04.07.2025

**An den Beratungen zur Stellungnahme haben maßgeblich folgende Autoren mitgewirkt - alphabetisch:**

- RA Dr. Tilmann Dittrich, LL.M.
- RA Stefan Hessel, LL.M.
- Holger Könnecke, M.Sc., CII-Executive Advisory Board
- Dr. Michael Littger, LL.M., CII-Strategie Direktor
- Irina Rosensaft, CII-Governance Direktor

**Prof. Dr. Dennis-Kenji Kipker**
Research Director
dennis.kipker@cyberintelligence.institute

**Rainer Fahs, Chairman**
office@eicar.org

---

# Schriftliche Stellungnahme

# zum

# Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 23.06.2025

## Zusammenfassung und fachliche Einordnung

Der aktuelle Referentenentwurf eines „Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ datiert auf den 23.6.2025 und hält relevante Änderungen bereit:

- Zwar werden nur punktuelle Änderungen vorgenommen, diese haben aber erhebliche Auswirkungen u.a. auf den Anwendungsbereich, die Zusammenarbeit zwischen Wirtschaft und Behörden, die Cybersicherheitsstandards in der Bundesverwaltung und die Rolle des BSI im nationalen Cybersicherheitsgefüge, die eine erhebliche Stärkung erhält.
- Deutlich wird damit: Im Rahmen der ministeriellen Abstimmung war man durchaus bemüht, einiges von der Kritik aus dem Gesetzgebungsverfahren unter der Ägide der alten Bundesregierung aufzugreifen, um die Regelungen zur nationalen Umsetzung von NIS-2 in Teilen praktikabler zu gestalten und die Cybersecurity dadurch zu verbessern.

Gemessen an der Tatsache, dass die Umsetzung von NIS-2 in Deutschland schon seit mittlerweile über zwei Jahren möglich ist und angegangen wird, enthält der vorgelegte

Entwurf leider noch viele Schwächen und Unklarheiten, teilweise auch Maßgaben, die der Erhöhung des allgemeinen Cybersicherheitsniveaus nicht förderlich sind, insbesondere

- **Systematik:** Zu vermissen ist eine Vereinheitlichung der Systematik des nationalen Cybersicherheitsrechts, die zwischen bereichsspezifischen und allgemeinen Vorgaben und der Cybersicherheit in Bund und Ländern unterscheidet – denn letztlich verlangt NIS-2, dass in einem föderalen Deutschland einheitliche Cybersicherheitsstandards definiert werden. Auch Diskrepanzen zur asynchronen KRITIS-Dachgesetzgebung wirken sich nachteilig aus.

- **Begriffsbestimmung**: Zahlreiche Begriffsbestimmungen genügen den Anforderungen an Rechtsklarheit nicht oder schaffen fragwürdige Abgrenzungen (Betreiber, Ausnahmekriterien, Online-Marktplatz, Diensteanbieter u.a.), die nicht zuletzt neue Unsicherheiten im Anwendungsbereich nach sich ziehen.

- **Anwendungsbereich**: Auf die Kritik zu weit gezogener Anwendungsbereiche durch die Einbindung von Nebentätigkeiten reagiert der aktuelle Entwurf mit einem neuen Ausnahmetatbestand für „vernachlässigbare Geschäftstätigkeiten“. Seine Ausgestaltung bedarf einer kritischen Würdigung auch der EU-Rechtskonformität.

- **Rolle des BSI**: Der neu anvisierte Befugnisaufwuchs des BSI in seiner unterstützenden Rolle sowie die Aufwertung des IT-Grundschutzes mit faktischem Gesetzrang für den Bund entspricht dem Ziel der NIS-2-Richtlinie, ein einheitliches Niveau der IT-Sicherheit zu realisieren. Auch die neue Balance zwischen BSI und BNetzA insbesondere im Energiesektor ist unter diesem Aspekt zu begrüßen. Unbefriedigend erscheint weiterhin die unklare Rolle des BSI im nationalen Verwaltungsgefüge, die durch seine künftigen Aufgaben im Rahmen des CRA weiter an Relevanz gewinnt.

- **Meldestelle**: Weiterhin mangelt es an Klarstellung, dass gemeldete Informationen nur zur Verbesserung der Informationssicherheit verwendet werden dürfen und eine Weitergabe der Informationen zur Ausnutzung gemeldeter Sicherheitslücken nicht stattfindet. Sonstige Gefährdungen wie Sabotage oder Desinformation sollten in den Meldekatalog aufgenommen werden.

- **Maßnahmenkatalog**: Dem Maßnahmenkatalog aus § 30 BSIG-E ist eine willkürliche Reihenfolge von Maßnahmen zu entnehmen, die sich keiner logischen Prozessfolge für die Unternehmenspraxis zuordnen lassen. Teilweise werden singuläre Lösungen benannt, die nicht ausreichen, um NIS-2 konform oder cybersicher zu sein.

- **Datenschutz**: Im Hinblick auf den Datenschutz enthält der Entwurf erhebliche Schwächen, die teils sogar unionsrechtswidrig sein dürften, so zum Beispiel die Anforderung, nur „offensichtliche Datenschutzverletzungen“ infolge eines Cybersicherheitsvorfalls an die Datenschutzaufsicht zu melden und wie die Befugnisse von BSI und BfDI auch künftig klar voneinander abzugrenzen sein sollen.

## Inhaltsverzeichnis


Zusammenfassung und fachliche Einordnung ..... 1

- Zu § 1 BSIG-E (Bundesamt für Sicherheit in der Informationstechnik) ..... 4
- Zu § 2 BSIG-E: Arbeitsteilung ..... 5
- Zu § 2 BSIG-E: Ausnahmekriterien ..... 5
- Zu § 2 BSIG-E: Betreiber ..... 5
- Zu § 2 BSIG-E: Hersteller ..... 6
- Zu § 2 BSIG-E: Online-Marktplatz ..... 6
- Zu § 2 Nr. 8 BSIG-E (Begriffsbestimmung, hier: „DNS-Diensteanbieter“) ..... 6
- Zu § 2 Nr. 10 BSIG-E (Begriffsbestimmung, hier: „erhebliche Cyberbedrohung“) ..... 7
- Zu § 2 Nr. 11 BSIG-E (Begriffsbestimmung, hier: „erheblicher Sicherheitsvorfall“) ..... 8
- Zu § 2 Nr. 12 BSIG-E (Begriffsbestimmung, hier: „Forschungseinrichtung“) ..... 8
- Zu § 2 Nr. 13 BSIG-E (Begriffsbestimmung, hier: „Geschäftsleitung“) ..... 9
- Zu § 2 Nr. 17 BSIG-E (Begriffsbestimmung, hier: „Informationssicherheit“) ..... 9
- Zu § 2 Nr. 19 BSIG-E (Begriffsbestimmung, hier: „Institutionen der Sozialen Sicherung ..... 10
- Zu § 2 Nr. 22 BSIG-E (Begriffsbestimmung, hier: „kritische Anlage“) ..... 11
- Zu § 2 Nr. 26 BSIG-E (Begriffsbestimmung, hier: „Managed Service Provider“) ..... 12
- Zu § 2 Nr. 38 BSIG-E (Begriffsbestimmung, hier: „Schwachstelle“) ..... 13
- Zu § 2 Nr. 41 BSIG-E (Begriffsbestimmung, hier: „Systeme zur Angriffserkennung“) ..... 13
- Zu § 3 BSIG-E (Aufgaben des Bundesamtes) ..... 14
- Zu § 5 BSIG-E (Allgemeine Meldestelle für die Sicherheit in der Informationstechnik) ..... 16
- Zu § 6 BSIG-E (Informationsaustausch) ..... 17
- Zu § 7 BSIG-E (Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte) ..... 17
- Zu § 28 BSIG-E (Besonders wichtige und wichtige Einrichtungen) ..... 18
- Zu § 28 Abs. 3 BSIG-E: „Vernachlässigbare“ Geschäftstätigkeiten ..... 19
- Zu § 29 BSIG-E (Einrichtungen der Bundesverwaltung) ..... 20
- Zu § 30 BSIG-E (Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen) ..... 22
- Zu § 31 BSIG-E (Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen) ..... 23
- Zu § 32 BSIG-E (Meldepflichten) ..... 24
- Zu § 33 BSIG-E (Registrierungspflicht) ..... 25
- Zu § 38 BSIG-E (Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen) ..... 26
- Zu § 39 BSIG-E (Nachweispflichten für Betreiber kritischer Anlagen) ..... 26
- Zu § 43 BSIG-E (Informationssicherheitsmanagement) ..... 27
- Zu § 44 BSIG-E (Vorgaben des Bundesamtes) ..... 27
- Zu § 48 BSIG-E (Amt des Koordinators für Informationssicherheit) ..... 28
- Zu Anlage 1: Betreiber von Erzeugungsanlagen nach § 3 Nummer 18d EnWG ..... 29
- Zu Anlage 1: Ladepunktbetreiber nach § 2 Nummer 8 LSV ..... 29
- Zu Anlage 1: Passagier- und Frachtbeförderungsunternehmen ..... 30
- Zu Anlage 2: Produktion, Verarbeitung und Vertrieb von Lebensmitteln ..... 30
- Zu Artikel 14 des NIS2UmsuCG ..... 30
- Zu Artikel 21 des NIS2UmsuCG ..... 31
- Zu Artikel 32 NIS-2-RL ..... 31

## Zu den Vorschriften im Einzelnen:

- **Zu § 1 BSIG-E (Bundesamt für Sicherheit in der Informationstechnik)**

  § 1 BSIG bestimmt in der geltenden Fassung wie auch im Entwurf, dass das BSI eine Bundesoberbehörde ist. Zugleich ist die Stärkung des BSI in seiner Unterstützerrolle im Geschäftsbereich des Bundesinnenministeriums und zentrale Stelle für Informationssicherheit auf nationaler Ebene ist. In dieser Funktion führt es seine Aufgaben gegenüber den Bundesministerien auf der Grundlage von wissenschaftlich-technischen Erkenntnissen durch. Nach wie vor ist bei dieser gewählten Formulierung unklar, weshalb sie trotz bereits seit mehreren Jahren geäußerter Kritik keine Anpassung erfährt. Dies betrifft einerseits die Rolle des BSI und dessen Forderung nach institutioneller Unabhängigkeit, zu deren Zwecken unter anderem auch die „AG BSI" eingerichtet wurde. Dabei ist es zwingend notwendig, dass im Zuge der stetig und in den vergangenen Jahren massiv erweiterten behördlichen Befugnisse eine zeitnahe Lösung gefunden wird. Der Verfasser dieser Stellungnahme hat entsprechende Vorschläge z.B. zur Sitzung der AG BSI am 8. September 2023 persönlich zur Diskussion gestellt, sowie in Ko-Autorenschaft einen entsprechenden Fachbeitrag publiziert, der konkrete rechtliche Möglichkeiten zur Unabhängigstellung des BSI in gradueller Abstufung aufzeigt.[1] Andererseits lässt sich mittels sachlicher Argumentation nicht rechtfertigen, weshalb das BSI ausschließlich „gegenüber den Bundesministerien" seine Aufgaben auf der „Grundlage wissenschaftlich-technischer Erkenntnisse" durchführt. Das BSI ist eine Fachbehörde und hat deshalb seine Aufgaben gegenüber allen betroffenen Einrichtungen nach diesem Maßstab auszuführen – zumal aus dem Wortlaut der Vorschrift nicht hervorgeht, was die alternativen Handlungsmaßstäbe des BSI gegenüber den anderen auch durch das Gesetz betroffenen Einrichtungen wären. Im Ergebnis geht es somit darum, Komplexitäten in der Aufgabenwahrnehmung zu reduzieren, zentrale und verlässliche Entscheidungswege zu etablieren und Verfahren nationaler Informationssicherheit effizienzsteigernd orientiert am größtmöglichen Nutzen für die Informationssicherheit auszugestalten.

[1] Kipker/Mayr, Zur Unabhängigkeit des BSI: Die juristische Analyse einer politischen Debatte, DuD 2023, 790-795, online abrufbar unter: https://link.springer.com/article/10.1007/s11623-023-1864-z

- **Zu § 2 BSIG-E: Arbeitsteilung**

  Die NIS-2-Richtlinie geht implizit davon aus, dass jedem regulierten Dienst jeweils eine einzelne verantwortliche Einrichtung zuzuordnen ist. Diese Vorstellung entspricht jedoch nicht der tatsächlichen wirtschaftlichen Praxis. In vielen Fällen werden regulierte Dienste arbeitsteilig von mehreren Einrichtungen gemeinsam erbracht. Dies wirft die Frage auf, welches der beteiligten Unternehmen in solchen Konstellationen Adressat der Pflichten der NIS-2-Richtlinie ist. Das deutsche Umsetzungsgesetz zur NIS-2-Richtlinie sollte eine ausdrückliche Regelung enthalten, die die Zuweisung von Pflichten in arbeitsteiligen Strukturen klar regelt.

- **Zu § 2 BSIG-E: Ausnahmekriterien**

  Der Anwendungsbereich der NIS-2-Richtlinie ist grundsätzlich auch eröffnet, wenn Dienste oder Tätigkeiten – auch nur in geringem Umfang – als Nebentätigkeit erbracht werden. Allerdings sieht die Richtlinie einige wenige Ausnahmen für Nebentätigkeiten vor, wobei unterschiedliche Maßstäbe angewendet werden:

  - In einigen Sektoren sind Tätigkeiten ausgenommen, wenn sie lediglich einen nicht wesentlichen Teil der allgemeinen Tätigkeit ausmachen.
  - Im Bereich der Abfallbewirtschaftung hingegen greift die Ausnahme nur, wenn die Abfallbewirtschaftung nicht die Hauptwirtschaftstätigkeit ist.

  Die unklare Abgrenzung der Ausnahmen erschwert es Unternehmen, ihre eigene Betroffenheit rechtssicher zu prüfen, da ungewiss ist, wann und unter welchen Bedingungen eine Ausnahme tatsächlich greift. Das Umsetzungsgesetz sollte die Ausnahmekriterien daher eindeutig definieren.

- **Zu § 2 BSIG-E: Betreiber**

  Es ist problematisch, dass zahlreiche sektorspezifische Regelungen auf den Begriff des „Betreibers“ Bezug nehmen, ohne dass dieser in der NIS-2-Richtlinie eindeutig definiert ist. Zwar ist der Begriff im europäischen Rechtsrahmen bekannt, seine Verwendung erfolgt jedoch in unterschiedlichen Rechtsakten uneinheitlich. Diese terminologischen Unklarheiten führen zu vermeidbarer Rechtsunsicherheit. Es ist deshalb sinnvoll, den Begriff des Betreibers im nationalen Recht zu definieren. Mindestens sollte gesetzlich festgehalten werden, dass als Betreiber diejenigen gelten, die – unabhängig von Eigentumsverhältnissen – die regulierten Dienste oder Tätigkeiten rechtlich, wirtschaftlich oder faktisch maßgeblich beeinflussen.

- **Zu § 2 BSIG-E: Hersteller**

  Die NIS-2-Richtlinie erfasst Hersteller von Medizinprodukten, chemischen Erzeugnissen und vielen weiteren Produkten. Im europäischen Recht existieren jedoch verschiedene Definitionen des Herstellerbegriffs. Sowohl die NIS-2-Richtlinie als auch der Referentenentwurf lassen jedoch offen, welche Definition im Rahmen der NIS-2-Umsetzung maßgeblich sein soll. Da die verschiedenen Herstellerbegriffe zu unterschiedlichen Ergebnissen bei der Anwendbarkeit führen, ist eine Klarstellung dringend erforderlich, um Rechtsunsicherheit zu vermeiden. Da die NIS-2-Richtlinie ein hohes Cybersicherheitsniveau in der EU zum Ziel hat, sollte ein spezifischer, cybersicherheitsrechtlicher Herstellerbegriff zugrunde gelegt werden, der jene Akteure erfasst, die für den Schutz der Produktion verantwortlich sind.

- **Zu § 2 BSIG-E: Online-Marktplatz**

  Die NIS-2-Richtlinie erfasst im Sektor der Anbieter digitaler Dienste auch Anbieter von Online-Marktplätzen. Zur Definition von Online-Marktplätzen verweist die Richtlinie auf Art. 2 lit. n der UGP-Richtlinie 2005/29/EG. Demnach gilt jeder Dienst, der es Verbrauchern mithilfe von Software, einschließlich einer Website, eines Teils einer Website oder einer Anwendung, die vom oder im Namen des Gewerbetreibenden betrieben wird, ermöglicht, Fernabsatzverträge mit anderen Gewerbetreibenden oder Verbrauchern abzuschließen, als Online-Marktplatz. Im Referentenentwurf wird auf § 312l Abs. 3 BGB verwiesen, ohne dass dies einen sachlichen Unterschied bewirkt. Unternehmen, die einen Webshop betreiben, eröffnen Dritten jedoch zunehmend die Möglichkeit, über ihre Plattform Waren im eigenen Namen zu verkaufen. Da dies allerdings in der Regel nur in geringem Umfang geschieht, ist es nicht sachgerecht, solche Marktplätze einem kritischen Sektor zuzuordnen. Die Systematik der NIS-2-Richtlinie deutet darauf hin, dass der europäische Gesetzgeber insbesondere solche Marktplätze erfassen wollte, die maßgeblich zum Absatz von Waren Dritter beitragen und deshalb eine kritische Funktion erfüllen. Daher sollte eine Ausnahme für Anbieter vorgesehen werden, bei denen der Online-Marktplatz nur einen unwesentlichen Teil der Gesamttätigkeit ausmacht.

- **Zu § 2 Nr. 8 BSIG-E (Begriffsbestimmung, hier: „DNS-Diensteanbieter“)**

  Der Referentenentwurf übernimmt die Definition eines DNS-Diensteanbieters nach Art. 6 Nr. 20 Var. 1 NIS-2-Richtlinie wortgleich. Demnach gilt als DNS-Diensteanbieter jede Einrichtung, die für Internet-Endnutzer öffentlich verfügbare rekursive Dienste

zur Auflösung von Domain-Namen anbietet. Diese Formulierung ist äußerst weitreichend und bedarf dringend einer Konkretisierung oder zumindest einer engeren Auslegung in der Gesetzesbegründung.

- In der derzeitigen Fassung umfasst der Begriff potenziell auch Betreiber von Heimroutern, Unternehmensnetzwerken, Hotel-WLANs oder gemeinnützigen Initiativen wie Freifunk, sofern sie DNS-Dienste für Endnutzer bereitstellen. Die in der Gesetzesbegründung enthaltene Einschränkung, dass Anbieter nicht als eigenständige DNS-Diensteanbieter zu betrachten sind, wenn DNS-Dienste als „untrennbarer Teil eines Internetzugangsdienstes“ angeboten werden, greift zu kurz. In der Praxis sind DNS-Dienste technisch fast immer von Internetzugangsdiensten trennbar.
- Die Problematik wird dadurch verschärft, dass DNS-Diensteanbieter nach § 28 Abs. 1 Nr. 2 BSIG-E ohne Rücksicht auf Schwellenwerte erfasst werden. Anders als bei anderen Einrichtungen fehlt hier jegliche Differenzierung nach Größe, Nutzerzahl oder Kritikalität des Dienstes. Selbst minimal betriebene DNS-Dienste im privaten oder gemeinnützigen Bereich könnten so unter das volle Regime der NIS-2-Umsetzung fallen – mit erheblichen und für die Betreiber nicht leistbaren Aufwänden, die offensichtlich nicht beabsichtigt waren.

Um eine übermäßige und unverhältnismäßige Regulierung nicht intendierter Akteure zu vermeiden, sollte daher klargestellt werden, dass nur solche DNS-Diensteanbieter erfasst sind, die in einem nennenswerten Umfang rekursive DNS-Dienste im Rahmen einer kommerziellen Tätigkeit für die Öffentlichkeit anbieten und nicht lediglich im Rahmen geschlossener Nutzergruppen oder als Nebenfunktion.

- **Zu § 2 Nr. 10 BSIG-E (Begriffsbestimmung, hier: „erhebliche Cyberbedrohung“)**

Für die Definition der „einfachen“ Cyberbedrohung wird zur Konkretisierung zur Förderung eines einheitlichen begrifflichen Verständnisses richtigerweise auf Art. 2 Nr. 8 der Verordnung (EU) 2019/881 (Cybersecurity Act) verwiesen, § 2 Nr. 6 BSIG-E. Danach bezeichnet eine Cyberbedrohung einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte. Eine „erhebliche Cyberbedrohung“ soll demgegenüber eine Cyberbedrohung sein, die das Potenzial besitzt, die informationstechnischen Systeme, Komponenten und Prozesse aufgrund der besonderen technischen

Merkmale der Cyberbedrohung erheblich zu beeinträchtigen. Eine solche erhebliche Beeinträchtigung liegt laut Entwurf dann vor, wenn sie erheblichen materiellen oder immateriellen Schaden verursachen kann. Diese verwendete Formulierung ist aus zweierlei Gründen zu unbestimmt und sollte deshalb konkretisiert werden: So geht nicht deutlich aus der Vorschrift hervor, wie die „Erheblichkeit“ vom „Regelfall“ anzugrenzen ist und welche Ressourcen für diesen Fall zur Bewältigung der Cyberbedrohung herangezogen werden sollen. Überdies ist rechtlich unbestimmt, was mit einem „immateriellen Schaden“ gemeint sein soll und wie sich dieser bemerkbar macht bzw. auch von einem Datenschutzvorfall infolge einer realisierten Cyberbedrohung abzugrenzen ist. Dadurch entsteht das Risiko missverstandener oder zu weit ausgelegter Meldemaßnahmen von Unternehmen als unmittelbare Folge einer Rechtsunsicherheit. Dies führt zu ersparenswerten Mehraufwänden sowohl auf der Seite der durch NIS2UmsuCG betroffenen wie auch der beteiligten Behörden.

- **Zu § 2 Nr. 11 BSIG-E (Begriffsbestimmung, hier: „erheblicher Sicherheitsvorfall“)**

  Die für die vorgenannten Definition „erhebliche Cyberbedrohung“ genannten rechtlichen Probleme setzen sich bei der Definition des „erheblichen Sicherheitsvorfalls“ fort, denn insbesondere in der zweiten Variante lit. b) liegt ein solcher Vorfall dann vor, wenn er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann. So ist auch hier unklar, was mit „erheblichen“ Schäden sowie mit „immateriellen“ Schäden im Kontext des IT-Sicherheitsrechts gemeint sein soll. In der Praxis dürfte überdies generell die „erhebliche Cyberbedrohung“ vom „erheblichen Sicherheitsvorfall“ nur schwer begrifflich abgrenzbar sein, soweit sich die Beeinträchtigung bzw. Betriebsstörung noch nicht realisiert hat. Unabhängig von einer konkretisierenden Rechtsverordnung sollten hier weitere Bemessungskriterien ausgeführt werden.

- **Zu § 2 Nr. 12 BSIG-E (Begriffsbestimmung, hier: „Forschungseinrichtung“)**

  Laut Definition ist eine Forschungseinrichtung eine Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen.

Weitergehende Konkretisierungen werden nicht gegeben. Bereits jetzt gibt es in der Praxis Rechtsunsicherheit darüber, wie das „primäre Ziel“ zu verstehen sein soll und welche Bemessungskriterien hierfür anzulegen sind, und ebenso, ob die Rechtsträgerschaft der Forschungseinrichtung eine Relevanz für die Einstufung von kommerziellen Zwecken besitzt. Überdies stellt sich die Frage, weshalb nicht auch Forschungseinrichtungen des Bundes in den Katalog betroffener Einrichtungen aufgenommen werden, die Cyberbedrohungen ebenso ausgesetzt sind wie mit kommerziellem Hintergrund betriebene Forschungseinrichtungen[2].

- **Zu § 2 Nr. 13 BSIG-E (Begriffsbestimmung, hier: „Geschäftsleitung“)**

  Diese Vorschrift dient der Umsetzung von Art. 20 der NIS-2-Richtlinie und will die Leitungsorgane der betroffenen Einrichtungen stärker für die Cybersicherheit in die Pflicht nehmen. NIS-2 selbst spricht hier von den „Leitungsorganen wesentlicher und wichtiger“ Einrichtungen, ohne dies aber in besagtem Artikel näher zu konkretisieren. Auch die Vorschrift in § 2 Nr. 13 BSIG-E sorgt schon jetzt bei den betroffenen Unternehmen für Rechtsunsicherheit, da an die Weite bzw. Enge der Definition unmittelbare organisatorische Folgen im Unternehmen angeknüpft sind. Deshalb wäre eine inhaltliche Konkretisierung der Begriffsdefinition wünschenswert. Zurzeit wird auf die Kriterien des „Führens der Geschäfte“ und kumulativ „zur Vertretung“ der Einrichtung verwiesen, wobei sich die inhaltliche Anknüpfung aus dem Gesetz, einer Satzung oder dem Gesellschaftsvertrag ergeben kann. Jedoch ist beispielsweise auch eine einfachvertragliche bzw. arbeitsvertraglich eingeräumte Vertretungsbefugnis möglich, wie es zum Beispiel für Abteilungsleiter der Fall sein kann, die für ihren Bereich ebenso die Geschäfte führen und die Gesellschaft nach außen hin rechtswirksam vertreten können – dies dürfte gerade für größere Unternehmungen mit entsprechender Abteilungsgröße relevant sein.

- **Zu § 2 Nr. 17 BSIG-E (Begriffsbestimmung, hier: „Informationssicherheit“)**

  In verschiedenen anderen Stellungnahmen zum NIS2UmsuCG wird bereits auf die begrifflichen Unschärfen zu Informationssicherheit, Datensicherheit, Netzsicherheit,

[2] vgl. AG KRITIS, Stellungnahme zum Regierungsentwurf des NIS2UmsuCG vom 02.10.2024, S. 5, online abrufbar unter: https://ag.kritis.info/wp-content/uploads/2024/10/20241027-Stellungnahme-NIS2UmsuCG-RefE-v02102024-AG-KRITIS-v1.1.pdf

Netz- und Informationssicherheit, IT-Sicherheit, Cybersicherheit und Sicherheit in der Informationstechnik verwiesen (so GDD, Stellungnahme zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, S. 2, online abrufbar unter: https://www.gdd.de/wp-content/uploads/2024/10/GDD-Stellungnahme-NIS2UmsuCG-mm.pdf). Richtigerweise ist hier unbedingt ein einheitliches Begriffsverständnis zu schaffen, da die vorgenannten Begriffe allesamt über eine unterschiedliche Bedeutung und Weite verfügen und daher teils nicht zum gesetzlichen Rahmen passen. Optimalerweise sollte sich der Gesetzgeber hier auf einen zentralen Begriff festlegen. Unabhängig davon ist der vorliegende Begriff der „Informationssicherheit" auch unzureichend ausdefiniert, indem er wesentliche Schutzziele unterschlägt und nur auf die Vertraulichkeit, Integrität und Verfügbarkeit verweist. Das Kriterium der Authentizität sowie ggf. auch das Kriterium der Nichtabstreitbarkeit hingegen wird ausgeklammert.

- **Zu § 2 Nr. 19 BSIG-E (Begriffsbestimmung, hier: „Institutionen der Sozialen Sicherung**

  Die Aufnahme von Sozialleistungsbehörden als kritische Einrichtungen gemäß NIS-2 ist grundsätzlich gerechtfertigt, da diese Institutionen eine systemrelevante Rolle spielen.

  - Ein Kritikpunkt betrifft die unklare oder uneinheitliche Definition, welche Einrichtungen konkret unter die Kategorie „Sozialleistungsbehörden" fallen. Die Abgrenzung zwischen kommunalen und staatlichen Trägern, Mischformen (wie kommunale Zweckverbände) sowie privat-rechtlich organisierte Akteure mit öffentlichem Auftrag (z. B. freie Wohlfahrtspflege) ist in der Praxis nicht immer eindeutig.
  - Ein weiterer Kritikpunkt ist die Überlastung kleinerer und mittlerer Verwaltungseinheiten durch die erweiterten Compliance-Anforderungen. Die Einführung umfangreicher Berichtspflichten, Risikomanagementstrukturen und technischer Schutzsysteme droht zu einer Überregulierung zu führen, die eher lähmt als schützt. So erscheint das geforderte Schulungsniveau in der geforderten Zeit kaum erreichbar. Zudem könnte die Einführung zusätzlicher Pflichten durch NIS-2 zu Doppelregulierung und Zielkonflikten führen, insbesondere wenn bestehende Sicherheitsmaßnahmen nach anderen Standards umgesetzt wurden.

Bei der nationalen Umsetzung sollten daher folgende Aspekte berücksichtigt werden:

- Entwicklung sektorspezifischer Anwendungshilfen und Abgrenzungskriterien durch das BSI sowie standardisierten Prüfmechanismen, die abbildbar sind;
- Schaffung finanzieller und personeller Ausgleichsmechanismen für besonders betroffene kommunale Träger;
- Einrichtung zentraler Kompetenzzentren (z. B. auf Landesebene), die kleinere betroffene Behörden unterstützen;
- Berücksichtigung bestehender Sicherheitsarchitekturen, um Doppelregulierung zu vermeiden;
- Förderprogramme zur Schulung von Mitarbeitenden sowie insbesondere der Leitungsebene im Bereich Cybersicherheit.

- **Zu § 2 Nr. 22 BSIG-E (Begriffsbestimmung, hier: „kritische Anlage“)**

  Der bislang geltende zentrale Begriff der „kritischen Infrastruktur“ wird künftig durch die „kritische Anlage“ ersetzt, die Bestandteil der „besonders wichtigen Einrichtungen“ ist, die von den „wichtigen Einrichtungen“ abzugrenzen sind (auf die übermäßige Komplexität dieser Begriffe und den Vorschlag zur unmittelbaren Orientierung am europäischen Rahmen nach NIS-2 wird in der im späteren Verlauf folgenden Stellungnahme zu § 28 BSIG-E verwiesen). Die Bestimmung der kritischen Anlage soll durch Rechtsverordnung erfolgen, die gegenwärtig nicht vorliegt, aber sich vermutlich künftig an den zahlenmäßigen Maßgaben der BSI-KritisV orientieren wird. Mangels weitergehender begrifflicher Konkretisierung können sich betroffene Unternehmen zurzeit deshalb noch nicht auf den neuen Anwendungsbereich vorbereiten. Hier stellt sich deshalb die Frage, ob die neue zusätzliche Kategorie der „kritischen Anlagen“ in dieser Form tatsächlich erforderlich ist, um das gesetzgeberische Ziel zu erreichen. Es bestehen schon jetzt praktische Unsicherheiten dergestalt, ob die höheren Anforderungen für die gesamte Einrichtung oder nur für den Betrieb der kritischen Anlage heranzuziehen sind. Im Sinne einer Vereinfachung der Handhabung und zur Verbesserung der Rechtssicherheit wäre deshalb anzudenken, die zusätzliche Bestimmung der „kritischen Anlage“ im Gesetzentwurf entfallen zu lassen. Die zusätzliche Kritikalität dieser Anlagen könnte hingegen bereits über die Maßnahmen des Risikomanagements Eingang in die Betrachtung finden, das ja gerade in § 30 Abs. 1 BSIG-E bereits verlangt, dass sich die zu leistenden Maßnahmen zum Risikomanagement u.a. am Ausmaß der

Risikoexposition und den gesellschaftlichen und wirtschaftlichen Auswirkungen zu orientieren haben. Auf diese Weise könnte eine verkomplizierende Begriffsdefinition entfallen, ohne den Schutzbedarf herabzusetzen.[3] Durch eine solche Änderung würde ebenfalls die Definition der „kritischen Komponenten“ angetastet, deren Anwendungsfälle konkret untergesetzlich zu bestimmen wären, ohne auf die kritischen Anlagen Bezug zu nehmen. Generell ist in diesem übergreifenden Zusammenhang anzumerken, dass die begriffliche Unterscheidung zwischen „kritischen Anlagen“, „kritischen Komponenten“ und „kritischen Dienstleistungen“ nicht zu einer praktikableren Handhabbarkeit der Regelungen seitens betroffener Einrichtungen beiträgt.

- **Zu § 2 Nr. 26 BSIG-E (Begriffsbestimmung, hier: „Managed Service Provider“)**

  Teilweise wird angemerkt, dass die Definition des „Managed Service Provider“ (MSP) zu weit gefasst ist und zahlenmäßig bzw. inhaltlich begrenzt sein sollte. Bei einem MSP handelt es sich um einen Anbieter von Diensten im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten der Kunden oder aus der Ferne. Eine Eingrenzung der Begriffsdefinition sollte jedoch unabhängig von rechtlichen Fragestellungen allein schon deshalb nicht vorgenommen werden, da die MSP als Bestandteil der digitalen Lieferkette eine essenzielle Funktion auch für die Verfügbarkeit und Integrität von IT-Systemen wahrnehmen und eine Vielzahl an Unternehmen insbesondere in Deutschland derartige Leistungen anbieten und ansonsten Regelungslücken entstehen würden.

  Positiv hervorzuheben ist daher die Klarstellung in der Gesetzesbegründung, dass ein bestimmter Kundenkreis keine Voraussetzung für die Einstufung als Managed Service Provider (MSP) ist. Damit wird zutreffend anerkannt, dass auch Unternehmen, die den zentralen IT-Betrieb innerhalb eines Unternehmensverbunds übernehmen, in der

[3] vgl. zur Kritik der „Überkomplexität“ auch AG KRITIS, Stellungnahme zum Regierungsentwurf des NIS2UmsuCG vom 02.10.2024, S. 5, online abrufbar unter: https://ag.kritis.info/wp-content/uploads/2024/10/20241027-Stellungnahme-NIS2UmsuCG-RefE-v02102024-AG-KRITIS-v1.1.pdf

Regel als MSP einzustufen sind. Auch die NIS-2-Richtlinie selbst stützt diese Sichtweise. Erwägungsgrund 16 NIS-2-Richtlinie stellt klar, dass interne Rechenzentrumsdienste nur dann vom Anwendungsbereich der Richtlinie ausgenommen sind, wenn sie sich „[…] im Besitz der betreffenden Einrichtung befinden und von dieser ausschließlich für eigene Zwecke betrieben werden“. Diese Wertung lässt sich auf Managed Services übertragen: Sobald ein Unternehmen IT-Dienstleistungen für andere juristische Personen erbringt, ist der Anwendungsbereich der NIS-2-Richtlinie eröffnet. Diese Auslegung entspricht auch der Umsetzung der NIS-2-Richtline in anderen Mitgliedstaaten.

Bei der Umsetzung ist dennoch darauf zu achten, dass die Vorgaben künftig im Gleichlauf mit den Anforderungen aus dem EU Cyber Resilience Act (CRA) realisiert werden, die auch auf verschiedene MSP zutreffen werden.

- **Zu § 2 Nr. 38 BSIG-E (Begriffsbestimmung, hier: „Schwachstelle“)**

  Die Begriffe „Schwachstelle“ und „Sicherheitslücke“ haben grundsätzlich eine unterschiedliche Bedeutung, wie auch aus der vorgeschlagenen Gesetzesänderung hervorgeht. Die bisherige „Sicherheitslücke“ wird technisch als „Eigenschaft von Programmen oder sonstigen informationstechnischen Systemen“ beschrieben, wohingegen die „Schwachstelle“ deutlich weiter gefasst ist als eine Eigenschaft von IKT-Produkten oder IKT-Diensten, die von Dritten ausgenutzt werden kann, um sich gegen den Willen des Berechtigten Zugang zu den IKT-Produkten oder IKT-Diensten zu verschaffen oder die Funktion der IKT-Produkte oder IKT-Dienste zu beeinflussen. Zur besseren Nachvollziehbarkeit des Handlungsrahmens im Sinne einer unabhängigen fachlich-technischen Arbeit wird empfohlen, auch in Zukunft nicht den Begriff der „Schwachstelle“, sondern denjenigen der „Sicherheitslücke“ zu verwenden. Alternativ könnte der Begriff der Sicherheitslücke beibehalten werden und die Schwachstelle als zusätzliche Definition aufgenommen werden, um anhand der jeweiligen Befugnisgrundlagen eine Abgrenzung durch Einzelverweis vorzunehmen.

- **Zu § 2 Nr. 41 BSIG-E (Begriffsbestimmung, hier: „Systeme zur Angriffserkennung“)**

  Der zwingende Einsatz von Systemen zur Angriffserkennung (SzA) ist in Fachkreisen ohnehin bereits seit Längerem umstritten, siehe dazu noch im Folgenden. Schon im

geltenden Recht ist die Definition der SzA denkbar weit gefasst und auch durch die gesetzlich vorgeschlagenen Regelungen wird die neue Definition in ihrer Weite nicht eingeschränkt, indem SzA definiert werden als durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme, wobei die Angriffserkennung durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten, erfolgt. Das BSI hat die Anforderungen zum Einsatz von SzA im KRITIS-Bereich durch eine Orientierungshilfe aus dem Jahr 2022[4] weitergehend konkretisiert. In der praktischen Umsetzung besteht dennoch weiterhin Unsicherheit darüber, ob für den Einsatz von SzA in wesentlichen und wichtigen Diensten jenseits der kritischen Infrastrukturen diese ähnlichen oder gar denselben Anforderungen genügen müssen, was sich durch eine Vielzahl am Markt verfügbarer Produkte weiter verschärft. An dieser Stelle wäre ein Verweis auf weitergehende untergesetzliche Konkretisierungen, beispielsweise durch das BSI, hilfreich bzw. alternativ eine begrifflich einengende Definition denkbar.

- **Zu § 3 BSIG-E (Aufgaben des Bundesamtes)**

  Der Katalog der Aufgabenzuweisungen des BSI wurde in den vergangenen Jahren durch verschiedene Gesetzesnovellen laufend erweitert, damit einhergehend auch sein Ausbau als zentrale Stelle für Informationssicherheit in Deutschland. Wie bereits für den Entwurf des § 1 BSIG-E angemerkt gehen damit auch gesteigerte Erwartungen an die unabhängige und fachlich-sachliche Tätigkeit des BSI einher, die im gegenwärtigen Status des Gesetzentwurfs nicht angemessen wiedergegeben werden. Die grundsätzliche Stärkung des BSI im aktuellen Entwurf wird begrüßt. Dies betrifft seine ausdrückliche, behördenübergreifende Unterstützerrolle in der Gesetzesbegründung zu § 3 (Aufgaben des Bundesamtes) Nummer 17, sowie die Erhebung des IT-Grundschutzes zu „mittelbaren Gesetzesrang“ in § 44 Abs. 1 n.F.

  Unter diesem Gesichtspunkt hervorhebenswert ist zudem § 3 Abs. 18 BSIG-E. Schon nach geltendem Recht enthält diese Vorschrift die Bestimmung von Unterstützungsaufgaben des BSI gegenüber Polizeien, Strafverfolgungsbehörden und

[4] BSI, Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung, online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.html

Nachrichtendienstbehörden. Daraus geht jedoch noch nicht ausreichend eindeutig hervor, auf welchem Wege die Unterstützungsleistung erfolgt, welche Ziele sie bezweckt und welchen Einschränkungen sie zu genügen hat. Im Zweifelsfall ist nach gegenwärtigem Stand nicht eindeutig aus der gesetzlichen Formulierung heraus klärbar, worin die „gesetzlichen Aufgaben" von Sicherheitsbehörden bestehen sollen, bei denen das BSI Unterstützungsleistungen erbringt. So können gesetzliche Aufgaben auch solche sein, die die IT-Sicherheit schwächen, indem beispielsweise Maßnahmen nach der StPO zur Durchführung von Quellen-Telekommunikationsüberwachungen oder Online-Durchsuchungen durchgeführt werden – für die das BSI weder zuständig ist noch als Cybersicherheitsbehörde irgendwie geartete Unterstützung leisten darf. Deshalb sollten diese Aufgaben schon hier weitergehend konkretisiert werden bzw. zumindest festgestellt werden, dass diese Unterstützungsleistungen nicht zu einer Schwächung der Cybersicherheit, sondern zu ihrer Stärkung führen müssen, indem beispielsweise Unterstützung bei der Aufklärung von Cyberkriminalität geleistet wird. Überdies mutet die bereits geltende – und durch NIS2UmsuCG nur geringfügig angetastete – Ausnahmeregelung unter diesem Gesichtspunkt eigentümlich an, schlägt sie in § 3 Nr. 18 lit. c) BSIG-E doch vor, dass die Unterstützung auch gewährt werden darf, soweit sie erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die „unter Nutzung der Informationstechnik erfolgen". Es ist dringend anzuraten, diesen zweiten Halbsatz zu streichen, um einer Ausweitung der Unterstützungsleistungen gegen die Ziele der Informationssicherheit unter dem Dach der Aufgabenzuweisungen des BSI entgegenzuwirken (so richtigerweise auch GDD, Stellungnahme zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, S. 2 f., online abrufbar unter: https://www.gdd.de/wp-content/uploads/2024/10/GDD-Stellungnahme-NIS2UmsuCG-mm.pdf).

Gemäß der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA) gelten spezielle Anforderungen für die Informationssicherheit im hochregulierten Bereich der Finanzunternehmen. § 3 Nr. 29 BSIG-E schreibt deshalb richtigerweise vor, dass das BSI mit der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zur Aufgabenerfüllung kooperiert und Informationen austauscht, soweit dies zur Aufgabenerfüllung erforderlich ist. Diese Formulierung ist jedoch nicht weitreichend genug, da schon jetzt in der Umsetzungspraxis der europäischen und nationalen Regulierung zur Informationssicherheit Abgrenzungsschwierigkeiten zwischen den Tätigkeiten von

BSI und BaFin, bestehen, die bei den betroffenen Unternehmen zu Mehraufwänden und vor allem zu Rechtsunsicherheit über Zuständigkeiten führen. § 3 Nr. 29 BSIG-E sollte daher um eine Vorgabe ergänzt werden, dass nicht nur Kooperation und Informationsaustausch stattfinden, sondern eine Abstimmung und Klärung eventueller Zuständigkeitsüberschneidungen stattfindet, die durch die regulierten Finanzunternehmen an BSI und BaFin herangetragen werden.

- **Zu § 5 BSIG-E (Allgemeine Meldestelle für die Sicherheit in der Informationstechnik)**

  Infolge des bereits für § 3 BSIG-E skizzierten zunehmenden Ausbaus des BSI als zentrale Stelle für Informationssicherheit in Deutschland geht eine erheblich gesteigerte Verantwortung für den Umgang mit den erlangten, teils hochsensiblen und unter Umständen auch geschäftsgeheimnisbezogenen Daten einher. Nur wo ein Vertrauen in die behördlichen Strukturen zur Informationssicherheit in Deutschland herrscht, kann auch eine funktionierte nationale digitale Sicherheitsarchitektur aufgebaut werden. Auf die mit der fehlenden institutionellen Unabhängigkeit des BSI einhergehenden Probleme wurde in dieser Stellungnahme bereits u.a. unter § 1 BSIG-E eingegangen. Hervorzuheben sei an dieser Stelle jedoch erneut, dass das BSI mangels institutioneller Unabhängigkeit nach wie vor dem Geschäftsbereich des Bundesministeriums des Innern und für Heimat (BMI) zuzuordnen ist, dem auch Polizei- und Nachrichtendienstbehörden unterfallen. Deshalb scheint hier gem. § 5 Abs. 3 BSIG-E eine eindeutige Klarstellung dergestalt geboten, dass die gemeldeten Informationen ausschließlich zur Verbesserung der Informationssicherheit verwendet und weitergegeben werden dürfen und eine Verwendung und Weitergabe der Informationen zur Ausnutzung von ebenjenen festgestellten oder gemeldeten Sicherheitslücken bzw. Schwachstellen nicht stattfindet. Abweichungen vom in der Vorschrift gegenwärtig wiedergegebenen intendierten Ermessen, eine Information zu Zwecken der Verbesserung der Informationssicherheit weiterzugeben, müssen auf absolute Ausnahmefälle beschränkt sein, sind zu dokumentieren und einzelfallbezogen zu begründen und dürfen nicht ausschließlich auf eine Weisung aus dem BMI zurückzuführen sein, ggf. ist hier zusätzlich ein abschließender Katalog

berechtigter bzw. widerstreitender Interessenspositionen zu nennen, die denen der Informationssicherheit in einer verfassungsrechtlichen Abwägung ebenbürtig sind.[5]

- **Zu § 6 BSIG-E (Informationsaustausch)**

  Die Einrichtung einer Online-Plattform zum Informationsaustausch über Cyberbedrohungen, Schwachstellen, Beinahevorfälle und IT-Sicherheitsmaßnahmen sowie zur Aufdeckung und Abwehr von Cyberangriffen (Information Sharing Portal) ist zu begrüßen, da sie zu einer deutlich verbesserten Aufbereitung, verlässlichen Quelle und schnellen Verteilung cybersicherheitsrelevanter Informationen führt. Hier sollte jedoch von Anfang an sichergestellt werden, dass alle relevanten behördlichen Akteure eingebunden werden, indem ein ganzheitlicher Ansatz verfolgt wird, der nicht nur die Informationssicherheit, sondern ebenso die hybride Bedrohungslage adressiert, beispielsweise Gefährdungen durch Sabotage oder Desinformation. Hilfreich wäre überdies die Integration von zielgruppengerechten Handlungsempfehlungen und Unterstützungsangeboten in das Information Sharing Portal. In den Prozess der Erarbeitung der Teilnahmebedingungen und Aufbau der Plattform sollten deshalb zu bestmöglicher Effizienz und Effektivität der Plattform Verbände und relevante Wirtschaftsakteure von Anfang an einbezogen werden.

- **Zu § 7 BSIG-E (Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte)**

  Gem. § 7 Abs. 1 BSIG-E ist das BSI befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, zu kontrollieren. Gemäß den Absätzen 6 und 7 (und an weiteren Stellen im BSIG-E die Sicherheit der Kommunikationstechnik des Bundes betreffend) werden hiervon aber umfassende Ausnahmetatbestände vorgesehen, so für das Auswärtige Amt, die Streitkräfte und den Militärischen Abschirmdienst, ohne dass erkennbar wäre, wie für diese Einrichtungen auf alternativem Wege vergleichbare Kontrollmechanismen vorgesehen wären. Im Sinne eines einheitlichen Niveaus der Informationssicherheit

[5] vgl. auch Claudia Plattner, Präsidentin des BSI, Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestags am 4. November 2024, S. 14, online abrufbar unter: https://www.bundestag.de/ausschuesse/a04_inneres/anhoerungen/1026172-1026172

in der deutschen Verwaltung ist zu empfehlen, diese Ausnahmen zu streichen – unabhängig von den gegebenen europarechtlichen Möglichkeiten.

§ 7 Abs. 8 BSIG-E bestimmt überdies, dass wenn das BSI im Rahmen seiner Kontrollen feststellt, dass ein Verstoß gegen die Verpflichtungen des BSIG eine offensichtliche Datenschutzverletzung zur Folge hat, die gem. Art. 33 DS-GVO meldepflichtig ist, es unverzüglich die zuständigen Aufsichtsbehörden hierüber unterrichtet. Unklar ist, warum sich diese Vorschrift zur Weitergabe ausschließlich auf „offensichtliche Datenschutzverletzungen“ beschränkt, obwohl der europarechtliche Rahmen an dieser Stelle deutlich enger gefasst ist. Hier sollte eine Weitergabe bereits bei der „bloßen Möglichkeit“ der Datenschutzverletzung erfolgen.

- **Zu § 28 BSIG-E (Besonders wichtige und wichtige Einrichtungen)**

  Nach wie vor erschließt sich nicht, weshalb der deutsche Gesetzgeber nicht die europäischen Begrifflichkeiten in der Unterscheidung zwischen „wesentlichen“ und „wichtigen“ Einrichtungen übernimmt und anstelle dessen mit den „besonders wichtigen“ und den „wichtigen“ Einrichtungen neue Alternativbegriffe einführt, die Rechtsunsicherheit stiften. Auch die zusätzliche neue Subkategorie der „Betreiber kritischer Anlagen“ ist wie zuvor dargestellt nicht zwingend notwendig, um dem gesteigerten Schutzbedarf dieser durch das Gesetz adressierten Einrichtungen auf angemessene Weise gerecht zu werden.

  An verschiedenen Stellen hat es in der Vergangenheit Kritik an der tatbestandlichen Weite der durch NIS-2 und damit auch NIS2UmsuCG zusätzlich adressierten Unternehmen gegeben. Dazu ist festzustellen: Weder an der europäischen Size-Cap-Rule in quantitativer Hinsicht noch qualitativ mit Blick auf die sektoralen Zugehörigkeiten lassen sich im bundesdeutschen Recht deutliche Anpassungen vornehmen, ohne gegen die Vorgaben des Europarechts zu verstoßen. Der tatsächliche rechtliche Gestaltungsspielraum des deutschen Gesetzgebers ist hier limitiert. Die Frage der Umsetzung und Überprüfbarkeit von ca. 30.000-40.000 durch NIS-2 betroffenen Unternehmen ist davon losgelöst zu sehen und betrifft erst einmal nicht das in Rede stehende Gesetzgebungsverfahren zu NIS2UmsuCG, sondern dessen spätere Umsetzung.

- **Zu § 28 Abs. 3 BSIG-E: „Vernachlässigbare“ Geschäftstätigkeiten**

  Der Referentenentwurf sieht eine von den Grundsätzen der NIS-2-Richtlinie abweichende Sonderregelung vor. Nach § 28 Abs. 3 BSIG-E können bei einer Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung „vernachlässigbar“ sind. Wann eine Geschäftstätigkeit „vernachlässigbar“ ist, wird im Gesetzentwurf nicht definiert. Es handelt sich um einen unbestimmten Rechtsbegriff. Aus der Formulierung „im Hinblick auf die gesamte Geschäftstätigkeit“ lässt sich jedoch ableiten, dass eine relative Bestimmung erforderlich ist. Ob eine Tätigkeit vernachlässigbar ist, muss durch die jeweilige Einrichtung im Einzelfall unter Berücksichtigung der Gesamttätigkeit der Einrichtung geprüft werden. Ob als Maßstab für die jeweilige Geschäftstätigkeit der Umsatz, der Personaleinsatz oder andere Faktoren heranzuziehen sind, bleibt offen. In den Umsetzungsgesetzen anderer EU-Mitgliedstaaten findet sich keine entsprechende Formulierung. Auch andere Gesetze bieten keine Orientierung.

  Da der Anwendungsbereich der NIS-2-Richtlinie in vielen Punkten sehr weit ist, ist das Ziel einer maßvollen Beschränkung nachvollziehbar. Zudem stellt der aktuelle Entwurf gegenüber dem bisher in den deutschen Entwürfen verfolgten Konzept der „zuzuordnenden Geschäftstätigkeit“ eine Verbesserung dar, da damit der Anwendungsbereich gegenüber der NIS-2-Richtlinie weniger stark beschnitten wird. Der Referentenentwurf liegt damit näher an einer 1:1 Umsetzung der Richtlinie. Außerdem erfordert die Neuregelung keine aufwändige und kaum umsetzbare Quotelung von Mitarbeiterzahl, Jahresumsatz und Bilanzsumme mehr.

  Dennoch ist auch die neue Regelung aus den folgenden Gründen kritisch zu sehen:

  - Zweifel an EU-Rechtskonformität: Die NIS-2-Richtlinie sieht keine Ausnahme für „vernachlässigbare“ Tätigkeiten vor. Durch die Ausnahmeregelung wird der Anwendungsbereich gegenüber der NIS-2-Richtlinie verkleinert. Bei der NIS-2-Richtlinie handelt es sich, wie Art. 5 NIS-2-Richtlinie ausdrücklich klarstellt, um eine Mindestharmonisierung.
  - Fragwürdiges Kriterium: Ein Kriterium, das auf das Verhältnis einer bestimmten Tätigkeit zur gesamten Geschäftstätigkeit eines Unternehmens abstellt, überzeugt inhaltlich nicht. Das zentrale Ziel der NIS-2-Richtlinie besteht in der Stärkung der Cybersicherheit in der EU. Für die Beurteilung der Relevanz eines

Dienstes oder einer Tätigkeit kann deshalb nicht maßgeblich sein, welches Gewicht sie im Gesamtgefüge der jeweiligen Einrichtung einnimmt.

- Mangelnde Bestimmtheit: Weder Gesetzestext noch Gesetzesbegründung geben Anhaltspunkte dafür, nach welchen Kriterien sich bestimmt, ob ein Dienst oder eine Tätigkeit im Hinblick auf die gesamte Geschäftstätigkeit einer Einrichtung vernachlässigbar ist. Denkbar wäre auf den Umsatz, den Personaleinsatz oder die aufgewandten Sachmittel abzustellen.
- Zuständigkeitskonflikte: Abweichungen von der NIS-2-Richtlinie können insbesondere bei grenzüberschreitend tätigen Unternehmen zu problematischen Konstellationen führen.

Deutschland sollte – wie alle anderen EU-Mitgliedstaaten – die Vorgaben der NIS-2-Richtlinie konsequent umsetzen. Gleichzeitig sollte jedoch weiterhin die in Erwägungsgrund 16 der NIS-2-Richtlinie vorgesehene Möglichkeit genutzt werden, bei der Hinzurechnung von Partnerunternehmen und verbundenen Unternehmen Ausnahmen vorzusehen.

Um den Anwendungsbereich der NIS-2-Richtlinie sinnvoll zu beschränken, sollten – statt unklarer Ausnahmeregelungen auf der ersten Ebene – Auslegungsspielräume bei der Bestimmung der regulierten Sektoren genutzt werden. Diese sind in der NIS-2-Richtlinie teils unbestimmt definiert. Der deutsche Gesetzgeber könnte präzisierende Definitionen aufnehmen. Anders als die jetzt gewählte Lösung in § 28 Abs. 3 BSIG-E oder die zuvor formulierte abweichende Schwellenwertberechnung kann diese Lösung zumindest als eine zulässige Interpretation der NIS-2-Richtlinie durch den deutschen Gesetzgeber präsentiert werden.

- **Zu § 29 BSIG-E (Einrichtungen der Bundesverwaltung)**

  Im Hinblick auf die Risiken eines Abfalls des Informationssicherheitsniveaus von Einrichtungen der Bundesverwaltung im Vergleich zu privatwirtschaftlichen Akteuren wird auf die umfassende Kritik verwiesen, die bereits in verschiedenen anderen Stellungnahmen adressiert wurde.[6] Bei der Bewertung der Bedrohungslage in der Informationssicherheit kann nicht derart deutlich zwischen staatlichen und

[6] so z.B. auch AG KRITIS, Stellungnahme zum Regierungsentwurf des NIS2UmsuCG vom 02.10.2024, S. 6 ff.[6]; Prof. Timo Kob, Stellungnahme NIS2UmsuCG, S. 3 ff.[6]; GDD, Stellungnahme zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, S. 4, online abrufbar unter: https://www.gdd.de/wp-content/uploads/2024/10/GDD-Stellungnahme-NIS2UmsuCG-mm.pdf

nichtstaatlichen Akteuren unterschieden werden, sondern alle Einrichtungen sind gleichermaßen erfasst – man wird im Gegenteil sogar davon auszugehen haben, dass in Zeiten der hybriden Bedrohungslage und von Cyberwarfare und internationalen Spionageaktivitäten staatliche Einrichtungen noch stärker im Fokus stehen als manches mittelständische Unternehmen, das neuerdings ebenso in den Anwendungsbereich von NIS-2 fällt. Gleichwohl ist es jedoch nicht so – wie teils auch suggeriert wird – dass Einrichtungen der Bundesverwaltung kaum oder gar keine Informationssicherheit umzusetzen haben, da sich in den §§ 43 ff. BSIG-E Spezialregelungen zu diesem Themenkomplex finden, auf die noch im Folgenden eingegangen wird. Dennoch sollte unter Berücksichtigung vorgenannter Kritik berücksichtigt werden, dass trotz der Ausnahmetatbestände im Endeffekt ein Informationssicherheitsniveau realisiert werden sollte, das demjenigen der privatwirtschaftlich betroffenen Einrichtungen mindestens ebenbürtig ist. Unter diesem Gesichtspunkt ist auch die Regelung des § 37 BSIG-E (Ausnahmebescheid) zu sehen, denn europarechtlich kann zwar vorgesehen sein, dass bestimmte öffentliche Bereiche von der Regulierungshoheit auch nach NIS-2 ausgenommen sind, ob diese rechtliche Konsequenz jedoch auch zwingend in das nationale Recht übertragen werden muss, kann man durchaus hinterfragen, denn die Informationssicherheit sollte vielleicht gerade in diesen sicherheitssensiblen Bereichen mit einem höchstmöglichen Standard gewährleistet werden.

Unter rechtssystematischen Gesichtspunkten ist die Regelung des § 29 BSIG-E ungünstig, da sie im Zusammenhang mit den §§ 43 ff. BSIG-E zu sehen ist. Zu empfehlen wäre deshalb, die Definition der „Einrichtungen der Bundesverwaltung“ aus § 29 Abs. 1 BSIG in die Begriffsbestimmungen gem. § 2 BSIG-E zu übertragen, damit sie an späterer Stelle wiederverwendet werden kann und eine systematische Verbindung über das gesamte Gesetz hinweg zwischen § 29 BSIG-E und §§ 43 ff. BSIG-E hergestellt werden kann. Auch dürfte ein unmittelbar in § 29 BSIG-E enthaltener Verweis sinnvoll sein, dass trotz der Ausnahmetatbestände in den §§ 43 ff. BSIG-E eigenständige Regelungen für die Informationssicherheit in der Bundesverwaltung vorgesehen sind.

- **Zu § 30 BSIG-E (Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen)**

  § 30 BSIG-E enthält mit der Festlegung der Risikomanagementmaßnahmen von besonders wichtigen und wichtigen Einrichtungen ein Kernelement der nationalen Umsetzung von NIS-2. Wenngleich die nationalen Umsetzungsspielräume infolge der sehr konkreten Regelung aus Art. 21 NIS-2 nur begrenzt sind, sind Verbesserungen an dieser Stelle angeraten. Dies betrifft insbesondere die unmittelbare Übernahme des europarechtlich vorgegebenen Maßnahmenkatalogs in § 30 Abs. 2 BSIG, der im Sinne eines Mindestkatalogs diejenigen Maßnahmen zur Informationssicherheit beschreibt, die in jedem Falle minimal umzusetzen sind. Dieser aus dem europäischen Recht kommende Katalog ist nicht nur irreführend, sondern auch unpraktikabel, indem er einzelne Maßnahmen in den Vordergrund stellt, die teils noch nicht einmal auf jedes durch NIS-2 betroffene Unternehmen anwendbar sind. Überdies suggeriert er, durch einzelne Produkte eine NIS-2-Konformität herstellen zu können, wo es eigentlich doch auf die Etablierung eines fortlaufenden Risikomanagementsystems zur Informationssicherheit ankommt. Empfohlen wird deshalb, auf die Übernahme dieses Katalogs zu verzichten und im Wege einer „unionsrechtskonformen Auslegung“ auf die Umsetzung von Risikomanagement nach Stand der Technik gem. § 30 Abs. 1 BSIG-E zu verweisen. Dies würde vielen betroffenen Einrichtungen nicht nur die Umsetzung erleichtern, sondern auch nicht unbedingt nötige Mehraufwände bei der Umsetzung vermeiden. Dass dies realisierbar ist, belegt die Umsetzung im mitgliedstaatlichen Vergleich, wo teils zwar inhaltliche Übernahmen des Katalogs stattfinden, teils aber auch kein Bezug auf den Katalog genommen und beispielsweise auf untergesetzliche Konkretisierungen verwiesen wird. Der verwendete Maßnahmenkatalog nach NIS-2 ist überdies auch zu unbestimmt – so werden Begriffe wie „Cyberhygiene“ aufgelistet, ohne zu definieren, was hierunter zu verstehen ist und inwieweit sich die damit verbundenen Maßnahmen zur Informationssicherheit von den bereits beschriebenen anderen Maßnahmen unterscheiden. Überdies stellt sich die Frage, ob nicht auch jenseits der besonders wichtigen Einrichtungen Branchenverbände an der Erarbeitung eigener und bereichsspezifischer Standards zur Informationssicherheit mitwirken können sollten, die mit dem BSI abgestimmt werden.

  Kritisch zu würdigen ist ebenfalls der § 30 Abs. 6 BSIG-E, der vorschreibt, dass besonders wichtige Einrichtungen und wichtige Einrichtungen durch

Rechtsverordnung nach § 56 Abs. 3 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden dürfen, wenn diese über eine Cybersicherheitszertifizierung gem. europäischer Schemata nach Art. 49 der Verordnung (EU) 2019/881 (Cybersecurity Act) verfügen. Fraglich ist an dieser Stelle, weshalb eine ausschließliche Bezugnahme auf das CSA-Framework stattfindet, wenn anstelle dessen grds. mehrere Optionen zur Verfügung stehen, um ein Risikomanagement nach NIS-2 durchzuführen und nachzuweisen. Hinzu tritt an dieser Stelle, dass sich die Cybersecurity Certification Schemes nach CSA bereits seit Jahren in der Erstellung befinden, insbesondere mit Blick auf Schlüsseltechnologien wie Cloud und 5G und somit zumindest zurzeit keine verlässliche Nachweisgrundlage darstellen können.

- **Zu § 31 BSIG-E (Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen)**

  Wie bereits dargelegt stellt sich die Frage, ob neben den wesentlichen Einrichtungen nach NIS-2 eine weitere Kategorie von betroffenen Einrichtungen in Form der Betreiber kritischer Anlagen benötigt wird – dies ist nur dann der Fall, wenn ohne eine solche Regelung Schutzlücken in der Informationssicherheit bestünden. Da § 30 BSIG-E zur Bewertung des Informationssicherheitsniveaus bereits an eine individuelle Risikoanalyse eines Unternehmens anknüpft, können hierüber bereits solche betroffenen Einrichtungen mit einer höheren Risikoprävalenz abgedeckt werden. Insoweit enthält auch der § 31 Abs. 1 BSIG-E keine nennenswerten inhaltlichen Erkenntnisse, die über die Regelung in § 30 Abs. 1 BSIG-E hinausgingen.

  Überdies wurde auch die Verpflichtung zum Einsatz von Systemen zur Angriffserkennung (SzA) für die Betreiber kritischer Anlagen in der Vergangenheit mehrfach kritisiert. Dies einerseits aus europarechtlichen Gründen, weil diese starre Festlegung nicht mit den technischen Zielen aus der jüngst veröffentlichten Durchführungsverordnung (EU) 2024/2690 korreliert, andererseits aber auch aus technischen Gründen, weil nicht klar ist, warum SzA gegenüber anderen Maßnahmen, die im Rahmen eines Risikomanagements nach NIS-2 zu ergreifen sein können, eine besonders herausgehobene Stellung genießen sollten, zumal der Aufbau und Betrieb von SzA mit erheblichen wirtschaftlichen Aufwänden verbunden sein kann.

- **Zu § 32 BSIG-E (Meldepflichten)**

  Grundsätzlich ist zu begrüßen, dass nach NIS-2 ein mehrstufiges Meldeverfahren vorgesehen ist, das an den unterschiedlichen Informations- und Kenntnisstand der betroffenen Einrichtungen zum jeweiligen Zeitpunkt anknüpft. Auch hier sollte jedoch ein Augenmerk darauf gelegt werden, das Meldeverfahren möglichst unbürokratisch zu gestalten und Mehraufwände durch Mehrfachmeldungen zu vermeiden. Der mit der Vorschrift nunmehr verfolgte Ansatz, einen Gleichlauf zwischen KRITIS-DachG und NIS2UmsuCG herzustellen, indem eine gemeinsame Meldestelle geschaffen wird, ist deshalb begrüßenswert. Darüber hinaus sind jedoch im Bereich der Informationssicherheit in Deutschland weitere Behörden eingebunden, so u.a. die Bundesnetzagentur (BNetzA) und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Wie ebenfalls in dieser Stellungnahme bereits dargelegt kann mit einer Verletzung der Informationssicherheit zugleich auch eine Datenschutzverletzung nach DS-GVO einhergehen, die zusätzliche Meldepflichten auslöst. Hier ist es den betroffenen Unternehmen nicht mehr zumutbar, zahlreiche verschiedene Meldekanäle mit unterschiedlichen formalen Anforderungen an die Meldung gleichzeitig zu bespielen und zu ermitteln, welcher Meldekanal auf welcher Rechtsgrundlage für den Einzelfall einschlägig ist. Daher ist anzuraten, die Zentralisierung einer gemeinsamen Meldestelle weiter auszudehnen und weitere Behörden und ggf. die Datenschutzaufsicht einzubeziehen, sodass die Meldung ohne Zutun der betroffenen Einrichtung stets an die zuständigen Stellen weitergegeben wird. Hierdurch wird nicht nur die Akzeptanz der Meldepflicht verbessert, sondern auch ein höheres Informationssicherheitsniveau insgesamt erzielt, da die Meldungen stets an der richtigen Stelle zeitnah ankommen. Überdies sind in der nationalstaatlichen Umsetzung in europäischer Koordination Maßnahmen zu bestimmen, wie insbesondere bei multinationalen Unternehmen, die in mehreren EU-Mitgliedstaaten gleichzeitig tätig sind, ggf. Meldewege erleichtert werden können.

  Problematisch ist nun, dass Unternehmen zur Vermeidung von Bußgeldsanktionen verpflichtet sein können, Sachverhalte an das BSI zu übermitteln, die Rechtsverstöße offenlegen. Dadurch kommen Unternehmen und ihre Leitungspersonen in den Zwiespalt, entweder der Meldepflicht nachzukommen oder Rechtsverstöße geheim zu halten. Dieser Zwiespalt schwächt die Effektivität der Meldungen. Zur Gewährleistung zumindest der personellen Selbstbelastungsfreiheit sehen Parallelregelungen in anderen Rechtsgebieten, u.a. §§ 42 Abs. 4, 43 Abs. 4 BDSG, ein

Beweisverwertungsverbot vor. Die Inhalte einer Meldung dürfen nicht in Straf- und Ordnungswidrigkeitenverfahren gegen den Meldepflichtigen verwendet werden. Ebenso ist ein Auskunftsverweigerungsrecht sinnvoll, wie dies in § 40 Abs. 4 S. 2 BDSG7 geregelt ist. Beide Instrumente sind zur Effektivität auch in das BSIG aufzunehmen.

- **Zu § 33 BSIG-E (Registrierungspflicht)**

  Besonders wichtige und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter sind verpflichtet, sich gem. § 33 Abs. 1 BSIG-E spätestens nach drei Monaten bei einer gemeinsamen Registrierungsmöglichkeit von BSI und BBK zu registrieren und die in der Vorschrift bestimmten Angaben zu übermitteln. Nach gegenwärtigem Stand herrscht bei den (potenziell) durch NIS-2 betroffenen Unternehmen nach wie vor eine erhebliche Rechtsunsicherheit hinsichtlich der eigenen Betroffenheit. Zwar obliegt den betroffenen Einrichtungen selbst die Prüfpflicht, ob sie von bestimmten Regularien aufgrund des Vorliegens der tatbestandlichen Voraussetzungen betroffen sind, jedoch erscheint es sinnvoll, seitens des BSI eine bestmögliche Unterstützung bei der Identifikation der eigenen Betroffenheit anzubieten. Einige Ansätze werden in verschiedenen öffentlichen Stellungnahmen diskutiert, wenngleich diese sicherlich noch nicht ausgereift sind (so zum Beispiel Deutsche Industrie- und Handelskammer, Stellungnahme zum Entwurf von NIS2UmsuCG, S. 9 f., online abrufbar unter: https://www.dihk.de/resource/blob/117740/ff85113d4d8e5ff606301f57a3aeecdd/recht-dihk-stellungnahme-umsetzungs-und-cybersicherheitsstaerkungsgesetz-data.pdf). Denkbar wäre darüber hinaus auch eine Rückmeldung des BSI bei registrierten Unternehmen nach Registrierungseingang, sollten diese nicht vom Anwendungsbereich von NIS2UmsuCG betroffen sein und sollte insoweit eine juristische Fehleinschätzung vorliegen.

[7] *Heinelt/Dittrich/Basar*, NIS-2: Sanktionen und Strafrecht – Teil 1, CB, S. 151 mit Nachweisen zu ähnlichen Regelungen in Fußnote 34.

- **Zu § 38 BSIG-E (Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen)**

  Grundsätzlich ist es begrüßenswert, dass die Pflicht zur Informationssicherheit auch als Bestandteil einer ordnungsgemäßen Geschäftsorganisation benannt wird, um ihre Relevanz zu herauszustellen. Insoweit ist auch nicht den teilweise vertretenen Auffassungen zu folgen, dass sich diese Gewährleistungsverantwortung bereits aus dem allgemeinen Gesellschaftsrecht ergäbe – denn ansonsten wäre es auch nicht notwendig, die Informationssicherheit speziell zu regulieren, weil sich diese ebenfalls als Maßgabe aus der allgemeinen Pflicht zur ordnungsmäßigen Geschäftsleitung z.B. nach GmbHG oder AktG ableiten könnte.

  Dennoch ist die Vorschrift in ihrer gegenwärtigen Fassung noch zu unbestimmt, dies betrifft neben der Definition des Begriffs „Geschäftsleitung“ wie eingangs dargestellt insbesondere die Schulungspflichten gem. § 38 Abs. 3 BSIG-E. Gegenwärtig müssen Geschäftsleitungen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und Risikomanagementpraktiken im Bereich der Informationssicherheit zu erlangen und dies beurteilen zu können. Es wird jedoch nicht konkretisiert, welchen Umfang solche Schulungen haben müssen, ob mit der Schulung entsprechende Nachweise zu erbringen sind und was die „Regelmäßigkeit“ bedeutet. Dies ist einerseits unter dem Gesichtspunkt der Informationssicherheit selbst verbesserungswürdig, andererseits aber auch deshalb, weil für die betroffenen Geschäftsleiter selbst unklar ist, ab welchem Zeitpunkt und in welcher Regelmäßigkeit sie ihre gesetzlichen Pflichten erfüllt haben.

- **Zu § 39 BSIG-E (Nachweispflichten für Betreiber kritischer Anlagen)**

  Gemäß dieser Vorschrift haben die Betreiber von kritischen Anlagen die Umsetzung der Informationssicherheitsmaßnahmen alle drei Jahre gegenüber dem BSI nachzuweisen. Auf den Begriff und die Notwendigkeit des Betreibers einer kritischen Anlage wurde bereits in anderen Teilen dieser Stellungnahme eingegangen. Für die besonders wichtigen Einrichtungen räumt das BSIG in § 61 BSIG-E jedoch bereits umfassende Aufsichts- und Durchsetzungsmaßnahmen ein. Deshalb stellt sich die Frage, inwieweit die dreijährige Nachweispflicht darüber hinausgehend noch

nennenswerte Vorteile bringt bzw. ob durch sie bestimmte wirtschaftliche und personelle Kapazitäten in der Informationssicherheit nicht eher gebunden als gefördert werden.

Unabhängig hiervon sollte angedacht werden, die Anforderungen an Dokumentation und Nachweis auch jenseits der Betreiber kritischer Anlagen im Allgemeinen für besonders wichtige und wichtige Einrichtungen nach NIS2UmsuCG gesetzlich weiter zu konkretisieren, da die Ausgestaltung dieser Anforderungen aktuell in der Praxis ebenfalls noch mit erheblichen Unsicherheiten verbunden ist.

- **Zu § 43 BSIG-E (Informationssicherheitsmanagement)**

  Die Vorschrift konkretisiert die Anforderungen an das Informationssicherheitsmanagement in der Bundesverwaltung. Auf die in diesem Zusammenhang bestehenden rechtssystematischen Schwächen wurde in dieser Stellungnahme bereits im Vorfeld im Rahmen des § 29 BSIG-E eingegangen – durch eine fehlende Bezugnahme steht das gesamte Kapitel 3 des BSIG-E mehr oder weniger „mitten im Raum“.

  Wo auf der einen Seite ein möglichst umfassendes Lagebild zur Informationssicherheit in Deutschland aufgebaut werden soll, müssen auf der anderen Seite auch möglichst umfassende Informationsgrundlagen zur Verfügung stehen. Im öffentlichen Bereich bezieht dies alle Behörden ein, deren Aufgabenbereich unmittelbar oder mittelbar durch Fragen der Informationssicherheit tangiert ist. An dieser Stelle sieht § 43 Abs. 5 S. 4 BSIG-E eine deutliche Privilegierung von Bundesnachrichtendienst (BND) und Bundesamt für Verfassungsschutz (BfV) vor, indem diese von den gesetzlich angeordneten Meldepflichten explizit ausgenommen werden. Diese Privilegierung sollte gestrichen werden, da sie nicht im Sinne einer Verbesserung der Informationssicherheit ist und die in die Abwägung einzubeziehenden Geheimschutzinteressen an dieser Stelle nicht das Interesse an mehr Informationssicherheit überwiegen.

- **Zu § 44 BSIG-E (Vorgaben des Bundesamtes)**

  § 44 BSIG-E bestimmt in Abs. 1, dass die Einrichtungen der Bundesverwaltung die jeweils geltenden Fassungen der Mindeststandards für die Sicherheit in der Informationstechnik des Bundes erfüllen müssen. Abs. 2 bestimmt, dass das

Bundeskanzleramt und die Bundesministerien als zusätzliche Mindestanforderungen die BSI-Standards und das IT-Grundschutz-Kompendium des BSI in der jeweils geltenden Fassung einhalten müssen. Beide Regelungen sind jedoch am Ende des jeweiligen Absatzes mit einer Ausnahme dergestalt versehen, dass die Ausnahmen nach § 7 Abs. 6 und 7 BSIG-E entsprechend gelten. Diese Vorschriften wiederum enthalten umfangreiche Ausnahmetatbestände betreffend die Auslandsinformations- und -kommunikationstechnik nach § 9 Abs. 2 des Gesetzes über den Auswärtigen Dienst sowie für die Informations- und Kommunikationstechnik, die von den Streitkräften für ihre Zwecke oder dem Militärischen Abschirmdienst im Geschäftsbereich des Bundesministeriums der Verteidigung genutzt wird. Gerade für diese genannten Fälle sollte Informationssicherheit eigentlich eine herausgehobene Rolle spielen, da nicht nur sicherheitssensitive Bereiche betroffen sind, sondern unter Umständen auch geheimschutzrelevante Daten verarbeitet werden. Daher ist es an dieser Stelle nicht empfehlenswert, durch entsprechende Ausnahmetatbestände das Mindestniveau der Informationssicherheit herabzusetzen.

Ein vergleichbarer Ausnahmetatbestand findet sich in der Vorgabe nach § 44 Abs. 6 S. 3 BSIG-E, der die grundlegende Verpflichtung von Einrichtungen der Bundesverwaltung bestimmt, IT-Sicherheitsprodukte beim BSI abzurufen. Hiervon ausgenommen werden die in § 2 Nr. 21 BSIG-E genannten Gerichte und Verfassungsorgane sowie die Auslandsinformations- und -kommunikationstechnik gem. § 7 Abs. 6 BSIG-E.

- **Zu § 48 BSIG-E (Amt des Koordinators für Informationssicherheit)**

  § 48 BSIG-E legt fest, dass die Bundesregierung eine Koordinatorin oder einen Koordinator für Informationssicherheit bestellt. Diese Bestimmung ist dem Grunde nach begrüßenswert, jedoch fehlt es an einer konkretisierenden inhaltlichen Ausgestaltung, welche Anforderungen und Befugnisse mit dem Amt verbunden sind und wo dieses strukturell anzusiedeln ist. Ein Koordinator für Informationssicherheit bzw. CISO Bund wird nur dann effektiv arbeiten können und seiner Aufgabenbestimmung hinreichend gerecht, wenn er entsprechende Durchsetzungsbefugnisse erhält, sein Tätigkeithorizont klar umschrieben ist und er hinreichend unabhängig im nationalen Verwaltungsgefüge angesiedelt wird und entsprechend agieren kann. Hierzu liegen bereits verschiedene öffentliche

Vorschläge vor, unter anderem auch in den Stellungnahmen zu NIS2UmsuCG (u.a. Claudia Plattner, Präsidentin des BSI, Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestags am 4. November 2024, S. 2. f. online abrufbar unter: https://www.bundestag.de/ausschuesse/a04_inneres/anhoerungen/1026172-1026172). Insgesamt wird es für die Frage der Verortung des Amts des Koordinators für Informationssicherheit in entscheidendem Maße darauf ankommen, wie unabhängig das BSI tatsächlich ist bzw. sein wird. Eine Stabsstelle jedoch, die weder mit ausreichenden Befugnissen ausgestattet ist noch eine hinreichende Unabhängigkeit besitzt, wird den Anforderungen an das Amt eines Koordinators für Informationssicherheit kaum gerecht werden können. Insoweit ist eine dringende inhaltliche Konkretisierung des § 48 BSIG-E geboten, um das Amt künftig mit Leben zu füllen.

- **Zu Anlage 1: Betreiber von Erzeugungsanlagen nach § 3 Nummer 18d EnWG**

  In Anhang I der NIS-2-Richtlinie werden im Energiesektor auch Erzeuger im Sinne von Art. 2 Nr. 38 der Richtlinie (EU) 2019/944 erfasst. Um eine sachgerechte Abgrenzung sicherzustellen, sollte – analog zu anderen Bereichen wie der Abfallbewirtschaftung – klargestellt werden, dass Einrichtungen nicht erfasst werden, wenn die Energieerzeugung nicht ihre Hauptwirtschaftstätigkeit darstellt. Alternativ könnte für Energieerzeugungsanlagen ein Schwellenwert für die erzeugte Strommenge festgelegt werden, um eine unverhältnismäßige Belastung von Betreibern kleinerer Anlagen zu vermeiden und die Energiewende nicht zu gefährden.

- **Zu Anlage 1: Ladepunktbetreiber nach § 2 Nummer 8 LSV**

  In Anhang I der NIS-2-Richtlinie werden im Energiesektor auch Betreiber von Ladepunkten erfasst. Um eine sachgerechte Abgrenzung sicherzustellen, sollte – analog zu anderen Bereichen wie der Abfallbewirtschaftung – klargestellt werden, dass Einrichtungen nicht erfasst werden, wenn der Betrieb von Ladepunkten nicht ihre Hauptwirtschaftstätigkeit darstellt. Alternativ könnte für Ladepunkte ein Schwellenwert für die abgegebene Strommenge festgelegt werden, um eine unverhältnismäßige Belastung von kleineren Betreibern zu vermeiden und die Energiewende nicht zu gefährden.

- **Zu Anlage 1: Passagier- und Frachtbeförderungsunternehmen**

  Die NIS-2-Richtlinie verweist für die Definition von Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt auf die Verordnung zur Gefahrenabwehr auf Schiffen und in Hafenanlagen (EG) Nr. 725/2004. Allerdings ist die Definition an der angegebenen Stelle nicht zu finden, sodass der Verweis ins Leere läuft. Vermutlich wollte die EU mit der missglückten Regelung in der NIS-2-Richtlinie Betreiber in die Pflicht nehmen, deren Schiffe in den Anwendungsbereich der Verordnung (EG) Nr. 725/2004 fallen. Dazu zählen Fahrgastschiffe sowie Frachtschiffe mit einer Bruttoraumzahl von mindestens 500 Registertonnen.

- **Zu Anlage 2: Produktion, Verarbeitung und Vertrieb von Lebensmitteln**

  Sowohl die NIS-2-Richtlinie als auch der Referentenentwurf erfassen Lebensmittelunternehmen im Sinne von Art. 3 Nr. 2 der Lebensmittelbasisverordnung (EG) Nr. 178/2002, die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind. Das Umsetzungsgesetz sollte klarstellen, welche Kriterien ein Lebensmittelunternehmen erfüllen muss, um als Großhändler eingestuft zu werden. Dadurch wird sichergestellt, dass betroffene Unternehmen ihre Pflichten zuverlässig bestimmen können und eine einheitliche Anwendung der gesetzlichen Anforderungen gewährleistet ist. Ein geeignetes Abgrenzungskriterium ist der bewusste und gezielte Vertrieb von Waren an gewerbliche Abnehmer, Einzelhändler oder andere Unternehmen.

- **Zu Artikel 14 des NIS2UmsuCG**

  Artikel 14 des Entwurfs sieht Folgeänderungen im Hinweisgeberschutzgesetz vor. Statt einer rein redaktionellen Änderung sollte aber eine inhaltliche Anpassung erfolgen und der restriktive Anwendungsbereich in § 2 Abs. 1 Nr. 3 lit. Q HinSchG aufgegeben werden. Ziel des Gesetzes ist der Schutz von hinweisgebenden Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit Informationen über Rechtsverstöße erlangt haben und diese an Meldestellen offenlegen möchten, § 1 Abs. 1 HinSchG, zudem werden auch die betroffenen Personen geschützt, § 1 Abs. 2 HinSchG.

- **Zu Artikel 21 des NIS2UmsuCG**

  In Artikel 21 sind Anpassungen in §§ 391, 392 SGB V für die IT-Sicherheit von Krankenhäusern und Gesetzlichen Krankenversicherungen vorgesehen. Übersehen wird aber der Änderungsbedarf bei § 390 SGB V, der die IT-Sicherheit in der vertragsärztlichen Versorgung regelt. Auch die vertragsärztliche Versorgung wird künftig in den Anwendungsbereich der NIS-2-Richtlinie fallen, sofern die Größenvorgaben für wichtige und besonders wichtige Einrichtungen erfüllt sind. Zur Vermeidung von Rechtsunsicherheit und einer ggf. auch europarechtswidrigen Doppelregulierung muss in § 390 Abs. 6 SGB V eine Ausnahme eingerichtet werden, wonach die Vorschrift dann nicht einzuhalten ist, wenn der Leistungserbringer bereits durch das § 30 BSIG-E angemessene Vorkehrungen treffen muss.

- **Zu Artikel 32 NIS-2-RL**

  Art. 32 NIS-2-RL regelt die Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wesentliche Einrichtungen und schreibt in Abs. 4 lit. g vor, dass die zuständige Behörde, also in Deutschland das BSI, befugt sein muss, „für einen bestimmten Zeitraum einen mit genau festgelegten Aufgaben betrauten Überwachungsbeauftragten zu benennen, der die Einhaltung der Artikel 21 und 23 durch die betreffenden Einrichtungen überwacht;“ Im ersten Referentenentwurf aus der vorherigen Legislaturperiode (Stand: 03.04.2023) war der Überwachungsbeauftragte im von der Richtlinie genutzten Wortlaut noch in § 64 Abs. 5 BSIG-RefE (2023) vorgesehen. In sämtlichen nachfolgenden Entwürfen wird er nicht mehr genannt.

  Diese Umsetzung genügt den Vorgaben der Richtlinie nicht, sie ist also unionsrechtswidrig. Dies ergibt sich aus einem sprachlichen Vergleich zum englischen Richtlinien-Text, der von einem Monitoring Officer spricht. Dadurch wird klar, dass die Richtlinie die Compliance-Funktion eines Monitorships etablieren wollte.8 Diese Funktion ist vor allem aus den USA bekannt, wo das Organisationskonzept des Compliance Managements auch seine Ursprünge hat. Beim Compliance Monitorship handelt es sich um eine unabhängige Person, die in einem „nicht-complianten“ Unternehmen die Einhaltung der Rechtskonformität

[8] *Kipker/Dittrich*, Die Geschäftsleitung im Fokus des IT-Sicherheitsrechts – Teil 2, CB 2024, S. 18.

unterstützt und überwacht. Gerade durch diese Unabhängigkeit wird eine Wirksamkeit und Akzeptanz in den Unternehmen erzielt. Wenn die Richtlinie also dieses Instrument etablieren will, ist die Umsetzung über behördliche Case-Manager nicht ausreichend, da hier gerade die behördliche Aufsichtskomponente zu strikt fortgeführt wird.