Annika Woitke

Prüfgrundlagen nach § 8a

Welche Prüfgrundlagen gibt es und wer trifft die Entscheidung, welche zu nutzen ist?

Wer gemäß dem IT-Sicherheitsgesetz als Betreiber einer kritischen Dienstleistung anzusehen ist, muss geeignete Vorkehrungen gemäß „Stand der Technik" zur Vermeidung von Störungen an informationstechnischen Systemen, Komponenten und Prozessen treffen (§ 8a Abs. 1 BSIG) und dies dem BSI mindestens alle zwei Jahre nachweisen (§ 8a Abs. 3 BSIG). Für „KRITIS"-Unternehmen ist es daher empfehlenswert, ein Informationssicherheitsmanagementsystem einzuführen und zu pflegen, welches im Rahmen eines Audits geprüft werden kann. Der Beitrag stellt die hierzu notwendigen Schritte dar.

1 Einführung

Betreiber einer kritischen Dienstleistung (kDL) i. S. d IT-Sicherheitsgesetzes sind verpflichtet geeignete Vorkehrungen gemäß dem „Stand der Technik" zur Vermeidung von Störungen an informationstechnischen Systemen, Komponenten und Prozessen zu treffen (§ 8a Abs. 1 BSIG) und dies dem BSI mindestens alle zwei Jahre nachzuweisen (§ 8a Abs. 3 BSIG). Für „KRITIS"-Unternehmen ist es daher empfehlenswert, ein Informationssicherheitsmanagementsystem (ISMS) zum Nachweis der Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität ihrer kritischen Dienstleistungen einzuführen und zu pflegen. Dieses ISMS kann in einem Audit geprüft werden, um gegenüber dem BSI den erforderlichen Nachweis zu erbringen.

Wesentlich Frage dabei ist, auf welcher Prüfgrundlage dieses KRITIS-Audit stattfinden kann, denn im Gesetz werden keine speziellen Vorgaben für die Prüfung gemacht. Vielmehr beschränkt sich die Verpflichtung darauf, einen Nachweis über die Umsetzung gemäß dem Stand der Technik zu erbringen. Auf welche Weise dieser Nachweis erbracht wird, ist dabei der Entscheidung des jeweiligen Unternehmens in Abstimmung mit der prüfenden Stelle überlassen.

Doch obwohl sich die meisten Unternehmen im Kontext von Zertifizierungen und Audits erst einmal darüber freuen, keinen strengen Vorgaben folgen zu müssen, kann sich diese Entscheidung schwierig gestalten. Eine konkrete Definition von „Stand der Technik" gibt es nicht, inwieweit die eigene Einschätzung folglich der des Prüfers entspricht, ist völlig unklar.

Aus diesem Grund sieht das BSI drei Prüfgrundlagen vor.

- Es kann eine Prüfung auf Grundlage eines **B**ranchen**s**pezifischen **S**icherheits**s**tandards (sog. B3S) durchgeführt werden.
- Es kann eine eigene Prüfgrundlage genutzt werden, die alle relevanten Aspekte abdeckt. Dafür kann das Dokument: „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Abs. 2 BSIG" vom BSI, in Kombination mit einer klassischen Prüfgrundlage verwendet werden.
- Es kann ein Audit unter Berücksichtigung vorhandener Prüfungen bzw. Prüfgrundlagen durchgeführt werden, beispielsweise eine klassische Prüfgrundlage, wie die ISO/IEC 27001, in Kombination mit branchenspezifischen Vorgaben.

Dem Unternehmen ist es hingegen selbst überlassen, welche dieser Varianten es wählt. Tatsächlich muss die Prüfgrundlage nicht einmal zwingend identisch zu der Methodik sein, mit der das ISMS implementiert wurde, obwohl dies der Einfachheit wegen zu empfehlen ist. So kann beispielsweise die Methodik vom IT-Grundschutz zur Einführung des ISMS genutzt werden, die Prüfung aber nach ISO/IEC 27001 vorgehen.[1]

2 Prüfung mit B3S

Gehört das Unternehmen einer Branche an, zu der es einen anerkannten B3S gibt, scheint es naheliegend, diesen als Prüfgrundlage zu verwenden. Ein B3S beschreibt den Geltungsbereich und die jeweiligen branchenspezifischen Mindestanforderungen, die

Annika Woitke, M. Sc.

Beraterin Informationssicherheit bei der datenschutz nord GmbH

E-Mail: awoitke@datenschutz-nord.de

1 Abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/zertifizierung-von-managementsystemen_node.html;jsessionid=E2E14994A3CAF075CF7DB42DB7E11C5E.internet462 (letzter Abruf 1.5.2021).

zur Umsetzung gemäß dem „Stand der Technik“ erfüllt sein müssen. Das BSI hat hierzu Orientierungshilfen veröffentlicht, in denen die generellen Vorgaben zu den Inhalten, die ein B3S erfüllen muss, beschrieben sind. Der B3S ist nach der Feststellung der Eignung vom BSI für zwei Jahre gültig. Danach muss erneut geprüft werden, inwiefern die Beschreibungen und Maßnahmen im B3S noch dem aktuellen Stand der Technik entsprechen.

Zum aktuellen Zeitpunkt gibt es B3S für die Branchen Energie, Wasser, Ernährung, IT und TK, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr. Eine Übersicht vorhandener branchenspezifischer B3S ist auf der Website des BSI zu finden[2]. Es kann mehr als einen B3S für eine Branche geben. So gibt es beispielsweise für den Sektor Gesundheit drei verschiedene B3S, die jeweils eigene Aspekte innerhalb ihrer Branche abdecken: Labore, Arzneimittel und Impfstoffe sowie medizinische Versorgung (Krankenhaus).

Alle Unternehmen des jeweiligen Sektors können diesen Standard umsetzen, sofern dieser öffentlich zugänglich ist. Die aufgelisteten Anforderungen müssen sinngemäß auf die zu prüfenden Anlagen des Unternehmens abgebildet werden. Es ist allerdings im Vorfeld zu prüfen, ob der Geltungsbereich des B3S den des KRITIS-Betreibers vollständig abdeckt oder ob zusätzlich noch individuelle Maßnahmen zu treffen sind. Das Unternehmen muss selber entscheiden, ob der B3S eine angemessene Grundlage darstellt; die prüfende Stelle ist nicht dazu verpflichtet, eine Konformitätsbewertung des B3S vorzunehmen.

3 Eigene Prüfgrundlage

Soll die Prüfung ohne einen B3S durchgeführt werden, muss auf andere Weise sichergestellt sein, dass die § 8a Abs. 1 BSIG Anforderungen erfüllt sind. Dafür muss im Vorfeld eine geeignete Prüfgrundlage definiert und dokumentiert werden. Das Unternehmen entscheidet diese in Abstimmung mit der prüfenden Stelle, die daraufhin ein entsprechendes Prüfverfahren definieren kann. Als Anhaltspunkte dafür können die Vorgaben der bereits erwähnten B3S-Orientierungshilfe[3] gemäß § 8a Abs. 2 BSIG genutzt werden. Diese ist allerdings in erster Linie als Begleitung zur Erstellung eines eigenen Standards gedacht und stellt keine konkreten Vorgaben. Wird diese Variante gewählt, muss das Unternehmen daher selber Maßnahmen aus dieser Orientierungshilfe ableiten. Zudem können andere, vom BSI anerkannte, B3S dabei helfen, die notwendigen Anforderungen zu finden, wenn der Geltungsbereich entsprechend auf die eigene Branche angepasst wird. Auch Standards, wie ISO/IEC 27001, ISO/IEC 27001 auf Basis von IT-Grundschutz, der Kriterienkatalog C5 oder das NIST Cybersecurity Framework sind eine nützliche Orientierung.

4 Prüfung auf Basis vorhandener Prüfungen

Sofern ein Audit auf Basis vorhandener Prüfungen durchgeführt werden soll, dürfen bis zu einem Jahr alte Nachweise berücksichtigt werden. Ältere Dokumentationen können zwar in Form einer Dokumentenanalyse in die Prüfung einfließen, allerdings muss dennoch eine aktuelle Prüfung stattfinden, da sich der Umsetzungsstand im Laufe der Zeit bereits verändert haben könnte. Die Aspekte, die durch diese vorherigen Prüfungen nicht abgedeckt wurden, kommen dann in den Prüfplan für die neue Prüfung.

Entscheidend ist, dass der Geltungsbereich der kritischen Infrastruktur, die geprüft werden soll, vollständig abgedeckt und die dafür relevanten zusätzlichen Rahmenbedingungen alle berücksichtigt werden. Eine ISO/IEC 27001-Zertifizierung umfasst beispielsweise nicht zwingend den gesamten Geltungsbereich eines Unternehmens, sondern kann einen individuell angepassten Geltungsbereich haben, der die kritischen Dienstleistungen nicht vollständig abdeckt. Ein aktuelles ISO/IEC 27001-Zertifikat lässt sich daher nur als Nachweis verwenden, wenn dieses den gesamten Geltungsbereich der kritischen Dienstleitungen umfasst.[4]

Eine reine ISO/IEC 27001-Zertifizierung ersetzt allerdings keinen § 8a BSIG Nachweis, da die Berücksichtigung aller speziellen Anforderungen für kritische Dienstleistungen nicht sichergestellt ist. Sie kann daher lediglich als Teilnachweis genutzt werden, die speziellen Anforderungen für kritische Dienstleistungen müssen zusätzlich geprüft werden.[5]

Um welche speziellen Anforderungen es sich dabei handelt, wird im Folgenden näher erläutert.[6]

4.1 Spezielle Anforderungen einer § 8a-Prüfung

Eine kritische Infrastruktur muss neben den individuellen Schutzzielen des Unternehmens auch passende KRITIS-Schutzziele für die betriebenen kDLs berücksichtigen. Das primäre KRITIS-Schutzziel ist die Aufrechterhaltung der Versorgungssicherheit der Bevölkerung. Je nach Branche wird dieses Schutzziel in mehrere Teilziele aufgeteilt, um die Versorgungssicherheit in dem jeweiligen Bereich erreichen zu können, wie beispielsweise die Ausfallsicherheit von IT- und Kommunikationssystemen. Diese Schutzziele sind in die Risikobetrachtung aufzunehmen und in allen Prozessen und Maßnahmenumsetzungen zu betrachten.

Im Vergleich zu einer reinen ISO/IEC 27001 oder einer ähnlichen Zertifizierung, müssen die damit zusammenhängenden Risiken deutlich strenger bewertet werden. So muss die Vermeidung von Versorgungsengpässen bei kritischen Dienstleistungen, im Hinblick auf das primäre KRITIS-Schutzziel – die Versorgungssicherheit der Bevölkerung – eine kritischere Bewertung erhalten, als bei einem Unternehmen, das nicht unter die „KRITIS“-Verordnung fällt. Bei der Bestimmung des Schutzbedarfs und bei der darauffolgenden Risikoanalyse muss das Risikoausmaß für die Bevölkerung abgewogen werden.

Ein gravierender Unterschied zu einer herkömmlichen Zertifizierung ist, dass es keine dauerhafte Risikoakzeptanz geben darf,

2 Abrufbar unter https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Uebersicht-der-B3S/uebersicht-der-b3s_node.html (letzter Abruf 1.5.2021).

3 Abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/b3s_Orientierungshilfe_1_0.pdf?__blob=publicationFile&v=1 (letzter Abruf 1.5.2021).

4 Siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Orientierungshilfe_8a_3_v11.pdf?__blob=publicationFile&v=5, Kapitel 5.1.3 (letzter Abruf 1.5.2021).

5 Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Orientierungshilfe_8a_3_v11.pdf?__blob=publicationFile&v=5, Kapitel 5.1 (letzter Abruf 1.5.2021)

6 Siehe hierzu ergänzend bei *Mangels*, DuD 2021, Heft 9, dieses Heft.

solange noch wirtschaftliche vertretbare Maßnahmen zur Risikominderung getroffen werden können. Erst wenn bereits mehrere Maßnahmen zur Reduzierung des Schadensausmaßes getroffen wurden, kann ein eventuell weiterhin bestehendes Restrisiko akzeptiert werden. Dies geschieht in Abstimmung mit den notwendigen Beteiligten, wie Geschäftsführung, Informationssicherheitsbeauftragten etc. Handelt es sich nachweislich um Risiken, die mit der kDL des KRITIS-Betreibers nicht zusammenhängen, ist eine dauerhafte Risikoakzeptanz möglich. In einem Audit muss dies allerdings nachvollziehbar belegt werden können.

Aufgrund dessen, dass bei einem „KRITIS"-Unternehmen der störungsfreie Betrieb der kritischen Dienstleistung entscheidend ist, müssen die Maßnahmen zur Risikominderung aktiv den Schutzzielen (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität) dienen. Das Abschließen einer Versicherung gegen Schäden ist beispielsweise keine akzeptable Maßnahme für ein KRITIS-Unternehmen, da dies bloß die wirtschaftlichen Schäden abdecken würde. Ein mehrfach redundantes Rechenzentrum dagegen wäre eine geeignete Maßnahme zur Wahrung der Verfügbarkeit der Dienstleistung.

Ein Unternehmen, welches eine kritische Dienstleistung betreibt und somit unter § 8a BSIG fällt, hat eine Frist von zwei Jahren, um seine technischen und organisatorischen Vorkehrungen gegenüber dem BSI nachzuweisen. Im IT-Sicherheitsgesetz ist nachzulesen, welche Schwellenwerte die einzelnen Sektoren erreichen müssen, um als „KRITIS" zu gelten. Vergrößert ein Unternehmen, das ursprünglich nicht die Schwellenwerte erreicht hatte, sein Tätigkeitsfeld, beispielsweise durch den Ausbau einer Abteilung, kann es dadurch den notwendigen Wert erreichen, um als KRITIS zu gelten.

Ein Krankenhaus zum Beispiel, das durch einen Umbau mehr stationäre Patienten behandeln kann, hätte demzufolge nach Ablauf der zweijährigen Frist dem BSI ihren Stand der Technik als Nachweis zu erbringen. Die Frist beginnt nach Vollendung der Umbaumaßahmen. Kann diese Frist nicht eingehalten werden, oder konnten Maßnahmen einer vorherigen Prüfung nicht rechtzeitig umgesetzt werden, besteht die Möglichkeit, den Dialog zum BSI zu suchen. Werden die Fristen ohne Angabe von Gründen oder Austausch mit dem BSI nicht eingehalten, ist mit Bußgeldern von Seiten des BSI zu rechnen.[7]

4.2 Vorteile eines B3S

Im Anbetracht der Anforderungen an eine § 8a–Prüfung, erscheint ein vorhandener B3S die einfachste Wahl als Prüfgrundlage zu sein: Ein Dokument, das genau auf die eigene Branche angepasst ist und alle erforderlichen Anforderungen übersichtlich auflistet. Der KRITIS-Betreiber hat keinen Aufwand damit, sich eine Prüfgrundlage zusammenzusuchen und muss nicht befürchten, versehentlich zu viele oder zu wenige Anforderungen erfüllt zu haben.

Zudem ist die Praktikabilität eines B3S ein ausschlaggebender Vorteil für das zu auditierende Unternehmen. Der B3S vermittelt die Sicherheit, die branchenspezifischen Anforderungen und somit die Best Practices der jeweiligen Branche vollständig berücksichtigt zu haben. Die Maßnahmen, die in ihrer Kritikalität als verpflichtend („Muss") oder als optional („Soll" oder „Kann") gekennzeichnet sind, wurden bereits mit Erfolg in der Praxis getestet und geben dem Unternehmen einen hilfreichen Leitfaden.

5 Erstellung eines B3S

Doch was ist mit den Betreibern kritischer Infrastrukturen, die Branchen angehören, zu denen es noch keine anerkannte B3S gibt? Die einfache Antwort „selber einen B3S erstellen" ist zweifelsfrei leichter gesagt als getan.

Zu beachten ist, ein B3S kann nur von Betreibern oder Branchenverbänden beim BSI eingereicht werden. Unternehmen eines gemeinsamen Sektors können also gemeinsam einen Standard erarbeiten. Dabei sollten jedoch zusätzlich interessierte Parteien eingebunden werden, die unterschiedliche Schwerpunkte und Blickwinkel einbringen, damit der B3S für eine Vielzahl von KRITIS-Betreibern der Branche anwendbar ist. Ziel sollte es sein, den B3S generisch zu erstellen, damit er möglichst für alle Branchenteilnehmer gelten kann. Die bereits erwähnte „*Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG*" dien hierbei als Leitfaden.[8]

Alle Anforderungen und Maßnahmen in dem B3S müssen möglichst explizit ausformuliert werden. Bei Verweisen auf bereits bestehende Vorgaben, wie anderen Standards, Normen oder Regelwerke, muss eine unmissverständliche Zuordnung möglich sein.

Wird ein Antrag auf Anerkennung eines B3S-Entwurfs beim BSI eingereicht, wird dieser am Maßstab der Orientierungshilfe sowie einer branchenspezifischen Betrachtung geprüft. Dafür stimmt das BSI sich mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe ab.[9] Ist die Eignung des B3S festgestellt, entsteht daraus ein anerkannter branchenspezifischer Sicherheitsstandard, der von jedem Unternehmen des Sektors angewandt werden kann.

Die Gebühren für die Eignungsprüfung und Abnahme durch das BSI sind in der *Besondere Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen* festgelegt.[10] Die Gebühren richten sich nach dem benötigten Zeitaufwand und sind unabhängig vom Ergebnis der Prüfung. Nach der Prüfung, listet das BSI die angefallenen Arbeitsstunden auf und stellt dem Antragsteller die Kosten in Rechnung.

Der B3S ist für zwei Jahre gültig und gilt als Stand der Technik. Danach muss er erneut zur Prüfung eingereicht werden. Gab es in der Zwischenzeit neue Erkenntnisse oder gravierende Änderungen in der Branche, muss der B3S überarbeitet und auf den neuesten Stand gebracht werden. Wird der B3S nicht erneut zur Prüfung eingereicht, kann die alte Version nicht mehr als Prüfgrundlage verwendet werden. Ein Unternehmen mit einer kritischen Dienstleistung muss entweder einen anderen B3S seiner

7 Vgl. bei *Kipker/Scholz*, DuD 2021, S. 40.

8 Abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/b3s_Orientierungshilfe_1_0.pdf?__blob=publicationFile&v=1 (letzter Abruf 1.5.2021).

9 Siehe unter https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Eignungspruefung-von-B3S/eignungspruefung-von-b3s_node.html

10 Siehe unter https://www.gesetze-im-internet.de/bmibgebv/BJNR135900019.html (letzter Abruf 1.5.2021).

Branche auswählen oder eine Prüfung ohne eine B3S-Grundlage durchführen.

6 Anforderungen in einem B3S

Vom BSI gibt es grundsätzliche Kriterien an einen B3S. Demzufolge müssen die Maßnahmen dem Stand der Technik entsprechen – das heißt, sie müssen mit Erfolg in der Praxis und innerhalb der jeweiligen Branche erprobt sein. Ausschlaggebend ist zudem, dass diese Erprobung nicht so lange her sein darf, dass dieser Stand bereits veraltet sein könnte. Darüber hinaus müssen branchenspezifische Gegebenheiten berücksichtigt werden. Das bedeutet beispielsweise, dass Medizingeräte im Gesundheitswesen vor Ausfällen geschützt sein müssen, weil ein Ausfall oder eine Störung dieser Geräte die kritische Dienstleistung massiv einschränken und gefährden würde. Alle Maßnahmen müssen effektiv wirken, keine negativen Auswirkungen haben und der Aufwand für die Maßnahmen sollte im Verhältnis zum Schadensausmaß in der Bevölkerung stehen. Das Schadensausmaß ist dabei jenseits von betriebswirtschaftlichen Aspekten zu berücksichtigen.

Bei näherer Betrachtung der öffentlich zugänglichen, vom BSI anerkannten branchenspezifischen B3S, fällt auf, dass sich deren Mindestanforderungen inhaltlich stark ähneln. Obwohl die Branchen selbstverständlich unterschiedliche Schwerpunkte haben und die Maßnahmen dementsprechend ausgerichtet sind, ist das Grundgerüst meistens eng an die ISO/IEC 27001 oder dem IT-Grundschutz angelehnt. Diese Tatsache kann die Arbeit mit diesen Standards enorm erleichtern, da ein Zurechtfinden in den bereits vertrauten Strukturen erleichtert wird. Der Ursprung dieses Grundgerüsts liegt in der bereits erwähnten Orientierungshilfe vom BSI. Im Gegensatz zu den ISO-Standards, werden die B3S bei ihren Mindestanforderungen allerdings deutlich konkreter und lassen viel weniger Interpretationsspielraum. Folgende Struktur ist erkennbar:

- **Geltungsbereich**
  Es wird zunächst darauf hingewiesen, dass der Betreiber der kritischen Infrastruktur seinen Geltungsbereich abstecken muss und dieser mindestens die kritische Dienstleistung sowie falls notwendig, auch extern erbrachte Leistungen umfassen muss.
- **Gesetzlicher Rahmen**
  Danach folgt eine Beschreibung zum gesetzlichen Rahmen, der die jeweilige Branche umfasst.
- **Schutzziele**
  Die Schutzziele, als Maßgabe für die Schutzbedarfsfeststellung und der Risikoanalyse, die später noch genannt werden, werden aufgelistet. Dabei handelt es sich in jedem B3S um die Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität. Teilweise werden Integrität und Authentizität gleichgesetzt, je nach Ausrichtung der Branche des B3S. In der Orientierungshilfe wird zudem empfohlen, auch branchenspezifische Schutzziele zu definieren. In den bisher freigegebenen B3S hat diese Empfehlung allerdings noch keine Anwendung gefunden, da sich die branchentypischen Gefährdungen bereits durch die vorhandenen Schutzziele abdecken lassen.
- **Gefährdungen**
  Es werden die Gefährdungen analysiert, die auf das Unternehmen wirken können. In der Orientierungshilfe wird empfohlen, sich dabei an den elementaren Gefährdungen des BSI zu orientieren, was alle bisher vorhandenen B3S auch tatsächlich tun.[11] Ergänzend werden die branchenspezifischen Gefährdungen aufgelistet.
- **Bedrohungen und Schwachstellen**
  Die Orientierungshilfe schreibt vor, Bedrohungen und Schwachstellen zu benennen und deren Relevanz, im Hinblick auf die Branche und die KRITIS-Schutzziele, zu bewerten. Im Rahmen dessen gibt es bei den B3S hingegen leichte Unterschiede in der Vorgehensweise. Die meisten Standards nennen entweder im selben Kapitel oder im Anhang eine Liste von Schwachstellen für ihren Sektor sowie von branchenspezifischen Gefahren. Manche Standards verweisen allerdings darauf, dass sich die Angriffsszenarien ständig ändern und dass daher auf eine explizite Beschreibung und Benennung von Bedrohungsszenarien und Schwachstellen verzichtetet wird.
- **Risikomanagement**
  Jeder B3S enthält ein umfassendes Kapitel zum Risikomanagement, in dem sowohl die Risikoidentifikation und -beurteilung, als auch die Risikobehandlung gefordert werden. Die Anforderung der Orientierungshilfe ist, dass diese Schritte nachvollziehbar dokumentiert, aktualisiert und in regelmäßigen Abständen auf Vollständigkeit und Fehlerlosigkeit geprüft werden müssen. Einige Branchen-B3S verweisen in diesen Kapiteln vollständig auf die ISO/IEC 27001, die in ihren Kapiteln 6.1, 6.2 und 8 die Kriterien für ein Risikomanagement vorgibt, und ergänzen nur das konkrete Vorgehen dabei. So werden spezifische Handlungsschritte und Beispiele genannt, die bei der Risikoidentifikation und -behandlung helfen können. Zudem wird in den B3S betont, dass Risiken, die zum Ausfall oder einer Störung der kritischen Dienstleistung führen, mit absoluter Priorität zu behandeln sind. Wie in der Orientierungshilfe vorgeschlagen, wird zudem in den Kapiteln zum Risikomanagement explizit darauf hingewiesen, dass Abhängigkeiten zwischen IT-Systemen des eigenen Unternehmens und denen von Dritten als Risikofaktor zu berücksichtigen sind. Ebenso wird in jedem B3S betont, dass die allgemeine Gefährdungslage und deren potentielle Weiterentwicklung zu beschreiben und bei der Wahl der Risiken einzubeziehen sind.
- **Branchentypische Themen**
  Die „typischen abzudeckenden Themen", wie sie in der Orientierungshilfe genannt werden, sind in jedem B3S vorzufinden. Die ersten vier Themen sind die Kernaspekte, in die am meisten Zeit investiert werden sollte. Die sodann folgenden Themenfelder nehmen, je nach Branche, einen größeren oder kleineren Umfang ein, jedoch sind ausnahmslos alle Punkte in jedem B3S vertreten:
  - Informationssicherheitsmanagementsystem (ISMS)
  - Asset Management
  - Risikoanalysemethoden
  - Continuity Management
  - Notfallmanagement und Übungen
  - Branchenspezifische Technik
  - Technische Informationssicherheit (Maßnahmenkategorien)
  - Personelle und organisatorische Sicherheit
  - Bauliche/physische Sicherheit

11 Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Elementare_Gefaehrdungen.pdf?__blob=publicationFile&v=4 (letzter Abruf 1.5.2021)

- Vorfallserkennung und -bearbeitung
- Überprüfung im laufenden Betrieb
- Externe Informationsversorgung und Unterstützung
- Lieferanten, Dienstleister und Dritte

7 Ablauf einer Prüfung mit einem B3S als Prüfgrundlage

In einem externen Audit überprüft ein unabhängiges Prüfteam die Umsetzung der Maßnahmen der jeweils gewählten Prüfgrundlage. Hat das Unternehmen sich, in Abstimmung mit der prüfenden Stelle, für einen B3S entschieden, wird dieser als Rahmenkonstrukt für das Audit verwendet. Dabei wird prinzipiell nur der Grad der Umsetzung, und nicht die Eignung des B3S als Prüfgrundlage bewertet. Die prüfende Stelle kann den B3S als Referenzdokument heranziehen, um die einzelnen Maßnahmen durchzugehen. Es muss ein Branchenexperte in dem Prüfteam vertreten sein.

Zu Beginn des Audits wird überprüft, ob der Geltungsbereich der kritischen Dienstleistung passend gewählt ist. Sind beispielsweise Prozesse oder IT-Systeme, die zum Betrieb der kritischen Dienstleistung notwendig sind nicht vollständig im Geltungsbereich, sollte der Betreiber diesen entsprechend ausweiten. Zudem ist zu prüfen, ob der B3S alle individuellen Gegebenheiten des Unternehmens abdeckt. Da der B3S nur branchentypische Gegebenheiten ansprechen kann, sind die Vorgaben sinngemäß auf das Unternehmen anzuwenden. Sind nicht alle Gegebenheiten des KRITIS-Betreibers durch den B3S abgedeckt, ist zu prüfen, ob weitere individuelle Maßnahmen getroffen wurden.

Der Geltungsbereich sollte grafisch und übersichtlich dargestellt werden, sodass die Prüfer den Umfang und die Abhängigkeiten zu anderen Komponenten und Prozessen gut erkennen können. Danach wird eine Beschreibung der Anlagen und Komponenten der kritischen Dienstleistung erfragt, die möglichst gut nachvollziehbar für die Prüfer ist. Infolgedessen, dass Audits üblicherweise vor Ort bei dem Unternehmen stattfinden, kann stichprobenartig geprüft werden, ob diese Beschreibungen mit den Gegebenheiten vor Ort übereinstimmen. Ebenso wird in der Prüfung ein Netzstrukturplan gefordert, der die Kommunikationsschnittstellen zu externen Netzen, andere Standorte oder zu ausgelagerten Teilen der kritischen Dienstleistung umfassen.

Schließlich werden, genau wie in einem herkömmlichen Audit, die einzelnen Aspekte des B3S durchgegangen und die Maßnahmen aufgelistet, die das Unternehmen getroffen hat. Dazu dokumentiert der Prüfer, ob und in welchem Ausmaß die Maßnahmen umgesetzt sind. Entdeckt die prüfende Stelle Abweichungen vom Standard, wird dies entweder als schwerwiegender Sicherheitsmangel, als geringfügiger Sicherheitsmangel oder als Empfehlung klassifiziert. Sind keine Abweichungen zu finden, wird dies als „Keine Abweichung" vermerkt. Besonders gute Umsetzungen von Maßnahmen können positiv hervorgehoben werden. [12]

Nach dem Audit erstellt der KRITIS-Betreiber eine Mängelliste, in der die Sicherheitsmängel, die im Audit aufgedeckt wurden, mit ihrer Klassifizierung, einer Risikobetrachtung und einem Umsetzungsplan aufgelistet werden. Diese muss im Anschluss an das Audit beim BSI eingereicht werden, um den Nachweis über die Umsetzung der technischen und organisatorischen Maßnahmen zu erhalten.[13]

8 Ablauf einer Prüfung mit der Orientierungshilfe als Teilnachweis

Die Aspekte der Orientierungshilfe können in die Kapitel des Hauptnachweises eingegliedert werden. Ist der Hauptnachweis beispielsweise eine ISO/IEC 27001-Zertifizierung, werden die Maßnahmen der Orientierungshilfe innerhalb der Kapitel 4-10 sowie des Annex untergebracht und im Rahmen der Prüfung des jeweiligen Kapitels mit abgefragt. Alternativ können die Aspekte der Orientierungshilfe im Anschluss an die Themen des Hauptnachweises abgefragt werden. In diesem Fall würden allerdings viele Themen redundant besprochen werden, was mehr Zeit in Anspruch nimmt.[14]

9 Ausblick

Mit der Zunahme der B3S für verschiedene Branchen in den letzten Jahren, hat sich der Kreis der KRITS-Unternehmen, die auf diese Art der Prüfgrundlage zurückgreifen können, deutlich vergrößert. Auch wenn ein B3S nie eine verpflichtende Grundlage bilden wird, so ist sie für viele Unternehmen die bevorzugte Wahl, die das Umsetzen der technischen und organisatorischen Maßnahmen gemäß dem Stand der Technik erheblich vereinfacht.

Aufgrund der Komplexität des Prozesses zur Erstellung und Einreichung eines B3S bleibt abzuwarten, ob sich in Zukunft für jede Branche ein eigener Standard finden lässt. Die Praxis zeigt, dass eine § 8a-Zertifizierung mithilfe einer herkömmlichen Zertifizierung in Ergänzung mit der Orientierungshilfe vom BSI, für viele KRITIS-Betreiber eine äquivalent nützliche Prüfgrundlage bildet, wie es ein B3S ermöglicht.

Klare Empfehlung ist es, bei einer Prüfung dieselbe Methodik wie bei der Einführung des ISMS einzusetzen. Handelt es sich dabei nicht um eine Zertifizierung, die alle § 8a-Aspekte abdeckt, muss diese allerdings entsprechend den Anweisungen der Orientierungshilfe ergänzt werden.

12 Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Orientierungshilfe_8a_3_v11.pdf?__blob=publicationFile&v=5 (letzter Abruf 1.5.2021)

13 Hierzu bei *Atug*, DuD 2020, S. 668.

14 Ebenso *Mangels*, DuD 2021, Heft 9, dieses Heft.