Fabian Mangels

KRITIS zu Zeiten einer Pandemie

Was sollten Betreiber beachten?

Gerade in Zeiten einer anhaltenden Pandemie – zweifellos auch außerhalb eines solchen Ausnahmeszenarios – ist es aufgrund einer nachweislich erhöhten Abhängigkeit von Informationstechnologie (IT) wichtig, Informationssicherheitsmaßnahmen so weit wie möglich aufrechtzuerhalten, umzusetzen, sie an neue Gegebenheiten anzupassen und kontinuierlich weiterzuentwickeln. Dies betrifft insbesondere die Betreiber Kritischer Infrastrukturen (KRITIS). Der Beitrag zeigt auf, welche Maßnahmen hierbei zu ergreifen sind.

1 Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im vergangenen Jahr 2020 zwei Cyber-Sicherheitswarnungen (CSW 2020-190290-1013[1], CSW 2020-199453-1013[2]) herausgegeben, die die Auswirkungen des Corona-Virus SARS-CoV-2 auf die IT-Sicherheitslage analysieren. Das BSI wies in diesem Zusammenhang vor allem auf eine steigende Anzahl von Schadprogrammen sowie DDoS- (Distributed-Denial-of-Service) und Social Engineering-Angriffen hin. Weiterhin enthielten die CSW Hinweise und Maßnahmen zur Absicherung von VPN-Zugängen, die für einen Fernzugang auf Unternehmensnetzwerke durch das verstärkte Arbeiten im Homeoffice essentiell sind.

Die Bundesregierung definiert KRITIS in ihrer nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) wie folgt: „Kritische Infrastrukturen (KRITIS) sind 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".[3] KRITIS sind demzufolge für die Allgemeinheit bedeutsame und notwendige Basisdienste, welche besonders schützenswert anzusehen sind, bspw. betrifft dies die zuverlässige Stromversorgung industrieller Produktionsanlagen sowie die generelle Energie- und Wasserversorgung von Gebäuden, die stetige Trinkwasser- sowie Nahrungsversorgung der Bevölkerung und funktionstüchtige Informations- und Kommunikationstechnik für Bankgeschäfte oder das Versicherungswesen. Ohne ein intaktes Transportwesen würden Waren, wie Treib- und Brennstoffe für Kraftfahrzeuge und Heizungsanlagen, und jedwede Dienstleistungen weder zur Fertigung noch zum Absatzmarkt kommen. Natürlich zählen auch Einrichtungen und Organisationen des Gesundheitsbereichs zu KRITIS, damit auch die Bereitstellung dieser zwingend notwendigen Dienstleistungen in hoher Qualität und Stabilität für die Bevölkerung in der Bundesrepublik Deutschland gewährleistet werden können.[4]

2 Sektoren

KRITIS werden in neun Sektoren aufgeteilt, welche wiederum aus 31 Branchen bestehen. Unterschieden werden Organisationen und Einrichtungen unabhängig ihrer privatwirtschaftlichen oder öffentlich-rechtlichen Rechtsform aus den Sektoren Energie, Gesundheit, Informationstechnik und Telekommunikation, Transport und Verkehr, Medien und Kultur, Wasser, Finanz- und Versicherungswesen, Ernährung sowie Staat und Verwaltung. Diese KRITIS-Sektoren mit zugeordneten Branchen bilden eine wesentliche Grundlage für das Funktionieren der Gesellschaft. Die Sektoren Medien und Kultur sowie Staat und Verwaltung werden allerdings nicht weiter durch das IT-Sicherheitsgesetz (IT-SiG) reguliert.[4]

1 BSI, „Auswirkungen von SARS-CoV-2 (Corona) auf die IT-Sicherheitslage," 20. März 2020, https://www.bve-online.de/download/corona-bsi-analyse (letzter Abruf 1.7.2021).

2 BSI, „Strategische Auswirkungen der COVID-19-Pandemie auf die IT-Sicherheitslage Deutschlands," 7. April 2020, https://www.bve-online.de/download/corona-bsi-aktuellelage-080420 (letzter Abruf 1.7.2021).

3 BMI, „Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)", 17. Juni 2009, S. 3 https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3 (letzter Abruf 1.7.2021).

4 Vgl. BBK & BSI, „Kritische Infrastrukturen – Definition und Übersicht", 2021, https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html; BSI, „Was sind Kritische Infrastrukturen?", https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html; OpenKRITIS, „Kritische Infrastrukturen," 2021, https://www.openkritis.de/it-sicherheitsgesetz/index.html (letzter Abruf 1.7.2021).

Fabian Mangels, M.Sc.

Berater Informationssicherheit bei der datenschutz nord GmbH

E-Mail: fmangels@datenschutz-nord.de

Im neuen IT-SiG 2.0 werden die Sektoren Entsorgung und Unternehmen im besonderen öffentlichen Interesse (UNBÖFI) zusätzlich mit aufgenommen.[5]

3 Rechtsgrundlage

Die KRITIS-Rechtsgrundlage besteht aus mehreren, zusammengehörigen Gesetzen und Verordnungen auf europäischer und nationaler Ebene: NIS-Richtlinie, IT-Sicherheitsgesetz, BSI-Gesetz und BSI-Kritisverordnung.

Das im August 2009 in Kraft getretene Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)[6] bildet die Rechtsgrundlage für Kritische Infrastrukturen und deren Betreiber. Konkretisierungen bzgl. der Umsetzung des BSIG und die Definition Kritischer Infrastrukturen werden in der zugehörigen Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)[7] getroffen. Die BSI-KritisV ordnet u. a. Unternehmen verschiedener Branchen KRITIS-Sektoren zu und legt Schwellenwerte zur Bestimmung fest, ob es sich bei einem Betreiber um eine Kritische Infrastruktur handelt oder eben nicht.

Das seit Juli 2015 wirksame Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz – IT-SiG)[8] erweitert als Artikelgesetz das BSIG neben noch anderen bestehenden Gesetzen, wie u. a. dem Energiewirtschaftsgesetz (EnWG), Atomgesetz (AtG), Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) und BKA-Gesetz (BKAG).

Auf europäischer Ebene wurde im Juli 2016 die EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie)[9] veröffentlicht. Die darin geforderten Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus waren mit dem 2015 in Kraft getretenen IT-SiG in Deutschland bereits nahezu in nationales Recht überführt worden, so dass im Juni 2017 das NIS-Richtlinien-Umsetzungsgesetz verabschiedet werden konnte.

Der erste Teil der BSI-KritisV zur Umsetzung des IT-SiG trat im Mai 2016 für Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung in Kraft.

Durch die im Juni 2017 veröffentlichte erste Änderungsverordnung der BSI-KritisV, wurden schließlich auch die Unternehmen aus den Sektoren Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr zur Umsetzung des IT-SiG verpflichtet.[10]

Das neue IT-SiG 2.0, welches voraussichtlich noch im Jahr 2021 in Kraft treten wird, erweitert die deutsche KRITIS-Regulierung zusammen mit der BSI-KritisV 2.0 umfangreich, sodass deutlich mehr Pflichten für Betreiber und mehr Befugnisse für den Staat entstehen.[11]

4 Betreiber von Anlagen

Die Versorgungssicherheit der Gesellschaft und Wirtschaft in den KRITIS-Sektoren soll durch die Regulierungen des IT-SiG mit dem BSIG und der BSI-KritisV in der Bundesrepublik Deutschland gewährleistet werden. Davon betroffen sind Einrichtungen und Organisationen der sieben Sektoren aus den §§ 2 bis 8 der BSI-KritisV, welche kritische Dienstleistungen gemäß § 1 Abs. 3 BSI-KritisV in eigenen Anlagen erbringen und dabei definierte Schwellenwerte der Verordnung überschreiten. Sie sind dann Betreiber Kritischer Infrastrukturen gemäß § 10 Abs. 1 BSIG und müssen den Verpflichtungen, wie die Umsetzung von Sicherheitsmaßnahmen, Vorfallmeldungen und Prüfungen, nachkommen.

Im § 2 Abs. 10 BSIG ist definiert, dass nur Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen anzusehen sind, die eine hohe Bedeutung für das Funktionieren des Gemeinwesens haben. Ein bedeutender Versorgungsgrad ist durch das Erreichen oder Überschreiten von den in der BSI-KritisV aufgeführten Schwellenwerte pro Anlage abhängig. Die Verordnung nimmt für die Versorgungssicherheit der Bevölkerung grundsätzliche eine Kenngröße von 500.000 versorgten Personen pro Anlage. Die Schwellenwerte sind dabei die für 500.000 Personen umgerechnete Leistung pro Anlage, basierend auf einem Durchschnittsverbrauch pro Person.

Betreiber erbringen die konkrete Ausgestaltung kritischer Dienstleistungen in KRITIS-Anlagen, welche in die sieben Sektoren als Anlagenkategorien aufgeteilt und im Anhang der BSI-KritisV definiert sind. Die Anlagen dienen Betreibern zur Identifikation der eigenen KRITIS-Betroffenheit und der anschließend notwendigen Festlegung des Geltungsbereichs im Unternehmen. Betreiber müssen unabhängig vom BSI, als zuständige Cyber-Sicherheitsbehörde, Anlagen als KRITIS erkennen sowie registrieren.[4, 12]

5 Pflichten

Unternehmen, die KRITIS-Sektoren zuzuordnen sind und Anlagen besitzen, welche die Schwellenwerte als Kritische Infrastruk-

5 Vgl. *Kipker/Scholz*, DuD 2021, S. 40.

6 BMJV, „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)", 14. August 2009, https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html (letzter Abruf 26.7.2021).

7 BMJV, „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)", 22. April 2016, https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html (letzter Abruf 26.7.2021).

8 BGBl, „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)", 17. Juli 2015, S. 1324, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1622561974541 (letzter Abruf 26.7.2021).

9 ABl, EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, 6. Juli 2016, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016L1148 (letzter Abruf 26.7.2021).

10 Vgl. BSI, „Rechtsgrundlagen: NIS-Richtlinie, IT-Sicherheitsgesetz, BSI-Gesetz, BSI-Kritisverordnung", 2021, https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Rechtsgrundlagen/rechtsgrundlagen_node.html; OpenKRITIS, „KRITIS-Gesetzgebung", 2021, https://www.openkritis.de/it-sicherheitsgesetz/gesetzgebung-kritis-bsig.html (letzter Abruf 26.7.2021).

11 Vgl. *Kipker/Scholz*, DuD 2021, S. 40.

12 Vgl. BSI, „Pflichten für KRITIS-Betreiber", 2021, https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Pflichten-fuer-KRITIS-Betreiber/Pflichten-fuer-KRITIS-Betreiber_node.html; OpenKRITIS, „KRITIS-Betreiber", 2021, https://www.openkritis.de/betreiber/index.html; OpenKRITIS, „KRITIS-Anlagen", 2021, https://www.openkritis.de/it-sicherheitsgesetz/kritis-anlagen.html (letzter Abruf 26.7.2021).

tur überschreiten, unterliegen den Pflichten des BSIG (§§ 8a bis 8c) und der BSI-KritisV. Die Pflichten beinhalten die mögliche Identifikation als KRITIS und anschließende Registrierung beim BSI mit einer Kontaktstelle, Meldepflichten, die Festlegung des Geltungsbereichs, die Umsetzung von Informationssicherheitsmaßnahmen nach dem Stand der Technik und regelmäßige Prüfungen als Nachweis des Umsetzungsstands der Informationssicherheitsmaßnahmen.

Ähnlich wie die Verankerung der Informationssicherheit in einem Unternehmen, bspw. durch die Etablierung eines ISMS (Information Security Management System) nach ISO/IEC 27001, muss auch die Verantwortung für die Umsetzung der Pflichten für KRITIS-Betreiber durch die Geschäftsführung getragen werden. Die Durchführung kann hingegen durch die Geschäftsführung delegiert werden.[10]

5.1 Identifikation

Betreiber sind für die Identifikation von KRITIS-Anlagen und die Feststellung der eigenen Betroffenheit selbst verantwortlich. Die möglichen Anlagen müssen kritische Dienstleistungen in einem der festgelegten KRITIS-Sektoren zur Versorgung der Bevölkerung erbringen. Für die Analyse sind relevante Dienstleistungen und Sektoren in der BSI-KritisV definiert. Kritische Infrastrukturen befinden sich immer in einem der KRITIS-Sektoren; die Betreiber selbst können auch in anderen Sektoren tätig sein. Außerdem ist es wichtig, dass die Wertschöpfung der kritischen Dienstleistung in Anlagen auf deutschem Bundesgebiet stattfindet. Der Betreiber kann auch international tätig sein; entscheidend ist dabei aber der Standort einer Anlage. Eine umfangreiche Liste der KRITIS-Anlagen pro Sektor kann der BSI-KritisV entnommen werden. Als Anlage werden generell Betriebsstätten, Standorte oder sonstige ortsfeste Einrichtungen der kritischen Dienstleistung verstanden. Als weiteres Kriterium müssen Anlagen spezifische Schwellenwerte innerhalb eines Kalenderjahres überschreiten. Diese Schwellenwerte stehen ebenso in der BSI-KritisV. Betreiber müssen zudem das Überschreiten der Schwellenwerte fristgerecht erkennen und dem BSI jährlich melden. Die Ermittlung des Schwellenwertes einer Anlage für das zurückliegende Kalenderjahr muss grundsätzlich bis zum 31. März des Folgejahres geschehen. Bei einigen Anlagen sind auch abweichende Stichtage und Fristen in der Verordnung vermerkt.[13]

5.2 Registrierung

Werden von einem Betreiber schließlich Anlagen als Kritische Infrastruktur identifiziert, muss sich dieser selbst als KRITIS-Betreiber mit den dazugehörigen Anlagen fristgerecht bis zum 1. April des Folgejahres beim BSI registrieren. Der Austausch mit dem BSI zu Vorfällen und Meldungen der KRITIS-Anlagen erfolgt über eine einzurichtende Kontaktstelle sowie nach erfolgter Registrierung in einem Portal des BSI. Nach § 8b Abs 3 BSIG muss eine Kontaktstelle eingerichtet und registriert werden. Diese Kontaktstelle muss für das BSI jederzeit erreichbar sein, d. h. Betreiber müssen über die registrierte Kontaktstelle rund um die Uhr (24 / 7) ansprechbar und handlungsfähig sein. Die Registrierung als KRITIS-Betreiber und von KRITIS-Anlagen – im Formular als angeschlossene Infrastrukturen bezeichnet – erfolgt über ein Online-Formular des Melde- und Informationsportals (MIP)[14] beim BSI. Meldungen und Informationen werden über das Traffic Light Protokoll (TLP) ausgetauscht. Nach § 8b Abs. 5 können Betreiber neben einer eigenen Kontaktstelle dem BSI mit anderen KRITIS-Betreibern im selben Sektor auch eine gemeinsame übergeordnete Ansprechstelle (GÜAS) benennen. Der Informationsaustausch mit dem BSI geschieht dann hauptsächlich über diese GÜAS.[15]

5.3 Meldepflicht

Für KRITIS-Betreiber besteht nach § 8b Abs. 4 BSIG eine Meldepflicht, Informationen zu IT-Störungen, Angriffen und Vorfällen sind unverzüglich nach der Erkennung an das BSI weiterzuleiten. Für die Erstmeldung hat grundsätzlich Schnelligkeit vor Vollständigkeit Vorrang. Es sind zwei Arten von IT-Störungen zu unterscheiden, die die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit informationstechnischer Systeme, Komponenten oder Prozesse betreffen können. Erstens Störungen, die zum Ausfall oder erheblicher Beeinträchtigung der KRITIS-Anlage geführt haben. Zweitens erhebliche Störungen, die zum Ausfall oder erheblicher Beeinträchtigung der KRITIS-Anlage führen können. Als Leitfrage für eine solche Beurteilung sollte herangezogen werden, ob die (mögliche) Einschränkung relevant für die Versorgungslage der kritischen Dienstleistung ist. Die Störungsmeldungen werden über das MIP vom BSI nach dem TLP übermittelt und können mit S/MIME (Secure / Multipurpose Internet Mail Extensions) oder PGP (Pretty Good Privacy) verschlüsselt werden. Inhalte für die Meldung, wie die Beschreibung des Vorfalls, möglicher Ursachen und der Ausfall von Anlagen oder Dienstleistungen, werden in Online-Formularen abgefragt. Der weitere Ablauf nach Absenden der Erst- und Folgemeldungen hängt vom Verlauf der Störung beim Betreiber sowie dem konkreten Sachverhalt ab. Eine Bewältigung der Störung kann durch den Betreiber selbst oder durch externe Dienstleistung erledigt werden und / oder es erfolgt eine Einbindung weiterer Behörden zur Strafverfolgung. Das BSI wertet eingereichte Störungen in einem KRITIS-Lagebild aus und gibt, wenn notwendig, Warnmeldungen an andere Betreiber heraus. Es kann außerdem bei der Bewältigung von KRITIS-Störungen mit einem Mobile Incident Response Team (MIRT) unterstützend tätig werden. Darüber hinaus kann das BSI von Amts wegen weitere Aufsichts- oder Sicherheitsbehörden, wie das BKA (Bundeskriminalamt) oder BfV (Bundesamt für Verfassungsschutz) in die Vorfallsaufklärung einbinden.[16]

5.4 Geltungsbereich

Die Definition des KRITIS-Geltungsbereichs der Anlagen im Unternehmen muss nach der Feststellung der eigenen KRITIS-Betroffenheit und spätestens vor Beginn einer Prüfung vom Be-

13 Vgl. OpenKRITIS, „Identifikation von KRITIS-Anlagen", 2021, https://www.openkritis.de/betreiber/identifikation-kritische-infrastruktur.html (letzter Abruf 26.7.2021).

14 BSI, „Melde- und Informationsportal – Für meldepflichtige Betreiber nach IT-Sicherheitsgesetz (IT-SiG)", 2021, https://mip.bsi.bund.de/ (letzter Abruf 26.7.2021).

15 Vgl. OpenKRITIS, „Registrierung als KRITIS", 2021, https://www.openkritis.de/betreiber/registrierung-kritis-anlagen.html (letzter Abruf 26.7.2021).

16 Vgl. OpenKRITIS, „KRITIS-Meldepflichten", 2021, https://www.openkritis.de/betreiber/meldepflichten-bsig.html (letzter Abruf 26.7.2021).

treiber vorgenommen werden. Der Geltungsbereich beschreibt und dokumentiert pro registrierte Anlage die für den Betrieb und zur Gewährleistung der Versorgungssicherheit notwendigen Prozesse und Technologien. Des Weiteren werden hierdurch die Grenzen für notwendige angemessene Informationssicherheitsmaßnahmen und der Geltungsbereich für BSIG-Nachweisprüfungen definiert. Der Geltungsbereich sollte die durch den Betreiber erbrachte kritische Dienstleistung vollständig und exakt beschreiben. Die KRITIS-Anlage sollte dazu mit ihren unbedingt notwendigen Prozessen und Komponenten eingegrenzt werden. Komponenten umfassen in der Regel IT-Systeme, IT-Anwendungen, Infrastrukturen und auch OT (Operational Technology, Betriebstechnik). Auch Schnittstellen zu externen Parteien sollten im Geltungsbereich klar ersichtlich sein und wiedergeben, welche Teile der IT oder der KRITIS-Anlage von Dritten betrieben werden oder zu wen Abhängigkeiten bestehen. Es ist wichtig zu wissen, dass für ausgelagerte IT und Komponenten der Betreiber der Anlage voll verantwortlich bleibt. Die Betriebsverantwortung wird stärker in Hinblick auf das Service Management und die Dienstleistersteuerung gewichtet. Neben der Erfüllung der 13 Anforderungen an die Beschreibung und Darstellung des Geltungsbereichs muss zudem ein Netzstrukturplan der Kritischen Infrastruktur erstellt werden[17]. Insgesamt gibt es zehn allgemeine Anforderungen als Orientierungshilfe für die Darstellung des Geltungsbereichs durch einen Netzstrukturplan[12]. Allgemein sollte dieser einen relevanten und angemessenen Überblick der kritischen Dienstleistung und KRITIS-Anlage nach dem Charakter „was läuft wo" wiedergeben können.[18]

5.5 Maßnahmen

Betreiber Kritischer Infrastrukturen müssen nach § 8a Abs. 1 BSIG geeignete organisatorische und technische Maßnahmen für eine angemessene Informationssicherheit in KRITIS-Anlagen treffen. Im KRITIS-Geltungsbereich müssen demzufolge regelmäßig Sicherheitsvorkehrungen vorgenommen und Maßnahmen umgesetzt werden, die zudem den Stand der Technik implementieren. Als Orientierung für Informationssicherheitsmaßnahmen in KRITIS-Anlagen kann der Anforderungskatalog des BSI für KRITIS-Betreiber und Prüfer herangezogen werden[19]. Der Katalog enthält 100 wesentliche Anforderungen als Empfehlung für Betreiber und Prüfer für die Umsetzung von angemessenen Maßnahmen in Organisation und Technik. Unter Angemessenheit werden Vorkehrungen verstanden, die zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der involvierten Systeme, Komponenten oder Prozesse beitragen. Angemessen aus der Sicht des BSIG sind Informationssicherheitsmaßnahmen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen KRITIS steht. An diesem Verständnis sollte sich die Auswahl und Umsetzung von Maßnahmen orientieren. Ein Mindestniveau an Informationssicherheit wird im IT-SiG nicht explizit vorgegeben. Technische Maßnahmen zur Sicherung von IT, OT und der Infrastruktur müssen – wie bereits erwähnt – den Stand der Technik vorsehen. Eine Orientierung verschafft die Handreichung zum Stand der Technik[20] des Bundesverbands IT-Sicherheit e. V. (TeleTrusT) mit aktuell verbreiteten Maßnahmen, die diesem Kriterium entsprechen. Des Weiteren kann auf von Branchenvertretern gemeinsam definierte Branchenstandards (B3S) einiger KRITIS-Sektoren, allgemein anerkannte Industrienormen wie ISO/IEC 27001 und 27002, BSI IT-Grundschutz und NIST oder weitere einschlägige branchenspezifische Regularien des DIN (Deutsches Institut für Normung), VDE (Verband Deutscher Elektrotechniker) und ISO (International Organization for Standardization) zurückgegriffen werden. Überdies müssen Risiken der KRITIS-Anlagen im Geltungsbereich durch den Betreiber in einem Risiko-Management behandelt werden sowie Verantwortlichkeiten und Prozesse für Unternehmens- und KRITIS-Risiken definiert sein. Management-Systeme wie ein ISMS oder BCMS (Business Continuity Management System) helfen dabei die Behandlung von Risiken langfristig und strukturiert in einer Strategie bzw. Prozessen zu organisieren, anstatt nur reaktiv und kurzfristig nach Vorfällen oder Prüfungen handeln zu müssen.[21]

5.6 Prüfung

Alle zwei Jahre müssen Betreiber Kritischer Infrastrukturen die Angemessenheit und Wirksamkeit der Informationssicherheitsmaßnahmen in den Anlagen der kritischen Dienstleistung durch Prüfungen oder Audits nachweisen. Die Betreiber müssen dabei die § 8a BSIG – Nachweisprüfungen selbst planen und beauftragen. In der Regel untersuchen externe Prüfer den zuvor festgelegten KRITIS-Geltungsbereich, das Risiko-Management und die vorhandenen Informationssicherheitsmaßnahmen auf Angemessenheit sowie Wirksamkeit. Die Ergebnisse werden in einem Prüfbericht und in BSI-Formularen pro KRITIS-Anlage dokumentiert. Die Formulare und Anhänge müssen anschließend fristgerecht vom Betreiber an das BSI übermittelt werden, das diese dann sichtet und prüft. Feststellungen und Mängel aus der Prüfung müssen durch nachhaltige Verbesserungsmaßnahmen möglichst in einem strukturierten und priorisierten Maßnahmenplan behoben werden. Sollten Unstimmigkeiten bei den Nachweisprüfungen auftauchen, kann das BSI nach § 8a Abs. 4 BSIG Tiefenprüfungen selbst durchführen oder veranlassen, um die Einhaltung der KRITIS-Anforderungen des BSIG bei Betreibern Kritischer Infrastrukturen zu bewerten.[22]

Kommen KRITIS-Betreiber den in den Rechtsgrundlagen verankerten Pflichten und Anforderungen nicht nach, können Sanktionen durch Bußgelder verhängt werden. Verstöße gegen KRITIS-Vorgaben der §§ 8a bis 8c BSIG werden als Ordnungswidrigkeiten in § 14 Abs. 1 BSIG definiert. Bußgelder können nach §

17 BSI, „Informationen zur Wahl des Geltungsbereichs", 2021, https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Infos-fuer-Pruefer/Informationen-zur-Wahl-des-Geltungsbereichs/informationen-zur-wahl-des-geltungsbereichs.html (letzter Abruf 26.7.2021).

18 Vgl. OpenKRITIS, „KRITIS-Geltungsbereich", 2021, https://www.openkritis.de/betreiber/geltungsbereich-kritis.html (letzter Abruf 26.7.2021).

19 BSI, „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen", 28. Februar 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Konkretisierung_Anforderungen_Massnahmen_KRITIS.pdf;jsessionid=C6984A79A45B1F2176D8FDBCF302DC26.internet471?__blob=publicationFile&v=3 (letzter Abruf 26.7.2021).

20 TeleTrusT, „IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum ‚Stand der Technik' – Technische und organisatorische Maßnahmen", vom 5. Februar 2021, https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf (letzter Abruf 26.7.2021).

21 Vgl. OpenKRITIS, „Cyber Security in KRITIS", 2021, https://www.openkritis.de/betreiber/cyber-security-kritis.html (letzter Abruf 26.7.2021).

22 Hierzu ebenfalls *Woitke,* DuD 2021, Heft 9; *Stradomsky*, DuD 2021, Heft 9, beide in diesem Heft.

14 Abs. 2 BSIG zwischen 100.000 und 50.000 EUR betragen. Mit dem IT-SiG 2.0 werden sich die Bußgelder bei Verstößen deutlich erhöhen und auch mehr Tatbestände aufgenommen.[23]

6 KRITIS – wie komme ich da wieder heraus?

KRITIS-Betreiber sind genauso attraktive Angriffsziele für Cyber-Attacken wie andere Unternehmen, nur haben sie einen besonders hohen Einfluss auf die Versorgungssicherheit der Gesellschaft. Die Absicherung der zum Teil mit einem langen Lebenszyklus behafteten IT- und OT-Systeme, die für eine kritische Dienstleistung eingesetzt werden, kann hochkomplex sein. Hiermit sind unter Umständen auch erhebliche Aufwände für die Betreiber verbunden, die mit einer KRITIS-Einstufung einhergehen.

Ein provokativer Ansatz könnte demzufolge sein, wie eine vorhandene KRITIS-Einstufung wieder aufgehoben werden kann. Im einfachsten Fall wird durch die jährliche Prüfung festgestellt, dass die Anlagen zur Erfüllung einer kritischen Dienstleistung die in der BSI-KritisV festgelegten Schwellenwerte unterschreiten. Damit würde die KRITIS-Einstufung aufgehoben und die gesetzlichen Pflichten für den Betreiber Kritischer Infrastrukturen wegfallen. Ein weiterer Ansatz könnte die Aufteilung von betriebenen Anlagen in kleinere verfolgen, die einzeln betrachtet den festgelegten Schwellenwert nicht erreichen. Die BSI-KritisV sagt zunächst einmal aus, dass der Schwellenwert jeweils pro Anlage bestimmt werden muss. Bei der Aufteilung von Anlagen muss allerdings die „gemeinsame Anlage" berücksichtigt werden, welche auch pro KRITIS-Sektor in der Verordnung definiert ist. Unter diesem Gesichtspunkt müssten für die Schwellenwertberechnung dann wieder mehrere Anlagen zusammen betrachtet werden. Eine letzte Möglichkeit wäre den kompletten Bereich der kritischen Dienstleistung und der involvierten Anlagen durch einen anderen Betreiber (juristische Person) zu verantworten. Die KRITIS-Anlagen würden demgemäß nicht im eigenen Verantwortungsbereich liegen und die gesetzlichen KRITIS-Vorschriften wären nicht mehr vom ursprünglichen Betreiber zu erfüllen.

Es sollte jedoch bedacht werden, dass selbst wenn die betriebenen Anlagen die Schwellenwerte unterschreiten und die KRITIS-Vorgaben nicht anwendbar sind, es sich durchaus lohnen kann, Informationssicherheit als strategische Aufgabe in einem Unternehmen zu verfolgen und ein ISMS zur Organisation der Informationssicherheit kontinuierlich, nachhaltig und dauerhaft zu betreiben. Alle Unternehmen sollten in der heutigen Zeit auf Cyber-Angriffe vorbereitet und angemessene Maßnahmen zur Sicherstellung des kontinuierlichen Betriebs und dem Fortbestand der Unternehmung umgesetzt haben.

23 OpenKRITIS, „KRITIS-Prüfungen", 2021, https://www.openkritis.de/pruefung/index.html; OpenKRITIS, „Sanktionen für KRITIS", 2021, https://www.openkritis.de/it-sicherheitsgesetz/sanktionen-kritis-bsig.html (letzter Abruf 26.7.2021); vgl. *Kipker/Scholz*, DuD 2021, S. 40.