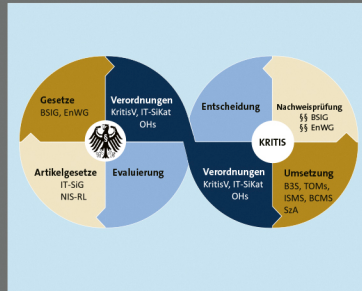
15.1	Weiterbildung und schriftliche Prüfung	377
15.2	Überprüfung Ihrer Antworten	378

16 Fazit und Ausblick 385

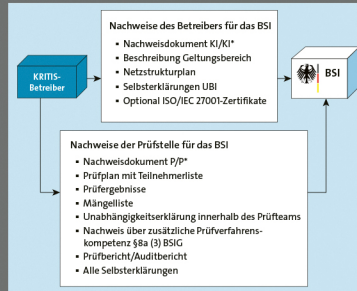
Literaturverzeichnis	389
Index	395

Alles zur KRITIS-Verordnung

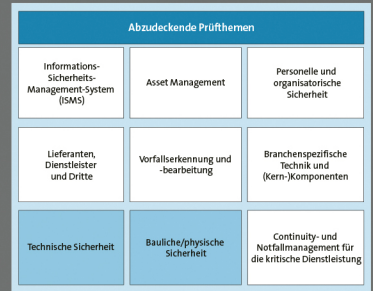
Der Schutz kritischer Infrastrukturen ist wichtiger denn je! Wer Sorgfaltspflichten ignoriert oder Vorfälle nicht meldet, kann sich empfindliche Strafen einhandeln. Dieser Leitfaden erläutert Ihre Pflichten als Betreiber und zeigt Ihnen, was Sie in der Nachweisprüfung erwartet. Auditoren finden Infos zur zusätzlichen Prüfverfahrenskompetenz und Anleitungen zur eigenständigen Durchführung von KRITIS-Audits.



Zusammenhänge verstehen



Nachweise einreichen



Prüfverfahrenskompetenz erwerben

Der Schutz kritischer Infrastrukturen

Transportwesen, Wasserwerke, Krankenhäuser, Energieversorger – gehört auch Ihre Organisation zur kritischen Infrastruktur? Dann gilt es, sich jetzt über gesetzliche Nachweispflichten zu informieren.

Die Nachweisprüfung in der Praxis

Wie bereiten Sie sich ideal auf die Nachweisprüfung vor und wie kommen Sie Ihren Pflichten als Betreiber nach? Was ist im Audit besonders wichtig und wie bearbeiten Sie die Prüfung nach? In diesem Ratgeber erfahren Sie, worauf Sie besonders achten müssen.

Prüfverfahrenskompetenz nach dem BSIG

Gute Prüfer sind rar gesät. Wenn Sie selbst die erforderliche Prüfverfahrenskompetenz erwerben wollen, bilden Sie sich mit diesem Fachbuch in den relevanten Gesetzen und Prozessen weiter und bereiten sich erfolgreich für die Eignungsprüfung vor.

 **Begleitdokumente und Schulungsmaterial stehen zum Download bereit.**



Jacqueline Naumann schult seit 2018 Sicherheitsbeauftragte und Auditoren zur ISO/IEC 27001 und zur »Zusätzlichen Prüfverfahrenskompetenz für § 8a BSIG«. Seit 2017 auditiert sie nach IT-Sicherheitskatalog und führt seit 2018 Nachweisprüfungen nach § 8a BSIG durch.

Aus dem Inhalt

- Die Kritisverordnung
- Die IT-Sicherheitskataloge
- Unterstützung und Orientierungshilfen durch das BSI
- Vorgaben für die Nachweisprüfung
- Ihre Pflichten als KRITIS-Betreiber
- Einen branchenspezifischen Sicherheitsstandard (B3S) erstellen
- Planung der Nachweisprüfung
- Vorarbeiten für die Nachweisprüfung
- Die Nachweisprüfung durchführen
- Prüfung der eingereichten Nachweise durch das BSI
- Aus der Praxis: Untersuchung zu Umfang und Komplexität der Nachweisprüfung
- Zusätzliche Prüfverfahrenskompetenz nach dem BSIG

