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 24.06.2024

Berlin, 03.07.2024

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 24.06.2024 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

Die vorliegende Fassung des Referentenentwurfs berücksichtigt viele Anregungen aus der letzten Stellungnahme des VKU. Allerdings existieren weiterhin **verbesserungswürdige Punkte**:

- Die **IT-Sicherheitspflichten** innerhalb eines Querverbundsunternehmens sind so **komplex** beschrieben, dass sie kaum noch verständlich sind. Die massive **Ausdehnung der Vorgaben des Energiewirtschaftsgesetzes** auch auf die nicht für den Betrieb des Netzes / Anlage notwendigen IT-Systeme (reguläre Office IT**) wird abgelehnt** (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 wird. Nicht alle Energieanlagen, sondern **nur kritische Energieanlagen** dürfen in den **Anwendungsbereich** des **EnWG** mit seinen IT-Sicherheitskatalogen fallen (siehe die Ausführungen zu § 5c EnWG).
- Die **IT-Sicherheitskataloge** für die Energieversorgungsnetze und Energieanlagen dürfen sich zudem **nur auf die Netze und die (kritischen) Anlagen** beziehen und nicht auf die Office-IT. In jedem Fall müssen im Hinblick auf die zu erfüllenden IT-Sicherheitspflichten und die Form der Nachweise eine **strikte Abstufung zwischen Betreibern von kritischen Anlagen und bloßen (besonders) wichtigen Einrichtungen** erfolgen (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 **Bestimmung des Betreibers ist weiterhin auslegungsbedürftig** und sollte innerhalb der Gesetzesbegründung präzisiert werden (siehe die Ausführungen zu § 28 Abs. 6 BSIG). Auch ist die **Zuordnung der Mitarbeiter- und Umsatzzahlen**

innerhalb eines **Konzerns unklar**, wenn z.B. Mutter- und Tochterunternehmen einen unterschiedlichen Geschäftszweck verfolgen (siehe die Ausführungen zu § 28 Abs. 3 BSIG).

- In Bezug auf §§ 2, 6, 11, 28 Abs. 7, 8; 30 Abs. 1, 5, 6, 39, 40 BSIG wird weiterhin auf unsere Stellungnahme vom 28.05.2024 verwiesen.

Stellungnahme

1. § 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 (KMU-Empfehlung) 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 aufzunehmen** (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.

Ein Problem ergibt sich jedoch im Bereich der Konzernstrukturen. Für diese gilt (außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft) die oben genannte KMU-Empfehlung. Verkürzt gesprochen führt dies dazu, dass bei Partnerunternehmen und verbundenen Unternehmen wechselseitig die Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme zugerechnet werden. Während bei Partnerunternehmen eine Zurechnung anteilsmäßig im Verhältnis der jeweils gehaltenen Geschäftsanteile / Stimmrechte erfolgt, werden bei verbundenen Unternehmen 100% der Daten hinzugerechnet.[1] Diese absolute Zurechnung wird dazu führen, dass die zuvor vorgenommene Einschränkung der Betrachtung nur auf die der Einrichtungsart zuzuordnende Geschäftstätigkeit (§ 28 Abs. 3 Nr. 1 BSIG) häufig ins Leere laufen wird.

Ein Beispiel wäre, wenn Unternehmen A Wasser- und Abfalldienste erbringt, aber in diesen einzelnen Geschäftsbereichen jeweils unter den Schwellenwerten bleibt. Ist nun aber das deutlich größere Unternehmen B mit mehreren tausend Mitarbeitern, das keinerlei Tätigkeiten im Bereich von Wasser- und Abfalldiensten erbringt, an Unternehmen A mit mindestens 25% beteiligt, so würde Unternehmen A durch die Zurechnung im Rahmen der KMU-Empfehlung in beiden Bereichen über den maßgeblichen Schwellenwert gedrückt. In größeren Konzernverbünden würde die Begrenzung auf die zuzuordnende Geschäftstätigkeit somit meist leerlaufen.

Sinnvoll erscheint es, die Daten von Partner- oder verbundenen Unternehmen nur insoweit hinzuzurechnen, als dass das Partnerunternehmen oder verbundene Unternehmen ebenfalls in der zu betrachtenden Geschäftstätigkeit engagiert ist.

Formulierungsvorschlag:

§ 28 Abs. 3 BSIG

Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist auf

1. die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen und
2. außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung 2003/361/EG mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden.

Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG sind nur insoweit hinzuzurechnen, als dass das Partner- oder verbundene Unternehmen die gleiche Geschäftstätigkeit wie die betrachtete Einrichtung durchführt.
Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG sind nicht hinzuzurechnen, […].

[1] Siehe hierzu die ausführlichen Erläuterungen im „Benutzerleitfaden zur Definition von KMU“ der Kommission.

Im Übrigen sollte in der Gesetzesbegründung unmissverständlich festgeschrieben werden, dass die in den Anlagen 1 und 2 genannten Einrichtungsarten bzw. die in der BSI-Kritisverordnung genannten Anlagen jeweils einzeln zu betrachten sind, bevor auf die Norm des § 28 Abs. 3 S. 1 Nr. 1 BSIG abgestellt wird. Es muss klar sein, dass z.B. bei einem Querverbundsunternehmen, das eine Energieerzeugungsanlage (vgl. Anlage 1 Nr. 1.1.4), ein Elektrizitätsverteilernetz (vgl. Anlage 1 Nr. 1.1.2) und ein Fernkältenetz betreibt (vgl. Anlage 1 Nr. 1.2.1) die Zahlen der jeweiligen Einrichtungsart strikt zu trennen sind und nicht aufaddiert werden.

Zudem muss klargestellt werden, dass die Zahlen der Fernwärmeversorgung und der Fernkälteversorgung ebenfalls strikt getrennt voneinander zu betrachten sind. Da beide Einrichtungsarten in einer Zeile genannt werden (vgl. Anlage 1 Nr. 1.2.1) könnte ansonsten Spielraum für eine andere Interpretation bestehen. **Es wird angeregt beide Einrichtungsarten in unterschiedlichen Zeilen zu beschreiben.**

b. Abs. 4 – Ausnahmen vom Anwendungsbereich

Die Regelung des § 28 Abs. 4 BSIG wurde im Vergleich zur Vorfassung deutlich überarbeitet. Dabei wird zunächst begrüßt, dass neben den §§ 31, 32, 35 und 39 BSIG in der überarbeiteten Fassung auch die §§ 30, 63 und 64 BSIG mit in den Ausschlusstatbestand aufgenommen wurden. So werden in diesem Bereich die spezialgesetzlichen Regelungen (EnWG / TKG) sinnvoll abgegrenzt von den allgemeinen Regelungen des BSIG. Der VKU hatte exakt diese Überarbeitung gefordert, weshalb wir diesen Teil der Neufassung begrüßen.

Allerdings kommt es weiterhin im Bereich der Registrierung 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. Zwar verweist § 5c Abs. 8 EnWG teilweise auf den § 33 Abs. 1 BSIG, allerdings nicht vollständig. So wird beispielsweise nicht auf den § 33 Abs. 1 Nr. 5 BSIG verwiesen und auch auf § 33 Abs. 2 BSIG wird von § 5c Abs. 8 EnWG nur teilweise verwiesen (z.B. in Bezug auf Betreiber von Energieanlagen nur auf die kritischen Energieanlagen).

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, 39, 63 und 64 sind nicht anzuwenden auf besonders wichtige Einrichtungen und wichtige Einrichtungen, die […].

Gänzlich neu aufgenommen wurde in die vorliegende Fassung § 28 Abs. 4 S. 2, 3 BSIG. Hintergrund ist laut Gesetzesbegründung die Sondersituation in Querverbundsunternehmen, also Unternehmen die neben dem Sektor der Energie auch noch in weiteren Sektoren (z.B. Wasser) tätig sind (teilweise auch Mehrspartenunternehmen genannt). **Zunächst begrüßt der VKU, dass sich speziell mit der Situation in Querverbundsunternehmen beschäftigt wird, da in der Mitgliedschaft des VKU sehr häufig solche Arten von Unternehmen anzutreffen sind**. Ein Stadtwerk ist üblicherweise ein Querverbundsunternehmen.

Die Regelungen des § 28 Abs. 4 BSIG und § 5c EnWG, sowie die dazugehörige Gesetzesbegründungen sind allerdings so komplex, dass sie kaum noch verständlich sind. Bildet man zur Veranschaulichung dieser Regeln als Beispiel ein Querverbundsunternehmen

- mit einer kritischen Energieerzeugungsanlage (Schwellenwert der BSI-KritisV überschritten),
- einer kritischen Trinkwassergewinnungsanlage (Schwellenwert der BSI-KritisV überschritten) und
- einer Anlage zur thermischen Behandlung von Siedlungsabfällen (Schwellenwert der BSI-KritisV wird nicht überschritten, d.h. es liegt insoweit nur eine wichtige Einrichtung vor)

so soll wohl folgendes gelten:

- Die IT-Systeme, die für den sicheren Anlagenbetrieb der kritischen Energieerzeugungsanlage notwendig sind, werden über § 5c EnWG (bzw. der IT-Sicherheitskataloge) reguliert (§ 28 Abs. 4 S. 1 Nr. 2 BSIG)
- Die IT-Systeme, die für den sicheren Anlagenbetrieb der kritischen Trinkwassergewinnungsanlage notwendig sind, werden über das BSIG reguliert (§ 28 Abs. 4 S. 2 Var. 1, S. 3 BSIG)
- Die IT-Systeme, die für den sicheren Anlagenbetrieb der unkritischen Anlage zur thermischen Behandlung von Siedlungsabfällen notwendig sind, werden über das BSIG reguliert (§ 28 Abs. 4 S. 2 Var. 2, S. 3 BSIG)
- Alle IT-Systeme in diesem Querverbundsunternehmen, die nicht für den sicheren Anlagenbetrieb unmittelbar notwendig sind (Office-IT ohne Schnittstellen zu den Anlagen) werden einheitlich über § 5c EnWG (bzw. die IT-Sicherheitskataloge) reguliert (Umkehrschluss aus § 28 Abs. 4 S. 3 BSIG bzw. die korrespondierende Gesetzesbegründung (S. 163, 216))

Insbesondere der Umstand, dass zukünftig anscheinend alle IT-Systeme, die nicht für den sicheren Anlagenbetrieb unmittelbar notwendig sind, einheitlich über § 5c EnWG und die dortigen IT-Sicherheitskataloge reguliert werden sollen, ist erklärungsbedürftig. Aus der Gesetzesbegründung geht nicht hervor, warum diese massive Änderung zum bisherigen

status quo vorgenommen wird. Diese Änderung führt zu einer deutlichen Verschiebung der Zuständigkeiten (und damit auch des Einflusses) vom BSI zur BNetzA.

Der VKU kann die Auswirkungen in der Kürze der Stellungnahmefrist nicht abschließend beurteilen. **Nach unserer ersten Einschätzung sollten die nicht für den sicheren Anlagenbetrieb unmittelbar notwendigen IT-Systeme einheitlich über das BSIG reguliert werden und unter Aufsicht des BSI stehen.** Diese IT-Systeme haben sehr häufig nichts mit den speziell bei der BNetzA beaufsichtigten Sektoren zu tun und sind eher allgemeiner Natur (z.B. ein SAP-System zur Lohnabrechnung). Teilweise wird auch in den branchenspezifischen Sicherheitsstandards (B3S) auf eben diesen unkritischen Bereich eingegangen, womit wiederum eine Überschneidung stattfinden würde. Zudem würden eine Vielzahl von Unternehmen erstmals durch die BNetzA reguliert und beaufsichtigt werden. Es stellt sich die Frage, ob hierfür die erforderlichen Mitarbeiter zur Verfügung stehen und warum Doppelstrukturen mit dem BSI aufgebaut werden sollen. Zudem könnten die strengen Regelungen der IT-Sicherheitskataloge mittelbar auf alle Querverbundsunternehmen durchschlagen, so insbesondere mögliche Pflichten zum Aufbau eines ISMS oder zur Implementierung von Systemen zur Angriffserkennung (siehe insbesondere näher die Ausführungen zu § 5c Abs. 3 EnWG).

Sollte an dieser Regulierung festgehalten werden, so muss in der Gesetzesbegründung dargelegt werden, warum man diese massive Änderung im Vergleich zum status quo vornimmt.

Weiterhin müsste § 28 Abs. 4 S. 3 BSIG angepasst werden. Nach dieser Norm gilt S. 2 für alle informationstechnischen Systeme, die für den Betrieb der kritischen Anlage erforderlich sind. Sowohl § 28 Abs. 4 S. 2 BSIG, als auch die Gesetzesbegründung hierzu beziehen sich jedoch auch auf Betreiber unterhalb der Kritis-Schwellenwerte, nämlich die besonders wichtigen und wichtigen Einrichtungen in den Anlagen 1 und 2.

Zudem muss der letzte Absatz der Gesetzesbegründung zu § 28 Abs. 4 BSIG überarbeitet werden. Dieser wurde unverändert aus der letzten Fassung des Gesetzes übernommen und „hängt in der Luft“. Zudem beschreibt er eigentlich das Gegenteil des soeben dargelegten, da nach den dortigen Ausführungen für die sonstige IT, welche für die Erbringung der Dienste genutzt wird, die Vorgaben des BSIG gelten sollen (und gerade nicht diejenigen des EnWG).

Im Übrigen wird auf die Ausführungen zu § 5c EnWG verwiesen, wo spezielle Ausführungen hauptsächlich für die reinen Energieversorgungsunternehmen gemacht werden.

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[2] erfolgt. Eine solche Klarstellung ist auch deshalb wichtig, weil dies Auswirkungen auf die Frage hat, wann eine 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.

2. § 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.[3] 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-

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

[3] 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, das 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.

3. § 63 BSIG - Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

Gemäß § 63 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, 32, 38 Abs. 3 BSIG 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.** § 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 § 63 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 exante 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 § 63 Abs. 4 BSIG nicht nur auf § 63 Abs. 3 BSIG (Anforderung der Nachweise), sondern auch auf § 63 Abs. 1 BSIG (Verpflichtung zur Auditierung, Prüfung und Zertifizierung) erstreckt werden. Anderenfalls existieren keine ermessenleitenden Kriterien für die Festlegung der Verpflichtungen aus § 63 Abs. 1 BSIG.

Formulierungsvorschlag:

§ 63 - 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.**

4. § 5c EnWG

Erstmals werden die neuen Regelungen des EnWG inklusive der Gesetzesbegründung bekanntgemacht. Man muss 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. Es kommt dabei jedoch zu einer massiven Ausweitung des Anwendungsbereichs der Normen im Vergleich zu den bisherigen Regelungen des § 11 EnWG.

Der Schwerpunkt der folgenden Kommentierung liegt auf den Auswirkungen, die sich für die Betreiber von Energienetzen und Energieanlagen ergeben. Zu den speziellen Auswirkungen auf Querverbundsunternehmen (also Unternehmen die neben dem Sektor Energie noch in weiteren Sektoren tätig sind) und die massive Ausweitung der Regeln des

EnWG auch auf diese Unternehmen, wird auf die Ausführungen zu § 28 Abs. 4 BSIG verwiesen.

a. § 5c Abs. 1 EnWG – Anforderungen an die Betreiber von Energieversorgungsnetzen

Die massive Ausweitung des Anwendungsbereichs der Normen des EnWG wird zunächst nur in der Gesetzesbegründung deutlich. Denn dort heißt es:

> *„Entsprechend des Art. 21 Abs. 1 NIS2-Richtlinie werden die Cybersicherheitsanforderungen auf alle Telekommunikations- und Datenverarbeitungssysteme, die die Betreiber zur Erbringung ihrer Dienste nutzen, erweitert."*
>
> *„In Absätzen 1 und 2 werden die IT-Sicherheitskataloge entsprechend den Vorgaben der NIS2-Richtlinie erweitert und werden alle Dienste, die die Betreiber erbringen, umfassen und nicht nur diejenige, die für den sicheren Netz- oder Anlagenbetrieb notwendig sind."*

Es soll also der „Scope" bzw. der Geltungsbereich massiv ausgeweitet werden. Über den Scope bzw. den Geltungsbereich wird festgelegt, welche Systeme, Prozesse und Komponenten betrachtet und abgesichert werden und welche Bereiche nicht mitbetrachtet werden.[4] Bisher war es so, dass der Scope / Geltungsbereich sich im Bereich der Energienetze nur auf die TK/EDV-Systeme erstreckt hat, welche Teil der Netzsteuerung sind, sowie auf die TK/EDV-Systeme, die zwar nicht Teil der Netzsteuerung sind, aber deren Ausfall die Sicherheit des Netzbetriebs gefährden könnte.[5] Zukünftig soll der Scope / Geltungsbereich auf alle Telekommunikations- und Datenverarbeitungssysteme, die die Betreiber zur Erbringung ihrer Dienste nutzen erweitert werden. Ganz konkret bedeutet dies, dass auch die Office-IT oder die IT zur Abrechnung in der Kantine im Geltungsbereich liegt.

Der VKU kann die Auswirkungen in der Kürze der Stellungnahmefrist nicht abschließend beurteilen. **Nach unserer ersten Einschätzung sollten die nicht für den sicheren Netzbetrieb unmittelbar notwendigen IT-Systeme weiterhin im Regelungsbereich des BSIG und unter Aufsicht des BSI verbleiben.** Hintergrund ist, dass die IT-Sicherheitskataloge deutlich zu streng sind für die nicht für den sicheren Netzbetrieb unmittelbar notwendigen IT-Systeme. Insbesondere die Pflichtentiefe und die Notwendigkeit eine Zertifizierung bzw. der ex ante-Nachweise ist in Bezug auf diese IT-Systeme nicht angemessen (siehe hierzu näher die Ausführungen zu § 5c Abs. 3 EnWG). In Bezug auf die Querverbundsunternehmen wird auf die Ausführungen zu § 28 Abs. 4 EnWG verwiesen.

---

[4] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-Nachweise/Konkretisierung-Geltungsbereich/konkretisierung-geltungsbereich_node.html.

[5] IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, S. 6.

Zudem muss man feststellen, dass die in der Gesetzesbegründung beschriebene Vorgabe nicht durch den Wortlaut des § 5c Abs. 1 S .1 EnWG gedeckt ist. Dort wird abgestellt auf *„einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für den sicheren Netzbetrieb notwendig sind".* Dies entspricht dem aktuellen Wortlaut des § 11 Abs. 1a S. 1 EnWG, der aber gerade durch den Bezug auf den „sicheren Netzbetrieb" die zuvor beschriebene Eingrenzung des Scopes / Geltungsbereichs vornimmt. IT-Systeme, die nicht für sicheren Netzbetrieb notwendig sind, werden nicht umfasst.[6] Die Office-IT (ohne Verbindung zum Netzbetrieb, z.B. in Form eines SAP-Systems) oder die Kantinen-IT sind aber nicht notwendig für einen sicheren Netzbetrieb.

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

Auch für die Betreiber von Energieanlagen wird der Scope / Geltungsbereich auf sämtliche IT-Systeme des Unternehmens ausgeweitet. **Auch hier wird dies wird lediglich in der Gesetzesbegründung beschrieben, findet sich jedoch nicht hinreichend im Wortlaut von § 5c Abs. 2 EnWG wieder.**

Im Bereich der Betreiber der Energieanlagen wird aber auch der persönliche Anwendungsbereich der Norm massiv ausgeweitet. 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 Einrichtungen sind. 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.**

Formulierungsvorschlag:

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

(2) Der Betreiber einer Energieanlage, der ~~besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes vom [einsetzen: Datum und Fundstelle von Artikel 1] oder wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist~~ **eine kritische Anlage nach § 2 Absatz 1 Nummer 21 des BSI-Gesetzes betreibt** und […].

Sollte keine Anpassung des Gesetzeswortlauts erfolgen, kommen insbesondere auf eine Vielzahl von kleinen Betreibern von Energieanlagen zusätzliche hohe Aufwände zu, die

[6] Kipker/Reusch/Ritter/Voigt/Böhme, 1. Aufl. 2023, EnWG § 11 Rn. 79.

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.

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.

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

Die Gesetzesbegründung stellt zunächst fest, dass die IT-Sicherheitskataloge erweitert werden auf alle Dienste, die die Betreiber erbringen und nicht nur diejenigen umfassen, die für den sicheren Netz- oder Anlagenbetrieb notwendig sind. Zudem würden die Kataloge auch für alle IT-Systeme von Querverbundsunternehmen gelten, die nicht notwendig sind für den sicheren Netz- oder Anlagenbetrieb (siehe Ausführungen zu § 28 Abs. 4 BSiG). **Beides lehnt der VKU wie zuvor beschrieben ab. Sollte gleichwohl an dieser Form der Regulierung festgehalten werden, so müssen zumindest die Vorgaben zu den IT-Sicherheitskatalogen geschärft werden.**

Dies betrifft insbesondere die Pflichtentiefe der Anforderungen an die IT-Sicherheit. Die §§ 30, 31 BSIG stufen hierbei ab zwischen den Anforderungen, die die Betreiber von kritischen Anlagen vornehmen müssen (vgl. § 31 BSIG) im Vergleich zu den Anforderungen, die die (besonders) wichtigen Einrichtungen vornehmen müssen (vgl. § 30 BSIG und die entsprechende Gesetzesbegründung). Im Bereich des neuen EnWG heißt es in der Gesetzesbegründung insoweit:

> *„Die Bundesnetzagentur ist befugt die Maßnahmen im Sinne der Verhältnismäßigkeit insbesondere mit Blick auf den sicheren Netz- oder Anlagenbetrieb abzustufen und kann dabei sowohl höhere als auch niedrigere Anforderungen an die IT-Sicherheitsmaßnahmen vorsehen.“*

Dies ist nicht hinreichend bestimmt, sondern belässt der BNetzA einen Ermessensspielraum, ob sie eine solche Abstufung vornehmen möchte oder nicht. Dies wird abgelehnt. **Es wird gefordert, die dreistufige Form der Regulierung in den §§ 30, 31 BSIG auch verbindlich für den Bereich der IT-Sicherheitskataloge festzuschreiben. Dabei ist darauf zu achten, dass lediglich für Energienetze und kritische Energieanlagen ein ISMS durch die**

Betreiber aufzubauen und auch nur insoweit Systeme zur Angriffserkennung implementiert werden müssen.

Im Vergleich zu § 30 Abs. 1 S. 2 BSIG fehlt in § 5c Abs. 3 S. 2 EnWG 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. 3 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.

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. Diese Anforderungen könnten in Querverbundsunternehmen dann auf die gesamte Office-IT durchschlagen.

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

Zunächst ist äußerst positiv zu bemerken, dass nach § 5c Abs. 4 EnWG 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).

Unklar bleibt in diesem Zusammenhang jedoch die Aussage in der Gesetzesbegründung zu § 5c Abs. 3 EnWG, wonach die BNetzA auch strengere Nachweisanforderungen für den

sicheren Netz- oder Anlagenbetrieb vorsehen kann. Genannt werden in diesem Zusammenhang Sicherheitsaudits, Prüfungen und Zertifizierungen. **Es muss eindeutig festgeschrieben werden, dass sich mögliche Zertifizierungen nur auf die Betreiber von Energieversorgungsnetzten und kritischen Energieanlagenbeziehen beziehen und zwar auch nur insoweit, als das die IT-Systeme für den sicheren Netz- oder Anlagenbetrieb notwendig sind. Keinesfalls darf der Eindruck entstehen, dass sich die Pflicht zur Zertifizierung auch auf die nicht für den Netz- oder Anlagenbetrieb notwendigen IT-Systeme bezieht (wie z.B. die Office-IT ohne Verbindung zum Netz / kritischen Anlage).** Anderenfalls würden zukünftig auf eine Vielzahl von Querverbundsunternehmen erstmalig eine Zertifizierungspflicht zukommen.

e. § 5c Abs. 8 EnWG - Registrierung

Aus den gleichen Gründen wie in § 5c Abs. 2 EnWG müssen auch die Regelungen zur Registrierung in § 5c Abs. 8 auf solche Betreiber von Energieanlagen 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) Der Betreiber eines Energieversorgungsnetzes und ein Betreiber einer Energieanlage, **der eine kritische Anlage nach § 2 Absatz 1 Nummer 21 des BSI-Gesetzes betreibt** ~~besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Ge setzes oder wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist~~, ist verpflichtet, spätestens bis zum 1. April, erstmalig oder erneut, sich beim Bundesamt für Sicherheit in der Informationstechnik zu registrieren.

f. § 5c Abs. 9 EnWG – kritische Komponenten / 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.

5. § 95 EnWG – Bußgeldvorschriften

Es muss eine Klarstellung erfolgen, dass neben den Bußgeldern nach der DSGVO keine Bußgelder nach dem EnWG verhängt werden dürfen (siehe die vergleichbare Regelung in § 67 Abs. 10 BSIG). **Ferner fehlt eine Klarstellung, dass der gleiche Verstoß nur entweder nach dem EnWG oder nach dem BSIG mit einem Bußgeld versehen werden darf.**

Der Verweis in § 95 Abs. 2d EnWG ist dagegen in seiner Bedeutung unklar.