VERBAND KOMMUNALER UNTERNEHMEN e.V.

STELLUNGNAHME

zum NIS-2-Umsetzungs- und Cybersicherheits-stärkungsgesetz (NIS2UmsuCG)

Diskussionspapier des Bundesministeriums des Innern und für Heimat (BMI) für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschlandvom 27.09.2023

Berlin, 18.10.2023

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 „Diskussionspapier des Bundesministeriums des Innern und für Heimat (BMI) für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland“ 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 unserer Mitgliedsunternehmen entweder als Betreiber einer kritischen Anlage oder als Betreiber einer (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 **Diskussionsentwurf** 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.

Inhaltlich positiv zu bemerken sind vor allem folgende Punkte:

- Es wird bei der Bestimmung der **besonders wichtigen Einrichtungen** und **wichtigen Einrichtungen** nunmehr der **Systematik der NIS 2-Richtlinie gefolgt** und insbesondere die **Sektoren** mit hoher Kritikalität und sonstige kritische Sektoren in einer Anlage zu dem Gesetz **abschließend festgelegt**. (siehe die Ausführungen zu § 28 Abs. 1 BSIG).
- Auch **öffentliche Unternehmen können von den KMU-Ausnahmen** des Gesetzes **profitieren**. (siehe die Ausführungen zu § 28 Abs. 1 BSIG).
- Die **Daten eines Partner- oder verbundenen Unternehmens** sind bei der Cap-Size dann **nicht mit hinzuzurechnen**, wenn das jeweils zu prüfende Unternehmen selbst **bestimmenden Einfluss auf die Beschaffenheit und den Betrieb der eigenen informationstechnischen Systeme** ausübt. Dies ist positiv, da in Konzernverbünden so Erleichterungen geschaffen werden (siehe die Ausführungen zu § 28 Abs. 3 BSIG).
- **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. Von entscheidender Bedeutung ist nun, dass die Nachweiszeiträume im NIS2UmsuCG und im KRITIS-DachG parallel ausgestaltet werden, damit die Audits nur einmal und zwar gemeinsam durchgeführt werden müssen (siehe die Ausführungen zu § 39 Abs. 1 BSIG).

- Weiterhin ist es **sehr zu begrüßen**, dass i**m Grundsatz lediglich Betreiber von kritischen Anlagen ex-ante Nachweispflichten unterliegen**. Die Unternehmen können sich so deutlich besser auf die Umsetzung der Risikomanagementmaßnahmen konzentrieren, ohne in übermäßiger Bürokratie zu ersticken (siehe die Ausführungen zu §§ 39, 64 und 65 BSIG).

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

- **Unklarheiten** bestehen bei **Querverbundsunternehmen**, also Unternehmen, die in mehreren Sektoren tätig sind. Solche Unternehmen sind vielfach im VKU vertreten. Es stellt sich zum einen die Frage, wie der **Anwendungsbereich** dieser Unternehmen bestimmt wird, also welchen Pflichten diese Unternehmen unterliegen. Zum anderen stellt sich die Frage, wie die Querverbundunternehmen diese **Pflichten erfüllen** und **nachweisen** müssen. Es wird ein **kombiniertes Audit** gefordert, bei der Doppelprüfungen verhindert werden. Diese Fragen müssen entweder in der Gesetzesbegründung aufgegriffen werden oder aber in einer FaQ-Liste im Einzelnen ausgearbeitet werden (siehe die Ausführungen zu §§ 28 Abs. 1, 2; 4; 30 Abs. 1; 39 und 64 BSIG).
- Ähnliches gilt für Fragestellungen in Zusammenhang mit **Konzernunternehmen**. So muss der **bestimmende Einfluss auf die eigenen IT-Systeme** deutlicher herausgearbeitet werden, um den Anwendungsbereich klarer bestimmen zu können (siehe die Ausführungen zu §§ 28 Abs. 3, 5 BSIG). Zudem muss klarer herausgearbeitet werden, wie die **Pflichten innerhalb des Konzerns verteilt** sind und insbesondere festgelegt werden, dass **in einem Konzern bereits zertifizierte Systeme nicht von einem anderen Konzernunternehmen nochmals zertifziert werden müssen** (siehe die Ausführungen zu §§ 30 Abs. 1; 39 und 64 Abs. 1 BSIG).
- Für den Fall, dass eine **besonders wichtige Einrichtung gleichzeitig ein Betreiber einer kritischen Anlage** ist, muss das Gesetz ebenfalls nochmals überarbeitet und präzisiert werden. **Es muss klar sein, dass in einem solchen Fall Nachweise für den Bereich außerhalb der kritischen Anlagen nur im absoluten Ausnahmefall eingefordert werden** (siehe die Ausführungen zu §§ 28 Abs. 1, 2 und 64 Abs. 1 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.
- Die **spezialgesetzlichen Regelungen** im **TKG** und **EnWG** sind nicht Teil dieses Diskussionsentwurfs. **Für den VKU sind diese Regelungen jedoch ebenfalls von hoher Bedeutung**, da zahlreiche Mitglieder diesen Regelungen unterliegen und deshalb beispielsweise für die Energiebranche keine abschließende Beurteilung der Regelungen getroffen werden kann. **Auch diese Normen sollten frühzeitig mit der Wirtschaft diskutiert werden**.

Stellungnahme

1. § 2 Abs. 1 BSIG – Begriffsbestimmungen

a. Nr. 9 – erheblicher Sicherheitsvorfall

Die Definition zum „erheblichen Sicherheitsvorfall“ in § 2 Abs. 1 Nr. 9 lit. a § 2 Abs. 1 Nr. 10 BSIG lautet wie folgt:

> *„9. „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. 35 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-Richtlnie 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.

b. Nr. 34 - Sicherheit in der Informationstechnik

Diese Definition benennt richtigerweise die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen als Schutzziel. Dieser Dreiklang sollte im gesamten Gesetz einheitlich durchgehalten werden. Teilweise werden auch noch andere Begriffe, wie z.B. die Authentizität, genannt, ohne das sich sachlich ein Unterschied ergeben würde (siehe z.B. § 2 Abs. 1 Nr. 35; 30 Abs. 1 BSIG).

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 werden sollte, dass das Online Portal auch als Rückkanal für die Informationen des BSI zu Betreibern besonders von wichtigen Einrichtungen und wichtigen 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 der 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 wichtige Einrichtungen und wichtige Einrichtungen

In § 28 BSIG werden teilweise Begriffsbestimmungen vorgenommen (§ 28 Abs. 1 – 3, 5, 6 BSIG) und teilweise der sachliche und zeitliche Anwendungsbereich der Rechte und Pflichten für die Betreiber der kritischen Anlagen, der besonders wichtigen Einrichtungen und der wichtigen Einrichtungen festgelegt (§ 28 Abs. 4, 7, 8 BSIG). Dies passt nicht zur Systematik des Gesetzes, da ansonsten die Begriffsbestimmungen in § 2 BSIG festgelegt werden und Kapitel 1 die Überschrift „Anwendungsbereich“ trägt. **Es wird angeregt, die Begriffsbestimmungen einheitlich in § 2 BSIG zu regeln und in § 28 BSIG nur den Anwendungsbereich festzulegen.** Dies dient auch der Lesbarkeit und Übersichtlichkeit des Gesetzes.

a. Abs. 1, 2 – Definition besonders wichtige Einrichtung und wichtige Einrichtung

In den § 28 Abs. 1 – 3 werden die Begriffe der besonders wichtigen Einrichtung, der wichtigen Einrichtung sowie die Berechnung der entsprechenden „cap size“ reguliert. Die Systematik folgt dabei im Grundsatz der Systematik von Art. 3 der NIS 2-Richtlinie.

aa. Abschließende Listen für (besonders) wichtige Einrichtungen

Positiv zu bemerken ist zunächst, dass bereits dem BSIG nunmehr eine abschließende Liste (Anlage 1 und 2) mit Einrichtungsarten beigefügt wurde, die maßgeblich für die Bestimmung der besonders wichtigen und wichtigen Einrichtungen ist. Dies ist deshalb positiv, weil es den Unternehmen deutlich mehr Rechtssicherheit bietet, als wenn die entsprechenden Einrichtungen erst später in einer von der Exekutive zu erlassenden Rechtsverordnung bestimmt werden. **Weiterhin ist positiv, dass die Anlagen 1 und 2 im Hinblick auf die im VKU organisierten Sektoren nicht gegenüber der NIS 2-Richtlinie erweitert wurden, sondern offenbar eine 1:1 Umsetzung angestrebt wird. Für den VKU wäre die nicht dem Diskussionsentwurf beigefügte Anlage 3 ebenfalls wichtig zu beurteilen, da hier die Zentralregierung der öffentlichen Verwaltung bestimmt wird und teilweise VKU-Unternehmen eine öffentlich-rechtliche Rechtsform haben.** Allerdings wird davon ausgegangen, dass hierbei keine Regelungen für die Landesebene oder kommunale Ebene getroffen werden (vgl. die Gesetzesbegründung zu § 28 Abs. 1 Nr. 5 BSIG).

bb. Querverbundsunternehmen

Unklar ist, wie mit Querverbundsunternehmen, also Unternehmen die in mehreren Sektoren tätig sind, umzugehen ist. Werden diese allen Sektoren zugeordnet in denen sie tätig sind? Wenn ja, was bedeutet dies für die (besonders) wichtige Einrichtung in Hinblick auf die zu erfüllenden Pflichten, wenn die Pflichten in den verschiedenen Sektoren unterschiedlich sind. Muss ein Unternehmen operativ in dem Sektor tätig sein oder würde auch eine reine Holding-Gesellschaft erfasst werden, wenn die Tochterunternehmen in den Sektoren tätig sind? **Um diese Frage rechtssicher zu beantworten, schlagen wir vor, beispielhafte Fallkonstellationen in die Gesetzesbegründung oder gegebenenfalls ergänzend in einem FAQ-Katalog zu erläutern**. Im Übrigen wird auf die Ausführungen zu § 28 Abs. 4 BSIG verwiesen.

cc. Betreiber kritischer Anlagen als besonders wichtige Einrichtung

Gemäß § 28 Abs. 1 Nr. 4 BSIG ist ein Betreiber einer kritischen Anlage immer gleichzeitig auch eine besonders wichtige Einrichtung. Dies kann massive Konsequenzen nach sich ziehen:

Bisher bestand der Scope / Geltungsbereich bei der Risikobetrachtung von Betreibern von kritischen Anlagen (bzw. bisher Betreiber von kritischen Infrastrukturen) nur auf den kritischen Dienstleistungen, die durch Bertreiber bereitgestellt werden. Betreiber kritischer Anlagen sollen mit dem NIS-2-Umsetzungsgesetz in Zukunft über den Scope der kritischen Dienstleistungen (z.B. Versorgung der Bevölkerung mit Strom) hinaus auch für alle unkritischen Businessprozesse die zusätzlichen Anforderungen der besonders wichtigen Einrichtungen erfüllen (z.B. für die IT-Systemen der Betriebskantine). Aufgrund dieser deutlichen Ausweitung des Scopes besteht die Gefahr, dass knappe vor allem personelle Ressourcen durch administrative Prozesse in einem Maße gebunden werden, sodass es im Ergebnis zu einer Einbuße bei der IT-Sicherheit kommen kann. Dieses Risiko ist besonders

vor dem Hintergrund des sich weiter verschärfenden Fachkräftemangels sehr ernst zu nehmen. Durch unterschiedliche Nachweisregime für die kritischen Dienstleistungen im Scope der kritischen Anlagen und für die sonstigen unkritischen Businessprozesse im Scope der besonders wichtigen Einrichtungen besteht die Gefahr von übermäßigem bürokratischem Aufwand in den Unternehmen.

Es ist deshalb außerordentlich zu begrüßen, dass die Nachweispflichten für die besonders wichtigen Einrichtungen und wichtigen Einrichtungen deutlich entschärft wurden. Anpassungen müssen noch vorgenommen werden für den Fall, dass eine besonders wichtige Einrichtung gleichzeitig ein Betreiber einer kritischen Anlage ist (siehe hierzu näher Ausführungen zu § 64 BSIG).

b. 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 beurteilt werden, was bei Geltung des Artikel 3 Absatz 4 des Anhangs nicht der Fall wäre.

Ebenfalls sachgerecht und begrüßenswert ist der Umstand, dass für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft lediglich Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme dieser Organisationseinheit maßgeblich sind, ohne die o. g. Kommissionsempfehlung zu berücksichtigen. Dies ergibt sich direkt aus dem Gesetzeswortlaut, da die Empfehlung 2003/361/EG eben nicht auf diese unselbstständigen Organisationseinheiten der Gebietskörperschaft anwendbar ist. Allerdings sollte dies nochmals in der Gesetzesbegründung erläutert werden, da dieser Zusammenhang sonst ggf. missverstanden werden könnte. **Es wird vorgeschlagen, die folgende Ergänzung in die Gesetzesbegründung aufzunehmen** (Vgl. Gesetzesbegründung vom 03.07.2023 zu § 2 Abs. 1 Nr. 12 BSIG):

Formulierungsvorschlag:

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

Nicht ganz klar ist die Bedeutung von § 28 Abs. 3 S. 2 BSIG zur Hinzurechnung der Daten von Partnerunternehmen oder verbundenen Unternehmen. Es heißt wörtlich:

„Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG sind nicht hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse, unabhängig von seinem Partner oder verbundenen Unternehmen ist."

Diese Regelung zielt erkennbar auf Konzernstrukturen ab und soll wohl dem Erwägungsgrund 16 der NIS 2-Richtlinie folgend Artikel 6 Absatz 2 des Anhangs der Empfehlung 2003/361/EG modifizieren.

Wir verstehen den Halbsatz wie folgt: Die Daten eines Partner- oder verbundenen Unternehmens sind dann nicht mit hinzuzurechnen, wenn das jeweils zu prüfende Unternehmen selbst bestimmenden Einfluss auf die Beschaffenheit und den Betrieb der eigenen informationstechnischen Systeme etc. ausübt.

Eine derartige Beschränkung der Hinzurechnung der Daten von Partner- oder verbundenen Unternehmen ist im Grundsatz sachgerecht und absolut zu begrüßen. Über die Gesetzesbegründung wird klargestellt, dass es immer auf den bestimmenden Einfluss des zu betrachtenden Unternehmens auf seine eigenen informationstechnischen Systeme (und nicht auf die der Partner- und Verbundunternehmen) ankommt.

Unklar bleibt jedoch, wann der bestimmende Einfluss des betrachteten Unternehmens auf die eigenen informationstechnischen Systeme tatsächlich vorliegt und wann nicht. Abgestellt wird hierbei allgemein auf die rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme etc. Innerhalb eines Konzerns wird typischerweise zumindest ein rechtlich und wirtschaftlich bestimmender Einfluss des Mutterunternehmens auf ihre Töchter- und Enkelunternehmen bestehen. Es stellt sich jedoch die Frage, ob dies bereits ausreicht, um auch von einem bestimmenden Einfluss auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme zu sprechen. Hierzu folgendes Beispiel: Das Mutterunternehmen B hat auf Grund der Mehrheitsbeteiligung einen bestimmenden rechtlichen und wirtschaftlichen Einfluss auf ihr Tochterunternehmen A. Tochterunternehmen A steuert aber seine eigenen informationstechnischen Systeme in tatsächlicher Hinsicht selbstständig. Kann sich Tochterunternehmen A auf die oben zitierte Ausnahme berufen oder muss sich Tochterunternehmen A die Mitarbeiterzahlen und finanziellen Schwellenwerte von Mutterunternehmen B zurechnen lassen? **Es wird gefordert, die Kriterien für den bestimmenden Einfluss auf die informationstechnischen Systeme klarer auszuformulieren.** Ähnliches gilt für die Betreibereigenschaft in Bezug auf die Betreiber von kritischen Anlagen, wo die gleichen Kriterien maßgeblich sind (vgl. § 1 Abs. 1 Nr. 2 BSI-KritisV; siehe hierzu die Ausführungen zu § 28 Abs. 5).

c. Abs. 4 – Ausnahmen vom Anwendungsbereich

Nach § 28 Abs. 4 Nr. 2 BSIG gelten die Vorgaben aus § 30 BSIG (Risikomanagementmaßnahmen) und § 31 BSIG (Meldepflichten) nicht, für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des EnWG, soweit sie den Regelungen des § 5c des

Energiewirtschaftsgesetzes unterliegen. Der Energiesektor wird somit wie auch bisher überwiegend über das EnWG reguliert. Damit wird der aktuell geltende § 8d Abs. 2 BSIG fortgeführt. Es wird hierbei davon ausgegangen, dass der bisherige § 11 EnWG in den § 5c EnWG verschoben werden soll. Aktuell gibt es keinen § 5c EnWG.

Diese Ausnahme für den Energiesektor wird ausdrücklich begrüßt. Die Zusammenarbeit der Energiewirtschaft mit der BNetzA und die entsprechenden IT-Sicherheitskataloge haben sich seit langer Zeit bewährt. Allerdings kann die Regelung erst abschließend bewertet werden, wenn der neue § 5c EnWG bekannt ist.

Unklar ist, welche Pflichten in sogenannten Querverbundsunternehmen, also Unternehmen die in mehreren Sektoren tätig sind, gelten. So ist es z.B. nicht ungewöhnlich, dass ein Stadtwerk sowohl Telekommunikationsnetze betreibt, als auch die Trinkwasserversorgung übernimmt. Es stellt sich nunmehr die Frage, ob dieses Querverbundsunternehmen nur den Regelungen des TKG unterliegt, nur den Regelungen des BSIG oder beiden Regulierungen. Der Verweis auf das Wort „soweit“ (vgl. § 28 Abs. 4 Nr. 1 BSIG bzw. § 28 Abs. 4 Nr. 2 BSIG für den parallelen Fall der Energieunternehmen) wird zu keiner Lösung führen, da der Scope der Betrachtung im Rahmen der besonders wichtigen Einrichtungen / wichtigen Einrichtungen auf das gesamte Unternehmen ausgedehnt wurde. Es kann also nicht ohne weiteres darauf abgestellt werden, dass die Pflichten aus dem TKG nur „insoweit“ beachtet werden müssen, als das sie TK-Anlagen betreffen. Es handelt sich insgesamt um ein Unternehmen aus dem Sektor Telekommunikation und auch insgesamt um ein Unternehmen aus dem Sektor der Trinkwasserversorung. **Es wird gefordert klarzustellen, welche Pflichten für Querverbundsunternehmen in einem solchen Fall gelten.**

d. Abs. 5 – 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 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. Im Übrigen wird auf die Ausführungen zu § 28 Abs. BSIG verwiesen, wo sich dieses Problem in gleicher Weise für die Berechnung der maßgeblichen Schwellenwerte im Bereich der besonders wichtigen Einrichtungen / wichtigen Einrichtungen stellt.

e. 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).

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.**

Zum einen 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…“*). Ferner wird in Zusammenschau mit § 31 BSIG beschrieben, dass es bei der Beurteilung der Verhältnismäßigkeit der Maßnahmen auf die Größe der Einrichtung / des Betreibers ankommt und deshalb eine Abstufung zwischen den Pflichten des Betreibers der kritischen Anlagen / besonders wichtigen Einrichtungen / wichtigen Einrichtungen gemacht wird. Auch die wirtschaftlichen Auswirkungen und die Umsetzungskosten dürfen hierbei berücksichtigt werden, was in der Praxis von herausragender

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

Bedeutung ist. Zudem wird in der Gesetzesbegründung zu § 31 BSIG klargestellt, dass sich die strengen Anforderungen in Bezug auf die Betreiber der kritischen Anlagen nicht gleichzeitig auf die gesamte Einrichtung beziehen, obwohl der Betreiber einer kritischen Anlage gleichzeitig auch eine besonders wichtige Einrichtung ist (vgl. § 28 Abs. 6 Nr. 4 BSIG).

Innerhalb von Konzernstrukturen bestehen jedoch Gefahren von bürokratischen Doppelaufwänden, ohne dass es zu einer Verbesserung der Sicherheit der Unternehmen kommt. Zur Verdeutlichung kann auf das folgende Beispiel zurückgegriffen werden. Mutterunternehmen B, als auch das 100% Tochterunternehmen A sind in den erfassten Sektoren tätig und erreichen die maßgeblichen Schwellenwerte. Sie unterliegen somit grundsätzlich den Pflichten des BSIG. Was gilt aber nun, wenn Mutterunternehmen B die gesamten IT-Systeme des Tochterunternehmens A unter seiner Kontrolle hat und entsprechend zertifizieren lässt. Kann das Tochterunternehmen A sodann (zumindest teilweise) auf das entsprechende Zertifikat des Mutterunternehmens B verweisen oder muss eine komplette eigene Zertifizierung erfolgen? Zumindest für den rein technischen Teil des IT-Systems wäre dies überflüssig und würde zu keinem Sicherheitsgewinn führen. Im Bereich des Referentenentwurfs zum Kritis-DachG erkennt der Gesetzgeber eine grundsätzliche Anrechnung bestehender Zertifizierungen an (vgl. § 11 Abs. 7 Kritis-DachG). **Es wird gefordert, dass eine solche Anrechnung bestehender Zertifikate auch im Bereich des NIS 2-Umsetzungsgesetzes möglich ist.** Im Übrigen wird auf die Ausführungen zu den Nachweispflichten in §°39, 64, 65 BSIG verwiesen.

Weitere Besonderheiten treten bei Querverbundsunternehmen auf, also Unternehmen die in mehreren Sektoren tätig sind. Zunächst wird davon ausgegangen, dass diese den Anforderungen aller sie betreffenden Sektoren genügen müssen. In den unterschiedlichen Sektoren bestehen jedoch verschiedene Regelwerke, wie die Pflichten der IT-Sicherheit erfüllt werden können. So müssen beispielsweise Energieunternehmen die entsprechenden IT-Sicherheitskataloge der BNetzA erfüllen, während Wasserversorgungsunternehmen entweder den B3S-Wasser/Abwasser erfüllen können oder aber die ISO-27000-Reihe oder dem BSI-Grundschutz folgen. Bei allen Unterschieden gibt es jedoch Teile, die in allen IT-Sicherheitsmanagementsystemen gleich geregelt werden können und in Querverbundsunternehmen und/oder Konzernen teilweise auch bereits werden. Dies betrifft z.B. die Frage, wie mit Sicherheitsvorfällen umzugehen ist oder wie die Risikobetrachtung vorgenommen wird. Nicht zielführend wäre es, wenn diese übergreifenden Aspekte mehrfach in einem Querverbundsunternehmen zertifiziert werden müssten. **Vielmehr sollte es möglich sein, im Rahmen eines kombinierten Audits diese übergreifenden Aspekte nur einmal überprüfen zu lassen und im Übrigen für jeden Sektor nur das verbleibende Delta durch den Auditor zertifizieren zu lassen**. Dies würde die bürokratischen Aufwände deutlich verringern.

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. **Es muss sichergestellt werden, dass die Betreiber / Einrichtungen 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 § 57 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.

d. Abs. 7 – Informationsaustausch

Gemäß § 30 Abs. 7 BSIG werden die besonders wichtigen Einrichtungen verpflichtet, am Informationsaustausch teilzunehmen. Dies ist richtig, da ein Informationsaustausch untereinander von herausragender Bedeutung ist, um den Bedrohungen für die Informationssicherheit Herr werden zu können. In der Gesetzesbegründung wird der bidirektionale Austausch (also inklusive dem BSI) beschrieben. Dieser findet sich jedoch nicht im Gesetzestext wieder. **Es wird gefordert, diesen bidirektionalen Austausch auch im Gesetz festzuschreiben. Zudem sollte zumindest in der Gesetzesbegründung festgeschrieben werden, was genau der Austausch umfasst.** Geht es ausschließlich um die Cyber-Sicherheitswarnungen des BSI und soll dies mehr umfassen? Im Übrigen wird auf die Ausführungen zu § 6 BSIG verwiesen.

d. Abs. 9 – Branchenspezifische Sicherheitsstandards

Gemäß § 30 Abs. 9 BSIG können besonders wichtige Einrichtungen und ihre Branchenverbände branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach § 30 Abs. 1 BSIG vorschlagen. Diese Regulierung wird im Grundsatz sehr begrüßt, da schon bisher sehr gute Erfahrungen mit den branchenspezifischen Sicherheitsstandards

(auch B3S genannt) gemacht wurden. **Allerdings sollten auch wichtige Einrichtungen von diesen Sicherheitsstandards profitieren können und entsprechende B3S erarbeiten können.**

6. § 31 - Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

In Zusammenschau mit den Regelungen des § 30 Abs. 1 BSIG und der entsprechenden Gesetzesbegründung ist diese Regelung zu begrüßen. Es wird hinreichend deutlich gemacht, dass eine klare Abstufung besteht zwischen der Pflichtentiefe für die Betreiber von kritischen Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen. Über die Gesetzesbegründung wird für den thematisch bereits befassten Leser auch hinreichend deutlich, dass diese Abstufung auch bei innerhalb der Betreiber von kritischen Anlagen besteht, da diese immer auch gleichzeitig besonders wichtige Einrichtungen sind (vgl. § 28 Abs. 1 Nr. 4 BSIG). Ausweislich der Gesetzesbegründung gelten in einem solchen Fall die besonders hohen Anforderungen nur in Bezug auf versorgungsrelevante informationstechnische Systeme, Komponenten und Prozesse. Für die nicht versorgungsrelevanten Bereiche gelten diese erhöhten Anforderungen dagegen nicht. **Dieser Zusammenhang könnte in der Gesetzesbegründung jedoch nochmals etwas deutlicher dargestellt werden, da diese Ableitung relativ viel Vorwissen benötigt.**

Positiv ist festzustellen, dass die Einrichtung von Systemen zur Angriffserkennung nach § 31 Abs. 2 BSIG nur für die Betreiber von kritischen Anlagen verpflichtend wird. Die restlichen Betreiber von (besonders) wichtigen Einrichtungen könnten in einem ersten Schritt hiervon überfordert sein.

7. § 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.[2] 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-

[2] 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.[3] Durch § 38 Abs. 3 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.**

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.

8. § 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.**

Weiterhin ist es sehr zu begrüßen, dass im Grundsatz lediglich Betreiber von kritischen Anlagen ex-ante Nachweispflichten unterliegen. Dies bedeutet nicht, dass die (besonders) wichtigen Einrichtungen die Pflichten aus dem BSIG nicht erfüllen müssen, denn diese Pflichten ergeben sich bereits aus dem § 30 BSIG direkt. Es kommt aber zu einer deutlichen Verschlankung der Umsetzung, da Nachweise nur ausnahmsweise von den Behörden direkt eingefordert werden (vgl. die Kommentierung zu den §§ 64, 65 BSIG).

Offene Fragen bestehen jedoch, wenn innerhalb eines Konzerns bereits Nachweise über bestimmte IT-Systeme bestehen. Es stellt sich das Problem der doppelten Nachweiserbringung (siehe näher die Ausführungen in § 30 Abs. 1 BSIG). Auch bei Querverbundsunternehmen bestehen Besonderheiten bei einem kombinierten Audit. Auch insofern wird auf die Ausführungen in § 30 Abs. 1 BSIG verwiesen.

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

9. § 40 - Zentrale Melde- und Anlaufstelle

Gemäß § 40 Abs. 2 Nr. 4 BSIG hat das BSI unverzüglich die besonders wichtigen Einrichtungen und wichtigen Einrichtungen über sie betreffende Informationen nach den Nummern 1 bis 3 durch Übermittlung an die Kontaktdaten nach § 32 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 / Einrichtungen 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 / Einrichtungen 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.**

10. § 57 BSIG – Ermächtigung zum Erlass von Rechtsverordnungen

Gemäß § 57 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.

Zum Einsatz von IKT-Produkten, -Diensten und –Prozessen (§ 57 Abs. 3 BSIG) wird auf die Anmerkungen zu § 30 Abs. 6 BSIG verwiesen.

11. § 64 BSIG - Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

a. Abs. 1 – Abs. 4 - Nachweispflichten

Gemäß § 64 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 § 64 Abs. 3 BSIG. Die maßgeblichen Kriterien zur Ermessensausübung finden sich hierbei in § 64 Abs. 4 BSIG.

Positiv ist zunächst hieran, dass besonders wichtige Einrichtungen und wichtige Einrichtungen nicht ohne weiteres ex-ante Nachweispflichten unterliegen, wie dies bei Betreibern von kritischen Anlagen der Fall ist (vgl. § 31 BSIG).

Die ermessenssteuernde Norm in § 64 Abs. 4 BSIG folgt dabei 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 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 § 64 Abs. 4 BSIG nicht nur auf § 64 Abs. 3 BSIG (Anforderung der Nachweise), sondern auch auf § 64 Abs. 1 BSIG (Verpflichtung zur Auditierung, Prüfung und Zertifzierung) erstreckt werden. Anderenfalls existieren keine ermessenleitenden Kriterien für die Festlegung der Verpflichtungen aus § 64 Abs. 1 BSIG.

Formulierungsvorschlag:

§ 64 - 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.**

Offene Fragen bestehen jedoch, wenn innerhalb eines Konzerns bereits Nachweise über bestimmte IT-Systeme bestehen. Es stellt sich das Problem der doppelten Nachweiserbringung (siehe näher die Ausführungen in § 30 Abs. 1 BSIG). Auch bei Querverbundsunternehmen bestehen Besonderheiten bei einem kombinierten Audit. Auch insofern wird auf die Ausführungen in § 30 Abs. 1 BSIG verwiesen.

b. Abs. 8, 9 – Unterrichtungspflichten und Überwachungsbeauftragte

In § 64 Abs. 8 S. 2 BSIG wird auf „diese Richtlinie“ verwiesen. Es müsste „dieses Gesetz“ heißen.
Es ist unklar, welche Verpflichtungen durch den Überwachungsbeauftragten überwacht werden sollen. Die Verweise auf die §§ 28, 29 und 37 BSIG stimmen ersichtlich nicht.

12. § 65 BSIG - Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen

Für wichtige Einrichtungen sind gemäß dieser Vorschrift grundsätzlich die gleichen Aufsichtsmaßnahmen des Bundesamts vorgesehen, wie in § 64 BSIG für besonders wichtige Einrichtungen. Jedoch gilt für wichtige Einrichtungen als Voraussetzung zur Ausübung dieser Aufsichtsmaßnahmen, dass Tatsachen die Annahme rechtfertigen, dass eine wichtige Einrichtung die Anforderungen aus den §§ 30, 31 oder 32 BSIG nicht oder nicht richtig umgesetzt hat. **Dies ist zu begrüßen, da so eine weitere Abstufung von den wichtigen Einrichtungen zu den besonders wichtigen Einrichtungen geschaffen wird und dem Verhältnismäßigkeitsgrundsatz Rechnung getragen wird.**

13. TKG und EnWG

Leider sind die spezialgesetzlichen Regelungen im TKG und EnWG nicht Teil dieses Diskussionsentwurfs. Für den VKU sind diese Regelungen jedoch ebenfalls von hoher Bedeutung, da zahlreiche Mitglieder diesen Regelungen unterliegen und deshalb beispielsweise für die Energiebranche keine abschließende Beurteilung der Regelungen getroffen werden kann. **Es wird gefordert, auch diese spezialgesetzlichen Normen frühzeitig mit der Wirtschaft zu diskutieren.**

VKU Ansprechpartner
Wolf Buchholz

Fachgebietsleiter Kritische Infrastruktur und Cybersicherheit
Abteilung Recht, Finanzen und Steuern
Telefon: +49 30 58580-317
E-Mail: buchholz@vku.de