VERBAND KOMMUNALER UNTERNEHMEN e.V.

STELLUNGNAHME

Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 07.05.2024

Berlin, 28.05.2024

Der Verband kommunaler Unternehmen e. V. (VKU) vertritt über 1.550 Stadtwerke und kommunalwirtschaftliche Unternehmen in den Bereichen Energie, Wasser/Abwasser, Abfallwirtschaft sowie Telekommunikation. Mit über 300.000 Beschäftigten wurden 2021 Umsatzerlöse von 141 Milliarden Euro erwirtschaftet und mehr als 17 Milliarden Euro investiert. Im Endkundensegment haben die VKU-Mitgliedsunternehmen signifikante Marktanteile in zentralen Ver- und Entsorgungsbereichen: Strom 66 Prozent, Gas 60 Prozent, Wärme 88 Prozent, Trinkwasser 89 Prozent, Abwasser 45 Prozent. Die kommunale Abfallwirtschaft entsorgt jeden Tag 31.500 Tonnen Abfall und hat seit 1990 rund 78 Prozent ihrer CO2-Emissionen eingespart – damit ist sie der Hidden Champion des Klimaschutzes. Immer mehr Mitgliedsunternehmen engagieren sich im Breitbandausbau: 206 Unternehmen investieren pro Jahr über 822 Millionen Euro. Künftig wollen 80 Prozent der kommunalen Unternehmen den Mobilfunkunternehmen Anschlüsse für Antennen an ihr Glasfasernetz anbieten.
Zahlen Daten Fakten 2023
Wir halten Deutschland am Laufen – denn nichts geschieht, wenn es nicht vor Ort passiert: Unser Beitrag für heute und morgen: #Daseinsvorsorge. Unsere Positionen: www.vku.de

Verband kommunaler Unternehmen e.V. · Invalidenstraße 91 · 10115 Berlin
Fon +49 30 58580-0 · Fax +49 30 58580-100 · info@vku.de · www.vku.de

Der VKU bedankt sich für die Möglichkeit, zu dem „Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ vom 07.05.2024 Stellung nehmen zu können.

Bedeutung des Vorhabens für kommunale Unternehmen

Der Verband kommunaler Unternehmen (VKU) vertritt rund 1.500 kommunalwirtschaftliche Unternehmen in den Bereichen Energie, Wasser/Abwasser, Abfallwirtschaft sowie Telekommunikation. Wahrscheinlich wird jedes unser Mitgliedsunternehmen entweder als Betreiber einer kritischen Anlage oder als eine (besonders) wichtigen Einrichtung von der Regulierung des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz betroffen sein.

Positionen des VKU in Kürze

Der VKU begrüßt es zunächst ausdrücklich, dass die Wirtschaft frühzeitig und umfassend bei der Erarbeitung des Referentenentwurfs zum NIS-2-Umsetzungsgesetz einbezogen wird. Diese frühe Einbeziehung merkt man dem **Referentenentwurf** deutlich an, denn dieser setzt die entsprechenden Normen der NIS-2-Richtlinie grundsätzlich gut um. Die Umsetzungsspielräume werden genutzt, um **ganz überwiegend zu einem guten Ergebnis** zu kommen. Ein vergleichbares Vorgehen hätten wir uns auch im Vorfeld des Referentenentwurfs des Kritis-Dachgesetzes gewünscht.

Neben den vielen positiven Aspekten existieren aber auch noch **verbesserungswürdige Punkte**:

- Die Normen zur **Abgrenzung des BSIG zu den spezialgesetzlichen Normen des EnWG müssen überarbeitet** werden. Im Moment kommt es zu unklaren Doppelregulierungen von Unternehmen der Energiewirtschaft (siehe die Ausführungen zu § 28 Abs. 4 BSIG).
- Auch die **spezialgesetzlichen Regelungen des EnWG müssen geändert werden.** Insbesondere muss aus den Normen klar hervorgehen, dass die bisherige Logik des § 11 EnWG nicht geändert werden soll. Nicht alle Energieanlagen, sondern nur kritische Energieanlagen dürfen in den Anwendungsbereich des EnWG mit seinen IT-Sicherheitskatalogen fallen. Die IT-Sicherheitskataloge für die Energieversorgungsnetze und Energieanlagen dürfen sich zudem nur auf die (kritischen) Anlagen beziehen und nicht auf die Office-IT (siehe die Ausführungen zu § 5c EnWG).
- Die **Einzelfallprüfung** der **kritischen Komponenten** in § 41 BSIG ist in Bezug auf die Energiewirtschaft **nicht handhabbar**. Das Procedere sollte geändert und durch eine **Ausschlussliste generell nicht-vertrauenswürdiger Hersteller** ersetzt werden (siehe die Ausführungen zu § 41 BSIG).

- Die **Beteiligung der Betreiber und deren Wirtschaftsverbände an den weiteren Festlegungen muss sichergestellt werden**. Dies betrifft insbesondere die Beteiligung an der Festlegung der erforderlichen IT-Sicherheitsmaßnahmen (siehe die Ausführungen zu § 30 Abs. 5 BSIG) und die Beteiligung vor der Bestimmung der kritischen Anlagen über die neue Kritisverordnung (siehe die Ausführungen zu § 58 BSIG).
- Die **Spezialregelung für die IT-Dienstleister der Kommunen / Länder** ist unklar und überflüssig. Die Regelung **sollte gestrichen werden** (siehe die Ausführungen zu § 28 Abs. 9 BSIG).
- Die **Bestimmung des Betreibers ist weiterhin auslegungsbedürftig** und sollte innerhalb der Gesetzesbegründung präzisiert werden (siehe die Ausführungen zu § 28 Abs. 6 BSIG).
- Zukünftig sollten das **NIS-2-Umsetzungsgesetz und das Kritis-DachG parallel behandelt werden** und insbesondere gleichzeitig in den Bundestag eingebracht werden. Beide Gesetze können nicht getrennt voneinander beurteilt werden, sondern sind eng miteinander verwoben. So müssen insbesondere die Definitionen und die Nachweispflichten eng aufeinander abgestimmt werden, um Doppelaufwände zu verhindern.

Stellungnahme

1. § 2 Abs. 1 BSIG – Begriffsbestimmungen (erheblicher Sicherheitsvorfall)

Die Definition zum „erheblichen Sicherheitsvorfall“ in § 2 Abs. 1 Nr. 10 lit. a § 2 Abs. 1 Nr. 10 BSIG lautet wie folgt:

> *„10. „erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der*
> *a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann; oder […]“*

Gemäß § 2 Abs. 2 kann das BMI bzw. das BSI die erheblichen Sicherheitsvorfälle näher bestimmen.

Finanzielle Verluste waren bisher nicht Bestandteil der Regulierung für kritische Infrastrukturen und spielten auch keine Rolle bei der Aufrechterhaltung der kritischen Dienstleistung (vgl. der aktuelle § 8b Abs. 4 Nr. 2 BSIG). Zudem kann der Wortlaut der Norm so verstanden werden, dass jeder nur mögliche finanzielle Verlust, ganz gleich wie groß er ist, zu einem erheblichen Sicherheitsvorfall führen soll. Dies kann so nicht richtig sein, weil fast jeder Sicherheitsvorfall alleine durch die Arbeitskraft, die zur Behebung investiert werden muss, zu einem finanziellen Verlust führt. Verstärkt wird diese uferlose Weite der Definition dadurch, dass nach dem Wortlaut der Norm der finanzielle Verlust gar nicht eingetreten sein muss, sondern alleine die Möglichkeit des Eintritts ausreicht. Dies widerspricht zudem der Definition des Sicherheitsvorfalls in § 2 Abs. 1 Nr. 39 BSIG, der von einer tatsächlichen Beeinträchtigung ausgeht und die bloße Möglichkeit einer Beeinträchtigung nicht ausreichen lässt.

Eine solche uferlose Definition des Begriffs hat Auswirkungen in verschiedenen Bereichen des BSIG:

Zum einen hat dies einen Einfluss auf die Risikobetrachtung in § 30 BSIG, der explizit den Sicherheitsvorfall als eine maßgebliche Größe zur Betrachtung des Risikos definiert. Sollte jede Art von finanziellen Verlusten betrachtet werden müssen, so würde dies die Anzahl der zu betrachtenden Risikoszenarien ins Uferlose ausweiten.

Bei einem uferlosen Verständnis des erheblichen Sicherheitsvorfalls würde zudem jeder wie auch immer geartete Sicherheitsvorfall nach § 32 BSIG gemeldet werden. Zudem würden die Befugnisse des BSI im Bereich der Unterrichtungspflichten (§ 35 BSIG) und der Sensibilisierung der Öffentlichkeit (§ 36 Abs. 2 BSIG) ins unermessliche wachsen.

Um diesen offensichtlich nicht gewünschten Ergebnissen vorzubeugen, sollte der Gesetzeswortlaut wie folgt angepasst werden:

Formulierungsvorschlag:

§ 2 Begriffsbestimmungen

(1) […]
Nr. 10. „erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der

a) schwerwiegende Betriebsstörungen der Dienste oder **existenzbedrohende** finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann; oder
b) […]

Falls ein finanzieller Verlust existenzbedrohend ist, dann ist auch potentiell die zukünftige Erbringung der Dienstleistung in Gefahr. Falls eine solche Ergänzung auf Grund der Umsetzung der NIS-2-Richtlinie als nicht machbar angesehen wird, so muss zumindest die Gesetzesbegründung entsprechend klargestellt werden und auch in der näheren Bestimmung des BMI / BSI dieser Begriff entsprechend eng definiert werden.

2. § 6 BSIG – Informationsaustausch

Die Einrichtung eines geeigneten Online-Portals zum Austausch zwischen den Betreibern, deren Lieferanten und Dienstleistern sowie den Bundesbehörden ist sehr zu begrüßen. So können die relevanten Informationen an zentraler Stelle möglichst umfassend geteilt werden.

Klargestellt werde sollte, dass das Online Portal auch als Rückkanal für die Informationen des BSI zu Betreibern besonders wichtiger Einrichtungen und wichtiger Einrichtungen (vgl. § 5 Abs. 3 Nr. 4 BSIG in der Fassung vom 03.07.2023) **genutzt wird.** Nur wenn auch das BSI seine Informationen in dieser Form öffentlich teilt, kann der Sinn des Online-Portals erreicht werden. **Auch sollte der UP-Kritis eng bei dem Austausch eingebunden werden.**
Dieses Portal sollte als zentraler Ort für alle Formen von aktuellen Bedrohungen (also auch für physische Bedrohungen wie z.B. Naturkatastrophen, Stromausfälle, Sabotage) dienen. Gefordert wird die Etablierung eines zentralen „Sicherheitslagebilds“.

3. § 11 BSIG - Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

§ 11 Abs. 1 S. 1 BSIG lautet wie folgt:

> *„Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Einrichtung der Bundesverwaltung oder einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Einrichtung*

oder des betroffenen Betreibers oder einer anderen für die Einrichtung oder den Betreiber zuständigen Behörde die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind.[…]“

Laut Gesetzesbegründung soll der bisherige § 5b Abs. 1 BSIG hiermit fortgeführt werden. Allerdings verändert die neue Fassung die bisherige Fassung ganz maßgeblich an der oben unterstrichenen Stelle. Somit könnten Maßnahmen zur Wiederherstellung der Sicherheit der Funktionsfähigkeit der informationstechnischen Systeme nicht nur auf Ersuchen des betroffenen Betreibers oder betroffenen Einrichtung erfolgen, sondern auch auf Ersuchen einer „anderen für die Einrichtung oder den Betreiber zuständigen Behörde“. Ganz konkret könnte dies bedeuten, dass beispielsweise das BSI auf Ersuchen der BNetzA gegen den Willen der betroffenen Einrichtung den Notbetrieb für eine Netzgesellschaft übernimmt. Dies erscheint nicht realistisch und würde die Fähigkeiten des BSI überfordern.

Falls die Regelung anders gemeint ist, so muss sie klargestellt werden. Ist die Regelung wie zuvor beschrieben zu verstehen, so muss sie gestrichen werden.

4. § 28 BSIG - Anwendungsbereich, Betreiber kritischer Anlagen, besonders wichtiger Einrichtungen und wichtiger Einrichtungen

a. Abs. 3 – Bestimmung der Size-Cap nach KMU-Empfehlung

Positiv zu bemerken ist, dass bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme (außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft) **die Empfehlung 2003/361/EG mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden ist**. Durch die explizite Nichteinbeziehung von Artikel 3 Absatz 4 des Anhangs ist klargestellt, dass auch Unternehmen mit Beteiligung der öffentlichen Hand stets nach den zuvor genannten Größenschwellen des § 28 Abs. 1, 2 BSIG beurteilt werden, was bei Geltung des Artikel 3 Absatz 4 des Anhangs nicht der Fall wäre.

Weiterhin ist positiv zu vermerken, dass auf die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen ist. Ergänzend stellt die Gesetzesbegründung fest, dass bei der Bestimmung der maßgeblichen Mitarbeiterzahlen und des Umsatzes nur diejenigen Teile der Einrichtung einzubeziehen sind, die tatsächlich im Bereich der in den Anlagen 1 und 2 genannten Definitionen der Einrichtungskategorien tätig sind. Dies führt dazu, dass für unselbstständige Organisationseinheiten einer Gebietskörperschaft nur deren Mitarbeiterzahl bzw. Umsatz maßgeblich ist und nicht der Umsatz bzw. Mitarbeiterzahl der Gebietskörperschaft selbst. Auch sind mögliche Beteiligungen der Gebietskörperschaft bzw. der unselbstständigen Organisationseinheit der Gebietskörperschaft irrelevant, da hier die Empfehlung 2003/361/EG nach dem Gesetzeswortlaut nicht auf diese anwendbar ist. Allerdings sollte dieses Ergebnis nochmals in der Gesetzesbegründung erläutert werden,

da dieser Zusammenhang sonst ggf. missverstanden werden könnte. **Es wird vorgeschlagen, die folgende Ergänzung in die Gesetzesbegründung aufzuehmen** (vgl. Gesetzesbegründung vom 03.07.2023 zu § 2 Abs. 1 Nr. 12 BSIG):

Formulierungsvorschlag:

Gesetzesbegründung zu § 28 Abs. 3 BSIG

Um eine dem Sinn und Zweck der NIS-2-Richtlinie entsprechende Einbeziehung von Eigenbetrieben der Kommunen oder Landesbetriebe der Länder zu gewährleisten, wird hier klargestellt, dass bei solchen rechtlich unselbstständigen Organisationseinheiten einer Gebietskörperschaft die Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme des Eigenbetriebs bzw. Landesbetriebs selbst ausschlaggebend ist.

b. Abs. 4 – Ausnahmen vom Anwendungsbereich

Nach § 28 Abs. 4 Nr. 2 BSIG gelten die §§ 31 (besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen), 32 (Meldepflichten), 35 (Unterrichtungspflichten) und 39 (Nachweispflichten für Betreiber kritischer Anlagen) nicht für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des EnWG, soweit sie den Regelungen des § 5c des EnWG unterliegen. Nach der Gesetzesbegründung soll Abs. 4 den bisherigen § 8d Abs. 2 BSIG fortführen. Mit dem hier vorgeschlagenen Gesetzeswortlaut gelingt dies jedoch nicht. Vielmehr kommt es zu Widersprüchen mit dem neuen § 5c EnWG.

Nicht ausgeschlossen wird zum einen § 30 BSIG, der die Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen regelt. Dies bedeutet im Umkehrschluss, dass für die Betreiber von Energieversorgungsnetzen oder Energieanlagen (neben dem § 5c EnWG) immer auch der § 30 BSIG zu beachten ist. In den neuen Normen des § 5c EnWG werden jedoch teilweise auch Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen reguliert. So schreibt § 5c Abs. 1 EnWG (allen) Betreibern von Energieversorgungsnetzen vor, dass sie einen angemessenen Schutz der IKT-Systeme sicherstellen müssen, die für den sicheren Netzbetrieb notwendig sind. Nach § 5c Abs. 2 EnWG müssen Betreiber von Energieanlagen, die besonders wichtige oder wichtige Einrichtungen sind, ihre für den sicheren Anlagenbetrieb notwendigen IKT-Systeme schützen. Einzelheiten werden in den IT-Sicherheitskatalogen geregelt, der auch 10 Mindestvorgaben enthalten soll (vgl. die parallele Norm des § 30 Abs. 2 BSIG). Es kommt somit zu einer Doppelung der Pflichten oder zumindest zu Unklarheiten, in welchem Verhältnis § 30 BSIG zu § 5c Abs. 1 – 3 EnWG steht.

Es wird deshalb gefordert, dass auch die Anwendbarkeit von § 30 BSIG durch § 28 Abs. 4 Nr. 2 BSIG ausgeschlossen wird, soweit Betreiber von Energieversorgungsnetzen oder Energieanlagen von § 5c EnWG erfasst werden.

Weiterhin kommt es zu Doppelungen im Bereich der Dokumentationen der ergriffenen Maßnahmen bzw. des Nachweises dieser Dokumentationen für Betreiber von Energieversorgungsnetzen. So müssen nach § 5c Abs. 1 EnWG (letzter Satz) und § 5c Abs. 4 EnWG alle Betreiber von Energieversorgungsnetzen ihre Maßnahmen dokumentieren (Abs. 1) und diese Dokumentation der BNetzA übermitteln/nachweisen (Abs. 4). § 65, 66 BSIG wiederum regelt für die besonders wichtigen und wichtigen Einrichtungen ebenfalls Dokumentations- und Nachweispflichten. §§ 65, 66 BSIG sind allerdings durch § 28 Abs. 4 Nr. 2 BSIG ebenfalls nicht ausgeschlossen, sodass diese Pflichten nebeneinander stehen.

Es wird deshalb gefordert, dass auch die Anwendbarkeit von §§ 65, 66 BSIG durch § 28 Abs. 4 Nr. 2 BSIG ausgeschlossen wird, soweit Betreiber von Energieversorgungsnetzen oder Energieanlagen von § 5c EnWG erfasst werden.

Auch im Bereich der Registrierung kommt es zu Doppelungen. So gibt zum einen § 5c Abs. 8 S. 1, 2 EnWG die Registrierung von (allen) Betreibern von Energieversorgungsnetzen vor. Gleiches gilt für die Betreiber von Energieanlagen, die besonders wichtige oder wichtige Einrichtungen sind. Diese unterliegen allerdings auch den Registrierungspflichten nach § 33 BSIG. Die Pflichten stehen nebeneinander ohne die Pflichten abzugrenzen.

Es wird deshalb gefordert, dass auch die Anwendbarkeit von §§ 33 BSIG durch § 28 Abs. 4 Nr. 2 BSIG ausgeschlossen wird, soweit Betreiber von Energieversorgungsnetzen oder Energieanlagen von § 5c EnWG erfasst werden.

Formulierungsvorschlag:

§ 28 Abs. 4

Die §§ **30,** 31, 32, **33,** 35 und 39**, 65, 66** gelten nicht für: […].

In der Gesetzesbegründung zu § 28 Abs. 4 BSIG finden sich nunmehr Ausführungen zu den Pflichten von Querverbundsunternehmen. **Eine Klarstellung hatte der VKU gefordert, weshalb wir die Ausführungen im Grundsatz sehr begrüßen. Allerdings sollte die Gesetzesbegründung noch ein wenig geschärft werden.** Es sollte klargestellt werden, dass sich die spezialgesetzlichen Normen nur auf die im Anwendungsbereich dieser Normen befindlichen Anlagen beziehen. Es wird deshalb vorgeschlagen, die Gesetzesbegründung wie folgt anzupassen:

Formulierungsvorschlag:

Hierbei ist zu beachten, dass gemäß Absatz 4 die Anwendung der § **30,** 31, 32, **33,** 35**,** ~~und~~ 39**, 65, 66** nur jeweils ausgeschlossen ist, soweit die Unternehmen den Regelungen des TKG bzw. des EnWG unterliegen. Für Querverbundsunternehmen, die in unterschiedlichen Sektoren gleichzeitig tätig sind, ergeben sich daher mitunter mehrere gesetzliche

Vorschriften, die parallel für den jeweiligen Tätigkeitsbereich gelten. Somit gelten beispielsweise für ein Stadtwerk, dass im TK-Bereich, im Energiesektor und im Wasser-/Abwasserbereich tätig ist, jeweils für die **TK-Anlagen** ~~den TK-Bereich~~ die Anforderungen des TKG, für **die Anlagen des Energiesektors** ~~den Energiesektor~~ die Anforderungen des EnWG und für **die Anlagen im Bereich** ~~den~~ Wasser/Abwasser~~bereich~~ **die Anforderungen des BSIG. Für** ~~sowie für~~ die sonstige IT, welche für die Erbringung der Dienste **(außerhalb der Anlagen)** genutzt wird, **gelten allgemein** die Vorgaben des BSIG **(vgl. § 30 Abs. 1 BSIG)**.

Durch diese Anpassung wird auch klargestellt, dass der Erlass der IT-Sicherheitskataloge im Energiebereich bzw. TK-Bereich sich nur auf die dort verankerten Anlagen bezieht und nicht die IT für die allgemeinen Dienste mit umfasst.

Im Übrigen wird auf die Ausführungen zu § 5c EnWG verwiesen. **Die zu § 28 Abs. 4 BSIG gemachten Ausführungen gelten zudem sinngemäß auch für die Regelungen im Telekommunikationssektor** (§ 28 Abs. 4 Nr. 1 BSIG). Auch hier kommt es zu vergleichbaren Doppelregulierungen, die aufgelöst werden müssen.

c. Abs. 6 – Definition des Betreibers einer kritischen Anlage

Zunächst wird gefordert, dass der Betreiber einer kritischen Anlage deckungsgleich mit dem gleichlautenden Begriff im Kritis-DachG definiert und angewendet wird. Anderenfalls wird die Bestimmung des Anwendungsbereichs für die jeweiligen Unternehmen vollends unüberschaubar.

Die Definition des Betreibers einer kritischen Anlage ähnelt sehr der bisherigen Definition des Betreibers einer kritischen Infrastruktur in § 1 Abs. 1 Nr. 2 BSI-Kritisverordnung. Insbesondere wird weiterhin auf den bestimmenden Einfluss auf die kritische Anlage unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände abgestellt. Dieses pauschale Abstellen hat sich bereits in der Vergangenheit insbesondere innerhalb von Konzernen als problematisch erwiesen, weil dort sehr häufig die rechtliche und wirtschaftliche Kontrolle von der tatsächlichen Kontrolle abweicht. Tochtergesellschaften können beispielsweise tatsächlich Windkraftanlagen betreiben, während die rechtliche und wirtschaftliche Kontrolle der gesamten Tochtergesellschaft bei der Muttergesellschaft (ggf. als reine Holding-Gesellschaft) verbleibt. In solchen Fällen ist unklar, welches Kriterium entscheidend ist, zur Bestimmung der Betreibereigenschaft. **Die Gesetzesbegründung sollte hier eine Klarstellung enthalten und zumindest auf die entsprechende Rechtsprechung zur Betreibereigenschaft im Immissionsschutzrecht verweisen**. Dies ist zumindest in der Begründung zur alten BSI-Kritisverordnung[1] erfolgt. Eine solche Klarstellung ist auch deshalb wichtig, weil dies Auswirkungen auf die Frage hat, wann eine

[1] https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2016/kritis-vo.pdf;jsessionid=EF24D8703CD5D54459567A198CA583F3.2_cid295?__blob=publicationFile&v=1

natürliche oder juristische Person oder rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft einer bestimmten Einrichtungsart „zuzuordnen“ ist (vgl. § 28 Abs. 1 Nr. 4; Abs. 2 Nr. 3 BSIG). In den in Bezug genommenen Anlagen 1 und 2 wird ebenfalls häufig auf den Betreiber abgestellt.

d. Abs. 7, 8 – Zeitlicher Anwendungsbereich für Betreiber von kritischen Anlagen

§ 28 Abs. 7, 8 BSIG legt den zeitlichen Anwendungsbereich fest für die Betreiber von kritischen Anlagen. Dieser ist maßgeblich für die Beantwortung der Frage, auf welchen Zeitpunkt es bei der Betrachtung der Schwellenwerte ankommt und ab wann sodann die Pflichten für die Betreiber der kritischen Anlagen gelten.

Diese Regelungen finden sich bisher ausschließlich in der BSI-Kritisverordnung und können sich je nach Sektor und konkreter Anlage unterscheiden (siehe z.B. für den Sektor Energie Anhang 1, Teil 1 Nr. 3, 4 Kritis-Verordnung). **Es sollte nunmehr im BSIG die bisherige Regel aus der Kritis-Verordnung festgeschrieben werden, dass jeweils immer auf die Werte des Vorjahres abgestellt wird, um die Eigenschaft als kritische Anlage zu bestimmen. Zudem müssen auch die bisher gewährten 3 Monate Übergangsfrist weiterhin gelten** (siehe z.B. für den Sektor Energie Anhang 1, Teil 1 Nr. 3, 4 BSI-Kritisverordnung).

e. Abs. 9 – Sonderregeln für IT-Dienstleister der Kommunen / Länder

In § 28 Abs. 9 BSIG wird eine Öffnungsklausel vorgesehen, mit der die Länder die IT-Dienstleister der Kommunen / Länder vom Anwendungsbereich des NIS-2-Umsetzungsgesetzes ausnehmen können. Voraussetzung ist hierbei nach § 28 Abs. 9 Nr. 1 BSIG, dass die IT-Dienstleister im ausschließlichen mittel- oder unmittelbaren Eigentum von Gebietskörperschaften (ausgenommen des Bundes) stehen.

Zunächst existiert im deutschen Recht kein „mittelbares Eigentum“. Es existiert lediglich mittelbarer Besitz (§ 868 BGB).[2] Anscheinend sollen Konstellationen erfasst werden, in denen Kommune / Länder die gesellschaftsrechtlichen Anteile an einem IT-Dienstleister nicht unmittelbar selbst „gehören“, sondern dass diese Anteile von einer anderen Gesellschaft (z.B. GmbH) gehalten werden, die wiederum „im Eigentum“ der Kommune / Länder steht.

Die Regelung zielt erkennbar auf die IT-Dienstleister ab, die ganz überwiegend für die kommunalen Gebietskörperschaften bzw. die Länder die IT-Dienste erbringen. Allerdings könnten durch die sehr unklare Formulierung auch vom VKU vertretene Unternehmen

[2] Siehe zu den verschiedenen Formen des Eigentums Rösch in: Herberger/Martinek/Rüßmann/Weth/Würdinger, jurisPK-BGB, 10. Aufl., § 903 BGB (Stand: 15.03.2023), Rn. 15.

erfasst werden. So könnte beispielsweise ein 100%-IT-Tochterunternehmen eines Stadtwerkes (das wiederum zu 100% der Kommune gehört) hierunter fallen.

In einem solchen Falle müsste das Stadtwerk die Regelungen des BSIG (bzw. EnWG, TKG, etc.) erfüllen, während der eigene IT-Dienstleister bei Nutzung der Öffnungsklausel durch die Länder die Landesregel erfüllen müsste. Da aber der IT-Dienstleister wiederum Dienste für das Stadtwerk erbringt, das dem BSIG unterliegt, müsste der IT-Dienstleister auch diese Regeln erfüllen. Das Stadtwerk wird seine eigenen Pflichten vertraglich an den IT-Dienstleister weiterreichen. Gleiches gilt im Bereich der Regie- und Eigenbetriebe (z.B. relevant im Wasser/Abwasserbereich und im Bereich der Abfallwirtschaft). Hier unterliegt der Regie- und Eigenbetrieb den Regeln des BSIG, während der kommunale IT-Dienstleister (der gleichzeitig für die gesamte Kommune tätig ist) den Länderregeln unterliegt. Der Regie- und Eigenbetrieb verlässt sich für die IT auf die Dienstleistungen des kommunalen IT-Dienstleisters und muss ebenfalls seine Pflichten aus dem BSIG an den kommunalen IT-Dienstleister weiterreichen.

Es lässt sich feststellen, dass die Regelung des § 28 Abs. 9 BSIG unklar ist und im Ergebnis nicht dazu führt, dass der kommunale IT-Dienstleister nur die Landesregeln umsetzen muss. Zudem zersplittern die IT-Sicherheitspflichten noch weiter und werden unnötig komplex. **Aus diesen Gründen sollte die Regelung ersatzlos gestrichen werden.**

5. § 30 BSIG - Risikomanagementmaßnahmen

a. Abs. 1 Verhältnismäßigkeit der Maßnahmen

Die § 30 Abs. 1 BSIG legen die grundsätzlichen Pflichten zur Vornahme von verhältnismäßigen Maßnahmen zur Erhöhung der Informationssicherheit fest. **In Zusammenschau mit der Gesetzesbegründung sind diese Absätze ausdrücklich zu begrüßen.**

So bringt Abs. 1 klar zum Ausdruck, dass nicht nur bei den Betreibern von kritischen Anlagen, sondern auch bei den besonders wichtigen Einrichtungen / wichtigen Einrichtungen der Focus auf der Sicherung der Dienstleistungen liegt (*„die sie für die Erbringung ihrer Dienste nutzen…“*). **Allerdings sollte der Begriff des „Dienstes“ in die Definitionen des § 2 BSIG aufgenommen werden und nicht nur in der Gesetzesbegründung wiedergegeben werden.**

b. Abs. 5 – Ergänzende Festlegungen der erforderlichen Maßnahmen durch das BMI

Nach § 30 Abs. 5 BSIG kann das BMI ergänzende Festlegungen zu den erforderlichen Maßnahmen nach § 30 Abs. 2 BSIG treffen. Eine Anhörung der Betreiber ist bisher nicht vorgesehen. Dies ist nicht sinnvoll, da die erforderlichen Maßnahmen nur zusammen mit den Betreibern erarbeitet werden können. **Es wird gefordert, dass die Betreiber / Einrichtun-**

gen bzw. die entsprechenden Wirtschaftsverbände vor der Verabschiedung einer entsprechenden Rechtsverordnung angehört werden und sich diese Anhörung nicht in einem reinen Formalismus erschöpft.

c. Abs. 6 – Einsatz von bestimmten IKT-Produkten, -Diensten, -Prozessen

Gemäß § 30 Abs. 6 BSIG dürfen besonders wichtige Einrichtungen und wichtige Einrichtung durch Rechtsverordnung nach § 58 Absatz 4 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen.

Dieser Mechanismus kann weitreichende Folgen haben, da hierdurch faktisch der Einsatz von bestimmten Produkten, Diensten und Prozessen im IKT-Bereich untersagt werden kann. Sollten beispielsweise Cloud-Hyperscaler wie z.B. Microsoft, Amazon etc. eine entsprechende Zertifzierung nicht bekommen, so könnte deren Einsatz durch die besonders wichtigen Einrichtungen / wichtigen Einrichtungen untersagt werden.

Nicht geregelt sind jedoch Fragen des Bestandsschutzes, der Übergangsfristen und dem Verhältnis zum Einsatz von kritischen Komponenten. **Es wird gefordert, zumindest diese Themenkomplexe im Gesetz klarzustellen.** Sollte es nur wenige zertifizierte Anbieter für diese Produkte, Dienste oder Prozesse geben, so besteht die Gefahr der Schaffung von Monopolen / Oligopolen in diesem Bereich.

6. § 38 BSIG - Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Bereits heute besteht weitgehend Einigkeit, dass die allgemeinen Sorgfaltspflichten von Leitungsorganen und die gesellschaftsrechtlich gebotene Etablierung von Maßnahmen zum angemessenen Risikomanagement (vgl. § 91 Abs. 2, § 92 Abs. 1 AktG; § 43 GmbHG) auch die Pflicht zu angemessenen Maßnahmen für die IT-Sicherheit umfasst. Es handelt sich hierbei um eine Aufgabe der Unternehmensleitung.[3] Insoweit statuiert § 38 Abs. 1 BSIG lediglich den bisherigen Status Quo, der sich aus den allgemeinen gesellschaftsrechtlichen Regeln abgeleitet hat.

a. § 38 Abs. 2 BSIG – Haftungsverzicht / Vergleich über die Haftung

Anders als § 93 Abs. 4 S. 3 AktG enthält das GmbHG keine generelle Einschränkung für den Verzicht auf oder den Vergleich über Schadensersatzansprüche der Gesellschaft ge-

[3] Krieger/Schneider, Handbuch Managerhaftung, 4. Auflage 2023, Rz. 45.10.

gen ihren Geschäftsführer. Ein Verzicht oder ein Vergleich sind deshalb grundsätzlich zulässig. Die Entscheidung darüber obliegt gemäß § 46 Nr. 8 GmbHG den Gesellschaftern.[4] Durch § 38 Abs. 2 BSIG wird zumindest für die GmbH der Verzicht und der Vergleich im Grundsatz ausgeschlossen. Warum nur für den Bereich von Verstößen gegen IT-Sicherheitspflichten vom Grundsatz eines möglichen Verzichts oder Vergleichs bei einer GmbH abgewichen wird, erschließt sich nicht. **Sollte eine solche Modifizierung des GmbHG gewollt sein, so muss dies in der Gesetzesbegründung begründet werden.**

Neu aufgenommen wurde, dass ein Vergleich nicht mehr generell unzulässig ist, sondern nur dann, wenn er in einem groben Missverhältnis zu einer bestehenden Ungewissheit über das Rechtsverhältnis steht. Laut Gesetzesbegründung ist bei einem gerichtlich vorgeschlagenen Vergleich davon auszugehen, dass dieser angemessen ist. Zudem wird klargestellt, dass der Abschluss von D&O-Versicherungen weiterhin möglich ist.

Zunächst wird begrüßt, dass die Zulässigkeit von D&O-Versicherungen explizit klargestellt wurde. Auch wird begrüßt, dass nicht mehr jeglicher Vergleich unzulässig ist, sondern nur im Falle eines groben Missverhältnisses.

Allerdings sollten in der Gesetzesbegründung weitere Hinweise gegeben werden, wann ein grobes Missverhältnis vorliegt und wann nicht. Angenommen, es geht um einen Cyberschaden von EUR 1 Mio. und die Beweislage für das Unternehmen ist schwierig, weil z.B. der Angriffsvektor durch IT-forensische Maßnahmen nicht abschließend festgestellt werden konnte und es daher um die Kausalität einer Pflichtverletzung geht. Welche Vergleichsspanne ist dann angemessen? Mit anderen Worten: Was ist der zulässige Mindestbetrag für einen Vergleich mit dem Organ, EUR 100.000, 50.000, 10.000?

Zudem sollte auch der Verzicht auf die Ersatzansprüche ebenfalls nur dann unzulässig sein, wenn ein grobes Missverhältnis vorliegt. Anderenfalls steht zu vermuten, dass statt eines Verzichts schlicht Vergleiche in einer geringen Höhe geschlossen werden.

b. § 38 Abs. 3 – Verpflichtende Schulungen der Geschäftsleitung

Gemäß § 38 Abs. 3 BSIG muss die Geschäftsleitung besonders wichtiger Einrichtungen und wichtiger Einrichtungen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Es sollte klargestellt werden, ob es sich hierbei um eine spezielle und tiefergehende Schulung für die Geschäftsleiter handelt oder auch die Teilnahme an allgemeinen IT-Sicherheitsschulungen für die Belegschaft ausreichend ist.

[4] Fleischer, in: Münchener Kommentar GmbH, 4. Auflage 2023, § 43, Rn. 350.

7. § 39 BSIG - Nachweispflichten für Betreiber kritischer Anlagen

Äußerst positiv zu beurteilen ist, dass zukünftig die Nachweispflichten von den Betreibern von kritischen Anlagen alle drei Jahre und nicht mehr alle zwei Jahre erfüllt werden müssen. Dieser Nachweiszyklus entspricht den internationalen Normen der ISO 27000-Reihe und verhindert Doppelaufwände für die Unternehmen, weil sie anderenfalls Nachweise häufig doppelt erbringen müssen zu unterschiedlichen Zeitpunkten. **Von entscheidender Bedeutung ist, dass die Nachweiszeiträume im NIS2UmsuCG und im KRITIS-DachG parallel ausgestaltet werden, damit die Audits nur einmal und zwar gemeinsam durchgeführt werden müssen.**

8. § 40 - Zentrale Melde- und Anlaufstelle

Gemäß § 40 Abs. 3 Nr. 4 BSIG hat das BSI unverzüglich die Betreiber kritischer Anlagen über sie betreffende Informationen nach den Nummern 1 bis 3 durch Übermittlung an die Kontaktdaten nach § 33 Absatz 1 Nummer 2 zu unterrichten.

Positiv ist zunächst, dass das BSI (wie auch bereits heute gemäß § 8b Abs. 2 Nr. 4a BSIG) unverzüglich gewisse Informationen an die Betreiber weitergeben muss. Allerdings wird das BSI im Einzelfall kaum bewerten können, welche Informationen genau für welche Einrichtung von Relevanz ist, da das BSI nicht weiß, welche IT/OT-Systeme die Betreiber einsetzen. **Aus diesem Grund wird gefordert, dass das BSI im Zweifel die Informationen weitergibt, also bereits bei potentiell wichtigen Informationen diese weiterleitet. Zudem sollte darüber nachgedacht werden, die Informationen über das Online-Portal im Prinzip allen Betreibern / Einrichtungen zur Verfügung zu stellen. Die Betreiber / Einrichtungen können dann selbst bewerten, welche Informationen für sie relevant sind und welche nicht.**

9. § 41 BSIG - Untersagung des Einsatzes kritischer Komponenten

§ 41 BSIG beschreibt das Procedere der Untersagung von kritischen Komponenten. Bisher wurden nur im 5G-Bereich der Telekommunikationsnetze kritische Komponenten definiert. Zukünftig werden allerdings auch im Bereich der Energiewirtschaft kritische Komponenten existieren. Auf Grundlage von § 11 Abs. 1g S. 1 Nr. 2 EnWG (zukünftig § 5c Abs. 9 Nr. 2 EnWG) konsultiert und erarbeitet die BNetzA im Moment die Festlegung von kritischen Funktionen, aus denen sodann die kritischen Komponenten abgeleitet werden.[5] Durch die Festlegung werden die Übertragungsnetzbetreiber, aber auch die Betreiber von Energieanlagen sowie Verteilnetzbetreiber (soweit sie jeweils kritische Infrastrukturen betreiben) adressiert. Im Ergebnis werden somit hunderte Unternehmen neu in den An-

[5] https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/IT_Sicherheit/KriFu/start2.html

wendungsbereich des § 41 BSIG fallen. Dies steht im krassen Gegensatz zur ursprünglichen Idee des § 41 BSIG, der klar den 5G-Bereich der Telekommunikationsnetze mit seinen nur vier am Ausbau beteiligten Unternehmen im Blick hatte.

Vor diesem Hintergrund wird klar, dass die durch § 41 BSIG vorgesehene Einzelfallprüfung der Vertrauenswürdigkeit einzelner Komponenten durch das BMI für den Bereich der Energiewirtschaft keinen Bestand haben kann. Das BMI wird mit den tausenden Einzelfallprüfungen schlicht personell überfordert sein. In Konsequenz würde sich der Einbau / Austausch von Komponenten um mindestens zwei Monate bzw. vier Monate verzögern (vgl. § 41 Abs. 2 BSIG). Dies kann zu einer Gefährdung der Sicherheit der Energienetze und Energieanlagen führen, da z.B. der kurzfristige Austausch von defekten Komponenten verhindert wird. Auch die regulären Beschaffungsprozesse würden sich massiv verzögern, und der Ausbau der Energienetze weiter verzögert. Insgesamt handelt es sich um ein sehr bürokratisches Verfahren, dass im Ergebnis nicht zu mehr Sicherheit führen wird, aber die Planungssicherheit der Unternehmen untergräbt.

Vor diesem Hintergrund sollte das Prüfverfahren gemäß § 41 BSIG gestrichen und durch eine Ausschlussliste generell nicht-vertrauenswürdiger Hersteller ersetzt werden. Ergänzend wird auf die Stellungnahme des UP Kritis und des BDEW verwiesen.

10. § 58 BSIG – Ermächtigung zum Erlass von Rechtsverordnungen

Gemäß § 58 Abs. 4 BSIG werden durch Rechtsverordnung die kritischen Anlagen festgelegt. **Hierbei muss sichergestellt werden, dass die Definition der kritischen Anlagen deckungsgleich der Definition der kritischen Anlagen im Kritis-Dachgesetz ist.** Anderenfalls wird die bereits sehr komplexe Regulierung des Anwendungsbereichs beider Gesetze noch weiter verkompliziert.

Zudem muss wieder aufgenommen werden, dass diese Festlegung selbstverständlich nach Anhörung der betroffenen Betreiber und Wirtschaftsverbände erfolgt. Dies ist – anders als noch in der Vorfassung – nicht mehr im Gesetzestext vorhanden. Wir gehen von einem Redaktionsversehen aus, da die Absätze 1-3 jeweils eine entsprechende Anhörung der Wirtschaftsverbände vorsehen.

Zum Einsatz von IKT-Produkten, -Diensten und –Prozessen (§ 58 Abs. 3 BSIG) wird auf die Anmerkungen zu § 30 Abs. 6 BSIG verwiesen.

11. § 65 BSIG - Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

Gemäß § 65 Abs. 1 BSIG kann das Bundesamt einzelne besonders wichtige Einrichtungen verpflichten, Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen zur Prüfung der Erfüllung der Anforderungen nach den §§ 30, 31 und 32 durchführen zu lassen.

Die Möglichkeit, diese Nachweise anzufordern, findet sich in § 65 Abs. 3 BSIG. Die maßgeblichen Kriterien zur Ermessensausübung finden sich hierbei in § 65 Abs. 4 BSIG.

Positiv ist zunächst hieran, dass besonders wichtige Einrichtungen und wichtige Einrichtungen nicht ohne weiteres ex-ante Nachweispflichten unterliegen, wie dies bei Betreiber von kritischen Anlagen der Fall ist (vgl. § 39 BSIG). **Allerdings muss der Verweis auf § 31 BSIG gestrichen werden (gilt auch für § 65 Abs 3 S. 1 BSIG).** § 31 BSIG regelt die besonderen Anforderungen an die Risikomanagementmaßnahmen von *Betreibern kritischer Anlagen*. § 65 Abs. 1 BSIG regelt allerdings die Aufsichts- und Durchsetzungsmaßnahmen für *besonders wichtige Einrichtungen.* Der Verweis könnte so gelesen werden, dass auch von besonders wichtigen Einrichtungen die weitergehenden Anforderungen an die Betreiber von kritischen Anlagen auferlegt werden könnten. Dies ist aber offensichtlich nicht gewollt und auch nicht sinnvoll.

Die ermessenssteuernde Norm in § 65 Abs. 4 BSIG folgt einem risikobasierten Ansatz, so wie dies wohl aus Erwägungsgrund 124 der NIS-2-Richtlinie vorgegeben ist. **Im Grundsatz sind die Kriterien gut nachzuvollziehen, sollten jedoch noch ergänzt werden. So sollte explizit festgeschrieben werden, dass zum einen auch die Umsetzungskosten ein leitendes Kriterium sind (vgl. die Abwägung in § 30 Abs. 1 BSIG). Auch sollte in die Abwägung explizit einbezogen werden, ob es sich bei der besonders wichtigen Einrichtung bereits um einen Betreiber einer kritischen Anlage handelt**. In einem solchen Fall greifen die ex-Ante Nachweispflichten bereits in Bezug auf die kritischen Anlagen, die zweifellos das größte Risiko darstellen. **Im Regelfall sollte eine zusätzliche Nachweiserbringung und Anforderung für besonders wichtige Einrichtungen ausgeschlossen sein, wenn sie eine kritische Anlage betreiben.**

Zudem muss der Verweis in § 65 Abs. 4 BSIG nicht nur auf § 65 Abs. 3 BSIG (Anforderung der Nachweise), sondern auch auf § 65 Abs. 1 BSIG (Verpflichtung zur Auditierung, Prüfung und Zertifzierung) erstreckt werden. Anderenfalls existieren keine ermessenleitenden Kriterien für die Festlegung der Verpflichtungen aus § 65 Abs. 1 BSIG.

Formulierungsvorschlag:

§ 65 - Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

(4) Bei der Auswahl, von welchen Einrichtungen das Bundesamt nach Absatz 3 Nachweise anfordert, berücksichtigt das Bundesamt das Ausmaß der Risikoexposition, die Größe der Einrichtung **und mögliche Umsetzungskosten** sowie die Eintrittswahrscheinlichkeit und Schwere von möglichen Sicherheitsvorfällen sowie ihre möglichen gesellschaftlichen und wirtschaftlichen Auswirkungen. **Handelt es sich bei der besonders wichtigen Einrichtung gleichzeitig um den Betreiber einer kritischen Anlage, so soll im Regelfall auf eine Nachweiserbringung nach Abs. 3 verzichtet werden. S. 1 und 2 gelten entsprechend für die Ausübung des Ermessens in Abs. 1.**

12. § 5c EnWG

Erstmals werden die neuen Regelungen des EnWG bekanntgemacht. Auffällig ist zunächst, dass die korrespondierende Gesetzesbegründung sehr dünn gehalten und zur Auslegung der Normen unergiebig ist. Zudem muss man feststellen, dass mit den Regelungen des EnWG deutlich über die Anforderungen der NIS-2-Richtlinie hinausgegangen wird, also ein Gold Plating stattfindet. Es soll wohl die alte Logik des § 11 EnWG weitgehend „gerettet" werden und in die NIS-2-Umsetzung eingepasst werden. Dies gelingt jedoch nicht immer.

a. § 5c Abs. 2 EnWG – Anforderungen an die Betreiber von Energieanlagen

Besonders deutlich wird dies zunächst in § 5c Abs. 2 EnWG. Diese Norm statuiert die IT-Sicherheitspflichten für die Betreiber von Energieanlagen in Bezug auf die IT-Infrastrukturen des Anlagenbetriebs. Während der bisherige § 11 Abs. 1b BSIG diese Pflichten nur für die Betreiber von kritischen Infrastrukturen (zukünftig Betreiber von kritischen Anlagen) statuiert, erweitert der § 5c Abs. 2 EnWG diese Pflichten auf alle Betreiber von Energieanlagen, die besonders wichtige / wichtige Einrichtungen sind. Damit findet eine massive Ausweitung des Anwendungsbereichs statt. Da eine Einrichtung bereits ab 50 Mitarbeitern eine wichtige Einrichtung ist (vgl. § 28 Abs. 2 Nr. 3 BSIG), wären zukünftig fast alle Betreiber von Energieanlagen von den neuen Regelungen erfasst. Dies wird abgelehnt und passt auch nicht zur sonstigen Systematik des § 5c EnWG. Vielmehr sollten weiterhin ausschließlich Betreiber von Energieanlagen, die Betreiber von kritischen Anlagen sind, den speziellen Regelungen unterliegen. Sie sollten diesen Pflichten auch nur „insoweit" unterliegen, als dass sich diese Pflichten auf die kritischen Anlagen beziehen. Nicht erfasst sein dürfen die Pflichten für die sonstigen IT-Systeme außerhalb des Scopes der kritischen Anlagen, wie z.B. die reguläre Office-IT. Für diese IT-Systeme muss es bei den allgemeinen Regeln des BSIG verbleiben, ohne das die Pflichten nach EnWG (bzw. den IT-Sicherheitskatalogen) einschlägig sind (vgl. die Ausführungen zu § 28 Abs. 4 bzw. zu §§ 30, 31 BSIG).
Vor diesem Hintergrund wird folgende Änderung vorgeschlagen:

Formulierungsvorschlag:

§ 5c Abs. 2 EnWG - IT-Sicherheit im Anlagen- und Netzbetrieb

(2) Betreiber von Energieanlagen**, die kritische Anlagen nach § 2 Absatz 1 Nummer 21 des BSI-Gesetzes sind**~~die besonders wichtige Einrichtungen nach § 28 Absatz 1 Satz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von kritischen Anlagen und Einrichtungen (BSI-Gesetz) vom [...] oder wichtige Einrichtungen nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes sind~~ **und die** ~~und~~ an ein Energieversorgungsnetz angeschlossen sind, haben einen angemesse-

nen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind […].

Dieser Hintergrund sollte auch in der Gesetzesbegründung erläutert werden. Anderenfalls wird bereits jetzt absehbar große Verunsicherung in der Branche herrschen, welche Anforderungen zu erfüllen sind.

Sollte keine Anpassung des Gesetzeswortlauts erfolgen, kommen insbesondere auf eine Vielzahl von kleinen Betreibern von Energieanlagen zusätzliche hohe Aufwände zu, die sich mittelbar in höheren Strompreisen ausdrücken werden. Auch Unternehmen, die lediglich kleine bisher nicht als kritisch eingestufte Anlagen betreiben und z.B. Reststrom aus einer eigenen PV-Anlage einspeisen, könnten unter den Wortlaut der Regelung gefasst werden können und müssten sich plötzlich auch zertifizieren lassen. Ferner würden massive Abgrenzungsprobleme in Querverbundsunternehmen entstehen. Welchen Anforderungen würde in solchen Unternehmen die Office-IT unterliegen, die sowohl für den Sektor Energie, als auch für den Sektor Wasser genutzt wird?

Zudem würde die Systematik in Verbindung zum Kritis-Dachgesetz gesprengt, denn der dortige Anwendungsbereich erfasst nur die Betreiber von kritischen Anlagen. Die Bestimmung der Pflichten für die einzelnen Betreiber würde extrem unübersichtlich werden und voraussichtlich zu sehr vielen Missverständnissen führen. Dies würde sicherlich bei der BNetzA / BSI zu einem erhöhten Beratungsaufwand führen. Zudem müssten auch die Betreiber ihre wertvollen Ressourcen zunächst in die Klärung ihrer Betroffenheit vom NIS-2-Umsetzungsgesetz / Kritis-Dachgesetz stecken, anstatt in die Sicherheit investieren zu können.

b. § 5c Abs. 3 EnWG – Inhalt der IT-Sicherheitskataloge

Auch in Bezug zu § 5c Abs. 3 BSIG kommt es zu Unklarheiten bzw. Inkonsistenzen. Diese Norm regelt die Inhalte der IT-Sicherheitskataloge näher. In der jetzigen Fassung würden sich die IT-Sicherheitskataloge auf Grund der generellen Verweise auf § 5c Abs. 1 und Abs. 2 EnWG auch auf die wichtigen / besonders wichtigen Einrichtungen im Bereich der Energieanlagen beziehen (siehe Ausführungen zuvor). Die Norm lehnt sich dabei erkennbar an die §§30, 31 BSIG an, vollzieht aber dessen Abstufung der Pflichtentiefe von Betreibern kritischer Anlagen, besonders wichtiger Einrichtungen und wichtigen Einrichtungen nicht hinreichend nach.

Dies betrifft zunächst § 5c Abs. 3 S. 2 EnWG im Vergleich mit § 30 Abs. 1 S. 2 BSIG. In der EnWG Norm fehlt bei der Bewertung der Angemessenheit der IT-Sicherheitsmaßnahmen der Verweis auf die Umsetzungskosten. Diese Umsetzungskosten werden in § 30 Abs. 1 S.

2 BSIG explizit genannt. Auch für den Bereich der kritischen Anlagen sind die Umsetzungskosten ein maßgeblicher Faktor, der bei der Bewertung der Angemessenheit der Maßnahmen berücksichtigt werden kann. Dies ergibt sich aus dem Verweis des § 31 Abs. 1 auf den § 30 BSIG. Auch die Gesetzesbegründung des § 31 Abs. 1 BSIG nimmt explizit auf die Fragen der Wirtschaftlichkeit Bezug, wobei lediglich die Abwägung in Bezug auf die anderen Schutzgüter ggf. anders ausfallen muss. Zwar sind die Umsetzungskosten in § 5c Abs. 3 S. 1 EnWG erwähnt. Die fehlende Berücksichtigung bei der Bewertung nach § 5c Abs. 3 S. 2 EnWG könnte jedoch dazu führen, dass die Umsetzungskosten nicht ausreichend berücksichtigt werden. **Es wird deshalb folgende Änderung vorgeschlagen:**

Formulierungsvorschlag:

§ 5c Abs. 2 EnWG - IT-Sicherheit im Anlagen- und Netzbetrieb

(3) […] Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, sind das Ausmaß der Risikoexposition**,** ~~und~~ die Größe des Betreibers**, die Umsetzungskosten** sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.

Dieser Hintergrund sollte auch in der Gesetzesbegründung erläutert werden. Anderenfalls wird bereits jetzt absehbar große Verunsicherung in der Branche herrschen, welche Anforderungen zu erfüllen sind.

Zudem wird darauf hingewiesen, dass durch den jetzigen § 5c Abs. 3 S. 3 Nr. 11 EnWG faktisch alle Betreiber von Energieanlagen **Systeme mit Angriffserkennung** umsetzen müssten. Dies widerspricht dem § 31 Abs. 2 BSIG, der diese Pflicht auf die Betreiber von kritischen Anlagen beschränkt. **Dies ist ein weiterer Grund, warum der § 5c Abs. 2 EnWG auf die Betreiber von kritischen Anlagen beschränkt werden muss** (siehe hierzu die Ausführungen zu § 5c Abs. 2 EnWG).

Ferner sollte entweder der Begriff des Betreibers (von Energienetzen oder Energieanlagen) oder der Begriff der Einrichtung als Adressat verwendet werden. Hier sind noch Inkonsistenten vorhanden (vgl. beispielsweise § 5c Abs. 3 S. 2 EnWG im Vergleich zu § 5c Abs. 3 S. 3 Nr. 10 EnWG). **Es sollte eine einheitliche Terminologie gefunden werden.**

c. § 5c Abs. 4, 5 EnWG – Nachweiserbringung

Zunächst ist äußerst positiv zu bemerken, dass lediglich (alle) Betreiber von Energieversorgungsnetzen und Betreiber von kritischen Energieanlagen der BNetzA die Dokumentation der IT-Sicherheitsmaßnahmen übermitteln (bzw. nachweisen) müssen. Keine ex ante (also eine proaktive) Nachweispflicht haben dagegen die Betreiber von Energieanlagen, die lediglich eine besonders wichtige oder wichtige Einrichtung sind, aber nicht gleichzeitig eine kritische Anlage betreiben. (vgl. § 5c Abs. 4 EnWG).

Nach § 5c Abs. 5 EnWG kann die BNetzA im Einzelfall von Betreibern von Energieanlagen, die eine wichtige Einrichtung sind, ebenfalls die Maßnahmen nach § 5c Abs. 4 durchführen. Hier wurde wohl vergessen, auch auf den Betreiber der besonders wichtigen Einrichtung abzustellen, womit eine Regelungslücke verbleibt. Insgesamt sollten in den Regelungsbereich des § 5c EnWG allerdings ohnehin nur Betreiber von Energieanlagen fallen, die auch kritische Anlagen betreiben. **Aus Sicht des VKU ist § 5c Abs. 5 EnWG somit überflüssig und sollte gestrichen werden.** Hinzuweisen ist hierbei darauf, dass zwar jeder Betreiber einer kritischen Anlage gleichzeitig eine besonders wichtige Einrichtung ist (vgl. § 28 Abs. 1 S. 1 Nr. 1 BSIG), aber nicht jede besonders wichtige Einrichtung auch gleichzeitig ein Betreiber einer kritischen Anlage ist.

Es wird ferner darauf hingewiesen, dass im Rahmen der Nachweiserbringung eine Formulierung vergleichbar § 39 Abs. 3 BSIG fehlt. In dieser Norm wird geregelt, dass für Bestandsanlagen für den ersten Nachweis nach dem neuen Gesetz der letzte Nachweis nach dem alten Gesetz maßgeblich ist. Zudem wird dem BSI eine entsprechende Befugnis erteilt, diese Pflichten dann im Einzelfall festzulegen. **Es wird angeregt, eine entsprechende Regel auch in das EnWG einzufügen**. Dies dient, wie in der Gesetzesbegründung beschrieben, der Entzerrung der Nachweisprüfung. Hierbei sollte zusätzlich festgelegt werden, dass die Nachweiserbringung auch in Bezug auf die Systeme zur Angriffserkennung einheitlich gefordert werden. Es muss verhindert werden, dass die Zyklen für die Nachweise der Systeme zur Angriffserkennung von den restlichen Nachweisen abweichen.

d. § 5c Abs. 8 EnWG - Registrierung

Aus den gleichen Gründen wie in § 5c Abs. 2 und Absatz 5 müssen auch die Regelungen zur Registrierung in § 5c Abs. 8 auf solche Betreiber von Energieanalgen begrenzt werden, die kritische Anlagen betreiben. Betreiber von Energieanlagen, die keine kritischen Anlagen betreiben, aber wichtige oder besonders wichtige Einrichtungen sind, sollten nicht durch das EnWG reguliert werden. Die Pflicht zur Registrierung ergibt sich für diese Betreiber von Energieanlagen bereits aus § 33 BSIG.

Formulierungsvorschlag:

§ 5c Abs. 8 EnWG - IT-Sicherheit im Anlagen- und Netzbetrieb

(8) Betreiber von Energieversorgungsnetzen und solche Betreiber von Energieanlagen, **die kritische Anlagen nach § 2 Absatz 1 Nummer 21 des BSI-Gesetzes sind**
~~die besonders wichtige Einrichtungen nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder wichtige Einrichtungen nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes sind~~,
sind verpflichtet, spätestens bis zum 1. April, erstmalig oder erneut, sich beim Bundesamt für Sicherheit in der Informationstechnik zu registrieren. Dabei sind Angaben nach § 33 Absatz 1 Nummer 1 bis 4 des BSI-Gesetzes zu übermitteln. […]

e. § 5c Abs. 9 EnWG – kritische Kompontenten / kritische Funktionen

Es wird angeregt, im Gesetzestext / Gesetzesbegründung klarzustellen, dass von dieser Norm immer nur Betreiber von kritischen Anlagen betroffen sind, also auch Betreiber von Energieversorgungsnetzen die maßgeblichen Schwellenwerte erreichen müssen. Dies kann man zwar indirekt aus dem Begriff der kritischen Anlage / Funktion ableiten. Der Wortlaut von § 5c Abs. 9 S. 2 EnwG (bisher § 11 Abs. 1g S. 2 EnWG) führt aber häufig zu einem anderen Verständnis. Teilweise wird angenommen, dass alle Betreiber von Energieversorgungsnetzen diesen Regeln unterliegen.

Im Übrigen wird auf die Kommentierung von § 41 BSIG verwiesen.

13. § 95 Abs. 2a EnWG – Bußgeldvorschriften

§ 95 Abs. 2a EnWG regelt die Einzelheiten der Bußgelder im Bereich der Energiewirtschaft. Hierbei wird offenbar eine andere Abstufung gewählt, als es im BSIG vorgesehen ist. Während die § 61 Abs. 5 – 7 BSIG Bußgelder gemessen am Jahresumsatz nur zulassen, wenn der Jahresumsatz mehr als 500 Millionen Euro beträgt, findet sich diese Einschränkung im EnWG nicht wieder. **Damit eine Konsistenz hergestellt wird, sollten auch im Bereich der Energiewirtschaft Bußgelder gemessen am Jahresumsatz nur verhängt werden können, wenn das Unternehmen mindestens 500 Millionen Euro Jahresumsatz erwirtschaftet.**

Zudem wird jeweils von „einem Höchstbetrag von mindestens 1,4% / 2% des gesamten“ Jahresumsatzes gesprochen. **Hierbei handelt es sich offensichtlich um ein Redaktionsversehen. Es handelt sich bei der Bußgeldsumme um den Höchstbetrag, weshalb das Wort „mindestens“ gestrichen werden muss.**

Zudem muss eine Klarstellung erfolgen, dass neben den Bußgeldern nach der DSGVO keine Bußgelder nach dem EnWG verhängt werden dürfen (siehe die vergleichbare Regelung in § 61 Abs. 10 BSIG). **Ferner fehlt einer Klarstellung, dass der gleiche Verstoß nur entweder nach dem EnWG oder nach dem BSIG mit einem Bußgeld versehen werden darf.**

VKU-Ansprechpartner
Wolf Buchholz
Fachgebietsleiter Kritische Infrastruktur und Cybersicherheit
Abteilung Recht, Finanzen und Steuern

Telefon: +49 30 58580-317
E-Mail: buchholz@vku.de