KRITIS

Anforderungen, Pflichten, Nachweisprüfung

DAS VORWORT

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 Paragrafen 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 Paragrafen in Gesetze überführt werden und durch Verordnungen ihre Macht entfalten.

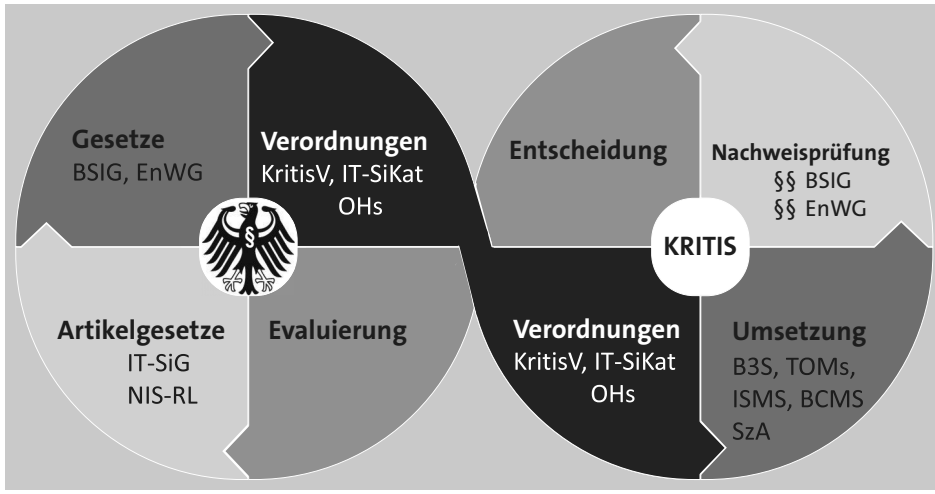

Abbildung 1 Doppelter Reformprozess für Kritische Infrastrukturen

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 Paragrafen 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 legte 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 GAiN, 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.