Konzeptpapier BAK „medizinische Versorgung“

Branchenspezifischer Sicherheitsstandard für die
Gesundheitsversorgung im Krankenhaus

BAK-Vorschlag für den DKG B3S Teil:

06 Hinweise zum Nachweisverfahren gemäß §8a (3) BSIG

Verfasser: BAK AK Prüfnachweise

Stand des Papiers: 06.02.2019

Status: Entwurf

Kategorie: TLP-WHITE

Version: BAK AK Prüfnachweis 1.0

Verteiler: Fachausschuss „Daten-Information und -Kommunikation“

Branchenarbeitskreis „Medizinische Versorgung“

Inhaltsverzeichnis

1 Einleitung

Das vorliegende Dokument stellt den Teil 06 des Branchenspezifischen Sicherheitsstandards für die Branche „medizinische Versorgung" dar. Es soll Betreiber, Prüfteams und prüfende Stellen dabei unterstützen, den Nachweis gemäß §8a (3) BSIG zu führen. Nachzuweisen ist, dass der jeweilig zu prüfende KRITIS-Betreiber angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse getroffen hat, die für die Funktionsfähigkeit der von ihm betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll er den Stand der Technik einhalten. Organisatorische und technische Vorkehrungen sind hierbei angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur beim KRITIS-Betreiber steht (vgl. BISG §8a (1)).

Die B3S-Dokumente Teil 01 bis Teil04 fokussieren insbesondere auf den branchenspezifischen Rahmen, den Geltungsbereich des B3S, die sich aus der Aufrechterhaltung der kDL ergebenden, branchenspezifischen Schutzziele, die branchenspezifische Gefährdungslage sowie die betreiberspezifische Risiko-Bewertung, die helfen soll die IT-heterogene Situation des jeweiligen KRITIS-Betreibers in der Erbringung der kDL zu berücksichtigen. Teil 05 des B3S definiert den jeweils gültigen „Stand der Technik" in Bezug auf ein grundlegendes IT-Sicherheitsmanagement und ein sinnvolles Maßnahmenportfolio zur Absicherung der kritischen Dienstleistung im Kontext der Branche „medizinische Versorgung".

Der vorliegende Teil 06 des B3S hat die Aufgabe, eine Prüfvorgabe zu machen, mit der die vom KRITIS-Betreiber ergriffenen IT-Absicherungsmaßnahmen gemäß §8a (1) BSIG in angemessener und praktikabler Weise auf Umsetzung und Wirkung überprüft werden können. Hierbei sind die Berücksichtigung der branchenspezifischen Besonderheiten sowie ein für den KRITIS-Betreiber wie für die prüfende Stelle ökonomisch, wie fachlich vertretbarer Verfahrensweg im Fokus. Es soll somit ein Prüfumfangsrahmen vorgegeben werden, der für KRITIS-Betreiber wie prüfende Stellen eine gewisse ökonomische Planungssicherheit garantiert und die gesetzlichen Anforderungen in sinnvollem Rahmen erfüllt.

Das primäre Ziel des B3S wird hierbei in der adäquaten Grundabsicherung und in der kontinuierlichen Verbesserung der Cyber-Security-Situation der KRITIS-Betreiber der „medizinischen Versorgung" gesehen. Ziel des vorliegenden Teil 06 ist es somit explizit, Prüfvorgaben für die durch die KRITIS-Verordnung definierten Betreiber Kritischer Infrastrukturen festzulegen. Den gemäß KRITIS-Verordnung nicht den KRITIS-Betreibern zuzurechnenden Einrichtungen im Kontext „medizinischer Versorgung" wird jedoch die Orientierung am vorliegenden B3S angeraten.

Grundsätzlich basiert der vorliegende Teil 06 des B3S auf der BSI-Orientierungshilfe zu Nachweisen gemäß §8a (3) BSIG in der Version 0.9.02 vom 30.06.2017 und passt diese Empfehlungen auf die branchenspezifischen Gegebenheiten an.

2 Beschreibung des Prüfgegenstandes - Prüfumfeld

§8a BSIG fordert in Absatz 1 „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen“, wobei der „Stand der Technik eingehalten“ werden soll.

Die Betrachtung der Angemessenheit und des Stands der Technik im Bereich „medizinische Versorgung“ des Sektors Gesundheit muss dabei die speziellen Bedingungen der Branche berücksichtigen:

- die hohe organisatorische und technische Heterogenität,
- die Nutzung von Legacy- und medizinische Spezialanwendungen sowie die Nutzung branchenspezifischen IT-Systemen mit einer starken Abhängigkeit von wenigen Anbietern,
- der Medizinproduktegesetzgebung, welcher die IT-gestützte Medizingeräten unterliegen, wobei der weltweite Regulations- und Qualitätssicherungsdruck bei Medizingeräten dazu führt, dass systemgebundene IT-Schwachstellen herstellerseitig in der Regel nur mittel- bis langfristig behoben werden,
- die hochgradig ökonomisch wie ordnungspolitisch Reglementierung deutscher Gesundheitseinrichtungen,
- je nach Finanzierungkontext die geringe budgetäre Handlungselastizität in Bezug auf Innovationsprozesse,
- die langen Abschreibungszyklen hochpreisiger medizinischer Spezialsysteme, deren initialen IT-Komponenten daher i.d.R. über den gesamten Lebenszyklus des Gerätes betrieben werden müssen,
- die Priorität von Patientensicherheit und Behandlungseffizienz in der medizinischen Versorgung, die umfangreiche und langwierige Vorbereitungsphasen vor technischen und organisatorischen Änderungen in den jeweiligen Institutionen bedingen.

Die aufgeführten Rahmenbedingungen führen dazu, dass Gefährdungen und Risiken der IT-Systeme häufig nicht auf IT-technisch unmittelbarem Weg behandelt werden können. Insbesondere muss der direkte Weg der Gefahrenvermeidung durch Beseitigung einer IT-Schwachstellen (z.B. durch Einspielen von Software-aktualisierungen oder dem Ersatz von Systemen) im konkreten Systemkontext durch einen indirekten Weg der Reduktion der Bedrohungen und damit der Ausnutzbarkeit der IT-Schwachstellen (z.B. weitgehende Isolation von gefährdete Systemen) oder entsprechende Notfallkonzepte ersetzt werden.

Eine Prüfung nach §8a muss somit insbesondere die Angemessenheit der getroffenen Absicherungsmaßnahmen im konkreten Branchenkontext betrachten und den Stand der anerkannten Technik in der Branche sowie die Verhältnismäßigkeit in Bezug auf die Wirkung einer Maßnahme auf den medizinischen Behandlungsprozess bewerten. In diesem Zusammenhang kommt der Branchenkompetenz im Prüfteam eine besondere Bedeutung zu.

Unabhängig von den Prüfvorgaben nach §8a sind die Meldepflichten von spezifischen

IT-Sicherheitsschwachstellen gemäß §8b des BSIG zu sehen, die einen großen Beitrag dazu leisten können, die Situation auf der Anbieterseite von branchenspezifischen IT-Systemen erheblich zu verbessern.

3 Rollen und Zuständigkeiten im Nachweisprozess

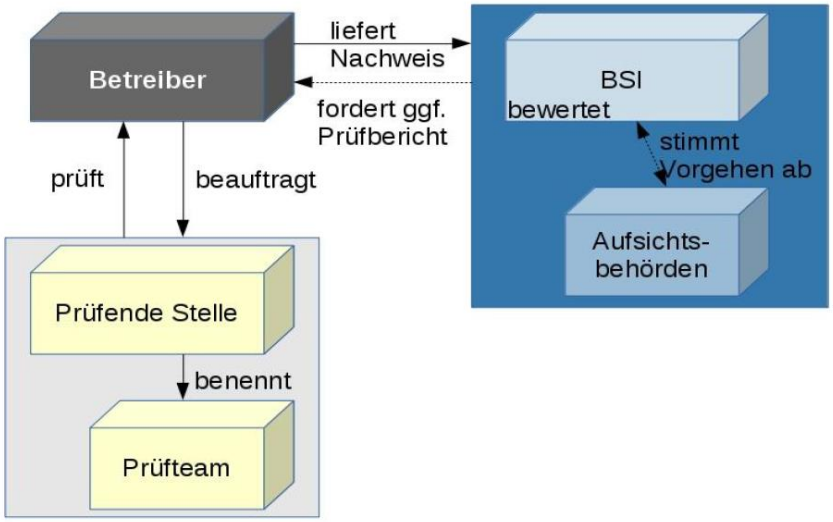

Abbildung 1: Rollen im Nachweisprozess, Quelle: BSI

3.1 BSI

Das BSI, als Aufsichtsbehörde gemäß BSIG, erhält vom KRITIS-Betreiber das entsprechende Nachweisdokument zur §8a Prüfung übermittelt (s. Kapitel 5.)

Das BSI nimmt das Nachweisdokument des Betreibers entgegen, prüft dieses auf Vollständigkeit und bewertet deren 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 des Nachweisdokuments 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. Weitere, unmittelbare Rückmeldungen an den KRITIS-Betreiber nach Abgabe der geforderten §8a Unterlagen sind nicht vorgesehen (Kapitel 5).

3.2 Aufsichtsbehörden

Liegt ein besonders relevanter Sicherheitsmangel vor, stimmt das BSI zusammen mit den zuständigen Aufsichtsbehörden im KRITIS-Betreiberkontext 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.

3.3 Betreiber

3.3.1 Allgemein

Die Betreiber Kritischer Infrastrukturen im Sinne des BSIG sind gemäß geltender Rechtsverordnung definiert und gemäß §8a (3) BSIG verpflichtet, 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, also im konkreten Kontext der Sicherstellung der kritischen Dienstleistung „medizinische Versorgung".

3.3.2 Aufgaben des Betreibers

Der Betreiber muss entsprechend den B3S-Dokumenten Teil 01 bis Teil 05

- den Geltungsbereich festlegen,
- die zugrundeliegenden kDL-relevanten Prozesse erheben und dokumentieren,
- die KRITIS-relevanten IT-Systeme identifizieren,
- eine Risikoanalyse und -bewertung der Systeme in Bezug auf die kDL durchführen,
- entsprechende Sicherheitsmaßnahmen planen, umsetzen und dokumentieren,
- eine Prüfgrundlage nach Abschnitt 3.3.3 auszuwählen,
- die Dokumentation entsprechend Abschnitt 3.3.4 bereitstellen.

Des Weiteren muss er alle 2 Jahre den Prüfnachweis gemäß §8a BSIG führen und das entsprechende Nachweisdokument an das BSI übermitteln.

3.3.3 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.

Um die Kommunikation zwischen Betreiber und prüfender Stelle zu vereinfachen und zu standardisieren, wird vom BAK „medizinische Versorgung" ein Prüfnachweisplaner-Tool herausgegeben, dessen Nutzung den KRITIS-Betreibern der Branche dringend empfohlen wird. Der bei einer Prüfung nach dem vorliegenden B3S zu wählende Prüfkatalog im vom Branchenarbeitskreis „medizinische Versorgung" empfohlenen

Prüfnachweisplaner ist mit „B3S“ gekennzeichnet und bildet den B3S Teil 05 als Prüfkatalog ab.

3.3.4 Dokumentationsbasis der Prüfgrundlage

Damit das Prüfteam die Prüfung nach §8a (3) BSIG ordnungsgemäß durchführen kann, benötigt es konkrete Unterlagen. Aufgabe des Betreibers ist es daher, die erforderlichen Unterlagen gemäß der von ihm gewählten Prüfgrundlage zu erarbeiten und Dokumente bzw. Nachweise zur Umsetzung angemessener IT-Absicherungsmaßnahmen vorzuhalten und – soweit nicht generell im Prüfdurchführungsprozess festgelegt (s. Abschnitt 4.1) – auf Anfrage der prüfenden Stelle entsprechend zur Verfügung zu stellen.

Der Betreiber hat ergänzend die Möglichkeit, der prüfenden Stelle bereits vorhandene Prüfunterlagen/Zertifikate mit Bezug zum Prüfkontext zur Verfügung zu stellen. Die prüfende Stelle entscheidet, ob und zu welchem Grad diese Nachweise in die Prüfung nach §8a einfließen und den Prüfaufwand im Kontext der §8a Prüfung reduzieren können.

3.3.5 Kontinuierlicher Verbesserungsprozess

Eine unmittelbare Rückkopplung in der Interaktion von Betreiber, prüfender Stelle, und BSI im Sinne eines kontinuierlichen Verbesserungsprozesses ist vom Gesetz nicht vorgesehen. Eine kontinuierliche Verbesserung in Bezug auf von Betreibern zu treffenden Absicherungsmaßnahmen muss jedoch generisches Anliegen der KRITIS-Betreiber sein. Die Maßnahmenplanung und kontinuierliche Verbesserung der IT-Sicherheitssituation erfolgt immer in der Managementverantwortung des KRITIS-Betreibers, insbesondere dann, wenn die Umsetzung entsprechender Verbesserungsmaßnahmen unmittelbar durch das BSI in Abstimmung mit den jeweiligen Aufsichtsbehörden eingefordert wird.

Unabhängig von der einzelnen Prüfung nach §8a und den hiermit einhergehenden Testtat-Meldepflichten, muss jeder KRITIS-Betreiber, somit für den Nachweis der Umsetzung ein gestuftes Umsetzungskonzept („Meilensteinplanung“) im Rahmen seiner IT-Sicherheitskonzeption erarbeiten, sodass dem Prüfteam glaubhaft vermittelt werden kann, welchen Weg der KRITIS-Betreiber in Bezug auf die Absicherung der kDL eingeschlagen hat und ob er diesen Weg konsequent und in angemessener Weise verfolgt.

3.4 Prüfende Stelle

3.4.1 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.

Diese stellt ein geeignetes, qualifiziertes und unabhängiges Prüfteam (siehe Abschnitt

3.5) zusammen, das die eigentliche Prüfung vorbereitet, durchführt und in einem Prüfbericht dokumentiert.

Die prüfende Stelle trägt die Verantwortung für die korrekte Durchführung der Prüfung (siehe Kapitel 4), die Qualifikation des Prüfteams sowie für den Prüfbericht inkl. der Dokumente, die sie für den Nachweis bereitstellen muss.

3.4.2 Aufgaben der prüfenden Stelle

Aufgabe der prüfenden Stelle ist es,

- die Rahmenbedingungen für die Prüfdurchführung festzulegen,
- das Prüfteam zusammenzustellen und dabei die Abdeckung aller Kompetenz-Bereiche nach Abschnitt 3.5.3 sicherzustellen und nachzuweisen,
- die Eignung der Prüfer zu bestätigen und die Kommunikation zwischen Betreiber und dem Prüfteam zu ermöglichen,
- die Einhaltung der Prüfprozesse und Verfahren zu gewährleisten,
- für einheitliche und gleichwertige Prüfungsdurchführung und Prüfergebnisse Sorge zu tragen.

Die prüfende Stelle übernimmt die Verantwortung für die ordnungsgemäße Durchführung der Prüfung und Dokumentation der Prüfergebnisse, unterzeichnet die Prüfdokumente und sendet diese an den Betreiber.

3.4.3 Geeignete prüfende Stellen

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

- Die Prüfung wird unabhängig, unparteilich, neutral und weisungsfrei und unter Einhaltung der ethischen Grundsätze (siehe Abschnitt 6.1 im Anhang) durchgeführt.
- Die erforderlichen Qualitätssicherungsprozesse (z. B. Qualitätsmanagement, Prüfprozess-Definition) sind durch die prüfende Stelle eingeführt, umgesetzt und dokumentiert.
- 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.

Grundsätzlich kommen prüfenden Stelle in Frage, welche die Kriterien der folgenden Unterkapitel erfüllen.

3.4.3.1. Akkreditierte Zertifizierungsstellen der DAkkS

Im Rahmen eines ISO/IEC 27001-Zertifizierungsverfahrens übernimmt die DAkkS die Funktion der „unabhängigen Instanz". Eine qualifizierte Zertifizierungsstelle ist für den Bereich ISO/IEC 27001 akkreditiert und muss die Umsetzung und Einhaltung der ISO/IEC 17021-1 und ISO/IEC 27006 gegenüber der DAkkS nachweisen. Damit erfüllen diese Stellen die notwendigen Qualitätsanforderungen.

Eine Übersicht in Deutschland akkreditierter Stellen zur ISMS-Zertifizierung kann auf der Internetseite der Deutschen Akkreditierungsstelle (DAkkS) abgerufen werden.

3.4.3.2. Zertifizierte IT-Sicherheitsdienstleister 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 DIN EN ISO/IEC 17025:2005.

Das Verfahren der Zertifizierung bzw. Anerkennung von Stellen ist in einer veröffentlichten Verfahrensbeschreibung festgelegt, die durch einen Begutachtungskatalog ergänzt werden.

Dabei kann eine Stelle für folgende Geltungsbereiche einen Antrag stellen:

- CC-Prüfstellen,
- TR-Prüfstellen,
- IT-Sicherheitsdienstleister: IS-Revision und IS-Beratung,
- IT-Sicherheitsdienstleister: Penetrationstester,

Diese Stellen erfüllen damit geeignete Qualitätsansprüche. Auf der Website des BSI findet sich eine Liste von Prüfstellen bzw. IT-Sicherheitsdienstleistern, die durch das BSI anerkannt bzw. zertifiziert sind und damit die Voraussetzung einer ordnungsgemäßen Prüfung erfüllen.

3.4.3.3. Interne Revisoren

Interne Revisoren die ein angemessenes und wirksames Revisionssystem und die Einhaltung der internationalen Standards für die berufliche Praxis der Internen Revision des Institute of Internal Auditors (IIA) durch ein Quality Assessment (QA) nachweisen können, sind als prüfende Stelle ebenfalls geeignet. Die unabhängige Instanz ist hier die Stelle, die die QA-Prüfungen durchführt. Diesem Verfahren liegen

der DIIR14-Revisionsstandard Nr. 3 „Prüfung von internen Revisionssystemen (Quality Assessments)“ und die IIA-Standards 1300ff zu Grunde.

Interne Revisoren haben für die §8a Nachweisführung entsprechende Qualitätskriterien einzuhalten. Diese werden in einem Quality Assessment der Internen Revision überprüft und nachgewiesen. Die folgenden sechs Mindestanforderungen lauten:

- Es ist eine offizielle schriftliche, angemessene Regelung für die Durchführung der Revision (Geschäftsordnung, Revisionsrichtlinie o. Ä.) vorhanden.
- Neutralität, Unabhängigkeit von anderen Funktionen sowie uneingeschränktes Informationsrecht sind sichergestellt.
- Die Interne Revision verfügt über eine angemessene quantitative und qualitative Personalausstattung.
- Der Prüfungsplan der Internen Revision wird auf Grundlage eines standardisierten und risikoorientierten Planungsprozesses erstellt.
- Art und Umfang der Prüfungshandlungen und -ergebnisse werden einheitlich, sachlich und ordnungsgemäß dokumentiert.
- Die Umsetzung der im Bericht dokumentierten Maßnahmen wird von der Internen Revision durch einen effektiven Follow-up-Prozess überwacht.

Durch die Einhaltung der internationalen Standards ist insbesondere die Unabhängigkeit der Internen Revision sichergestellt. Daneben ist auch der Ethikkodex des IIA für Interne Revisoren verpflichtend. Hier werden die Anforderungen an Rechtschaffenheit, Objektivität, Vertraulichkeit und Fachkompetenz beschrieben.

3.4.3.4. Wirtschaftsprüfungsinstitutionen

Aufgrund der hohen Verantwortung, die ein Wirtschaftsprüfer übernimmt, erfüllt er die besonderen Berufspflichten, die in der Wirtschaftsprüferordnung (WPO17) zusammengefasst sind. Dies sind u. a. Unabhängigkeit, Verschwiegenheit und berufswürdiges Verhalten. Die meisten Wirtschaftsprüfungen in Deutschland werden von den „Big Four Wirtschaftsprüfungsgesellschaften“ durchgeführt. Wirtschaftsprüfungsunternehmen, die bei der IDW registriert sind, können gegenüber dem BSI eine Selbsterklärung, dass die Anforderungen aus Abschnitt 6.1 im Anhang erfüllt sind.

3.4.3.5. Selbsterklärung gegenüber dem BSI

Ein Betreiber kann die Neutralität und Eignung einer prüfenden Stelle, d. h. die Erfüllung der Anforderung direkt beim BSI nachweisen. Die Qualität der Prüfung muss vergleichbar mit Zertifizierungsstellen nach ISO/IEC 17021 und ISO/IEC 27006 oder anderen einschlägigen Standards sein. Hierzu ist mit dem BSI Kontakt aufzunehmen. Das BSI überprüft anhand einer formellen Selbsterklärung der prüfenden Stelle, ob diese aus Sicht des BSI geeignet ist.

Das BSI bestätigt nach positiver Sichtung der Selbsterklärungsunterlagen die Eignung der prüfenden Stelle für die beabsichtigte Prüfung, behält sich aber vor, Stichproben bei der Umsetzung der Anforderungen durchzuführen.

3.4.3.6. Auffangregelung

Sofern keine prüfende Stelle zur Verfügung steht, die unter die zuvor genannten oder vergleichbaren Akkreditierungsregime fällt, ist im Ausnahmefall und nach Rücksprache mit dem BSI auch ein individueller Nachweis der Eignung einer vom Betreiber unabhängigen, prüfenden Stelle durch Selbsterklärung dieser Institution gegenüber dem BSI möglich. Hierzu sind mit Vorlauf von 3 Monaten zum jeweiligen §8a Abgabetermin mindestens 3 Angebotsanfragen und die Ablehnungsbescheide durch angeschriebene, akkreditierte oder BSI zugelassene, prüfende Stellen durch den Betreiber nachzuweisen.

3.5 Prüfteam

3.5.1 Allgemein

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

Ein Prüfteam besteht aus mindestens zwei qualifizierten Prüfern (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 6.1 des Anhangs aufgeführten „Ethischen Grundsätze“ zu befolgen.

3.5.2 Aufgaben des Prüfteams

Ein Prüfteam führt die §8a Prüfung gemäß der Prüfnachweisfestlegung (Kapitel 4) durch und erstellt einen Prüfbericht, der die Prüfergebnisse dokumentiert.

Dabei kann diese Prüfung

- als Einzelprüfung im Sinne des §8a BSIG oder
- als Zusatzprüfung z. B. im Rahmen einer DIN EN ISO/IEC 27001-Zertifizierung, d. h. eines Zertifizierungs-, Überwachungs- oder Re-Zertifizierungsaudits (nativ oder auf Basis von IT-Grundschutz)

durchgeführt werden.

3.5.3 Eignung

Das Prüfteam muss für eine Prüfung nach §8a mindestens folgende Kompetenzen abdecken:

- 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.

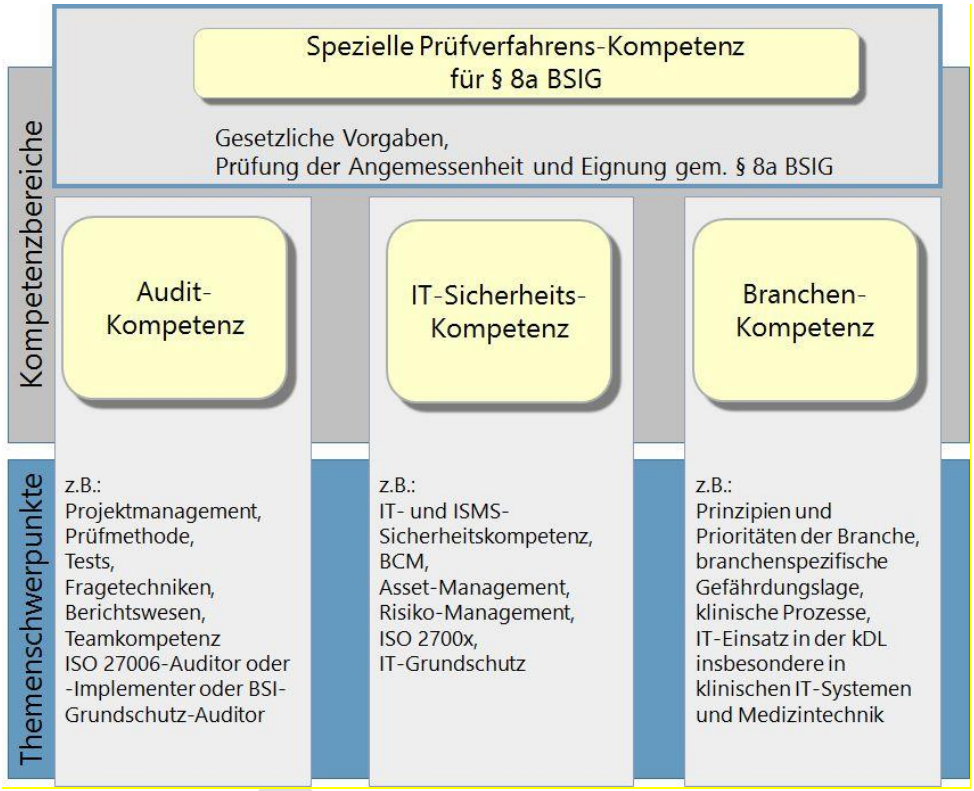

Abbildung 2: Kompetenzbereiche, Quelle: in Anlehnung an BSI

Tabelle 1 gibt eine Übersicht über typische Qualifikationen, über die geeignete Prüfer verfügen sollen. Dabei kann die Kompetenz auf mehrere Prüfer verteilt sein. Soweit die Prüfung in mehreren Prüfabschnitten erfolgt, ist wichtig, dass an jedem Prüfabschnitt Prüfer mit der hierfür ausreichenden Kompetenz beteiligt sind.

Anforderungen	Erläuterung	Nachweis
Spezielle Prüfverfahrens-Kompetenz für § 8a BSIG		
Spezielle Prüfverfahrens-kompetenz	Teilnahme an mehrtägiger Schulung „spezielle Prüfverfahrens-Kompetenz für § 8a BSIG“ inkl. Prüfung	Prüfungszeugnis / Zertifikat über die bestandene Prüfung
Audit-Kompetenz		
ISMS-Audit-Erfahrung	Innerhalb der letzten 5 Jahre verantwortliche Beteiligung an mindestens 4 Erstparteien-Audits	DIN EN ISO/IEC 27001-Auditor oder -Implementer

Anforderungen	Erläuterung	Nachweis
	(Internes Audit) im Kontext ISMS **oder** 3 Zweitparteien-Audits im Kontext ISMS **oder** 2 Drittparteien-Audits im Kontext ISMS	oder BSI-Grundschutz-Auditor, sowie vom Auftraggeber / Arbeitgeber erstellte Nachweise über mindestens 30 erbrachte Personentage
IT-Sicherheits-Kompetenz		
Kenntnisse zu IT-Sicherheit / Informationssicherheit	In den letzten 5 Jahren mindestens 3 Jahre Berufserfahrung im Bereich IT, davon mindestens 2 Jahre im Bereich Informationssicherheit	Zeugnis / Bescheinigungen eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten
Branchen-Kompetenz		
Branchenkenntnisse	In den letzten 5 Jahren mindestens 3 Jahre nachweisliche Branchenerfahrung im Bereich Gesundheitswesen, wobei Kenntnisse über die nachstehenden Themen erworben sein müssen: • Prinzipien und Prioritäten der Branche (insbesondere Patientensicherheit und Behandlungseffizienz, spezielle Gefährdungslagen) • Prozesskenntnisse der kDL • IT-Einsatz in der kDL insbesondere in klinischen IT-Systemen, Medizintechnik	Zeugnis / Bescheinigungen eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten

Tabelle 1: Kompetenzanforderungen an Prüfer

3.5.4 Aufrechterhaltung der fachlichen Kompetenz

Die prüfende Stelle muss ihre Anerkennungsgrundlage kontinuierlich aufrechterhalten (siehe Abschnitt 3.4.3). Die Prüfer müssen ihre Kompetenz kontinuierlich aufrechterhalten und dies gegenüber der prüfenden Stelle belegen.

Nachgewiesen werden kann die Aufrechterhaltung der branchenspezifischen Fachkompetenz beispielsweise durch den Besuch von „Erfahrungsaustausch-Tagen“

der DKG bzw. seiner Mitgliedsverbände. In Bezug auf die Aufrechterhaltung der „Speziellen Prüfverfahrenskompetenz zu §8a BSIG" wird eine Teilnahme an mindestens einer eintägigen Veranstaltung jährlich beim vom BSI anerkannten Schulungsanbietern empfohlen.

4 Durchführung der Prüfung

Der Nachweis nach §8a stellt gemäß BSIG ein Testat dar, also eine Zustandserfassung zum Zeitpunkt des Prüfereignisses. Die prüfende Stelle attestiert gegenüber dem BSI gemäß BSIG, dass der Betreiber die notwendigen Maßnahmen gemäß §8a (1) zur Absicherung der von ihm erbrachten kDL in angemessener Form ergriffen hat. Die Hauptmotivation des Gesetzgebers in Bezug auf §8a wird im Rahmen des B3S darin gesehen, dem BSI, und somit indirekt der Bundesregierung, ein signifikantes Lagebild zum Stand der Cyber-Gefährdungslage der Branche „medizinische Versorgung" zu ermöglichen und dort, wo schwerwiegende IT-Sicherheitsmängel unmittelbar erkennbar sind, im Einvernehmen bzw. im Benehmen mit den zuständigen Aufsichtsbehörden, regulativ einzugreifen.

Aufgrund der Heterogenität und Komplexität in der IT-Ausstattung der KRITIS-Betreiber „medizinische Versorgung" ist die Prüfung nach §8a immer als Schwerpunkt- bzw. Stichprobenprüfung zu sehen. Um hierbei ökonomische, wie fachliche Plan- und Vergleichbarkeit zu erreichen, soll die Prüfnachweisplanung i.d.R gemäß des aktuell zum Prüfzeitraum vom BAK „medizinische Versorgung" empfohlenen Prüfnachweisplaner-Tools erfolgen.

Durch eine Verkettung der Prüfungspläne zur Prüfung nach §8a über einen Zeitraum von vier Prüfperioden wird angestrebt, dem BSI ein möglichst umfassendes Prüf- und Lagebild in Bezug auf die kritische Infrastruktur „medizinische Versorgung" durch Kumulation der Prüfergebnisse über die der KRITIS zugerechneten Krankenhäuser zu ermöglichen.

4.1 Prüfungsvoraussetzung

Zur Prüfungsvorbereitung sind dem Prüfteam gemäß B3S zur Definition des Prüfplanes folgende Unterlagen zur Verfügung zu stellen:

- IT-Sicherheitsleitlinie
- IT-Sicherheitskonzept inkl. Meilensteinplanung
- Definition des betreiberspezifischen kDL-Scopes inkl. Risikoeinordnung gemäß B3S Teil 03 und Teil 04
- ISMS-Dokumentenübersicht gemäß B3S Teil 05
- Die Prüfpläne der vorangegangenen 4 Überprüfungen nach §8a (soweit durchgeführt), inkl. der an das BSI übertragenen Mängelliste sowie des Maßnahmenplans des KRITIS-Betreibers, der sich aus der jeweiligen, an das BSI gemeldeten Mängelliste ergeben hat.

Da es sich hierbei um IT-sicherheitstechnisch kritische Unterlagen handelt, ist die Geheimhaltungsverpflichtung der prüfenden Stelle und des Prüfteams vertraglich sicherzustellen.

Die Absicherung der kDL-relevanten IT-Systeme ist im Prüfprozess immer bezogen auf die Gesamtsicherheitskonzeption einer Einrichtung des Gesundheitswesens zu sehen. Das IT-Sicherheitskonzept bekommt daher in Bezug auf einen Nachweis nach §8a BSIG einen besonderen Stellenwert. Das IT-Sicherheitskonzept auf branchenspezifische Schlüssigkeit zu prüfen, ist im Sinne des B3S zentrales Anliegen und Prüfungsschwerpunkt eines branchenspezifischen Umsetzungsnachweises.

4.2 Festlegung des Prüftagekontingentes

Um eine möglichst planbare, strukturierte und in Bezug die Auswahl und die Belastbarkeit des Prüfergebnisses vergleichbare §8a-Prüfung für die Branche zu gewährleisten, strebt der B3S einen nach Fallzahlen, Fachbereichen und die IT-Komplexität erhöhenden Faktoren, wie Forschung- und Lehre, differenzierten, für Betreiber und prüfende Stelle verbindlichen Prüftageumfang an. Dieses nach Betreibergröße und Betriebskomplexität differenzierte Prüftagekontingent ergibt sich gemäß der aktuellen Empfehlung des BAK „medizinische Versorgung" bzw. aus dem jeweils vom BAK veröffentlichten, aktuellen Prüfnachweisplaner-Tool.

Die Festlegung der prüftagekontingentdefinierenden Fallzahl entspricht hierbei der Fallzahl gemäß Definition aus der jeweils aktuellen BSIG Verordnung. Die differenzierende Anzahl der Fachabteilungen entspricht der öffentlich zugänglichen Fachabteilungsstatistik gemäß veröffentlichtem Qualitätssicherungsreport des KRITIS-Betreibers. Das so ermittelte Prüftagekontingent darf vom Betreiber und der prüfenden Stelle in der Prüfplanerstellung nicht überschritten und höchsten um 5% unterschritten werden, soweit keine prüfungsverkürzenden Sachverhalte, wie z.B. eine entsprechend Zertifizierung nach ISO27001 oder BSI-Grundschutz usw. nachweisbar sind. Eine mögliche Unterschreitung des festgestellten Grundprüftagekontingentes auf Basis von vorgelegten Zertifikatsnachweisen oder Mehrfachprüfungssachverhalten (z.B. ein Rechenzentrum für mehrere KRITIS-Betreiber), ist durch die prüfende Stelle festzustellen und zu begründen.

4.3 Prüfplanfestlegung

Nach Vertragsabschluss mit der prüfenden Stelle, sind dem Prüfteam die geforderten Dokumente zur Prüfplanerstellung zur Verfügung zu stellen. Bei der Prüfplanerstellung ist zu differenzieren zwischen

- dem Formalteil (Prüfungskoordination/Nachweiserstellung),
- der formellen Dokumentenprüfung in Bezug auf das vorliegende ISMS und die gemäß Risikoanalyse definierten, kDL-relevanten IT-Systeme sowie
- der Vorortprüfung bzw. einem Realitätsabgleich.

Der formale und dokumentenzentrierte Teil der Prüfung soll hierbei ca. einen Zeitanteil von 35% des Gesamtprüfumfangs ausmachen. Der kDL-relevante und der

Vorort-Prüfungsanteil des Prüfplans ca. einen Umfang von 65% umfassen.

Um den Prüfplanerstellungsprozess und somit den Prüfrahmen auch über mehrere Prüfperioden hinweg nachvollziehbar und strukturiert zu gestalten, wird die Nutzung des vom BAK „medizinische Versorgung" zur Verfügung gestellte Prüfnachweisplaner-Tools als Koordinations-Tool in Bezug auf Prüfplanung, Prüfungsdurchführung und Prüfnachweis als Vertragsbestandteil mit der jeweiligen prüfenden Stelle dringend empfohlen.

Im Rahmen einer Prüfnachweisplanung mit Hilfe des BAK-Prüfnachweisplaner-Tools, wird eine differenzierte Prüfnachweisführung nach den Prüfungsschwerpunkten ISMS-Dokumentenprüfung, Basis-IT-Infrastrukturprüfung, Prüfung für die kDL-Erbringung besonders kritischer IT-Systemen sowie einer an die Betreibersituation angepassten Prüfung von für die kDL-relevanter aber minder kritischer IT-Systeme/Prüfsachverhalte gewährleistet.

4.4 Prüfungsdurchführung

Gemäß erstellter und an den Betreiber übermittelter Prüfplanung/ Prüfschwerpunktsetzung, erfolgt die Nachweisführung durch Dokumentensichtung und den Realitätsabgleich vor Ort.

4.5 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.

Als zugelassene Nachweise gelten insbesondere auch Nachweise in IT-Systemen zur Nachweisführung direkt (Log-Files, Berechtigungsmanagement-Systeme usw.), welche dem Prüfteam zugänglich gemacht werden. Ein Prüfteam ist in diesem Rahmen jedoch maximal zu lesendem Zugriff auf Systeme des Betreibers berechtigt bzw. sollte sich die Nachweisführung vom Betreiberpersonal in der Vorortprüfung vorzeigen lassen.

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

4.6 Prüffeststellung/Mängelliste

Das Prüfteam ist verpflichtet, den Prüfdurchführungsprozess gemäß der festgelegten

Prüfplanung zu dokumentieren. Es bietet sich an, die getroffenen Prüffeststellungen in strukturierter, nach der Schwere einer vom Prüfteam festgestellten IT-sicherheitsrelevanten Abweichung vom branchenspezifischen Stand der Technik zur IT-Absicherung der kDL differenzierten Art und Weise zu dokumentieren. Das Prüfteam kann dem Betreiber hierbei auch Empfehlungen zur Verbesserung des IT-Sicherheitsmanagement geben. An das BSI in der Prüfnachweisführung nach §8a letztlich zu übermitteln, sind jedoch nur die vom Prüfteam festgestellten, gravierenden und geringfügigen aber kDL-gefährdenden IT-Sicherheitsmanagementmängel.

Tabelle 2 definiert, wie die Begriffe „gravierender Mangel" und „geringfügiger Mangel" aus Sicht der Branche „medizinische Versorgung" in Bezug auf die Absicherung der kDL zu definieren sind.

Kategorie	Definition	Prüfbericht / Mängelliste
Schwerwiegender Mangel	die Schutzziele (Vertraulichkeit, die Integrität oder die Verfügbarkeit) der kDL wird vom Prüfteam als stark gefährdet angesehen. Nach Meinung des Prüfteams ist ein erheblicher Schaden zu erwarten.	Aufnahme in den Prüfbericht und Aufnahme in das Nachweisdokument
Geringfügiger Mangel	Das Prüfteam sieht das Erreichen der Schutzziele der kDL als beeinträchtigt an.	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.	Das Prüfteam kann während der Prüfung Empfehlungen aussprechen. Diese sind nicht Teil des Nachweisdokuments.

Tabelle 2: Mängelkategorien

Angaben zur Mängelbeseitigung sind in der Prüfnachweisführung gegenüber dem BSI im Rahmen der Übermittlung von Prüffeststellungen vom Betreiber oftmals nicht ad hoc in der Prüfnachweisführung darstellbar. Mängelbeseitigungsmaßnahmen sind – wenn überhaupt - zudem nur in nicht personalisierter und abstrakter Form möglich. Wichtig ist jedoch - je nach Ausprägung des Mangels - eine Stellungnahme zur Anerkennung und möglichst zeitnahen Behebung des vom Prüfteam festgestellten Mangels oder aber eine Begründung für die Abweisung dieser Prüfteam-Feststellung durch den Betreiber (siehe hierzu auch Abschnitt 4.7 Konfliktregelung).

Dieses Vorgehensmodell ist sinnvoll, da IT-Absicherungsmaßnahmen auch negative Auswirkungen auf die Erbringung der kDL haben können und somit budgetär, technisch und organisatorisch geprüft und abgestimmt werden müssen, bevor sie ergriffen werden können.

4.7 Konfliktregelung

Aufgrund der speziellen Branchengegebenheiten ist es nicht möglich, den prüfenden Stellen bzw. den Prüfteams auf Basis der Wahl der Prüfungsgrundlage ein weitgehend starres Bewertungsschema an die Hand zu geben. Die gewählte Prüfgrundlage ist somit im Branchenkontext als Referenzprüfgrundlage im Prüfungsgespräch bzw. in der Prüfnachweisführung zu verstehen und nicht als statische Prüfcheckliste. Eine Prüfung nach §8a ist demzufolge zu einem großen Teil von der subjektiven Bewertung durch das Prüfteam bestimmt, dem somit ein hohes Gewicht in Bezug auf die Nachweisführung nach §8a zukommt. Letzteres bedingt, das - neben Auditerfahrung und IT-technischer Fachkompetenz - insbesondere die Branchenkenntnis des Prüfteams von ausschlaggebender Bedeutung für eine sachgerechte Überprüfung ist.

Da es bei einem eher fachlich-qualitativ orientierten Prüfungsansatz zu unterschiedlichen Bewertungen der Risiken und der Wirksamkeit der gewählten IT-Absicherungsmaßnahmen durch KRITIS-Betreiber und Prüfteam kommen kann, soll die Festlegung und Übermittlung der geforderten „Mängelliste" an des BSI auch bei Meinungsverschiedenheiten zwischen Betreiber und Prüfteam möglichst konfliktfrei erfolgen. Ziel ist es, den Prüfprozess so effizient wie möglich zu gestalten und zu gewährleisten, dass sowohl KRITIS-Betreiber als auch prüfende Stellen bzw. das Prüfteam, die jeweilige Position in angemessener Form vertreten kann. Anstatt einer „Mängelliste" im Sinne einer kategorischen Mängelfeststellung durch das Prüfteam (schwerwiegender Mangel, geringfügiger Mangel), geht der vorliegende B3S von einer Darstellung der unterschiedlichen Bewertung von Betreiber und Prüfteam im Konfliktfall aus. Durch die Dokumentation der Prüfteam- und der Betreibersicht zu einer vom Prüfteam definierten Feststellung, ergibt sich für das BSI ein differenziertes, branchenfokussiertes Lagebild sowie die Möglichkeit einer problemadäquaten Bewertung des Sachverhaltes. Dieses Lagebild kann durch entsprechende Nachforderung von Detailinformationen und durch Nachfragen bei Betreiber und prüfender Stelle jederzeit durch das BSI verfeinert werden.

5 Nachweisdokument

Gegenüber dem BSI wird die Erfüllung der Anforderungen aus §8a (1) BSIG durch die Übermittlung von Nachweisdokumenten 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, müssen die in Tabelle 3 aufgeführten Formulare vom KRITIS-Betreiber vollständig ausgefüllt werden. Die Formulare - mit Ausnahme von Anlage PEB, welche eine sinnvolle Ergänzung in der Nachweisführung aber keine gesetzliche Verpflichtung des KRITIS-Betreibers darstellt - bilden zusammen die Nachweisdokumentation einer §8a Prüfung und müssen termingerecht vom KRITIS-Betreiber an das KRITIS Büro des BSI übermittelt werden.

Die für die §8a-Prüfung nach dem vorliegenden B3S gültigen Nachweisformulare befinden sich im Anhang des jeweilig aktuellen B3S Teil 06 Dokuments.

Information	Formular	Hinweise zur Bearbeitung
Angaben zur geprüften Kritischen Infrastruktur und zum Ansprechpartner	KI	vom KRITIS-Betreiber auszufüllen und zu unterschreiben
Angaben zur Eignung der prüfenden Stelle und zum Prüfteam	PS	von der prüfenden Stelle auszufüllen und zu unterschreiben
Angaben zur Prüfdurchführung	PD	von der prüfenden Stelle auszufüllen und zu unterschreiben
Angaben zum Prüfergebnis	PE	von der prüfenden Stelle auszufüllen und zu unterschreiben
Angaben zu aufgedeckten Sicherheitsmängeln	PEA	von der prüfenden Stelle auszufüllen und zu unterschreiben
Angaben zum Mängelbeseitigungsplan	PEB	vom Betreiber auf Basis von PEA zu erstellen und auf Anforderung an das BSI zu übermitteln

Tabelle 3: Information im Nachweisdokument und Formulare zur Erstellung

6 Anhang

6.1 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.

Angemessenheit und Gesamtbetrachtung: Neben der reinen Fachkompetenz des Auditors ist bei der Bewertung auch immer das Prinzip der Angemessenheit und Gesamtbetrachtung zu berücksichtigen. Es mögen isoliert betrachtete Lösungen nicht dem Stand der Technik entsprechen. Wenn diese jedoch durch andere Maßnahmen so abgefangen werden, kann dennoch in der Gesamtbetrachtung der Stand der Technik erreicht sein. Um diesem Grundsatz zu entsprechen, ist es notwendig, das Ziel hinter Maßnahmen zu erkennen und entsprechend der Erreichung dieses Zieles die Bewertung zugrunde zu legen und nicht allein auf der Bewertung einzelner, isolierter Maßnahmen zu bestehen.

6.2 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)
BAK	UP-KRITIS Branchenarbeitskreis

Begriff	Definition
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.
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 arbeitet. Hierzu gehört unter anderem auch die Geschäftsführung sowie Beauftragte der Geschäftsführung für den B3S (IT-Sicherheitsbeauftragte o.ä.). Außerdem Personen, die für Entwicklung, Verwirklichung oder Aufrechterhaltung der Schutzmaßnahmen verantwortlich sind.
Kompetenz	Angelernte Fähigkeit, die die Ausübung einer bestimmten Tätigkeit ermöglicht.
Kritische Dienstleistung (kDL)	Von einer Kritischen Infrastruktur erbrachte Dienstleistung
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

Begriff	Definition
	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.
Nachweis-dokument	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.
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.

6.3 Quellen

- Branchenspezifischer Sicherheitsstandard „medizinische Versorgung“, Teil 01-05 vom …
- Orientierungshilfe zum Nachweis gemäß §8a (3) BSIG Version 0.9.02 vom 30.06.2017
- BSI-Grundschutz 200-1
- DIN ISO 27001 usw.

6.4 Anhang Formulare zum Nachweisdokument

-

6.5 Link auf das aktuelle BAK Prüfnachweisplaner-Tool

-