Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 G

Universität Bremen

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

Universität Bremen | Postfach 33 04 40, 28334 Bremen
IGMR | **FB06**

Deutscher Bundestag
Ausschuss für Inneres und Heimat
- Sekretariat -
Platz der Republik 1
11011 Berlin

Fachbereich 06
Rechtswissenschaft

Prof. Dr. jur. Dennis-Kenji Kipker

Universitätsallee GW 1
28359 Bremen

Tel. 0421 5905 5465
Fax 0421 218 66052
kipker@uni-bremen.de

www.igmr.uni-bremen.de
igmr@uni-bremen.de

Bremen 31. Oktober 2024

Schriftliche Stellungnahme

zum

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

(BT-Drucksache 20/13184)

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

Zusammenfassung und Vorbemerkung:

Gemessen an der Tatsache, dass die Umsetzung von NIS2 in Deutschland schon seit mittlerweile fast zwei Jahren möglich ist und angegangen wird, enthält der vorgelegte Entwurf leider noch zu viele Schwächen und Unklarheiten, teilweise auch Maßgaben, die der Erhöhung des allgemeinen Cybersicherheitsniveaus nicht förderlich sind. Zu vermissen ist ebenfalls 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 nichts anderes, als dass selbst in einem föderalen Deutschland einheitliche Cybersicherheitsstandards definiert werden. Aufgrund der nach wie vor bestehenden Zersplitterung von Vorgaben verteilt auf unterschiedliche regulatorische Ebenen mit unterschiedlicher Verbindlichkeit sind wir weit von einer einheitlichen Umsetzung entfernt. Hier hätten die letzten Jahre eigentlich gezielt genutzt werden müssen und können, um eine stärkere politische Abstimmung zwischen Bund und Ländern zu erreichen. Auch werden verschiedene Punkte, die beispielsweise schon im Jahr 2023 bei Sitzungen der AG BSI adressiert wurden, nicht aufgegriffen. Damit hat man es mit dem vorgelegten Gesetzentwurf bislang leider versäumt, NIS-2 nicht nur zur Umsetzung eines europäischen Minimalstandards zu nutzen, sondern das nationale Cybersicherheitsrecht auf eine grundlegend solide Basis zu stellen, die Rechtsunsicherheit ausräumt und eine nachhaltige Entwicklung für die gesteigerte Bedrohungslage der kommenden Jahre schafft.

Hauptkritikpunkte betreffen dabei die nach wie vor im nationalen Verwaltungsgefüge unklare Rolle des BSI, die nicht angetastet wurde, obwohl das BSI nicht nur in seiner Rolle als Zentralstelle für Cybersicherheit einen massiven weiteren Ausbau erfahren soll, sondern mit NIS-2 auch

zahlreiche weitere Befugnisse erhalten wird. Jenseits von NIS-2 positioniert sich das BSI außerdem bereits jetzt für die nationale Umsetzung des europäischen Cyber Resilience Act (CRA), womit weitere ganz erhebliche Befugnisse einhergehen, die deutlich für eine größere Unabhängigkeit des BSI sprechen. Bereits mehrfach kritisierte begriffliche Schwächen, die sich bereits im geltenden Recht wiederfinden, werden nicht ausgeräumt – dies ist für den richtigen und rechtssicheren Umgang mit den Vorschriften durch die Betroffenen jedoch essenziell. Ganz zentral ist überdies die gesetzlich angeordnete Umsetzung von IT-Sicherheitsmaßnahmen nach NIS-2 in § 30 BSIG-E. Hier wird nahezu 1:1 auf den NIS-2-Maßnahmenkatalog verwiesen, was bei betroffenen Einrichtungen jedoch zu Unsicherheit darüber führt, welche Maßnahmen im Einzelnen zu realisieren sind und ob diese überhaupt in den konkreten betrieblichen Anwendungskontext passen. Zugegebenermaßen lässt hier bereits das europäische Recht mit einer willkürlich erscheinenden Aufzählung von Maßnahmen zur Cybersicherheit zu wünschen übrig, die nicht weiter konkretisiert werden, aber dennoch unmittelbare Pflicht sind. Im Ergebnis gerät dadurch jedoch zunehmend außer Fokus, dass Cybersicherheit eine Managementaufgabe ist, die sich an eine individuelle Risikobewertung anschließt, und deshalb zunächst nichts mit einzelnen Produkten und Insellösungen zur Cybersicherheit zu tun hat. Dasselbe gilt für die pauschale Anordnung zur Verwendung von Systemen zur Angriffserkennung. Diese Unsicherheit für betroffene Einrichtungen zieht sich bedauerlicherweise durch den gesamten Gesetzentwurf, so mit Blick auf die Anforderungen an Dokumentation und Nachweise, die Geschäftsleiterverantwortlichkeit sowie die Schaffung von betrieblicher Awareness und auch die Meldepflichten. Für letztere wird zum Beispiel auf „immaterielle Schäden“ verwiesen, ohne dass deutlich hervorgeht, was davon inhaltlich

umfasst sein soll und wie diese im Zweifelsfall von datenschutzrechtlichen Meldungen abzugrenzen sein sollen. Über den Bereich betroffener Privatunternehmen hinausgehend finden sich überdies auch im öffentlichen Teil des Gesetzesvorschlags weitere und auch systematische Schwächen, die an die Definition von Einrichtungen der Bundesverwaltung und an die künftige Rolle des CISO Bund anknüpfen.

Im Hinblick auf den Datenschutz enthält der Entwurf außerdem weitere erhebliche nennenswerte 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.

Im Hinblick auf das bisherige Verfahren und die Beteiligung relevanter Akteure ist überdies zu kritisieren, dass die BfDI bislang nicht ausreichend einbezogen wurde, obwohl im Gesetzentwurf wie dargestellt massive Befugniserweiterungen des BSI zur (personenbezogenen) Datenverarbeitung im Raum stehen und deshalb auch datenschutzrechtliche Regelungen in erheblichem Maße tangiert sind. § 69a Abs. 3 GOBT sieht ein ausdrückliches und frühzeitiges Beteiligungsrecht der BfDI vor, das bei der nationalen Umsetzung von NIS2 bislang leider nicht ausgeübt wurde.

Zu den Vorschriften im Einzelnen:

- **§ 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 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 nicht nur in einer Sitzung der AG BSI am 8. September 2023 persönlich zur Diskussion gestellt, sondern in Ko-Autorenschaft auch einen entsprechenden Fachbeitrag publiziert, der konkrete rechtliche Möglichkeiten zur Unabhängigstellung des BSI in gradueller Abstufung aufzeigt (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). Andererseits lässt sich mittels sachlicher Argumentation nicht recht-

fertigen, 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.

- **§ 2 Nr. 10 BSIG-E (Begriffsbestimmungen, 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. 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 informationstechni-

schen 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.

- **§ 2 Nr. 11 BSIG-E (Begriffsbestimmungen, 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.

- **§ 2 Nr. 12 BSIG-E (Begriffsbestimmungen, 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 (vgl. AG KRITIS, Stel-

lungnahme 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).

- **§ 2 Nr. 13 BSIG-E (Begriffsbestimmungen, 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 rechtswirk-

sam vertreten können – dies dürfte gerade für größere Unternehmungen mit entsprechender Abteilungsgröße relevant sein.

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

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

- **§ 2 Nr. 22 BSIG-E (Begriffsbestimmungen, 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 Maß-

nahmen 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 (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). 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.

- **§ 2 Nr. 26 BSIG-E (Begriffsbestimmungen, 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. 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.

- **§ 2 Nr. 38 BSIG-E (Begriffsbestimmungen, 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 beein-

flussen. 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.

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

  Der „Sicherheitsvorfall“ wird beschrieben als ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt. Wie bereits zuvor angemerkt ist ebenfalls die Authentizität von Daten ein anerkanntes Schutzziel der Cybersicherheit und sollte deshalb ebenso in die Definition des IT-Sicherheitsvorfalls aufgenommen werden, um Regelungslücken auszuschließen.

- **§ 2 Nr. 41 BSIG-E (Begriffsbestimmungen, 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 (BSI, Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung, online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.html) 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.

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

zungsschwierigkeiten 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.

- **§ 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 (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).

- **§ 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.

- **§ 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 Militäri-

schen Abschirmdienst, ohne dass erkennbar wäre, wie für diese Einrichtungen auf alternativem Wege vergleichbare Kontrollmechanismen vorgesehen wären. Im Sinne eines einheitlichen Niveaus der Informationssicherheit 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.

- **§ 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.

- **§ 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 (so z.B. auch AG KRITIS, Stellungnahme zum Regierungsentwurf des NIS2UmsuCG vom 02.10.2024, S. 6 ff. online abrufbar unter: https://ag.kritis.info/wp-

content/uploads/2024/10/20241027-Stellungnahme-NIS2UmsuCG-RefE-v02102024-AG-KRITIS-v1.1.pdf; Prof. Timo Kob, Stellungnahme NIS2UmsuCG, S. 3 ff., online abrufbar unter: https://www.bundestag.de/resource/blob/1027134/727dccd4a80e3a14cfdce9d59a1fab38/20-4-523-A.pdf; 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). Bei der Bewertung der Bedrohungslage in der Informationssicherheit kann nicht derart deutlich zwischen staatlichen und 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.

- **§ 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 ver-

bundenen 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.

- **§ 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.

- **§ 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.

- **§ 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/ff85113d4d8e5ff606301f

57a3aeecdd/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.

- **§ 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 aus-

reichende 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.

- **§ 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.

- **§ 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.

- **§ 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.

- **§ 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 Vor-

schläge 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.

Bremen, den 31. Oktober 2024

Prof. Dr. jur. Dennis-Kenji Kipker