DENNIS-KENJI KIPKER / TILMANN DITTRICH

Rolle der Kritischen Infrastrukturen nach dem neuen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Nationale Besonderheiten und europäische Überformung

IT-Sicherheitsrecht

Der Schutz von für die Gemeinschaft elementar-notwendigen Einrichtungen vor Cybergefahren stellt eine der größten Herausforderungen der aktuellen Zeit dar – und das nicht erst seit Beginn des Russland-Ukraine-Kriegs. Bislang maßgeblich waren hier in Deutschland das BSIG und die dessen Anwendungsbereich konkretisierende BSI-KritisV, ergänzt um die 2016 hinzugetretenen europäischen Anforderungen der ersten NIS-RL. Seither hat das IT-Sicherheitsrecht umfassende Überarbeitungen erfahren, indem nicht nur die europäischen Vorgaben in das nationale Recht implementiert wurden, sondern auch ein neues IT-Sicherheitsgesetz 2.0 in 2021 geschaffen wurde, das die Vorgaben des ersten deutschen IT-Sicherheitsgesetzes aus 2015 an die gegenwärtige Bedrohungslage anpasst und aktualisiert. Der nachfolgende Beitrag gibt nun auf Grund einer neuen NIS-2-RL und deren Umsetzung einen ersten Überblick über die umfassenden Änderungen für die bisherigen Kritischen Infrastrukturen und zeigt dabei Unterschiede im Vergleich zur geltenden Rechtslage auf. Lesedauer: 26 Minuten

I. Einführung und rechtspolitischer Hintergrund

2020 stellten die EU-Kommission und der Europäische Auswärtige Dienst die neue europäische Cybersicherheitsstrategie vor, die bereits in nicht unerheblichem Maße durch die Verwerfungen der Corona-Krise geprägt war, wodurch die Resilienz zu einem wesentlichen regulatorischen Aspekt wurde.[1] Die aktuelle EU-Cybersicherheitsstrategie brachte zwei neue Richtlinien mit sich: die NIS-2-RL[2] zur Ablösung der geltenden NIS-RL[3] und eine neue europäische Resilienz-RL[4] (auch CER-RL genannt), die beide Ende 2022 verabschiedet wurden und bis Oktober 2024 in den Mitgliedstaaten umgesetzt sein müssen. Für die Resilienz-RL, die Kritische Infrastrukturen (KRITIS) primär vor physischen Gefahren schützen soll, liegt bislang nur ein BMI-Eckpunktepapier für ein sog. „KRITIS-Dachgesetz" vor.[5] Die NIS-2-RL wird voraussichtlich durch das nationale NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in das nationale Recht übertragen – Besonderheit dabei: Der Gesetzentwurf[6] geht über die EU-Vorgaben hinaus und bringt ebenso verschiedene spezifische Neuerungen ausschließlich im nationalen Cybersicherheitsrecht mit sich. Daraus ergibt sich auch die zusätzliche Bezeichnung „Cybersicherheitsstärkungsgesetz", womit klar wird, dass das vielzitierte „IT-Sicherheitsgesetz 3.0" in dieser Form erst einmal nicht kommen wird.

II. Sicherheit in der Informationstechnik von Betreibern und Einrichtungen

Bislang sind die Vorschriften für Kritische Infrastrukturen vor allem in den §§ 8a, 8b BSIG[7] zu finden. Diese an der Relevanz von KRITIS bemessene knappe Darstellung dürfte zukünftig keinen Bestand mehr haben. So wird in Teil 3 des BSIG-RefE die Sicherheit in der Informationstechnik von Einrichtungen umfassend adressiert und bringt erhebliche Neuerungen mit sich.

1. Neuer Anwendungsbereich des BSIG und Abgrenzung zu weiteren Rechtsakten

Die gesetzlichen Vorschriften zur IT-Sicherheit beziehen sich nach § 28 Abs. 1 BSIG-E zukünftig auf Betreiber Kritischer Anlagen, besonders wichtige Einrichtungen und „lediglich" wichtige Einrichtungen, soweit dies durch die BSI-KritisV iSd § 57 Abs. 1 BSIG-E[8] entsprechend festgelegt wurde. Schon bei dieser Untergliederung wird deutlich, dass der deutsche Gesetzgeber den in NIS-2 verwendeten Wortlaut und die dortige Unterscheidung zwischen „wesentlichen" und „wichtigen" Einrichtungen für irreführend hielt und deshalb eine begriffliche Abweichung und Klarstellung zum europäischen Recht vornimmt. Die Betreiber der „Kritischen Anlagen" sind in diesem Zusammenhang als höchste Qualifikationsstufe zu sehen. Die bisherigen Anforderungen zu den „Unternehmen im besonderen öffentlichen Interesse" (UBI) aus IT-SiG 2.0 gem. § 2 Nr. 14 BSIG geltende Fassung gehen zukünftig in den besonders wichtigen und wichtigen Einrichtungen auf.

a) Kritische Anlage

Die Kritische Anlage ersetzt den bisherigen Begriff der Kritischen Infrastrukturen iSd BSIG, der sich im RefE zum NIS2UmsuCG nicht mehr wiederfindet. Die Definition nach neuem Recht ist bislang komplex und mehrstufig-verweisungslastig. Ausgangspunkt sind wie nach geltendem Recht die Begriffsdefinitionen zu Beginn des BSIG. Demnach ist nach § 2 Abs. 1 Nr. 19 BSIG-E eine Anlage, die für das Funktionieren des Gemeinwesens von hoher Bedeutung ist, als Kritische Anlage zu qualifizieren, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Zur weiteren Konkretisierung wird sodann auf § 28 Abs. 2a BSIG-E verwiesen – hier finden sich in

1 Abrufbar unter: https://www.consilium.europa.eu/de/policies/cybersecurity/.
2 RL (EU) 2022/2555 des Europäischen Parlaments und des Rates v. 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der VO (EU) Nr. 910/2014 und der RL (EU) 2018/1972 sowie zur Aufhebung der RL (EU) 2016/1148 (NIS-2-RL), ABl. L 333/80.
3 RL (EU) 2016/1148 des Europäischen Parlaments und des Rates v. 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194/1.
4 RL (EU) 2022/2557 des Europäischen Parlaments und des Rates v. 14.12.2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der RL 2008/114/EG des Rates, ABl. L 333/164.
5 Kipker/Dittrich MMR-Aktuell 2022, 454186.
6 Der Beitrag bezieht sich auf eine Synopse eines Referentenentwurfs, abrufbar unter: https://intrapol.org/2023/05/10/refe-fuer-ein-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/.
7 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik v. 14.8.2009, BGBl. I 2821.
8 Gegenwärtig § 10 Abs. 1 S. 1 BSIG.

Ergänzung des o.g. Quantitätskriteriums die ursprünglich in einem Absatz zusammen dargestellten Qualitätskriterien wieder. Erfasst sind demgemäß Anlagen in den Sektoren Energie, Verkehr und Transport, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Digitale Infrastruktur sowie Siedlungsabfallentsorgung. Redundant zu § 2 Abs. 1 Nr. 19 BSIG-E werden sodann nochmals die Quantitätskriterien aufgeführt, was der Verständlichkeit nicht eben zuträglich ist. Die letzte konkretisierende Verweisungsstufe bezieht sich sodann auf die BSI-KritisV nach § 57 Abs. 1 BSIG-E. Der Betreiber einer Kritischen Anlage ist nach § 28 Abs. 2 BSIG-E eine natürliche oder juristische Person oder eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine Kritische Anlage ausübt.

b) Besonders wichtige Einrichtungen

Bei der neuen Kategorie der „besonders wichtigen Einrichtungen" gem. § 28 Abs. 3 BSIG-E zeigt sich eine nationale Besonderheit: Da der bislang geltende Begriff der Kritischen Infrastruktur nicht in das NIS2UmsuCG übernommen wird, unterfällt jedoch der Betreiber der Kritischen Anlage als Subkategorie den besonders wichtigen Einrichtungen – im Ergebnis muss somit zukünftig primär nur zwischen besonders wichtigen und wichtigen Einrichtungen unterschieden werden. Hieraus erklärt sich u.a. auch die begriffliche Bezugnahme nur auf die „Anlage" und nicht auf die „Infrastruktur". Überdies ergeben sich bei den besonders wichtigen Einrichtungen Überschneidungen mit KRITIS im qualitativen/sektorbezogenen Bereich: Erfasst sind auch Großunternehmen, die den Sektoren Energie, Verkehr und Transport, Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten (B2B) oder Weltraum zuzuordnen sind. Ebenso umfasst sind mittlere Unternehmen als Anbieter von TK-Diensten oder öffentlich zugänglichen TK-Netzen. Qualifizierte Vertrauensdiensteanbieter, Top-Level-Domain-Name-Registries oder DNS-Diensteanbieter sind gar unabhängig von ihrer Unternehmensgröße betroffen – es ergibt sich für die besonders wichtigen Einrichtungen somit eine dreiteilige Abstufung von Unternehmen jedweder Größe, mittleren Unternehmen und Großunternehmen. Um betroffenen Einrichtungen die größenmäßige Zuordnung zu erleichtern, werden die zahlenmäßigen Bestimmungen aus der Empfehlung 2003/361/EG als Legaldefinitionen in die neuen Begriffsbestimmungen nach BSIG-E übernommen.

Demnach ist ein Großunternehmen ein Unternehmen oder eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, das oder die mindestens 250 Mitarbeitende beschäftigt oder einen Jahresumsatz von mindestens 50 Mio. EUR und zudem eine Jahresbilanzsumme von mindestens 43 Mio. EUR aufweist. Ein Unternehmen[9] oder eine rechtlich unselbstständige Organisationseinheit einer Körperschaft zählt dann als „mittleres Unternehmen", wenn es gem. § 2 Abs. 1 Nr. 23 BSIG-E mindestens 50 und höchstens 249 Mitarbeitende beschäftigt und zudem einen Jahresumsatz von weniger als 50 Mio. EUR oder eine Jahresbilanzsumme von weniger als 43 Mio. EUR aufweist, oder weniger als 50 Mitarbeiter beschäftigt und einen Jahresumsatz und eine Jahresbilanzsumme von jeweils mindestens 10 Mio. EUR und einen Jahresumsatz von höchstens 50 Mio. EUR sowie eine Bilanzsumme von höchstens 43 Mio. EUR aufweist.

Hingewiesen sei an dieser Stelle zusätzlich darauf, dass den besonders wichtigen Einrichtungen künftig auch Einrichtungen der „Zentralregierungen" der Mitgliedstaaten angehören. Damit sind sowohl die Bundesministerien als auch das Bundeskanzleramt vom Anwendungsbereich erfasst.

c) Wichtige Einrichtungen

Die wichtigen Einrichtungen sind gem. § 28 Abs. 4 BSIG-E sehr weit gefasst und dürften einen erheblichen Zuwachs betroffener Unternehmen zur Folge haben – u.a. hier gehen auch die bisherigen UBI nach IT-SiG 2.0 explizit auf.[10] Auch das von manchen Unternehmen in der Vergangenheit angeführte Argument auf das Nichterreichen der KRITIS-Versorgungsgrenze dürfte damit obsolet sein. Unter Verweis auf die BSI-KritisV aufgezählt werden mittlere Unternehmen und Großunternehmen in den Sektoren Energie, Transport und Verkehr, Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten (B2B), Weltraum, Logistik, Siedlungsabfall, Produktion, Chemie, Ernährung, verarbeitendes Gewerbe, Anbieter digitaler Dienste und Forschung. Erfasst werden ebenso Vertrauensdiensteanbieter. Wichtig zu wissen ist, dass sich die Eigenschaft als besonders wichtige (nach EU-Recht „wesentliche") und wichtige Einrichtung ausschließen – eine gleichzeitige Zuordnung in beide Kategorien ist somit nicht möglich.

d) Ausnahmen vom Anwendungsbereich

Ausnahmen vom Anwendungsbereich der Vorschriften des NIS2UmsuCG ergeben sich vor allem für Fälle bereichsspezifischer und spezialgesetzlicher Regelungen, die die allgemeine Natur der NIS-2-Regelungen kennzeichnen. Dies entspricht dem allgemeinen juristischen Grundsatz „lex specialis derogat legi generali", der auch schon für die NIS-RL und das bislang geltende BSIG Anwendung findet. Insoweit sind auch die aktualisierten Bereichsausnahmen zunächst wenig überraschend. So sind zunächst Einrichtungen ausgenommen, die der VO (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA) unterfallen.

Weitere Ausnahmen, die ebenfalls schon aus den geltenden Vorschriften gem. § 8d Abs. 2 Nr. 1, Nr. 3 BSIG bekannt sind, betreffen den Bereich der öffentlichen TK-Netze oder öffentlich zugänglicher TK-Dienste, da für diese die Sondervorschriften des TKG gelten, sowie der Telematikinfrastruktur, die durch die Vorschriften des SGB V besonders geschützt wird. Diese Ausnahmen greift auch § 28 Abs. 5 BSIG-E auf.

Allerdings dürften nicht alle Lex-specialis-Regelungen weitergehend Bestand haben. So ist geplant, dass die IT-Sicherheitsvorschriften für den Energiesektor, die bislang in § 11 EnWG geregelt sind,[11] durch das NIS2UmsuCG weitestgehend entfallen, da sich die Verpflichtungen für Einrichtungen im Energiesektor zukünftig einheitlich nach dem BSIG richten sollen und die Aufsicht im Energiesektor sodann entsprechend durch das BSI erfolgt. Der geplante § 11 Abs. 1a EnWG-E sieht daher nur noch die unverzügliche Weiterleitung einer Sicherheitsvorfall-Meldung des BSI an die BNetzA vor, wie aktuell in § 11 Abs. 1c S. 4 EnWG geregelt.

Besonders wichtige sowie wichtige Einrichtungen können zudem nach § 37 Abs. 1 BSIG-E durch das Bundesministerium des Innern und für Heimat auf Vorschlag des Bundeskanzleramts, des Bundesministeriums für Verteidigung sowie auf eigenes Betreiben von den Verpflichtungen nach dem BSIG befreit werden,

9 Sowohl für die Großunternehmen wie auch für die mittleren Unternehmen zieht der NIS2UmsuCG-E – wie von NIS-2 beabsichtigt – die Kommissionsempfehlung 2003/361/EG heran, hält aber im Einzelnen aus Verhältnismäßigkeitsgründen iSd Erwägungsgrund 16 NIS-2-RL Abweichungen vor.

10 Vgl. Monschke/Copeland CCZ 2022, 152.

11 Dittrich MMR 2022, 1039; Rath/Ekardt/Schiela MMR 2023, 83 (86); Schaller CR 2022, 635.

sofern durch die Einrichtung gleichwertige Vorgaben eingehalten werden. In diesem Zusammenhang sieht die Vorschrift die Möglichkeit eines einfachen Ausnahmebescheids für teilweise Befreiungen sowie eines erweiterten Ausnahmebescheids für eine gänzliche Befreiung vor. Ferner sind in § 37 Abs. 2 BSIG-E weitere (teilweise) Befreiungen für Einrichtungen zB aus dem Bereich der nationalen oder öffentlichen Sicherheit, Verteidigung oder der Strafverfolgung vorgesehen. Voraussetzung aber ist, dass ein adäquates IT-Sicherheitsniveau anderweitig sichergestellt ist.

2. Pflichten für betroffene Einrichtungen und Anlagen im Einzelnen

Die für Kritische Infrastrukturen bislang bestehenden Vorgaben werden mit dem NIS2UmsuCG nicht nur konkretisiert, sondern zugleich verschärft. Dies betrifft sowohl das Risikomanagement wie auch die Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten.

a) Risikomanagement

§ 30 Abs. 1 BSIG-E gilt sowohl für besonders wichtige als auch für wichtige Einrichtungen und enthält die bereits aus § 8a Abs. 1 BSIG bekannte Maßgabe, ein Risikomanagement zur Gewährleistung der IT-Sicherheit vorzuhalten. Wenig überrascht es deshalb, dass auch die Neufassung die Verpflichtung ausspricht, verhältnismäßige technische und organisatorische Maßnahmen (TOM)[12] zu ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die zur Diensteerbringung genutzt werden, zu vermeiden und Auswirkungen von Sicherheitsvorfällen auf eigene oder andere Dienste zu verhindern oder möglichst gering zu halten.

Diese TOM sollen gem. § 30 Abs. 2 BSIG-E den Stand der Technik einhalten – ebenfalls ein bereits durch das IT-SiG bekannter unbestimmter Rechtsbegriff.[13] Das kann unter Berücksichtigung einschlägiger europäischer und internationaler Normen geschehen. Ebenso findet sich in der Neufassung die Anforderung an die Angemessenheit zu treffender Maßnahmen wieder, die die zur Beurteilung notwendige Kosten-Nutzen-Abwägung enthält: So sind bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, das Ausmaß der Risikoexposition und die Größe der Einrichtung oder des Betreibers sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Eine solche Regelung ist notwendig, um unverhältnismäßige Bürden zu vermeiden und einen Bezug des Gesetzes zu seiner praktischen Umsetzung herzustellen. Das bedeutet aber auch, dass für die Betreiber von Kritischen Anlagen erhöhte Anforderungen an die Angemessenheitsbeurteilung anzulegen sind.

Notwendigerweise ist es nicht möglich, dass das BSIG iSe Kasuistik in einem abschließenden Katalog diejenigen TOM aufführt, die in jedem Falle geeignet sind, ein angemessenes und dem Stand der Technik entsprechendes IT-Sicherheitsniveau zu realisieren. Hierüber bestand in den letzten Jahren dennoch ein erhebliches Maß an Rechtsunsicherheit. Umso begrüßenswerter ist deshalb die nunmehr in § 30 Abs. 4 BSIG-E vorgenommene Konkretisierung der TOM, wonach diese einen gefahrenübergreifenden Ansatz verfolgen müssen, der darauf abzielt, die informationstechnischen Systeme, Komponenten und Prozesse und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen. Auch dieser Katalog ist nicht als abschließend zu verstehen, stellt aber zumindest doch einen rechtsverbindlichen „Minimalkonsens" dar und umfasst nachfolgende Anforderungen:

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs, wie Back-up-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstleistern (hier gelten gem. § 30 Abs. 8 BSIG-E weitere spezifische Besonderheiten unter Einbeziehung der Entwicklungsprozesse)
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
- Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie ggf. gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Für besonders wichtige Einrichtungen besteht weiterhin wie nach geltendem Recht in § 8a Abs. 2 BSIG die Möglichkeit, branchenspezifische Sicherheitsstandards (B3S) vorzuschlagen, um die IT-Sicherheitsanforderungen nach § 30 Abs. 1 BSIG-E zu erfüllen. Leider fehlt es in diesem Zusammenhang jedoch nach wie vor an einer Normierung der Eignungsfeststellung von B3S für einen Zeitraum von zwei Jahren,[14] was nicht nur mehr Rechtssicherheit, sondern auch eine fortlaufend gesicherte Aktualität von IT-Sicherheitsmaßnahmen gewährleisten würde. Wünschenswert wäre überdies, für wichtige Einrichtungen einen freiwilligen Orientierungsrahmen an B3S vorzugeben, wie dies für Krankenhäuser im Allgemeinen bereits in § 75c SGB V bestimmt wird.

b) Meldepflichten, Rückmeldungen und die Öffentlichkeit

Die Meldepflichten für Kritische Infrastrukturen sind nach geltendem Recht bereits aus § 8b Abs. 4 BSIG bekannt. Neuerdings findet sich die entsprechende Regelung in Umsetzung von NIS-2 in § 31 Abs. 1 BSIG-E. Dabei wird die neue und deutlich gestärkte Rolle des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) deutlich, indem IT-Sicherheit als ein essenzieller Bestandteil der nationalen Krisenprävention und -bewältigung anzusehen ist. Das BSIG wird somit zukünftig systematisch nicht mehr separat, sondern im Zusammenhang mit dem KRITIS-Dachgesetz und damit verbunden mit der Umsetzung der CER-RL zu sehen sein.[15] Deshalb wird hier auch die Neuerung eingebracht, dass die Meldungen an eine vom BSI im Einvernehmen mit dem BBK eingerichtete Meldemöglichkeit übermittelt werden. Die Funktion des BSI als zentrale Melde- und Anlaufstelle in der IT-Sicherheit wird in § 40 BSIG-E beschrieben. Die NIS-2-RL zeigt an dieser Stelle ihren Einfluss mit erweiterten Möglich-

12 Diese Vorschrift ist bereits aus sprachlicher Sicht zu begrüßen, da endlich nicht mehr der deutsche Sonderweg mit den organisatorischen und technischen Vorkehrungen im BSIG, sondern der aus dem IT-Umfeld und auch der DS-GVO gängigen Vokabel der technischen und organisatorischen Maßnahmen gegangen wird.
13 Kipker DuD 2016, 610.
14 Nadeborn/Dittrich ICLR 1/2022, 143 (153).
15 Vgl. Kipker/Dittrich MMR-Aktuell 2022, 454186.

keiten des Informationsaustauschs innerhalb der EU sowie mit der ENISA, um der grenzüberschreitenden Bedrohungslage gerecht zu werden.

Der Umgang mit Meldungen und die Meldepflichten bestimmen sich anhand nachfolgend aufgeführter Legaldefinitionen im BSIG:

§ 2 Abs. 1 Nr. 37 BSIG-E: Sicherheitsvorfall	Ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt.
§ 2 Abs. 1 Nr. 10 BSIG-E: Erheblicher Sicherheitsvorfall	Ein Sicherheitsvorfall, der ■ schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann; oder ■ andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Im Vergleich zum geltenden Recht soll das neue Meldeverfahren gem. § 31 BSIG-E mehrstufig ausgestaltet sein.[16] Dies ist begrüßenswert, da eine mehrstufige Meldung bislang zwar nicht ausdrücklich gesetzlich festgeschrieben war, jedoch von der Literatur in Teilen angenommen wurde.[17] Durch frühzeitig ansetzende Meldeverfahren wird überdies dem Bedürfnis nach möglichst schnellen Informationsflüssen Rechnung getragen. Die mehrstufige Meldepflicht gilt für Kritische Anlagen, besonders wichtige Einrichtungen und wichtige Einrichtungen.

Stufe 1 – frühe Erstmeldung	Unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, muss eine frühe Erstmeldung abgegeben werden, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte.
Stufe 2 – bestätigende Erstmeldung	Unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, muss eine Meldung über den Sicherheitsvorfall abgegeben werden, in der die in Stufe 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie ggf. die Kompromittierungsindikatoren angegeben werden.
Stufe 3 – Zwischenmeldung	Auf Ersuchen des BSI muss eine Zwischenmeldung über relevante Statusaktualisierungen getätigt werden.
Stufe 3a – Fortschrittsmeldung	Dauert der Sicherheitsvorfall zum Zeitpunkt der Stufe 4 noch an, legt die betreffende Einrichtung statt einer Abschlussmeldung zu diesem Zeitpunkt eine Fortschrittsmeldung und eine Abschlussmeldung innerhalb eines Monats nach Abschluss der Bearbeitung des Sicherheitsvorfalls vor.
Stufe 4 – Abschlussmeldung	Spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Stufe 2, vorbehaltlich Stufe 3a, erfolgt eine Abschlussmeldung, die Folgendes enthält: ■ ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen; ■ Angaben zur Art der Bedrohung bzw. zu Grunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat; ■ Angaben zu den getroffenen und laufenden Abhilfemaßnahmen; ■ ggf. die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

Der nach NIS2UmsuCG-E melderelevante Begriff des „erheblichen Sicherheitsvorfalls" ist inhaltlich nicht deckungsgleich mit den bisherigen, die Meldepflicht nach § 8b Abs. 4 BSIG auslösenden Ereignissen. Indem er jedoch erhebliche materielle oder immaterielle Schäden in die eine Meldepflicht auslösenden Kriterien einbezieht, dürfte zukünftig von einer inhaltlichen Erweiterung der Meldepflicht auszugehen sein.

Wo auf der einen Seite der Umfang der von einer Meldepflicht betroffenen Betreiber und Einrichtungen und deren inhaltliche Reichweite wächst, ergeben sich auf der anderen Seite neue Kooperationspotenziale und Möglichkeiten der Zusammenarbeit. In diesem Kontext ist in Umsetzung des Art. 23 NIS-2-RL der neue § 36 BSIG-E hervorzuheben. Dieser entspricht dem Kooperationsgedanken des BSIG zur Förderung operativer IT-Sicherheit und sieht eine Rückmeldung des BSI auf eine Meldung nach § 31 BSIG-E vor. Auf Grund der zeitlichen Kritikalität der übermittelten Informationen erfolgt diese Rückmeldung unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach Eingang der Frühwarnung. Auf Ersuchen der Einrichtung gibt das BSI Orientierungshilfen oder eine operative Beratung zur Vorfallsbewältigung. Bei vermutetem kriminellen Hintergrund kann das BSI überdies Hilfestellungen für die Meldung des Vorfalls an die Strafverfolgungsbehörden zur Verfügung stellen. Dies ist in Sachen behördlicher Zusammenarbeit ein erheblicher Schritt in die richtige Richtung, denn auf diese Weise können nicht nur Gefahrenabwehrmaßnahmen unterstützt, sondern auch die Strafverfolgung beschleunigt werden, da im Falle von Cybercrime wenige Stunden entscheidend sein können. Hierdurch wird zugleich die unternehmerische Motivation, mit den Behörden zusammenzuarbeiten, verbessert.

Eine zusätzliche Einbeziehung der Öffentlichkeit ist nach § 36 Abs. 2 BSIG-E möglich, falls deren Sensibilisierung erforderlich ist, um einen erheblichen Sicherheitsvorfall zu vermeiden oder einen bereits laufenden zu bewältigen sowie bei einem anderweitig öffentlichen Interesse an der Offenlegung. Generell stellt sich bei derartigen Vorschriften die Herausforderung, die öffentlichen Interessen und Partikularinteressen des Betreibers bzw. der Einrichtung in einen verfassungskonformen Ausgleich zu bringen.[18]

c) Registrierungspflicht

Für besonders wichtige Einrichtungen und wichtige Einrichtungen sowie für Kritische Anlagen sieht § 32 BSIG-E eine Registrierungspflicht vor, die als Vorgabe bereits aus § 8b Abs. 3 BSIG für Kritische Infrastrukturen bekannt ist. Auch hier ist folglich mit

16 Ein Stufenkonzept für die Meldepflicht bei Cybervorfällen wird auch gem. DORA vorgesehen, dazu Dittrich/Heinelt RDi 2023, 164 (167).
17 Nadeborn/Dittrich ICLR 1/2022, 273 (281) mwN.
18 S. zB zur Warnbefugnis des BSI nach geltendem Recht Dittrich NJW 2022, 2971 (2972); Hessel/Schneider NVwZ 2023, 717 (719); Kipker MMR 2023, 93.

einer erheblichen Ausdehnung der zahlenmäßigen Betroffenheit zu rechnen. Kommen Einrichtungen und Anlagenbetreiber ihrer Registrierungspflicht nicht nach, kann das BSI nach § 32 Abs. 2, Abs. 4 BSIG-E diese Registrierung selbst vornehmen. Außerdem kann im Falle der unterbliebenen Registrierung ein Bußgeld drohen. In diesem Zusammenhang ist aktuell auf das erste eingeleitete Bußgeldverfahren des BSI hinzuweisen, welches den Verstoß gegen die Registrierungspflicht zum Gegenstand hat.[19]

d) Nachweispflichten für besonders wichtige Einrichtungen

Das BSIG lebt vom Modell „Kooperation und Sanktion"[20]. Eine der bedeutendsten Plichten stellt deshalb die Nachweispflicht über die Einhaltung der IT-Sicherheitsvorschriften dar, die bislang in § 8a Abs. 3 S. 1 BSIG verortet ist. Nach der geplanten Neustrukturierung des Gesetzes soll diese Nachweispflicht gem. § 34 BSIG-E für besonders wichtige Einrichtungen gelten. Demnach haben diese Einrichtungen dem BSI die Erfüllung der Anforderungen nach § 30 Abs. 1 BSIG-E zu einem vom BSI nach der Registrierung festgelegten Zeitpunkt und anschließend im Zwei-Jahres-Turnus nachzuweisen. Während § 8a Abs. 3 S. 1 BSIG für den Nachweiszeitpunkt auf den Umstand abstellt, dass die Einrichtung in den Anwendungsbereich der BSI-KritisV fällt, gibt die nunmehr vorgesehene Regelung mehr Raum für Flexibilität und Konkretisierung. Ebenfalls neu ist die in § 34 Abs. 2 BSIG-E vorgesehene Möglichkeit, dass das BSI die Ausgestaltung des Nachweisverfahrens nach Anhörung von Vertretern der betroffenen Betreiber und Einrichtungen und der Wirtschaftsverbände konkretisierend festlegen kann. Der Nachweis soll weiterhin in geeigneter Weise, also etwa durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen.

e) Unterrichtungspflichten

Neben einer Meldepflicht besteht auch die Möglichkeit, dass das BSI im Falle eines erheblichen Sicherheitsvorfalls gem. § 35 Abs. 1 BSIG-E besonders wichtige und wichtige Einrichtungen anweist, die Empfänger ihrer Dienste unverzüglich über den Vorfall zu unterrichten, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnte. Dies kann ebenfalls durch eine Veröffentlichung im Internet geschehen. Zusätzlich teilen Einrichtungen aus den Sektoren Bankwesen, Digitale Infrastruktur, Verwaltung von IKT-Diensten und Digitale Dienste den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mit, die diese Empfänger als Reaktion auf die Bedrohung ergreifen können, § 35 Abs. 2 BSIG-E.

f) Compliance

Mit der NIS-2-RL wurde die Gewährleistung unternehmerischer IT-Sicherheit endgültig zum Thema der Geschäftsleitung – und dies setzt sich notwendigerweise auch mit dem NIS2UmsuCG fort. Dieser gesetzgeberische Trend ist jedoch keineswegs ausschließlich für die NIS-2-RL zu verzeichnen, sondern findet sich zB auch in DORA als spezieller Regelung für den Finanzsektor wieder[21]. In Umsetzung von Art. 20 NIS-2-RL schlägt § 38 BSIG-E deshalb dezidierte Pflichten für die Geschäftsleitung besonders wichtiger und wichtiger Einrichtungen vor.

Zur Geschäftsleitung iSd § 2 Abs. 1 Nr. 11 BSIG-E zählen diejenigen natürlichen Personen, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer Einrichtung berufen sind. Dies umfasst u.a. den Vorstand einer AG, Geschäftsführer der GmbH, Vorstände oder besondere Vertreter eines Vereins sowie die Leitungspersonen in öffentlichen Einrichtungen, etwa die Behördenleitung.

3. Billigungs- und Überwachungspflichten sowie Delegation

Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen zur Einhaltung von § 30 BSIG-E ergriffenen Risikomanagementmaßnahmen im Bereich der IT-Sicherheit zu billigen und ihre Umsetzung zu überwachen. Die Beauftragung eines Dritten zur Erfüllung dieser Verpflichtung ist nicht zulässig. Dies eröffnet die Frage, in welchem Umfang die Delegation von Verantwortlichkeiten auf Unternehmensangehörige im Zusammenhang mit der Einhaltung der Risikomanagement-Vorgaben zur IT-Sicherheit noch möglich ist. Dabei scheint bereits eine horizontale Delegation auf einen „Cyberressort"-Vorstand problematisch, da die Vorschrift die Verantwortung sämtlicher Leitungspersonen intendiert. Entsprechend den anerkannten Grundsätzen zur Compliance-Verantwortung bei der Ressortaufteilung[22] wird man bei einer solchen Aufteilung zumindest eine Überwachungspflicht der restlichen Geschäftsleitung annehmen dürfen. Aber auch die vertikale Delegation auf Unternehmensangehörige ist nur begrenzt zulässig. Erlaubt und unerlässlich ist die Verteilung von Aufgaben im Zusammenhang mit der IT-Sicherheit auf einzelne Unternehmensabteilungen (IT-Abteilung, Compliance-Abteilung usw) und damit korrespondierende Führungsfunktionen (Chief Information Security Officer oÄ).[23] Allerdings darf diese Delegation nicht so weit gehen, dass die Geschäftsleitung die Einhaltung der Vorgaben letztlich nicht mehr überwacht und billigt. Sie trägt mithin nach wie vor die Letztverantwortung.[24]

4. Haftung von Geschäftsleitern

Kommt es etwa in einer besonders wichtigen Einrichtung auf Grund eines durch die Geschäftsleitung mangelhaft überwachten Risikomanagementprozesses zu einem Cyberangriff mit betriebseinschränkenden Auswirkungen, kann eine Reihe an Kostenpositionen anfallen, für die sich das Unternehmen bei der Geschäftsleitung schadlos halten will. Zu solchen Kostenpositionen zählen u.a. die unmittelbaren wirtschaftlichen Einbußen für das Unternehmensgeschäft auf Grund von Betriebseinschränkungen in der Produktion/Dienstleistung[25], Lösegeldzahlungen, Kosten für externe Dienstleister (IT-Dienstleister, Rechtsberatung), mittelbare finanzielle Einbußen auf Grund von Reputationsschäden[26], Bußgelder infolge von DS-GVO- oder BSIG-Verstößen, Vertragsstrafen oder Schadensersatzzahlungen gegenüber Vertragspartnern auf Grund von Lieferverzögerungen, aber zB auch Lohnzahlungen für Mitarbeitende, die auf Grund der Betriebseinschränkungen ihrer Arbeit nicht nachgehen können, während die Voraussetzungen des Kurzarbeitergelds nicht erfüllt sind.[27]

Verletzt ein Geschäftsleiter seine Überwachungspflichten aus § 38 Abs. 1 BSIG-E, haftet er nach Absatz 2 der Einrichtung für den hieraus entstandenen Schaden. Für Geschäftsleiter von öffentlichen Einrichtungen bleibt die Amtshaftung unberührt. Hier gelten die allgemeinen Grundsätze nach § 839 BGB iVm Art. 34 S. 1 GG.

---

19 Dittrich MMR-Aktuell 2023, 457211.
20 Dittrich MMR 2022, 267 (269); im Ergebnis auch Hornung NJW 2015, 3334 (3336).
21 Dittrich/Heinelt RDi 2023, 164 (166).
22 Habbe/Gergen CCZ 2020, 281 (282); Hoffmann/Schieffer NZG 2017, 401 (405).
23 Habbe/Gergen CCZ 2020, 281 (282).
24 Bräutigam/Habbe NJW 2022, 809 (813 f.); Habbe/Gergen CCZ 2020, 281 (282 f.); Hoffmann/Schieffer NZG 2017, 401 (405 f.) sprechen vom „Kernbereich der Leitungsverantwortung" mwN.
25 Hornung/Schallbruch, IT-Sicherheitsrecht/Bertschek/Janßen/Ohnemus, 2021, § 3 Rn. 21.
26 Schmidt-Versteyl NJW 2019, 1637 (1638).
27 Erdogan/Dittrich CCZ 2022, 398.

Eine über die NIS-2-RL hinausgehende Besonderheit findet sich in § 38 Abs. 3 BSIG-E. Danach soll ein Verzicht der Einrichtung auf Ersatzansprüche gegen die Geschäftsleitung nach § 38 Abs. 2 BSIG-E oder ein Vergleich der Einrichtung über diese Ansprüche unwirksam sein.[28] Dies wirft u.a. die Frage auf, wie es sich verhält, wenn Einrichtungen Versicherungslösungen (Cyberversicherung, D&O-Versicherung, Vertrauensschadenversicherung[29]) für ihre Leitungspersonen abgeschlossen haben und diese demnach für die Schäden aus Cybereereignissen aufkommen, sich die Einrichtungen aber gesetzlich bei ihren Leitungspersonen schadlos halten müssen. Da es sich bei der D&O-Versicherung um ein Vertragsverhältnis zu Gunsten der Leitungsperson handelt, dürfte deren Heranziehung weiterhin zulässig sein.

Gem. § 38 Abs. 3 S. 2 BSIG-E soll wiederum dann eine Ausnahme gelten, wenn die Leitungsperson zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit ihren Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.

5. Schulungen und Fachkenntnisse

Damit die Geschäftsleitung den gesetzlich bestimmten Überwachungsaufgaben nachkommen kann, bestimmt § 38 Abs. 4 BSIG-E, dass Geschäftsleiter von besonders wichtigen und wichtigen Einrichtungen selbst an regelmäßigen Schulungen teilnehmen müssen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

a) Zusätzliche Anforderungen an Kritische Anlagen

Für Kritische Anlagen soll der dem § 8a Abs. 1a BSIG weitgehend entsprechende § 39 BSIG-E gelten, der die Verpflichtung zum Einsatz von Angriffserkennungssystemen enthält.[30] Die Umsetzung ist nach § 39 Abs. 2 BSIG-E auch in den Nachweisen gegenüber dem BSI gem. § 34 BSIG-E aufzunehmen.

Die Definition der Angriffserkennungssysteme nach § 2 Abs. 1 Nr. 38 BSIG-E wurde im Vergleich zu § 2 Abs. 9b BSIG redaktionell nur leicht verändert. Es handelt sich nach NIS2UmsuCG-E um 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.

b) BSI als zentrale Melde- und Anlaufstelle

Für besonders wichtige Einrichtungen und wichtige Einrichtungen sowie für Betreiber Kritischer Anlagen ist das BSI nach § 40 BSIG-E (wie bereits aktuell vergleichbar mit § 8b Abs. 1 BSIG) die zentrale Melde- und Anlaufstelle. Die Behörde fungiert dabei als nationale Verbindungsstelle zwischen Ländern, Bund und europäischen Institutionen sowie den EU-Mitgliedstaaten. Die Aufgabe des BSI, die Betreiber der Anlagen und Einrichtungen unverzüglich über Gefahren für die Sicherheit in der Informationstechnik (zB Informationen zu Schwachstellen, Schadprogrammen, versuchten oder erfolgten Angriffen) zu informieren, bleibt sinnvollerweise erhalten. Dies verdeutlicht die Notwendigkeit der Registrierung einer Kontaktstelle beim BSI, die folglich kein Selbstzweck ist. Innerhalb der Risikomanagementprozesse der einzelnen Unternehmen und Einrichtungen muss sichergestellt sein, dass die zur Verfügung gestellten Informationen zur IT-Sicherheit zeitnah bewertet und ggf. sofort berücksichtigt werden.

c) Untersagung des Einsatzes kritischer Komponenten

Die Regelungen zum Einsatz kritischer Komponenten, die durch das IT-SiG 2.0 Eingang in das BSIG gefunden haben, erfahren in § 41 BSIG-E lediglich redaktionelle Änderungen, die Bemessungspunkte für die Vertrauenswürdigkeit des Herstellers bleiben somit unverändert. Für Betreiber Kritischer Anlagen soll nach § 41 Abs. 1 BSIG-E – wie aktuell in § 9b Abs. 1 BSIG geregelt – beim erstmaligen Einsatz einer kritischen Komponente (§ 2 Abs. 13 BSIG, § 2 Abs. 1 Nr. 20 BSIG-E) eine Anzeige gegenüber dem BMI erfolgen.

d) Aufsichts- und Durchsetzungsbefugnisse

In Umsetzung der Art. 32 und 33 NIS-2-RL soll das BSI durch die §§ 64, 65 BSIG-E einen Katalog an Aufsichts- und Durchsetzungsmaßnahmen gegenüber wichtigen und besonders wichtigen Einrichtungen erhalten. Nach § 64 Abs. 1 BSIG-E kann das BSI bei besonders wichtigen Einrichtungen ohne Verdachtsmomente die Einhaltung der Anforderungen nach dem BSIG überprüfen. Dabei werden die Mitwirkungspflichten der Einrichtungen beschrieben. Zudem kann das BSI nach § 64 Abs. 3, Abs. 4 BSIG-E Anweisungen gegenüber den Einrichtungen erlassen. Gem. § 64 Abs. 5 BSIG-E besteht die Möglichkeit zur Benennung eines Überwachungsbeauftragten durch das BSI iSe Compliance-Monitorships. Soweit besonders wichtige Einrichtungen den Anordnungen des BSI nach Fristsetzung nicht nachkommen, kann die Behörde die Tätigkeit der betroffenen Einrichtung aussetzen oder Leitungspersonen die Wahrnehmung der Leitungsaufgaben vorübergehend untersagen. Für wichtige Einrichtungen gilt nach § 65 BSIG-E ein reduziertes Instrumentarium, das ihrer geringeren wirtschaftlichen Leistungsfähigkeit Rechnung trägt.

6. Sanktionsvorschriften

Es ist zu begrüßen, dass auch die vorgeschlagene Neufassung des BSIG am bereits aus § 14 BSIG bekannten Stufenkonzept für die Bußgeldtatbestände festhält und dieses nunmehr um die Anforderungen aus dem NIS2UmsuCG ergänzt. Unterschieden wird dabei zwischen allgemeinen Bußgeldtatbeständen und spezifischen Tatbeständen, die für die besonders wichtigen und wichtigen Einrichtungen gelten. Die vorgeschlagenen Bußgeldstufen des allgemeinen Rahmens reichen gem. § 59 Abs. 5 BSIG-E von 100.000 EUR über 500.000 EUR bis hin zu 20 Mio. EUR. Damit liegt der bebußbare Rahmen über den Anforderungen der NIS-2-RL, die in Art. 34 Abs. 4 einen Höchstrahmen von 10 Mio. EUR vorsieht. Der Bußgeldrahmen für die besonders wichtigen und wichtigen Einrichtungen wird in § 59 Abs. 6, Abs. 7 BSIG-E festgelegt. Eine zahlenmäßige Differenzierung zwischen besonders wichtigen Einrichtungen und den Betreibern Kritischer Anlagen findet dabei nicht statt, da die Differenzen im gesetzlichen Pflichtenkatalog zur IT-Sicherheit nur marginal sind. Zudem soll für die Betreiber Kritischer Anlagen gezielt der obere Bereich des Bußgeldrahmens ausgeschöpft werden. Die maximale Höhe des Bußgeldrahmens für besonders wichtige und wichtige Einrichtungen wird über Konzernregelungen bestimmt, die bereits aus der DS-GVO bekannt sind. So beträgt der Bußgeldrahmen für wichtige Einrichtungen bis zu 7 Mio. EUR bzw. bei besonders wichtigen Einrichtungen bis zu 10 Mio. EUR oder ein Höchstbetrag von mindestens 1,4% bzw. für besonders wichtige Einrichtungen von mindestens 2% des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens.

---

28 Rechtstechnisch dürfte es sich dabei um eine Verbotsnorm iSd § 134 Abs. 1 BGB handeln.

29 Erichsen CCZ 2015, 247 (249); Fortmann r+s 2019, 429 (440 ff.).

30 Hornung NJW 2021, 1985 (1987); Kipker/Scholz MMR 2019, 431 (433).

Zusätzlich zu den Bußgeldvorschriften sieht der § 59 BSIG-E Maßnahmen des Verwaltungszwangs vor, die aus Art. 34 Abs. 6 NIS-2-RL abgeleitet werden, in dem bestimmt wird, dass die Mitgliedstaaten Zwangsgelder verhängen können, um eine wesentliche oder wichtige Einrichtung zu zwingen, einen Verstoß gegen NIS-2 gemäß einer vorherigen Entscheidung der zuständigen Behörde einzustellen. Gem. § 59 Abs. 10 BSIG-E kann das BSI Zwangsgelder iHv bis zu 100.000 EUR verhängen.

III. Fazit

Auch wenn das NIS2UmsuCG wohl erst zum Jahresende 2023 verabschiedet wird, wird mit dem Gesetzesentwurf mehr als deutlich, welche Richtung der Weg der nationalen IT-Sicherheit in den nächsten Jahren einschlagen wird – und das nicht nur im Kontext von KRITIS. Die Zeiten, in denen Cybersecurity als „Kleinigkeit" abgetan werden konnte, sind ohnehin schon lange vorbei – dieses Gesetz jedoch geht weit über die europäischen Vorgaben hinaus und will nicht nur einen Mindeststandard an Cybersicherheit umsetzen, sondern ein flächendeckendes und einheitlich hohes Niveau unternehmerischer Cyber-Compliance schaffen, dessen Nichteinhaltung empfindlich sanktioniert werden kann. Mit Sicherheit werden dabei einige der Vorgaben kontrovers diskutiert werden und Fragen bei der praktischen Umsetzung aufwerfen, denn das NIS2UmsuCG ist das bislang komplexeste Rahmenwerk des deutschen IT-Sicherheitsrechts.

Schnell gelesen ...

- Das NIS2UmsuCG kommt voraussichtlich Ende 2023 und ist das bislang komplexeste Rahmenwerk des nationalen IT-Sicherheitsrechts.
- Gesetzlich ergeben sich zahlreiche Änderungen im Anwendungsbereich, der in erheblichem Maße erweitert wird und längst nicht mehr nur KRITIS betrifft.
- Insgesamt werden die Vorgaben zur Cybersecurity-Compliance deutlich verschärft und können mit erheblichen Bußgeldern belegt werden.

Professor Dr. Dennis-Kenji Kipker
ist Mitglied des Vorstands der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin und Mitherausgeber der MMR.

Tilmann Dittrich, LL.M.,
ist Rechtsreferendar im OLG-Bezirk Düsseldorf und Doktorand an einem Lehrstuhl für Strafrecht der Heinrich-Heine-Universität Düsseldorf.