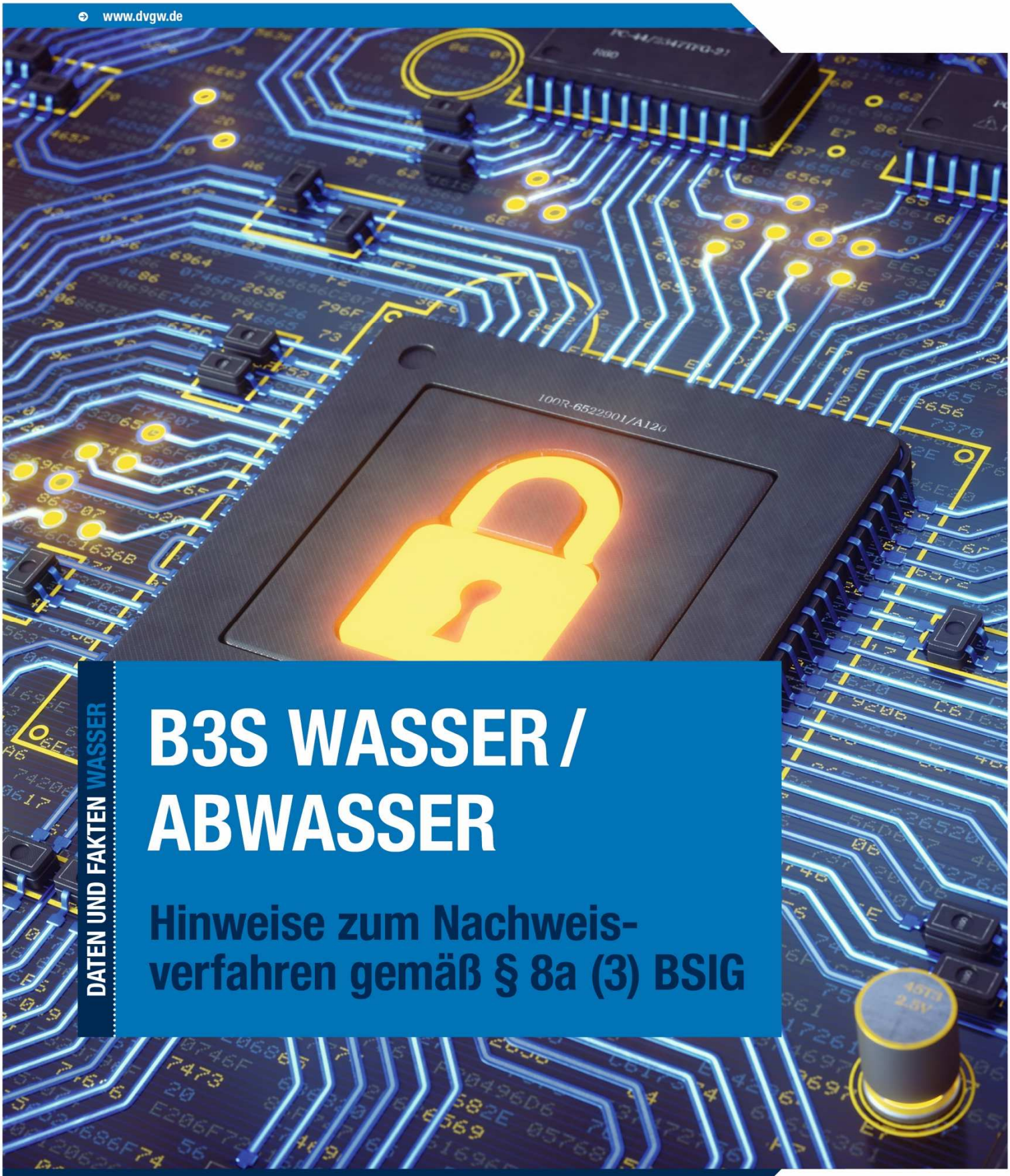
DWA
Klare Konzepte. Saubere Umwelt.

DVGW

INFORMATION

www.dvgw.de



DATEN UND FAKTEN WASSER

B3S WASSER / ABWASSER

Hinweise zum Nachweisverfahren gemäß § 8a (3) BSIG

Inhaltsverzeichnis

1 Einführung

Betreiber Kritischer Infrastrukturen im Sinne der BSI-KritisV sind nach § 8a (1) BSIG verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung (BSI-Kritisverordnung – BSI-KritisV) *„[...] angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen [...] ihrer informationstechnischen Systeme, Komponenten und Prozesse“* nach Stand der Technik zu treffen und dies gemäß § 8a (3) BSIG gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) geeignet durch „[...] Sicherheitsaudits, Prüfungen oder Zertifizierungen [...]“ – im weiteren Verlauf „Prüfung(en)“ genannt – nachzuweisen. Der Betreiber übermittelt dem BSI für jede Anlage zum einen die Auflistung der durchgeführten Prüfungen und zum anderen eine Liste der aufgedeckten Sicherheitsmängel – im weiteren Verlauf „Nachweisdokument“ genannt.

Das BSI kann die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse (im weiteren Verlauf „Prüfbericht“ genannt) verlangen sowie in Abstimmung mit den zuständigen Aufsichtsbehörden die Beseitigung von Sicherheitsmängeln anordnen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Eignung der Teile 1 – DVGW W 1060 (M) bzw. DWA-Merkblatt 1060 – und 2 – IT-Sicherheitsleitfaden inklusive zugehörigem Handbuch – des branchenspezifischen Sicherheitsstandards Wasser/ Abwasser (B3S WA) gemäß § 8a (2) BSIG festgestellt.

Dieses Dokument beinhaltet auf Grundlage der vom BSI herausgegebenen Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG als nicht normative Empfehlung Hinweise bezüglich des Nachweisverfahrens zur Umsetzung von § 8a (1) BSIG bei Anwendung der Teile 1 und 2 des B3S WA. Das Dokument wurde dem BSI vorgelegt.

2 Rollen und Zuständigkeiten im Nachweisprozess

Von den in diesem Dokument beschriebenen Rahmenbedingungen und Umsetzungshilfen sind die in Abbildung 1 dargestellten Rollen „Betreiber“, „prüfende Stelle“, „Prüfteam“, „BSI“ und „Aufsichtsbehörde“ betroffen.

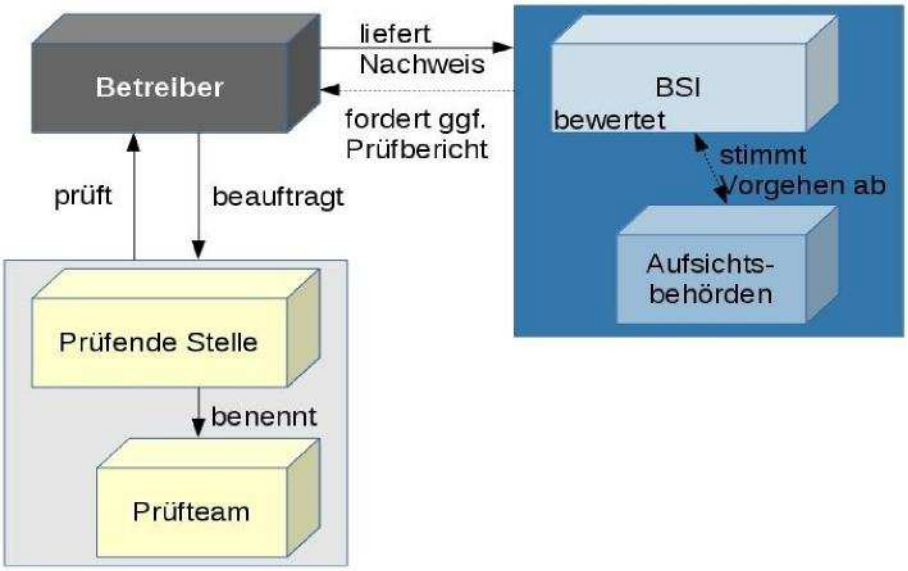


Abbildung 1: Rollen im Nachweisprozess, Quelle: BSI

Details zu den Rollen und Zuständigkeiten im Nachweisprozess sind in Abschnitt 8.1 im Anhang beschrieben.

3 Nachweisdokumente

Gegenüber dem BSI wird die Erfüllung der Anforderungen aus § 8a (1) BSIG durch das Nachweisdokument belegt. Damit das BSI die Eignung der Prüfung, die Angemessenheit und Wirksamkeit der Vorkehrungen zur Vermeidung von Störungen sowie die Schwere der aufgedeckten Sicherheitsmängel bewerten kann, sollte das Nachweisdokument die nachfolgend aufgeführten Informationen enthalten.

Das BSI stellt Formulare bereit, in denen die Betreiber die Information übermitteln können, die zum Nachweis erforderlich sind. Diese Formulare umfassen die folgenden Blätter:

- Blatt KI: Angaben zur geprüften Kritischen Infrastruktur und zum Ansprechpartner
- Blatt PS: Angaben zur Eignung der prüfenden Stelle und zum Prüfteam
- Blatt PD: Angaben zur Prüfdurchführung
- Blatt PE: Angaben zum Prüfergebnis und zu den aufgedeckten Sicherheitsmängeln

Das Blatt KI ist vom KRITIS-Betreiber auszufüllen und zu unterschreiben. Es bildet zusammen mit den Blättern PS, PD und PE, die von der prüfenden Stelle auszufüllen und zu unterschreiben sind, das Nachweisdokument. Es wird vom KRITIS-Betreiber an das KRITIS-Büro des BSI gesandt.

Die als Nachweisdokument vorgesehenen Formulare sind auf den Webseiten des BSI unter www.bsi.bund.de/Nachweise veröffentlicht.

4 Aufgaben des Betreibers

4.1 Übersicht

Der Betreiber muss die Umsetzung der Anforderungen gemäß § 8a (1) BSIG – angemessene Vorkehrungen zur Vermeidung von Störungen unter Berücksichtigung des Stands der Technik – für seine Anlagen gewährleisten.

Dazu muss er zunächst

- den Geltungsbereich festlegen,
- die zugrundeliegenden Prozesse erheben und dokumentieren,
- eine Risikoanalyse und -bewertung durchführen,
- entsprechende Sicherheitsmaßnahmen planen, umsetzen und dokumentieren.

Bei Anwendung des B3S WA ist hierfür der Ablauf gemäß Handbuch zum IT-Sicherheitsleitfaden maßgeblich.

Zum objektiven Nachweis der Umsetzung der Maßnahmen muss er anschließend eine geeignete prüfende Stelle (siehe Abschnitt 5) beauftragen, die eine Prüfung (Audit, Prüfung oder Zertifizierung) durchführt und dem Betreiber die Ergebnisse in einem Prüfbericht unter Auflistung der gegebenenfalls aufgedeckten Sicherheitsmängel übermittelt.

In einem letzten Schritt reicht der KRITIS-Betreiber dann mindestens alle zwei Jahre das Nachweisdokument (siehe Abschnitt 3) beim BSI ein. Nachweisdokumente sind dabei für jede Anlage gemäß BSI-KritisV separat einzureichen.

4.2 Beschreibung des Prüfgegenstandes

Eine geeignete Prüfung muss als Prüfgegenstand alle Anlagen und Systeme der Kritischen Infrastruktur gemäß BSI-KritisV umfassen, die für die Erbringung der kritischen Dienstleistung erforderlich sind. In Vorbereitung auf die Prüfung sollte der Umfang daher genau definiert und beschrieben werden. Die Vollständigkeit der zugrundeliegenden Informationen bestätigt der Betreiber in Blatt KI. Zusätzlich sind wesentliche Punkte dieser Beschreibung später auch im Blatt PD des Nachweisdokuments aufzunehmen.

Für die Prüfungsdurchführung und das Nachweisdokument sollten

- die Anlage(n),
- die vom Betreiber erbrachten Teile der kritischen Dienstleistung,
- die Teile der kritischen Dienstleistung, die von externen Dienstleistern erbracht werden (z. B. Auslagerung),
- das Zusammenspiel mit anderen Systemen sowie
- die Schnittstellen und Abhängigkeiten

beschrieben werden.

Für die Prüfungsdurchführung sollen zudem alle

- informationstechnischen Systeme,
- Komponenten,
- Prozesse und
- Rollen bzw. Personen

aufgeführt werden, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastruktur erforderlich sind oder deren Funktionsfähigkeit beeinflussen (können).

4.3 Sicherheitsdokumentation

Damit das Prüfteam die Prüfung nach § 8a (3) BSIG ordnungsgemäß durchführen kann, benötigt es einerseits konkrete Unterlagen und andererseits die Möglichkeit einer Vor-Ort-Prüfung mit Inaugenscheinnahme von Technik sowie der Möglichkeit zu Gesprächen mit Mitarbeitern des Betreibers (siehe hierzu auch Kapitel 7).

Bei Anwendung des B3S WA hat der Betreiber dem Prüfteam für die Dokumentenprüfung die im Merkblatt sowie die im Handbuch des IT-Sicherheitsleitfadens genannten Dokumente vorzulegen, einschließlich der in den relevanten Maßnahmen geforderten Dokumentationen.

4.4 Wahl der Prüfgrundlage

Der Betreiber wählt die Prüfgrundlage, nach der er die Prüfung durchführen lassen will. Er teilt diese der prüfenden Stelle im Vorfeld der Prüfung mit. Dabei können folgende Fälle unterschieden werden, die in Abschnitt 7.1 bzgl. der Durchführung von Prüfungen genauer beschrieben werden:

- Prüfung auf Grundlage des vom BSI anerkannten B3S WA (Abschnitt 7.1.1)
- Berücksichtigung vorhandener Prüfungen oder anderer Prüfgrundlagen (Abschnitt 7.1.2)

Der Betreiber hat die Möglichkeit, der prüfenden Stelle bereits vorhandene Prüfgrundlagen zur Verfügung zu stellen. Die prüfende Stelle entscheidet, ob und zu welchem Grad diese in die Prüfung einfließen können.

5 Prüfende Stelle

5.1 Allgemein

Eine prüfende Stelle ist eine geeignete Institution, die vom KRITIS-Betreiber beauftragt wird, festzustellen, ob der Betreiber wirksame und angemessene Vorkehrungen zur Vermeidung von Störungen gemäß § 8a (1) BSIG getroffen hat.

Damit eine prüfende Stelle als geeignet angesehen werden kann, hat sie die nachfolgend beschriebenen fachlichen und organisatorischen Anforderungen erfüllen.

Die prüfende Stelle stellt insbesondere das Prüfteam zusammen, das die eigentliche Prüfung vornimmt. Anforderungen an das Prüfteam sind in Kapitel 6 beschrieben.

5.2 Aufgaben

Aufgabe der prüfenden Stelle ist es,

- die Einhaltung der Prozesse und Verfahren festzustellen,
- für einheitliche und gleichwertige Prüfungsdurchführung und Prüfergebnisse Sorge zu tragen,
- die Qualitätsprüfung vorzunehmen,
- die Rahmenbedingungen für die Prüfdurchführung festzulegen (Prüfverfahren usw.),
- das Prüfteam zusammenzustellen und dabei die Abdeckung aller Kompetenz-Bereiche sicherzustellen,
- die Eignung der Prüfer zu bestätigen und
- die Kommunikation mit dem Betreiber auf der einen und dem Prüfteam auf der anderen Seite durchzuführen.

Die prüfende Stelle übernimmt die Verantwortung für die Prüfergebnisse, unterzeichnet die Prüfdokumente und sendet diese an den Betreiber.

5.3 Eignung

5.3.1 Allgemein

Von einer prüfenden Stelle ist die Einhaltung folgender Anforderungen zu gewährleisten:

- Die Prüfung wird unabhängig, unparteilich, neutral und weisungsfrei durchgeführt. Die Einhaltung der ethischen Grundsätze (siehe Abschnitt 8.1 im Anhang) ist sichergestellt.
- Die erforderlichen Prozesse (z. B. Qualitätssicherungsverfahren, Prüfprozess) müssen eingeführt, umgesetzt und in Konzepten dokumentiert sein.
- Die Art und der Umfang der Prüfungshandlungen und -ergebnisse werden einheitlich, sachlich und ordnungsgemäß dokumentiert.

- Es werden ausreichend kompetente personelle Ressourcen und geeignete Infrastrukturen zur Verfügung gestellt.

Damit die Qualität der Prüfergebnisse vergleichbar ist, sollten die Prüfungen auf der Grundlage gängiger Normen und Standards durchgeführt werden. Die Einhaltung der Anforderungen an die prüfende Stelle und die Umsetzung der Prozesse sollte durch eine unabhängige Instanz kontrolliert werden.

Eine prüfende Stelle kann als geeignet angesehen werden, wenn sie gegenüber dieser unabhängigen Instanz ihre Neutralität und Eignung nachgewiesen hat.

5.3.2 Akkreditierte Zertifizierungsstellen der DAkkS

Eine geeignete Stelle für die Durchführung der Prüfung gemäß § 8a (3) BSIG muss grundsätzlich eine Akkreditierung bei der DAkkS zur DIN EN ISO/IEC 27001-Zertifizierung vor- und die Umsetzung und Einhaltung der DIN EN ISO/IEC 17021-1 und ISO/IEC 27006 gegenüber der DAkkS nachweisen. Hiermit wird sichergestellt, dass die Qualitätsanforderungen durch die DAkkS als „unabhängige Instanz“ überwacht werden.

Darüber hinaus muss die Zertifizierungsstelle zusätzlich für die Verfahren nach DIN EN ISO 9001 (Qualitätsmanagement) oder DIN EN ISO 14001 (Umweltmanagement) mit den Scopes 24 (Abwasser) und/oder 27 (Wasser) akkreditiert sein. Hiermit wird gewährleistet, dass die Kompetenz vorhanden ist, Abläufe in der Trinkwasserver- und Abwasserentsorgung in Verbindung mit dem B3S WA nachvollziehen und beurteilen zu können.

5.3.3 Zertifizierte IT-Sicherheits-Dienstleister oder anerkannte Prüfstellen des BSI

Darüber hinaus bietet das BSI eine Zertifizierung von IT-Sicherheitsdienstleistern an. Grundvoraussetzung für die Anerkennung als Prüfstelle oder Zertifizierung als IT-Sicherheitsdienstleister ist die Erfüllung der Anforderungen der aktuellen DIN EN ISO/IEC 17021-1. Diese Stellen erfüllen damit ebenfalls entsprechende Qualitätsansprüche. Auf den Webseiten des BSI findet sich eine Liste der Prüfstellen bzw. IT-Sicherheitsdienstleister, die durch das BSI anerkannt bzw. zertifiziert sind und damit die Voraussetzung einer ordnungsgemäßen Prüfung erfüllen.

6 Prüfteam

6.1 Allgemein

Seitens der prüfenden Stelle wird ein Prüfteam mit der konkreten Prüfung bei einem KRI-TIS-Betreiber beauftragt.

Das Prüfteam hat alle zur Erbringung geeigneter Nachweise erforderlichen Anforderungen zu erfüllen und über die hierfür erforderliche Kompetenz zu verfügen. Ein Prüfteam besteht aus mindestens zwei qualifizierten Mitarbeitern (Teamleiter und Prüfer). Je nach Prüfumfang kann das Prüfteam um weitere Prüfer bzw. Fachexperten (z. B. zur Beisteuerung branchenspezifischer oder anlagenspezifischer Fachkenntnis) erweitert werden. Alle Mitglieder des Prüfteams haben die im Abschnitt 8.2 des Anhangs aufgeführten „Ethischen Grundsätze“ zu befolgen.

6.2 Aufgaben

Ein Prüfteam der prüfenden Stelle führt die Prüfung gemäß einem Prüfverfahren durch und erstellt einen Prüfbericht, der die Prüfergebnisse dokumentiert.

Dabei kann diese Prüfung

- als Einzelprüfung einer geeigneten prüfenden Stelle oder
- als Zusatzprüfung z. B. im Rahmen einer DIN EN ISO/IEC 27001-Zertifizierung, d. h. eines Zertifzierungs-, Überwachungs- oder Re-Zertifizierungsaudits (nativ oder auf Basis von IT-Grundschutz) durch Auditoren (Drittparteien-Audit)

durchgeführt werden.

6.3 Eignung

Damit die Prüfer geeignete Prüfungen und damit geeignete Nachweise zur Erfüllung der gesetzlichen Anforderungen erbringen können, müssen sie in den folgenden Bereichen Kompetenz nachweisen:

- Spezielle Prüfverfahrens-Kompetenz für § 8a BSIG
- Audit-Kompetenz
- IT-Sicherheits-Kompetenz bzw. Informationssicherheits-Kompetenz
- Branchen-Kompetenz

Abbildung 2 zeigt, welche Themengebiete in den einzelnen Kompetenzbereichen mindestens vorhanden sein sollten.

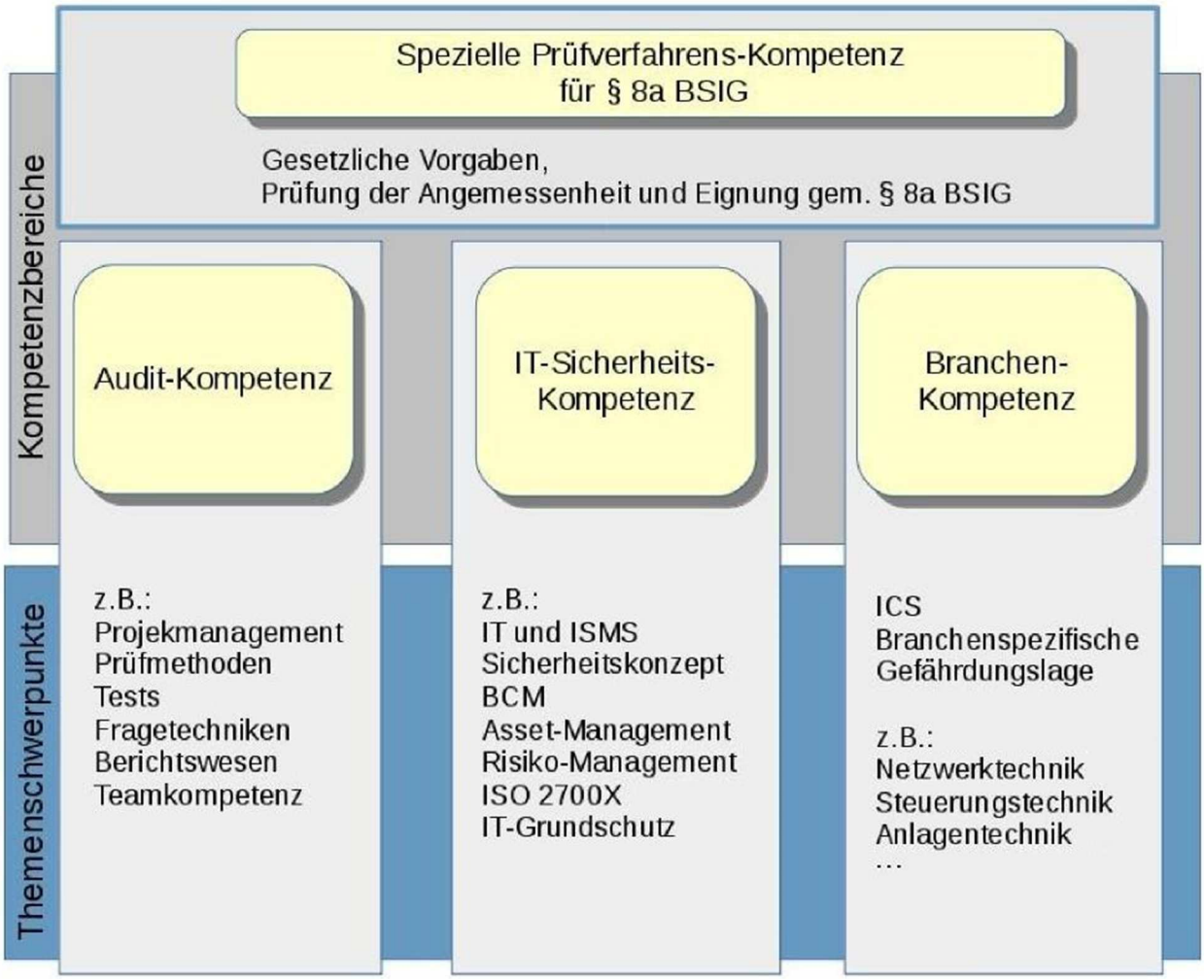


Abbildung 2: Themen der Kompetenzbereiche, Quelle: in Anlehnung an BSI

Tabelle 1 gibt eine Übersicht über typische Qualifikationen, über die geeignete Prüfer verfügen sollten. Dabei kann die Kompetenz auf mehrere Prüfer verteilt sein. Wichtig ist jedoch, dass an jedem Prüfabschnitt auch Prüfer mit der hierfür ausreichenden Kompetenz beteiligt sind.

Anforderungen	**Erläuterung**	**Nachweis**
Spezielle Prüfverfahrens-Kompetenz für § 8a BSIG		
Spezielle Prüfverfahrenskompetenz	Teilnahme an mehrtägiger Schulung „spezielle Prüfverfahrens-Kompetenz für § 8a BSIG“ inkl. Prüfung	Prüfungszeugnis / Zertifikat über die bestandene Prüfung

Anforderungen	Erläuterung	Nachweis
Audit-Kompetenz		
Alternative 1	Innerhalb der letzten 3 Jahre verantwortliche Beteiligung an mindestens 4 Erstparteien-Audits oder Zweitparteien-Audits inkl. IT-Anteil im Gesamtaufwand von insgesamt 30 PT	DIN EN ISO/IEC 27001-Auditor / BSI-Grundschutz-Auditor + vom Auftraggeber / Arbeitgeber bestätigte Kurzberichte
Alternative 2	Innerhalb der letzten 4 Jahre Durchführung von mindestens 4 ISMS Drittparteien-Audits im Gesamtaufwand von 20 PT	DIN EN ISO/IEC 27001-Auditor / BSI-Grundschutz-Auditor + vom Auftraggeber / Arbeitgeber bestätigte Kurzberichte
IT-Sicherheits-Kompetenz		
Alternative 1	In den letzten 5 Jahren mindestens 3 Jahre Berufserfahrung im Bereich IT, davon mindestens 2 Jahre im Bereich IT-/Informationssicherheit mit Schwerpunkt SPS/Speicherprogrammierbare Steuerungen und ICS/Industrial Control System	Zeugnis / Bescheinigungen eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten
Alternative 2	Mindestens 4 Jahre Berufserfahrung (Vollzeit) in der Informationstechnologie, davon mindestens 2 Jahre in einer Rolle oder Funktion die Tätigkeiten zur Informationssicherheit mit Schwerpunkt SPS/Speicherprogrammierbare Steuerungen und ICS/Industrial Control System beinhalten	Zeugnis / Bescheinigungen eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten

Anforderungen	Erläuterung	Nachweis
Branchen-Kompetenz		
Branchenkenntnisse	In den letzten 5 Jahren mindestens 3 Jahre Branchenerfahrung im Bereich Trinkwasserversorgung / Abwasserentsorgung mit entsprechenden Kenntnissen der Prozesse und des Anlagenbetriebs zur Erbringung der kritischen Dienstleistung (kann durch Aufnahme eines Fachexperten in das Prüfteam erfüllt werden)	Zeugnis / Bescheinigungen eines Dritten oder des zu prüfenden Betreibers über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten

Tabelle 1: Kompetenzanforderungen an Prüfer

Sofern die erforderliche Kompetenz nicht bei den Prüfern selbst vorliegt, ist in das Prüfteam ein Fachexperte mit den entsprechenden Kenntnissen aufzunehmen.

6.4 Aufrechterhaltung der Kompetenz

Die Prüfer und die prüfende Stelle haben ihre Fachkompetenz kontinuierlich durch den Austausch mit anderen Fachexperten aufrechtzuerhalten.

Regelmäßig stattfindende „Erfahrungsaustausch-Tage“ der prüfenden Stellen sollen den prüfenden Stellen und den Prüfern die Möglichkeit geben, sich über aktuelle Entwicklungen zu informieren und Erkenntnisse auszutauschen und zu diskutieren. Zur Aufrechterhaltung der „Speziellen Prüfverfahrenskompetenz zu § 8a BSIG“ ist eine jährliche Teilnahme an einer eintägigen Veranstaltung nachzuweisen. Die prüfende Stelle hat jährlich für die bei ihr berufenen Prüfer einen entsprechenden Erfahrungsaustausch durchzuführen. Nachweise anderer, gleichwertiger Prüfstellen können auch anerkannt werden. Innerhalb von drei Jahren ist jedoch mindestens eine Teilnahme am Erfahrungsaustausch der berufenden Prüfstelle nachzuweisen.

7 Durchführung der Prüfung

7.1 Prüfgrundlage(n)

7.1.1 Prüfgrundlage bei Anwendung des B3S WA gemäß § 8a (2) BSIG

Prüfgrundlage ist der durch das BSI anerkannte Branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S WA).

Der B3S WA beinhaltet laut DVGW W 1060 (M) bzw. DWA-Merkblatt 1060 in Verbindung mit dem IT-Sicherheitsleitfaden sowohl den Geltungsbereich als auch die Mindestanforderungen der umzusetzenden Maßnahmen einschließlich der Vorgaben für die zu erstellende Dokumentation. Der Betreiber muss die Vorgaben des B3S WA konkret auf seine Anlagen anpassen und einen entsprechenden Umsetzungsplan festlegen.

7.1.2 Berücksichtigung vorhandener Prüfungen

Grundsätzlich können vorhandene Prüfungen bei der Erbringung des Nachweises berücksichtigt werden, d. h. es besteht die Möglichkeit, für § 8a (3) BSIG erforderliche Prüfaspekte im Rahmen anderer Prüfungen abzudecken. Dabei müssen die Prüfungen aktuell sein, d. h. sie dürfen zum Zeitpunkt der Einreichung beim BSI nicht älter als ein Jahr sein. Ältere Nachweise können allenfalls in Form einer Dokumentenanalyse in die Prüfung einfließen, ersetzen aber nicht die aktuelle Prüfung (z. B. aufgrund geänderter Gefahrenlage und Wirksamkeit von Maßnahmen). Noch fehlende Aspekte müssen in den eigenen Prüfplan aufgenommen werden.

Insbesondere ist darauf zu achten, dass der Geltungsbereich die zu prüfende Kritische Infrastruktur vollständig abdeckt. Die Verantwortung für die vollständige Abdeckung des Geltungsbereichs liegt beim Betreiber. Die Vollständigkeit wird durch die prüfende Stelle ausdrücklich geprüft.

Hinweis zu ISO/IEC 27001-Zertifizierungen:

Bei einer reinen ISO/IEC 27001-Zertifizierung ist nicht von vornherein klar, dass Geltungsbereich und Maßnahmen geeignet sind. Deswegen reicht diese alleine nicht aus; wichtige Schutzziele für kritische Dienstleistungen könnten dabei unberücksichtigt bleiben.
Nur wer eine ISO/IEC 27001-Zertifizierung nachweist, im Rahmen der Umsetzung Risiken nur im Ausnahmefall akzeptiert hat und zusätzlich nachweist, dass Geltungsbereich und Maßnahmen geeignet sind, seine kritischen Dienstleistungen ausreichend zu schützen (inkl. gegenüber ISO/IEC 27001 zusätzlicher Anforderungen zum Schutz der Kritischen Infrastruktur), hat damit die Voraussetzungen zur Erfüllung der Anforderungen gemäß § 8a (1) und (3) BSIG geschaffen.

7.2 Prüfthemen und Prüfung des Geltungsbereichs

Die Prüfthemen sind im B3S WA konkret beschrieben, insbesondere sind dort die Maßnahmen aufgeführt, deren Umsetzung sichergestellt werden müssen.

Für die Eignung des Nachweises ist insbesondere die Überprüfung wichtig, ob der Geltungsbereich die informationstechnischen Systeme, Komponenten und Prozesse, die zur Kritischen Infrastruktur gehören, sowie diejenigen, die auf die Kritische Infrastruktur Einfluss haben, vollständig umfasst.

Dabei ist der Geltungsbereich unter dem Prüfaspekt

- der Vollständigkeit,
- der Eignung, Erforderlichkeit, Wirksamkeit und Angemessenheit und
- der Funktionsfähigkeit der kritischen Dienstleistung

zu überprüfen und zu bewerten.

Die Prüfung der Eignung des Geltungsbereichs im Sinne von § 8a (3) BSIG ist Teil des Prüfergebnisses und wird von der prüfenden Stelle immer geprüft und ausdrücklich bestätigt.

7.3 Prüfmethoden

Mögliche Prüfmethoden sind:

- mündliche Befragung (Interview),
- Inaugenscheinnahme von Systemen, Orten, Räumlichkeiten und Gegenständen,
- Analyse von dokumentierten Informationen,
- Einbeziehung bestehender Nachweise (z. B. Prüfung des Prüfberichts einer in anderem Kontext vorgenommenen Prüfung; vorhergehende ISO 27001-Zertifikate (siehe auch Abschnitt 7.1.2)).

Der Einsatz der unterschiedlichen Prüfmethoden hängt vom konkreten Fall ab und ist durch das Prüfteam festzulegen.

7.4 Aufwand der Prüfung

7.4.1 Generelle Faktoren

In die Bestimmung des Prüfsaufwands fließen im Wesentlichen folgende Faktoren ein:

- Anzahl der relevanten Anlagen nach BSI-KritisV
- Die in Bezug auf den Geltungsbereich relevante Personalausstattung
- Anzahl der relevanten Anwendungsfälle

7.4.2 Beispiel eines Kalkulationsschemas

Basis dieses Kalkulationsschemas ist das für den Geltungsbereich relevante Personal in der zu prüfenden Organisation. Die Tabelle 2 zeigt die vorgeschlagenen Audittage in Abhängigkeit von der Anzahl des Geltungsbereichs-relevanten Personals.

Geltungsbereichs-relevantes Personal	**Prüftage**
1 – 10	2
11 – 15	2,5
16 – 25	3
> 25	4

Tabelle 2: Prüftage

Auf Basis der Anzahl der im Geltungsbereich der Prüfung vorhandenen Anlagen sowie der übrigen Größen kann ein Komplexitätsfaktor mit den Kategorien „Niedrig“, „Mittel“ und „Hoch“ bestimmt werden.

		Anzahl Anwendungsfälle		
		Niedrig (1 - 7)	Mittel (8 - 14)	Hoch (≥ 15)
Anzahl Anlagen	hoch (>10)	+10 %	+20 %	+25 %
	Mittel (5 - 10)	+5%	+10%	+20 %
	Niedrig (1 - 5)	0%	+5%	+10%

Tabelle 3: Bestimmung des Komplexitätsfaktors

Der sich aus dem Kalkulationsschema ergebende minimale Prüfaufwand liegt bei 2 Prüftagen und der maximale bei 5 Prüftagen.

<u>Beispiel:</u>

Die zu prüfende Organisation beschäftigt 20 Mitarbeiter, die als Geltungsbereich relevantes Personal gelten, und hat 14 Anwendungsfälle identifziert und betreibt 8 Anlagen.

Gemäß Tabelle A 1 sind zunächst 3 Prüftage erforderlich. Mit Hilfe der Tabelle 3 wird der Komplexitätsfaktor bestimmt. Hier ergibt sich ein Aufschlag von 10%, somit ergibt sich ein Prüfaufwand von 3,3 Tagen.

Der für eine sinnvolle Prüfung tatsächlich notwendige Aufwand ist von der prüfenden Stelle (siehe Kapitel 5) unter Berücksichtigung der generellen Faktoren gemäß Abschnitt 7.4.1

und den spezifischen Gegebenheiten individuell für jede zu prüfende Organisation zu bestimmen.

Anmerkung:

Ein Prüftag entspricht 8 Stunden und enthält keine Reisezeiten. Auch Fahrzeiten zwischen Standorten bzw. Betriebsanlagen, werden hierbei nicht berücksichtigt. Einzige Ausnahme bilden Fahrzeiten, die 15 Minuten nicht überschreiten.

7.4.3 Prüfschritte

Jede Prüfung hat die in Tabelle 4 aufgeführten sechs Prüfschritte abzudecken. Der Zeitanteil ist eine Empfehlung und dient als Orientierung für die Prüftiefe der einzelnen Prüfschritte.

Phase	Tätigkeit	Zeitanteile
Schritt 1	Vorbereitung der Prüfung sowie Prüfung der Eignung des Geltungsbereichs	5 %
Schritt 2	Erstellung des Prüfplans	5 %
Schritt 3	Dokumentenprüfung	25 %
Schritt 4	Vor-Ort-Prüfung	55 %
Schritt 5	Nachbereitung der Vor-Ort-Prüfung	5 %
Schritt 6	Erstellung des Prüfberichtes	5 %

Tabelle 4: Orientierung zum relativen Zeitaufwand bei der Durchführung einer Prüfung als Nachweis der Umsetzung der Anforderungen § 8a (3) BSIG, Quelle: in Anlehnung an BSI

7.5 Prüfplan und mögliche Stichprobenauswahl

Jeder Prüfung muss ein dokumentierter Prüfplan zugrunde liegen. In diesem werden das Prüfteam, die Prüfobjekte, die Prüfziele sowie die beabsichtigte Prüfmethode im Vorfeld der Prüfung festgelegt. Ebenfalls werden die Rollen im Prüfteam und die benötigten Ansprechpartner beim Betreiber sowie die zeitlichen Abläufe festgeschrieben.

Eine komplette Prüfung des gesamten Geltungsbereichs ist in der Regel nicht mit wirtschaftlich vertretbarem Aufwand möglich, daher muss der Prüfer im Prüfplan eine angemessene Stichprobenauswahl aus den kritischen Prozessen festlegen. Bei der Wahl der Stichproben ist risikoorientiert vorzugehen (Berücksichtigung von Wahrscheinlichkeit und Auswirkungen auf die Erbringung der kritische Dienstleistung), allerdings ist darauf zu achten, dass in der Gesamtheit der Stichproben eine gute Abdeckung der Kritischen Infrastruktur, aber auch netztopologische Abdeckung erzielt wird. Bereiche mit höheren Risiken sollen stärker berücksichtigt werden.

In die Risikobetrachtung sollte insbesondere auch die Auswirkung auf die Versorgung durch die kritische Dienstleistung (Wie viele Menschen wären von einem Ausfall betroffen? Wie gravierend wäre eine Störung/ein Ausfall?) entsprechend der Größe des Betreibers einbezogen werden. Die Auswahl der Stichprobe ist zu begründen.

Ein auf mehrere Jahre angelegtes Prüfungskonzept ist zu empfehlen, damit jedes informationstechnische System, jede informationstechnische Komponente und jeder informationstechnische Prozess in absehbarer Zeit mindestens einmal geprüft wird. Die Stichprobe ist vom Prüfer bzw. der prüfenden Stelle zu wählen. Die Verwendung der gleichen Stichprobe über mehrere Prüfungen hinweg ist nicht zulässig. Im Prüfplan sollten vorherige Prüfungen berücksichtigt werden, um mittel/langfristig eine vollständige Abdeckung aller Komponenten/Prozesse zu erreichen. Insbesondere ist die Mängelliste aus letzten Prüfergebnissen (Prüfberichten) bei der Stichprobenauswahl im Prüfplan zu berücksichtigen.

7.6 Dokumentation des Prüfergebnisses im Prüfbericht

Der Prüfbericht als Nachweis gemäß § 8a (3) BSIG über die Umsetzung der Anforderungen nach § 8a (1) BSIG muss folgenden Kriterien genügen:

- Ist ein eigenständiges Dokument
- Ist in deutscher Sprache verfasst, alle Inhalte sind nachvollziehbar
- Hat eine eindeutige Bezeichnung, Versionsverwaltung und Änderungshistorie
- Enthält alle für die Bewertung relevanten Metainformationen (z. B. Geltungsbereich der Untersuchung, Prüfziel, Zeitpunkt, Ort und Dauer der Prüfung, Prüfende Stelle und Prüfteam, Prüfergebnisse usw.)
- Dokumentiert alle Prüfschritte nachvollziehbar und wiederholbar und legt die Prüfentscheidungen begründet dar
- Folgt den Vorgaben des B3S WA

Insbesondere sind Sicherheitsmängel und -empfehlungen im Prüfbericht zu dokumentieren.

7.7 Sicherheitsmängel, Abweichungen und Mängelkategorien

Die festgestellten Sachverhalte zu jeder geprüften Maßnahme sind im Prüfbericht aufzunehmen und hinsichtlich des Umsetzungsstatus zu bewerten. Wird eine Abweichung zu den Anforderungen gemäß § 8a (1) BSIG festgestellt, handelt es sich um einen Mangel, der zu dokumentieren und zu bewerten ist. Im gesamten Prüfbericht sind hierfür einheitlich die in Tabelle 5 definierten Mängelkategorien zu verwenden.

Kategorie	**Definition**	**Prüfbericht / Mängelliste**
Schwerwiegende oder erhebliche Abweichung bzw. Sicherheitsmangel	Eine „schwerwiegende Abweichung“ stellt eine gravierende Gefährdung bzw. ein gravierendes Risiko dar. Eine „erhebliche Abweichung“ stellt eine große Gefährdung bzw. ein großes Risiko dar. Es besteht akuter Handlungsbedarf. Die Abweichung muss umgehend bzw. zeitnah beseitigt werden, da die Vertraulichkeit, die Integrität oder die Verfügbarkeit der kDL stark gefährdet ist und erheblicher Schaden zu erwarten ist.	Aufnahme in den Prüfbericht und Aufnahme in das Nachweisdokument
Geringfügige Abweichung bzw. Sicherheitsmangel	Eine „geringfügige Abweichung“ stellt eine Gefährdung bzw. ein Risiko dar. Es besteht kein akuter Handlungsbedarf. Die zugrunde liegende Abweichung muss mittelfristig beseitigt werden. Die Vertraulichkeit, Integrität oder Verfügbarkeit der kDL kann beeinträchtigt werden.	Aufnahme in den Prüfbericht und Aufnahme in das Nachweisdokument
Empfehlung	Eine „Empfehlung“ stellt einen Verbesserungshinweis dar. Durch die Umsetzung der Empfehlung kann die Sicherheit erhöht werden. Empfehlungen können sein: • Verbesserungsvorschläge für die Umsetzung von Maßnahmen, • ergänzende Maßnahmen, die sich in der Praxis bewährt haben, oder • Kommentare hinsichtlich der Angemessenheit und Wirksamkeit von Maßnahmen. …	Aufnahme in den Prüfbericht empfohlen keine Aufnahme in das Nachweisdokument notwendig

Kategorie	Definition	Prüfbericht / Mängelliste
	Anmerkung: Eine teilweise oder nicht umgesetzte Maßnahme bzw. Anforderung darf nur dann als Sicherheitsempfehlung eingestuft werden, wenn das Prüfteam davon ausgehen kann, dass mittelfristig nicht mit einer Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit der Daten zu rechnen ist.	
Keine Abweichung	Es liegt kein Sicherheitsmangel vor, wenn die Anforderungen vollständig erfüllt werden und alle Maßnahmen vollständig, wirksam und angemessen umgesetzt sind. Es gibt keine ergänzenden Hinweise.	keine Aufnahme in das Nachweisdokument notwendig

Tabelle 5: Mängelkategorien

Anmerkung:

In der Mängelliste des Nachweisdokuments, das an das BSI gesendet wird, müssen jedoch einheitliche Mängelbewertungen vorgenommen werden. Daher muss der Prüfer (sofern seine Mängelkategorien von den Mängelkategorien in Tabelle 5 abweichen) seine Kategorien auf die in Tabelle 5 festgelegten Kategorien abbilden.

Neben dem Gesamtvotum ist das einheitliche Verständnis von einzelnen Abweichungen für die Bewertung der Mängel zwingend erforderlich. Wird ein Sicherheitsmangel als schwerwiegende Abweichung bewertet, so sind die Ursachen zu analysieren und nachvollziehbar zu dokumentieren.

Grundsätzlich sind alle Feststellungen, die ein Risiko darstellen oder korrigierende Maßnahmen benötigen, die nicht ohne Zeit- oder Ressourcenaufwand umgesetzt werden können, in den Prüfbericht aufzunehmen. Dabei sind neben den zu ergreifenden Maßnahmen die Frist(en) zur Beseitigung der Sicherheitsmängel und die geplante Nachverfolgung festzulegen und zu überwachen.

8 Anhang

8.1 Details zu Rollen und Zuständigkeiten im Nachweisprozess

8.1.1 Betreiber

Die Betreiber Kritischer Infrastrukturen im Sinne des BSIG sind gemäß § 8a (3) BSIG verpflichtet, alle zwei Jahre die Erfüllung der Umsetzung wirksamer und angemessener organisatorischer und technischer Maßnahmen gemäß § 8a (1) BSIG nachzuweisen. Die Maßnahmen dienen der Sicherstellung der Funktionsfähigkeit der Kritischen Infrastruktur zur Erbringung der kritischen Dienstleistungen.

Die Betreiber sollten zunächst geeignete Maßnahmen umsetzen, anschließend eine prüfende Stelle mit einer Prüfung beauftragen, dann bei der Prüfung als Ansprechpartner Auskunft geben und letztlich ein Nachweisdokument an das BSI übersenden.

Die Zuständigkeiten der Betreiber bzgl. Prüfungen und Nachweisen werden detailliert in Kapitel 4 beschrieben. Ihre Aufgaben bei der Unterstützung der prüfenden Stelle bzw. des Prüfteams während der Durchführung der Prüfung wird darüber hinaus in Kapitel 7 beschrieben. Jeder KRITIS-Betreiber trägt die Verantwortung für die Korrektheit des Nachweisdokuments.

8.1.2 Prüfende Stelle und Prüfteam

Mit der Prüfung der Umsetzung gemäß § 8a BSIG beauftragt der KRITIS-Betreiber eine prüfende Stelle. Diese stellt ein geeignetes, qualifiziertes und unabhängiges Prüfteam (siehe Kapitel 6) zusammen, das die eigentliche Prüfung vorbereitet, durchführt und in einem Prüfbericht dokumentiert. Die Zuständigkeiten der prüfenden Stelle bzgl. Prüfungen und Nachweisen werden detailliert in Kapitel 5 beschrieben.

Die prüfende Stelle trägt die Verantwortung für die korrekte Durchführung der Prüfung (siehe Kapitel 7) sowie für den Prüfbericht inkl. der Dokumente, die sie für das Nachweisdokument bereitstellen muss.

8.1.3 BSI

Das BSI erhält vom KRITIS-Betreiber das Nachweisdokument, also insbesondere die Mängelliste aus dem Prüfbericht und weitere Informationen zur durchgeführten Prüfung.

Das BSI nimmt das Nachweisdokument des Betreibers entgegen, prüft dieses auf Vollständigkeit und bewertet dessen Inhalte. Das BSI entscheidet auf Grundlage der vorliegenden Informationen, ob diese ausreichen oder ob – im Falle des Vorliegens von Sicherheitsmängeln – eine Übermittlung des gesamten Prüfberichts mit allen Prüfergebnissen erforderlich ist.

Erkenntnisse über häufig auftretende Mängel oder Sicherheitsprobleme fließen ggf. über die individuelle Betrachtung der Nachweisdokumente hinaus und ausschließlich anonymisiert in die allgemeine Lagebewertung (z. B. Liste der häufigsten Sicherheitsmängel in der Branche) und in Sicherheitsempfehlungen ein. Diese Bewertungen und Empfehlungen sollen helfen, Risiken bei anderen Betreibern vorzubeugen und bei eingetretenen Sicherheitsvorfällen geeignet zu beraten. Diese Information erhalten registrierte KRITIS-Betreiber über die auf Basis des § 8b BSIG angelegten Informationskanäle.

8.1.4 Aufsichtsbehörden

Liegt ein besonders relevanter Sicherheitsmangel vor, stimmt das BSI zusammen mit den zuständigen Aufsichtsbehörden das weitere Vorgehen ab. Das BSI kann in diesem Fall im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes bzw. im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung von Mängeln verlangen.

Da die Aufsichtsbehörden erst im Rahmen der Bewertung der Sicherheitsmängel beteiligt werden, wird ihre Rolle in diesem Dokument nicht weiter betrachtet.

8.2 Ethische Grundsätze

Um Vertrauen in eine objektive Prüfung zu schaffen, ist die Einhaltung der „Ethischen Grundsätze“ notwendig. Die „Ethischen Grundsätze“ müssen sowohl durch die Einzelpersonen als auch durch die prüfende Stelle eingehalten werden. Sie umfassen folgende Prinzipien:

- **Rechtschaffenheit und Vertraulichkeit**: Die Rechtschaffenheit begründet Vertrauen und schafft damit die Grundlage für die Zuverlässigkeit eines Urteils. Da im Umfeld der Informationssicherheit oft sensible Geschäftsprozesse und Informationen zu finden sind, ist die Vertraulichkeit der während einer Prüfung erlangten Informationen und der diskrete Umgang mit den Auskünften und Ergebnissen der Prüfung eine wichtige Arbeitsgrundlage. Prüfer beachten den Wert und das Eigentum der erhaltenen Informationen und legen diese nicht ohne entsprechende Befugnis offen, es sei denn, es bestehen dazu rechtliche oder berufliche Verpflichtungen.
- Fachkompetenz: Prüfer übernehmen nur solche Aufgaben, für die sie das erforderliche Wissen, Können und die entsprechende Erfahrung haben und setzen diese bei der Durchführung ihrer Arbeit ein. Sie verbessern kontinuierlich ihre Fachkenntnisse sowie die Effektivität und Qualität ihrer Arbeit.
- Objektivität und Sorgfalt: Ein Prüfer hat ein Höchstmaß an sachverständiger Objektivität und Sorgfalt beim Zusammenführen, Bewerten und Weitergeben von Informationen über geprüfte Aktivitäten oder Geschäftsprozesse zu zeigen. Die Beurteilung aller relevanten Umstände hat mit Ausgewogenheit zu erfolgen und darf nicht durch eigene Interessen oder durch Andere beeinflusst werden.

- Sachliche Darstellung: Ein Prüfer hat die Pflicht, seinem Auftraggeber wahrheitsgemäß und genau über die Untersuchungsergebnisse zu berichten. Dazu gehören die objektive und nachvollziehbare Darstellung der Sachverhalte in den Prüfberichten, die konstruktive Bewertung der dargestellten Sachverhalte und die konkreten Empfehlungen zur Verbesserung der Maßnahmen und Prozesse.
- Nachweise und Nachvollziehbarkeit: Die rationale Grundlage, um zu zuverlässigen und nachvollziehbaren Schlussfolgerungen und Ergebnissen zu kommen, ist die eindeutige und folgerichtige Dokumentation der Sachverhalte. Hierzu gehört auch eine dokumentierte und nachvollziehbare Methodik (Prüfplan, Bericht), mit der das Prüfteam zu seinen Schlussfolgerungen kommt
- Unabhängigkeit und Neutralität: Ein Prüfer muss weisungsfrei und unvoreingenommen die Prüfung durchführen und die Prüfungsergebnisse dokumentieren können. Jedes Prüfteam sollte zur Gewährleistung der Unabhängigkeit und Objektivität aus mindestens zwei Prüfern bestehen („4-Augen-Prinzip“). Alle Auditoren dürfen aus Gründen der Unabhängigkeit und Neutralität vorher nicht unmittelbar im geprüften Bereich beratend oder auch ausführend, z. B. bei der Erstellung von Konzepten oder Konfiguration von IT-Systemen, tätig gewesen sein.

8.3 Glossar

Begriff	**Definition**
Abweichung	Nichtkonformität. Auftretende Sicherheitsmängel werden als Abweichung aufgefasst.
Angemessen	Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.
Anlage	Kritische Infrastruktur gemäß Definition in der BSI-Kritisverordnung (BSI-KritisV)
Betreiber	Unternehmen, das eine Kritische Infrastruktur gemäß Rechtsverordnung nach § 10 (1) BSIG (BSI-KritisV) betreibt
DAkkS	Die Deutsche Akkreditierungsstelle GmbH (DAkkS) ist die nationale Akkreditierungsstelle mit Sitz in Berlin.

Begriff	Definition
Drittparteien-Audits	Audits, die von externen unabhängigen Organisationen durchgeführt werden. Solche Organisationen bieten die Zertifizierung oder Überprüfung der Konformität mit den Anforderungen.
Erstparteien-Audit	Manchmal auch Interne Audits genannt – werden von oder im Namen der Organisation selbst für interne Zwecke durchgeführt und können die Grundlage für die eigene Konformitätserklärung der Organisation bilden.
Geltungsbereich	Gesamtheit der Informationstechnischen Systeme, Komponenten und Prozesse, Rollen bzw. Personen, die für die Funktionsfähigkeit der von Betreibern nach BSI-KritisV betriebenen Kritischen Infrastrukturen maßgeblich sind bzw. auf diese Einfluss haben.
Geltungsbereich-relevantes Personal	Personal, das in der zu prüfenden Organisation nach Vorgaben und Regeln des B3S WA arbeitet. Hierzu gehört unter anderem auch die Geschäftsführung, Personal der Leitstelle sowie der Beauftragte der Geschäftsführung für den B3S WA (IT-Sicherheitsbeauftragte). Außerdem Personen, die für Entwicklung, Verwirklichung oder Aufrechterhaltung der Schutzmaßnahmen verantwortlich sind.
ICS (Industrial Control Systems)	Mess-, Steuer-, und Regelungssysteme, die in der Industrie und in den KRITIS Branchen zur Automation und Überwachung von Industrieanlagen eingesetzt werden.
Kompetenz	Angelernte Fähigkeit, die die Ausübung einer bestimmten Tätigkeit ermöglicht.
Kritische Dienstleistung (kDL)	Von einer Kritischen Infrastruktur erbrachte Dienstleistung (z. B. Abwasserreinigung, Trinkwasserversorgung, …)

Begriff	Definition
Kritische Infrastruktur	Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.
Maßnahmen	Gemäß § 8a (1) BSIG umzusetzende angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von informationstechnischen Systemen, Komponenten oder Prozessen. Zu diesen Vorkehrungen gehören auch infrastrukturelle und personelle Maßnahmen. Besonders kritische Prozesse bedürfen besonderer Sicherheitsmaßnahmen.
Nachweis	Bescheinigung eines unabhängigen Dritten über die Einhaltung eines angemessenen Sicherheitsniveaus durch den Betreiber. Die Umsetzung der angemessenen und wirksamen Maßnahmen kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen.
Nachweisdokument	Formulare, die der Betreiber pro Anlage beim BSI einreicht; bestehend aus einer Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel sowie der zur Bearbeitung erforderlichen Informationen.
Prüfbericht	Dokument der prüfenden Stelle, das die gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse enthält.
Prüfende Stelle	Institution, die den Nachweis erbringt, dass der Betreiber die Maßnahmen gemäß § 8a (1) BSIG umgesetzt hat.
Prüfmethode	Alle für die Ermittlung eines Sachverhaltes vom Prüfer im Rahmen der Prüfung verwendeten Methoden.

Begriff	Definition
Prüfplan	Dokument, in dem der Prüfer vor Prüfungsbeginn die Rahmenbedingungen für die Prüfung festlegt. Inhalt sind das Prüfverfahren bzw. die Prüfmethoden und die Festlegung des Stichprobenumfangs.
Prüfung	Geeigneter Nachweis der Umsetzung der Maßnahmen beim Betreiber. Sie wird durch unabhängige und qualifizierte Prüfer einer prüfenden Stelle durchgeführt. Unter Prüfungen versteht man Sicherheitsaudits, Prüfungen und Zertifizierungen gemäß § 8a (3) BSIG.
Prüfverfahren	Methode, nach der die prüfende Stelle die Nachweise erbringt.