VERBAND KOMMUNALER UNTERNEHMEN e.V.

STELLUNGNAHME

Regierungsentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 22.07.2024

Berlin, 02.10.2024

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

DIE KOMMUNALEN UNTERNEHMEN

Der VKU bedankt sich für die Möglichkeit, zu dem „Regierungsentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ vom 22.07.2024 Stellung nehmen zu können.

Bedeutung des Vorhabens für kommunale Unternehmen

Der Verband kommunaler Unternehmen (VKU) vertritt rund 1.550 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 Regierungsentwurfs berücksichtigt viele Anregungen aus der letzten Stellungnahme des VKU. Allerdings existieren weiterhin **verbesserungswürdige Punkte**:

- Die **IT-Sicherheitspflichten** innerhalb eines Mehrspartenunternehmens sind so **komplex** beschrieben, dass sie kaum noch verständlich sind. Die zumindest aus dem Wortlaut des BSIG ableitbare massive **Ausdehnung der Vorgaben des Energiewirtschaftsgesetzes** auch auf die nicht für den Betrieb des Netzes / Anlage erforderlichen IT-Systeme (reguläre Office IT) **wird abgelehnt** (siehe die Ausführungen zu § 28 Abs. 4 BSIG).
- Auch die **spezialgesetzlichen Regelungen des EnWG müssen geändert werden. Es muss klar geregelt werden, dass auch im Bereich der Betreiber von Energieversorgungsnetzen und Energieanlagen eine Abstufung der Pflichten stattfindet.** Die **dreistufige Abstufung** der Pflichten aus dem BSIG (Betreiber kritischer Anlagen, besonders wichtige Einrichtungen, wichtige Einrichtungen) muss sich auch im EnWG und den IT-Sicherheitskatalogen wiederfinden (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).

Stellungnahme

1. § 28 BSIG - Anwendungsbereich, Betreiber kritischer Anlagen, besonders wichtiger Einrichtungen und wichtiger Einrichtungen

a. Abs. 3 – Berechnung der Schwellenwerte nach der Size-Cap-Rule

Zunächst ist positiv zu vermerken, dass auf die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen ist (§ 28 Abs. 3 Nr. 1 BSIG). 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 Unternehmen, deren hauptsächliche Geschäftstätigkeit nicht einer Einrichtungskategorie gemäß Anlage 1 oder 2 dieses Gesetzes zuzuordnen ist, nicht in unverhältnismäßiger Weise erfasst werden (vgl. Gesetzesbegründung, S. 156). Wichtig ist dies insbesondere in Mehrspartenunternehmen, in denen eine Sparte nur einen kleinen Anteil an der gesamten Geschäftstätigkeit ausmacht (Beispiel: Ein Unternehmen der Wasserwirtschaft, das zu einem ganz kleinen Anteil auch Abfalldienste erbringt).

Positiv zu bemerken ist zudem, 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** (§28 Abs. 3 Nr. 2 BSIG). 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.

Ein Problem ergibt sich jedoch im Bereich der Konzernstrukturen. Für diese gilt (außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft) die zuvor 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.

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

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, […].

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 Mehrspartenunternehmen, 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.

Der reine Wortlaut des § 28 Abs. 3 Nr. 2 BSIG schließt die KMU-Empfehlung für unselbstständige Organisationseinheiten einer Gebietskörperschaft generell aus. Dieser Ausschluss ist zumindest teilweise zu weit gefasst. **Es muss in der Gesetzesbegründung klargestellt werden, dass sich dieser Ausschluss der KMU-Empfehlung nur auf die Zurech-**

nung der Zahlen der Partner- oder verbundenen Unternehmen bezieht. Dieser Ausschluss darf sich nicht darauf beziehen, wie die Mitarbeiterzahlen für eine unselbstständige Organisationseinheit einer Gebietskörperschaft isoliert (also ohne Partner- oder verbundene Unternehmen) **betrachtet errechnet werden**. Es muss also z.B. für einen kommunalen Abfallbetrieb in Form eines Eigenbetriebs klar sein, dass Teilzeitmitarbeiter auch nur anteilig bei den maßgeblichen Schwellenwerten hinzugerechnet werden. Insoweit muss Art. 5 des Anhangs der KMU-Empfehlung gelten.

b. Abs. 4 – Ausnahmen vom Anwendungsbereich

Die Regelung des § 28 Abs. 4 BSIG wurde im Vergleich zu den verschiedenen Vorfassungen deutlich überarbeitet. So werden in diesem Bereich die spezialgesetzlichen Regelungen (EnWG / TKG) im Grundsatz sinnvoll abgegrenzt von den allgemeinen Regelungen des BSIG.

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 nicht auf § 33 Abs. 3, 6 BSIG.

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, 36, 38, 39, 61 und 62 sind nicht anzuwenden auf besonders wichtige Einrichtungen und wichtige Einrichtungen, die […].

Die Abgrenzungsnorm des § 28 Abs. 4 BSIG wurde mehrfach im Laufe des Gesetzgebungsverfahrens angepasst und ist nicht einfach zu verstehen. **Insbesondere die auf Mehrspartenunternehmen abzielenden § 28 Abs. 4 S. 2, 3 BSIG sind komplex und bisher noch nicht eindeutig genug ausformuliert. Gleichwohl begrüßt es der VKU zunächst ausdrücklich, dass Normen geschaffen wurden, die speziell die Mehrspartenunternehmen adressieren**. Hierbei handelt es sich um Unternehmen, die innerhalb der gleichen Rechtspersönlichkeit in mehreren der in der BSI-KritisV bzw. den in den Anlagen 1 und 2 des BSIG genannten Sektoren tätig sind. In der Mitgliedschaft des VKU sind sehr häufig diese Art

von Unternehmen anzutreffen. Ein Stadtwerk ist üblicherweise ein Mehrspartenunternehmen, weshalb der Fall für den VKU besonders relevant ist. Für diese Unternehmen muss Klarheit bestehen, welcher Teil des eigenen Unternehmens unter welche Regulierung (BSIG, EnWG oder TKG) fällt.

Die grundsätzliche Lesart der Norm ist aus unserer Sicht wie folgt:

- Ausgegangen wird vom **Grundsatz**, dass für alle Unternehmen das BSIG anwendbar ist.
- § 28 Abs. 4 S. 1 Nr. 1 und Nr. 2 BSIG legen eine **Ausnahme** von diesem Grundsatz fest. Danach ist nicht das BSIG, sondern das EnWG (insbesondere § 5c EnWG) anzuwenden auf Betreiber von Energieversorgungsnetzen und Energieanlagen. Gleiches gilt nach § 28 Abs. 4 S. 1 Nr. 1 BSIG für die Betreiber von öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten. Für diese gilt das TKG (insbesondere §§ 165, 167, 168 TKG).
- Für Mehrspartenunternehmen bestimmt § 28 Abs. 4 S. 2, 3 BSIG teilweise eine Ausnahme von der Ausnahme (**Rückausnahme**).
    - Soweit neben den Energieversorgungsnetzen / Energieanlagen (bzw. den Telekommunikationsnetzen / Telekommunikationsdiensten) weitere kritische Anlagen betrieben werden oder das Unternehmen als (besonders) wichtige Einrichtung einer der in Anlage 1 oder 2 Einrichtungsarten zuzuordnen ist und die IT-Systeme für den Betrieb der weiteren kritischen Anlage erforderlich sind, ist die Rückausnahme anwendbar. § 28 Abs. 4 S. 1 Nr. 1 und Nr. 2 BSIG ist damit nicht anwendbar. Es verbleibt bei der Anwendbarkeit des BSIG.
    - Soweit neben den Energieversorgungsnetzen / Energieanlagen (bzw. den Telekommunikationsnetzen / Telekommunikationsdiensten) weitere kritische Anlagen betrieben werden oder das Unternehmen als (besonders) wichtige Einrichtung einer der in Anlage 1 oder 2 Einrichtungsarten zuzuordnen ist und die IT-Systeme für den Betrieb der weiteren kritischen Anlage nicht erforderlich sind, ist die Rückausnahme nicht anwendbar. § 28 Abs. 4 S. 1 Nr. 1 und Nr. 2 BSIG ist somit weiterhin anwendbar. Es verbleibt insoweit bei der Anwendbarkeit des EnWG bzw. TKG. Insbesondere über diese Ableitung existieren allerdings unterschiedliche Auffassung (siehe dazu sogleich).

Bildet man zur Veranschaulichung dieser Regeln als Beispiel ein Mehrspartenunternehmen

- 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 gilt nach unserer Lesart des Gesetzes folgendes:

- Die IT-Systeme, die für den sicheren Anlagenbetrieb der kritischen Energieerzeugungsanlage erforderlich sind, werden über § 5c EnWG (bzw. die IT-Sicherheitskataloge) reguliert (§ 28 Abs. 4 S. 1 Nr. 2 BSIG)
- Die IT-Systeme, die für den sicheren Anlagenbetrieb der kritischen Trinkwassergewinnungsanlage erforderlich 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 erforderlich sind, werden über das BSIG reguliert (§ 28 Abs. 4 S. 2 Var. 2, S. 3 BSIG)
- Alle IT-Systeme in diesem Mehrspartenunternehmen, die nicht für den sicheren Anlagenbetrieb unmittelbar erforderlich 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. 157, 201))

Allerdings verbleibt eine Vielzahl von Unklarheiten, die dringend einer Klarstellung bedürfen. Teilweise mag dies noch nach Verabschiedung des Gesetzes in Rahmen von FaQ etc. möglich sein. **Die folgenden Unklarheiten müssen aber bereits im Rahmen des Gesetzgebungsverfahrens geklärt werden**:

<u>Regulierung der „nicht erforderlichen“ IT-Systeme (Office-IT ohne Schnittstellen zu den Anlagen)</u>

Insbesondere über die Frage, unter welche Regulierung im obigen Beispiel die „nicht erforderlichen IT-Systeme“ (Office- IT ohne Schnittstelle zu den Anlagen) fallen, herrscht Unklarheit. Im Grundsatz geht es dabei um die Frage, ob nach der vorgesehenen Regulierung des Regierungsentwurfs das EnWG oder das BSIG einschlägig ist. Während der VKU die Auffassung vertritt, dass bisher eine Regulierung nach dem EnWG (inklusive der IT-Sicherheitskataloge) einschlägig wäre, ist man auf Seiten der Ministerien bzw. den nachgeordneten Behörden wohl der Auffassung, dass das BSIG einschlägig ist.

Unsere Interpretation der Anwendbarkeit des EnWG ergibt sich aus dem Gesetzeswortlaut und der Gesetzesbegründung. Denn nach § 28 Abs. 4 S. 3 BSIG ist die Rückausnahme des § 28 Abs. 4 S. 2 BSIG nur anwendbar „für alle informationstechnischen Systeme, die

für den Betrieb der weiteren kritischen Anlagen erforderlich sind." Im Umkehrschluss bedeutet dies, dass § 28 Abs. 4 S. 2 nicht anwendbar ist, soweit die IT-Systeme nicht erforderlich sind. Im obigen Beispiel verbleibt es deshalb bei der Anwendung des § 28 Abs. 4 S. 1 Nr. 2 BSIG und somit bei der Geltung des EnWG.

Gestützt wird dies durch die Gesetzesbegründung zu § 28 Abs. 4 BSIG (S. 157), wonach es heißt: *„Von der Rückausnahme nicht erfasst wird demgegenüber Unternehmens-IT, die für die Tätigkeit in diesen weiteren Sektoren nicht erheblich ist (z.B. „Office-IT" ohne Schnittstellen zu kritischen Anlagen)."*

Ferner heißt es in der Gesetzesbegründung zu § 5c Abs. 3 EnWG (S. 201): *„In Absätzen 1 und 2 werden die IT-Sicherheitskataloge entsprechend den Vorgaben der NIS-2-Richtlinie erweitert und werden alle Dienste, die die Betreiber erbringen, umfassen und nicht nur diejenige, die für den sicheren Netz- oder Anlagenbetrieb notwendig sind."* Daraus ergibt sich aus unserer Sicht, dass sämtliche IT-Systeme (also auch die „nicht erforderlichen IT-Systeme") im Grundsatz dem EnWG unterliegen. Wenn nun die Rückausnahme des § 28 Abs. 4 S. 2, 3 BSIG nicht einschlägig ist, so gilt weiterhin § 28 Abs. 4 S. 1 Nr. 2 BSIG und damit insgesamt das EnWG (eben auch für die „nicht erforderlichen IT-Systeme").

Der VKU fordert, dass die nicht für den sicheren Anlagenbetrieb unmittelbar erforderlichen IT-Systeme eindeutig und 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 würde 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. Weiter könnten die strengen Regelungen der IT-Sicherheitskataloge mittelbar auf alle Mehrspartenunternehmen durchschlagen, insbesondere die Pflichten zum Aufbau eines ISMS oder zur Implementierung von Systemen zur Angriffserkennung (siehe insbesondere näher die Ausführungen zu § 5c Abs. 3 EnWG). Ein entsprechender Formulierungsvorschlag findet sich unter dem nachfolgenden Punkt.

Reichweite der Rückausnahme von § 28 Abs. 4 S. 2, 3 BSIG

§ 28 Abs. 4 S. 3 BSIG ist ungenau und bedarf der Anpassung. Denn nach § 28 Abs. 4 S. 2 BSIG gilt die Rückausnahme für alle (besonders) wichtigen Einrichtungen, soweit sie über die in S. 1 Nr. 1 und Nr. 2 genannten Anlagen hinaus weitere kritische Anlagen betreiben oder aufgrund weiterer Tätigkeiten einer der in Anlage 1 oder 2 bestimmten Einrichtungsarten zuzuordnen sind. § 28 Abs. 4 S. 3 BSIG erklärt wiederum S. 2 nur für anwendbar für alle informationstechnischen Systeme, die für den Betrieb der weiteren kritischen Anlagen erforderlich sind. Kein Bezug genommen wird dagegen auf die weiteren Tätigkeiten

einer in Anlage 1 oder 2 bestimmten Einrichtungsart. Dies ist unlogisch, weil dann dieser Teil des S. 2 niemals Anwendung finden würde und überflüssig wäre. In Konsequenz würde die Rückausnahme beispielsweise nicht gelten bei obigen Mehrspartenunternehmen im Bereich der thermischen Behandlung von Siedlungsabfällen.

Formulierungsvorschlag:

§ 28 Abs. 4 S. 2, 3
Satz 1 gilt nicht für die dort aufgeführten besonders wichtigen und wichtigen Einrichtungen, soweit sie über die in Satz 1 Nummer 1 und 2 genannten Anlagen hinaus weitere kritische Anlagen nach § 2 Nummer 22 betreiben oder aufgrund weiterer Tätigkeiten einer der in Anlage 1 oder 2 bestimmten Einrichtungsarten zuzuordnen sind. Satz 2 gilt für alle informationstechnischen Systeme, die für den Betrieb der weiteren kritischen Anlage **oder für den Betrieb einer Anlage mit Bezug zu einer weiteren Tätigkeiten nach Anlage 1 oder 2** erforderlich **sind**. **Soweit die informationstechnischen Systeme nicht erforderlich sind, ist dieses Gesetz anwendbar.**

Erforderlichkeit der IT-Systeme

Es verbleibt unklar, wann ein IT-System „erforderlich" für den Betrieb der eine Anlage ist. Zum einen kommt es zu sprachlichen Ungenauigkeiten: Der Wortlaut § 28 Abs. 4 S. 3 BSIG nutzt das Wort „erforderlich". Die korrespondierende Gesetzesbegründung (S. 157) nutzt dagegen das Wort „erheblich", was aber anscheinend schlicht eine sprachliche Ungenauigkeit ist. Im Bereich des EnWG wird dagegen das Wort „notwendig" genutzt (vgl. § 5c EnWG und die Gesetzesbegründung, S. 201), ohne das klar wird, ob hierbei ein sachlicher Unterschied besteht. **Es wird deshalb gefordert, dass eine einheitliche Begriffsbestimmung genutzt wird im Zusammenhang mit der Abgrenzung von BSIG, EnWG und TKG.**

Im Bereich von Unternehmen, die physische (Industrie-)Anlagen betreiben wird zudem üblicherweise zwischen der „Operation Technology" (OT; bzw. OT-Netzwerk / Automatisierungsnetzwerk / Anlagennetzwerk genannt) und der Information Technology (IT; bzw. IT-Netzwerk / Enterprise Netzwerk genannt) unterschieden. Die OT ist die Hard- und Software, die insbesondere für die Anlagensteuerung und -überwachung eingesetzt wird. Die IT ist dagegen die Hard- und Software, die außerhalb der Anlagensteuerung eingesetzt wird (z.B. Office-Produkte; SAP-Abrechnungssysteme etc.).[2] Sehr häufig sind die OT- und die IT-Netzwerk „hart" voneinander getrennt, d.h. es besteht keine physische Verbindung zwischen ihnen. Hintergrund ist insbesondere die besondere Schutzbedürftigkeit der OT-Netzwerke. Es kann so verhindert werden, dass eine „gehackte" Office-IT auch zu einer „gehackten" OT führt und die kritische Dienstleistung weiterhin erbracht werden.

[2] Siehe z.B. die Ausführungen hier: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html

Setzt man voraus, dass „erheblich“ in der Gesetzesbegründung deckungsgleich mit dem Begriff „erforderlich“ ist, so verbleiben vor diesem Hintergrund weitere Unklarheiten. Ob ein IT-System erforderlich / erheblich ist für den Betrieb der Anlage soll wohl davon abhängen, ob eine Schnittstelle zu den (kritischen) Anlagen besteht oder nicht. Wir gehen somit davon aus, dass jegliche OT zur Steuerung der Anlagen erforderlich / erheblich im Sinne des Gesetzes ist, auch wenn im Gesetz / Gesetzesbegründung nur der Begriff der IT genannt wird. Weiter gehen wir davon aus, dass nur die IT mit Schnittstelle zu einer kritischen Anlage (oder dem OT-Netzwerk) erforderlich / erheblich sind. Unklar ist hierbei jedoch, ob eine Schnittstelle zum OT-Netzwerk dazu führt, dass das gesamte IT-Netzwerk erforderlich / erheblich im Sinne des Gesetzes ist oder sich dies nur auf die Schnittstelle selbst bezieht. Klar ist auf der anderen Seite, dass eine IT ohne Schnittstelle zu den Anlagen / OT nicht erforderlich / erheblich ist (in der Gesetzesbegründung als Office-IT bezeichnet).

Bei allen diesen Ausführungen handelt es sich jedoch um unsere Ableitung aus dem Gesetz, die aber in der Praxis weitreichende Folgen haben. **Es wird gefordert, dass zusammen mit der Branche diese Punkte bereits im Gesetzgebungsprozess zumindest in grober Weise geklärt werden und die zuvor vorgeschlagene Änderung am Wortlaut des § 28 Abs. 4 BSIG auch zum Anlass genommen wird, die entsprechende Gesetzesbegründung klarzustellen. Die Einzelheiten können im Anschluss durch begleitende FaQ-Papiere des BSI / BNetzA oder der Ministerien geklärt werden.**

Im Übrigen wird auf die Ausführungen zu § 5c EnWG verwiesen, wo spezielle Ausführungen hauptsächlich für die reinen Energieversorgungsunternehmen gemacht werden. In Bezug auf die Besonderheiten im Bereich von Mehrspartenunternehmen, die auch im Bereich der Telekommunikation tätig sind, wird auf die Ausführungen zum TKG verwiesen.

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 zur Bestimmung der Betreibereigenschaft ist. **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[3] 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.[4] 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 Anwendungsbereich 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 in die Länge ziehen. Insgesamt handelt es sich um ein sehr bürokratisches Verfahren, das im Ergebnis nicht zu mehr Sicherheit führen wird, aber die Planungssicherheit der Unternehmen untergräbt.

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

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

Vor diesem Hintergrund sollte das Prüfverfahren gemäß § 41 BSIG gestrichen und durch eine Ausschlussliste generell nicht-vertrauenswürdiger Hersteller ersetzt werden.

3. § 61 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 § 61 Abs. 3 BSIG. Die maßgeblichen Kriterien zur Ermessensausübung finden sich hierbei in § 61 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.

Die ermessenssteuernde Norm in § 61 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 § 61 Abs. 4 BSIG nicht nur auf § 61 Abs. 3 BSIG (Anforderung der Nachweise), sondern auch auf § 61 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:

§ 61 - 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

Mit den neuen Regelungen des § 5c EnWG wird deutlich über die von der NIS-2-Richtlinie vorgegebenen Anforderungen hinausgegangen (Gold Plating). 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 Mehrspartenunternehmen (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.“* (Gesetzesbegründung, S. 200)

> *„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.“* (Gesetzesbegründung, S. 201)

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.[5] 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.[6] 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.

Diese massive Ausweitung des Scopes wird abgelehnt und ist auch nicht durch die NIS2-Richtlinie vorgezeichnet. **Die nicht für den sicheren Netzbetrieb unmittelbar notwendigen IT-Systeme sollten 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 einer 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 Mehrspartenunternehmen wird auf die Ausführungen zu § 28 Abs. 4 EnWG verwiesen.

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.[7] 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. **Es wird gefordert, dass Gesetzesbegründung und Wortlaut des Gesetzes aufeinander abgestimmt werden. Zudem sollte der Begriff „notwendig“ überdacht werden, da im BSIG der Begriff „erforderlich“ bzw. „erheblich“ genutzt wird** (siehe näher die entsprechenden Ausführungen zu § 28 Abs. 4 BSIG).

[5] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-Nachweise/Konkretisierung-Geltungsbereich/konkretisierung-geltungsbereich_node.html.
[6] IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, S. 6.
[7] Kipker/Reusch/Ritter/Voigt/Böhme, 1. Aufl. 2023, EnWG § 11 Rn. 79.

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. Eine Ausweitung der Pflichten aus dem IT-Sicherheitskatalog auch auf die allgemeine Office-IT wird abgelehnt.** Die Ausführungen zu § 5c Abs. 1 EnWG gelten entsprechend.

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. **Es wird gefordert, dass innerhalb der IT-Sicherheitskataloge für die Pflichtentiefe danach unterschieden wird, ob es sich um einen Betreiber einer kritischen Anlage, eine besonders wichtige Einrichtung oder um eine wichtige Einrichtung handelt** (**dreistufige Regulierung**, siehe näher die Ausführungen zu § 5c Abs. 3 EnWG).

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 kann man die Norm so lesen, dass die Normen des EnWG bzw. die IT-Sicherheitskataloge auch für alle IT-Systeme von Mehrspartenunternehmen gelten, die nicht notwendig (bzw. „erforderlich“ oder „erheblich“) sind für den sicheren Netz- oder Anlagenbetrieb (siehe Ausführungen zu § 28 Abs. 4 BSiG). **Beides lehnt der VKU wie zuvor beschrieben ab. Die allgemeine Office IT sollte einheitlich über das BSIG reguliert werden.**

Zudem müssen 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 und auf letzter Stufe die 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.“* (Gesetzesbegründung, S. 201)

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 Energieanlagen ein ISMS durch die Betreiber aufgebaut werden muss 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 fast 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 Mehrspartenunternehmen auf die gesamte Office-IT durchschlagen. **Diese mögliche Auswirkung des Gesetzes wird abgelehnt und muss verhindert werden. Lediglich Betreiber von kritischen Energieanlagen dürfen verpflichtet werden, Systeme zur Angriffserkennung einzusetzen. Zudem muss die Regulierung der allgemeinen Office-IT aus der Regulierung des EnWG herausgelöst werden und weiterhin dem BSIG unterliegen.**

Die genauen Pflichten der Energieversorgungsnetzbetreiber und der Betreiber von Energieanlagen werden sich erst aus den noch zu erarbeitenden IT-Sicherheitskatalogen ergeben. Solange die IT-Sicherheitskataloge nicht existieren, existieren für die Unternehmen

formal gesehen kaum Pflichten aus dem EnWG. Sowohl § 5c Abs. 1 als auch Abs. 2 EnWG gehen davon aus, dass sich die angemessenen Schutzmaßnahmen der Betreiber aus den IT-Sicherheitskatalogen ergeben. Bisher sind den Betreibern jedoch noch keine Entwürfe der IT-Sicherheitskataloge bekannt, obwohl diese laut § 5c Abs. 1, 2 EnWG vor Verabschiedung beteiligt werden müssen. Es ist nunmehr unklar, welche Rechtslage gilt, falls das NIS2-Umsetzungsgesetz verabschiedet wird und in Kraft tritt, jedoch keine entsprechenden IT-Sicherheitskataloge vorliegen. **Es wird gefordert, die Betreiber der Energieversorgungsnetze / Energieanlagen (bzw. deren Verbände) möglichst frühzeitig in die Erstellung der Kataloge einzubeziehen. Zudem muss zeitnah transparent gemacht werden, welche Pflichten für die Betreiber gelten, sollten die IT-Sicherheitskataloge nicht rechtzeitig in Kraft treten. Ggf. müssen gesetzliche Übergangsregeln geschaffen werden für diesen Fall, sodass die bisherigen IT-Sicherheitskataloge weitergelten.** Schlicht die bisher geltenden IT-Sicherheitskataloge für weiter anwendbar zu erklären oder unverändert neu zu verabschieden, ist allerdings mit Risiken behaftet. Die Rechtsgrundlage zur Verabschiedung der IT-Sicherheitskataloge hat sich geändert, sodass wohl auch andere Erwägungen innerhalb der IT-Sicherheitskataloge getroffen werden müssen. Besonders betroffen sind dabei die Pflichten zum Einsatz von Systemen zur Angriffserkennung (SzA). Bisher ist deren Einsatz über § 11 Abs. 1e, 1f EnWG vorgeschrieben. Nach dem Gesetzesentwurf sollen diese Pflichten zukünftig in die IT-Sicherheitskataloge wandern (vgl. § 5c Abs. 3 Nr. 11 EnWG). Dies bedeutet aber auch, dass ohne einen entsprechenden IT-Sicherheitskatalog keine Pflicht zum Einsatz von SzA besteht.

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

Anders als noch im Referentenentwurf vorgesehen, sollen zukünftig nicht nur Betreiber von kritischen Energieanlagen, sondern alle Betreiber von Energieanlagen, die eine (besonders) wichtige Einrichtung darstellen, ihre Dokumentation über die Einhaltung der IT-Sicherheitskataloge proaktiv an die Bundesnetzagentur übermitteln. **Dies wird abgelehnt und gefordert, dass nur Betreiber von kritischen Energieanlagen proaktiv ihre Dokumentation an die Bundesnetzagentur übermitteln müssen.**

Im Bereich des BSIG wird richtigerweise bei der Nachweiserbringung unterschieden zwischen Betreibern von kritischen Anlagen und (nur) besonders wichtigen und wichtigen Einrichtungen. Während Betreiber von kritischen Anlagen nach § 39 BSIG einer ex ante (also einer proaktiven) Nachweispflicht unterliegen, gilt dies nicht für (besonders) wichtige Einrichtungen. Für diese wird von einer ex ante Nachweispflicht abgesehen. Vielmehr statuieren die §§ 61, 62 BSIG eine Nachweispflicht nur nach Einzelfallentscheidung durch das BSI, was sich gemäß § 61 Abs. 3 BSIG explizit auch auf die Vorlage der Dokumentation bezieht. Zudem wird klargestellt, dass die Nachweise frühestens drei Jahre nach Inkrafttreten des NIS2-Umsetzungsgesetzes angefordert werden dürfen. Es gibt keinen Grund für die Betreiber von Energieanlagen von dieser Logik abzuweichen. Zudem ist unklar, ob diese Dokumentation auf Grund der schieren Masse an Dokumenten überhaupt von der

BNetzA überprüft werden kann, wenn zukünftig faktisch alle Betreiber von Energieanlagen diese übermitteln müssten. Ferner ist im Rahmen der aktuellen Formulierung unklar, ab wann und in welchem Turnus die entsprechenden Dokumentationen vorgelegt werden müssen. Die Fristen dürfen nicht erst in den IT-Sicherheitskatalogen festgelegt werden, sondern müssen sich bereits aus dem Gesetz ergeben. Wie zuvor beschrieben sind die IT-Sicherheitskataloge der Branche nicht bekannt, sodass es ungewiss bleibt, ab wann die mögliche Übermittlung der Dokumentation erfolgen soll. **Es wird deshalb gefordert, dass § 5c Abs. 4 EnWG die in den §§ 61, 62 BSIG festgelegte Logik nachvollzieht.**

Formulierungsvorschlag:

§ 5c Abs. 4 EnWG - IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz

(4) Der Betreiber eines Energieversorgungsnetzes ~~oder der Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist~~ **und jeder Betreiber einer Energieanlage, die kritische Anlage nach § 2 Nummer 22 des BSI-Gesetzes ist** und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, hat der Bundesnetzagentur die Dokumentation über die Einhaltung der Anforderungen des jeweiligen IT-Sicherheitskatalogs nach Absatz 1 Satz 7 oder nach Absatz 2 Satz 10 zu übermitteln. **Die Bundesnetzagentur kann frühestens drei Jahre nach Inkrafttreten dieses Gesetzes gegenüber dem Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, die Vorlage der Dokumentation nach Absatz 2 Satz 10 anordnen. §§ 61 Abs. 4; 62 BSI-Gesetz gelten entsprechend.** […]

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 IT-Systeme beziehen, die 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 könnten zukünftig auf eine Vielzahl von Mehrspartenunternehmen erstmalig eine Zertifizierungspflicht zukommen.

Die Bedeutung von § 5c Abs. 5 EnWG verbleibt unklar. Nur in Bezug auf die Betreiber einer Energieanlage, der eine besonders wichtige oder wichtige Einrichtung darstellt, wird für die Bundesnetzagentur eine Ermächtigungsgrundlage geschaffen, um von diesen Informationen über die Einhaltung der IT-Sicherheitskataloge anzufordern. Warum diese Norm sich nicht auch auf Betreiber von Energieversorgungsnetzen erstreckt verbleibt unklar. Es

erscheint so, als ob anders als in § 5c Abs. 4 EnWG, eine Abstufung zwischen den verschiedenen Betreibern geschaffen werden soll. **Es wird gefordert § 5c Abs. 5 EnWG zu überarbeiten und insgesamt die Logik der §§ 39, 61, 62 BSIG in Bezug auf die Nachweise nachzuvollziehen.**

e. § 5c Abs. 12 EnWG – kritische Kompotenten / kritische Funktionen

In Bezug auf die kritischen Komponenten / kritischen Funktionen im Bereich der Energiewirtschaft 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 § 65 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.**

6. §§ 165, 167, 168 TKG – Änderungen am TKG

Anders als im BSIG oder im EnWG findet sich weder in den Normen des TKG noch in dessen Gesetzesbegründung ein Hinweis darauf, dass sich zukünftig die IT-Sicherheitspflichten auf die IT-Systeme des gesamten Unternehmens beziehen und nicht nur auf die IT-Systeme, die unmittelbar zum Betrieb der Telekommunikationsnetze / Telekommunikationsdienste erforderlich sind. Vielmehr wurden die §§ 165 Abs.2; 167 Abs. 1 Nr. 1 TKG nicht angepasst und bezieht sich weiterhin nur unmittelbar auf die Telekommunikationsnetze und Telekommunikationsdienste. **Es wird angeregt klarzustellen, dass der Scope / Geltungsbereich des Gesetzes erweitert wurde. Weiter sollte klarzustellen werden, ob dies für alle Betreiber von Telekommunikationsnetzen und Telekommunikationsdiensten gilt, oder nur für solche, die die Schwellenwerte der NIS2-Richtlinie erreichen. Es sollte dabei nicht über die Vorgaben der NIS2-Richtlinie hinausgegangen werden.** Einzelheiten zum Scope / Geltungsbereich finden sich entsprechend in der Kommentierung zu § 5 Abs. 1 EnWG.

Auch im Bereich der Telekommunikationswirtschaft stellt sich die Frage, welche Regelungen gelten, wenn zwar das NIS2-Umsetzungsgesetz in Kraft tritt, aber gleichzeitig nicht die entsprechenden IT-Sicherheitskataloge überarbeitet und veröffentlicht wurden. Zwar scheint hier das Problem nicht so virulent zu sein, da sich die entsprechenden Pflichten bereits direkt aus dem Gesetz ergeben (vgl. § 165 Abs. 2a TKG). **Es müssen gleichwohl die Betreiber Telekommunikationsnetze / Telekommunikationsdienste (bzw. deren Verbände) möglichst frühzeitig in die Erstellung der Kataloge einbezogen werden. Zudem muss zeitnah transparent gemacht werden, welche Pflichten für die Betreiber gelten,**

sollten die IT-Sicherheitskataloge nicht rechtzeitig in Kraft treten. Ggf. müssen Übergangsvorschriften geschaffen werden. Im Übrigen wird auf die Ausführungen zu § 5c Abs. 3 EnWG verwiesen.

Ebenso wie im Bereich der Energiewirtschaft stellt sich auch im Bereich des TKG die Frage, nach welcher Norm die nicht für die Telekommunikationsnetze / Telekommunikationsdienste erforderlichen IT-Systeme in Mehrspartenunternehmen reguliert werden. Je nach Lesart des Gesetzes wären entweder das TKG (inklusive der IT-Sicherheitskataloge) oder das BSIG einschlägig. **Der VKU fordert, dass die nicht für den sicheren Anlagenbetrieb unmittelbar erforderlichen IT-Systeme eindeutig und einheitlich über das BSIG reguliert werden und unter Aufsicht des BSI stehen.** Es wird auf die entsprechenden Ausführungen zu § 28 Abs. 4 BSIG verwiesen. Eine Regulierung der nicht erforderlichen IT-Systeme durch das BSIG macht auch deshalb Sinn, da anderenfalls unklar wäre, ob diese IT-Systeme bei Mehrspartenunternehmen unter das EnWG oder TKG oder unter beide Regulierungen fallen würden.