Berlin, 25.05.2024

Stellungnahme und Kommentierung

zum

Diskussionspapier des BMI für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland

Kontakt:
RA Karsten U. Bartels, LL.M.
HK2 RAe
Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Stellvertretender Vorstandsvorsitzender
Leiter TeleTrusT-AG "IT-Sicherheitsrecht"
bartels@hk2.eu

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
https://www.teletrust.de

I. Allgemeine Vorbemerkung

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) hält die Ausweitung der Regulierung gesetzlicher IT-Sicherheit in Deutschland und der EU für dringend geboten. Das betrifft sowohl die Verbreiterung der KRITIS-Regulierung durch die NIS2-Richtlinie, die CER-Richtlinie und deren Umsetzung sowie auch die horizontale Regulierung durch den EU Cyber Resilience Act.

Anlass dafür ist die historisch schlechte IT-Sicherheitslage, die weitere Zunahme der Bedrohungen sowie die mangelnde freiwillige Umsetzung von hinreichender IT-Sicherheit in Unternehmen und Verwaltung.

Neue IT-Sicherheitsgesetze sollten jedoch mit der vorhandenen Gesetzgebung abgeglichen und schlüssig in das rechtliche Regelungssystem eingefügt werden. Das ist bislang nur unzureichend geschehen und auch das BSIG-E und das NI2UmsuCG-E insgesamt erfüllen diesen Anspruch nicht.

II. Anmerkungen zu ausgewählten Regelungen des BSIG-E

1. § 6 BSIG-E, Informationsaustausch

TeleTrusT kritisiert § 6 BSIG-E: es ist aus Sicht der IT-Sicherheit wünschenswert, dass sämtliche Interessierten an die in der Norm genannten Informationen gelangen, nicht nur die Betreiber wichtiger und besonders wichtiger Einrichtungen, Einrichtungen der Bundesverwaltung sowie die Hersteller, Dienstleister und Lieferanten. Zwar ist nun vorgesehen, auch weiteren Stellen eine Teilnahme zu ermöglichen. Diese Kann-Regelung geht jedoch am Informationsinteresse der Öffentlichkeit und der Unternehmen vorbei. Es ist kein belastbarer Grund erkennbar, die betreffenden Informationen nicht schlicht zu veröffentlichen. Zumal es keinerlei Handhabe gibt, eine Weitergabe der Information durch Berechtigte zu verhindern.

Es sollte endlich davon Abstand genommen werden, den Informationszugang weiterhin "mitgliedschaftlich" zu organisieren, wie dies derzeit noch im Rahmen der Allianz für Cybersicherheit umgesetzt wird. So sind Teilnahmebedingungen inklusive einer Geheimhaltungsverpflichtung bislang Voraussetzung für die Informationsteilhabe bei der Allianz für Cybersicherheit.

In § 6 Abs. 2 BSIG-E sind nun ebenfalls Teilnahmebedingungen vorgesehen. TeleTrusT bezweifelt die Zulässigkeit und Notwendigkeit solcher Bedingungen. Sofern nicht im konkreten Einzelfall das Informationsinteresse der Öffentlichkeit aufgrund von Sicherheitsbedenken (durch eine Veröffentlichung) zurückstehen muss, sollte es einen freien Zugang zu den relevanten Informationen für Alle und einen "vorbehaltlosen" Ansatz des BSI geben.

2. § 13 BSIG-E, Warnungen

Der Referentenentwurf enthält eine zu weit gehende Befugnis für Warnungen durch das BSI. Das in § 13 Abs. 1 Ziff. 1 lit. a benannte Tatbestandsmerkmal der "anderen Sicherheitsrisiken in informationstechnischen Produkten und Diensten" wurde nicht definiert und ist unklar. Die Formulierung deutet daraufhin, dass hier ein allgemeiner Auffangtatbestand geschaffen werden soll. Dies lehnt TeleTrusT ab. Es sollte im Sinne des Bestimmtheitserfordernisses eng umrissen sein, unter welchen Voraussetzungen eine Warnung vorgenommen werden darf. Die Vergangenheit zeigt, dass der Tatbestand politisch motivierte Warnungen nicht ermöglichen darf.

Zudem berechtigt die Norm das BSI, die Öffentlichkeit über "Verstöße besonders wichtiger Einrichtungen oder wichtiger Einrichtungen gegen die Pflichten aus diesem Gesetz" zu informieren. Aufgrund der Formulierung besteht dieses Recht jedoch bei jeglichem Verstoß gegen eine jegliche Norm des BSIG, unabhängig von der Schwere. Da solche Informationen eine massive Wirkung entfalten können und in

geschützte Rechtspositionen der Unternehmen eingegriffen wird, ist eine derart weitgehende und diffuse Rechtsgrundlage abzulehnen.

3. § 15 BSIG-E

§ 15 zielt darauf ab, dem BSI die Befugnis zu erteilen, Maßnahmen zur Erkennung von Sicherheitsrisiken und Angriffsmethoden an Schnittstellen öffentlich zugänglicher informationstechnischer Systeme durchzuführen. Diese Befugnisse sind von zentraler Bedeutung für die proaktive Identifizierung und Abwehr von Cyberbedrohungen, um die Sicherheit nationaler Netzinfrastrukturen zu gewährleisten. Es wird anerkannt, dass ein solides Verständnis der Bedrohungslandschaft unerlässlich ist, um effektive Schutzmaßnahmen zu entwickeln und die Resilienz kritischer Informationsinfrastrukturen zu stärken.

Allerdings birgt § 15 potenzielle Unzulänglichkeiten in Bezug auf den Schutz von Betriebsgeheimnissen und die Wahrung der Privatsphäre von Nutzern. Es besteht das Risiko, dass die weitreichenden Befugnisse des BSI die grundgesetzlich garantierten Rechte der Bürger und Unternehmen untergraben. Es ist unklar, wie das Gesetz den notwendigen Schutz dieser Rechte sicherstellen will.

4. § 18 BSIG-E

Die im § 18 verwendete Formulierung "soweit erforderlich" gibt dem Bundesamt ein weitreichendes Ermessen darüber, wann es von den Herstellern von IKT-Produkten eine Mitwirkung an der Beseitigung oder Vermeidung von Sicherheitsvorfällen verlangt. Hier ist eine Schärfung der Voraussetzung wichtig für eine klare Rechtslage hinsichtlich der Voraussetzungen und Folgen der Norm.

5. §§ 24 f. BSIG-E

In § 24 Abs. 2 NIS2UmsuCG-E ist unklar, was "eine Gegendarstellung" ist, wie eine solche auszugestalten ist und wie das Bundesamt diese Gegendarstellung "den Daten" beifügen würde.

Zu § 25 Abs. 1 NIS2UmsuCG-E merken wir an: es ist nicht klar, ob die getroffene Regelung nur für "nicht automatisierte Verarbeitung" gilt, oder auch für die automatisierte Verarbeitung. Es scheint, als ginge der Entwurf davon aus, dass es bei einer automatisierten Verarbeitung stets zu einer Löschung der personenbezogenen Daten kommt, was nicht der Fall sein muss.

6. §§ 28 ff. BSIG-E, Anwendungsbereich

TeleTrusT begrüßt die Klarstellung und Vereinfachung in den Regeln zur Anwendbarkeit des § 28 BSIG-E im Verhältnis zum letzten Referentenentwurf.

Die besonders wichtigen Einrichtungen (mit Ausnahme der Betreiber kritischer Anlagen) und die wichtigen Einrichtungen allein durch die gesetzlichen Regelungen im BSIG-E selbst und deren Anlagen 1 und 2 nachvollziehbar zu machen, schafft Einfachheit und grundsätzlich Rechtssicherheit. Wichtig wäre, möglichst frühzeitig einen Entwurf der Verordnung gem. § 28 Abs. 7 f., i. V. m. § 58 Abs. 4 BSIG-E vorzulegen, damit sich die Betreiber frühzeitig auf Veränderungen einstellen können.

Die Darstellung der Regelungen hat sich seit dem Diskussionspapier nur wenig verbessert. Systematisch allein richtig, wäre es, zunächst die wichtigen, und dann darauf aufbauend die besonders wichtigen Einrichtungen zu definieren.

Weiterhin für verfehlt hält TeleTrusT die Nomenklatur. Die Begriffe "wichtige Einrichtungen" und "besonders wichtige Einrichtungen" sind in mehrfacher Hinsicht unvorteilhaft: erstens weichen sie ohne Not von den europäischen Begriffen ab. Das erschwert bereits die Kommunikation (nicht zuletzt auch mit Gesprächspartnern anderer Mitgliedsländer). Es ist deutlich weniger missverständlich und sprachlich

leichter zu fassen, wenn auch im deutschen Gesetz von wesentlichen und wichtigen Einrichtungen gesprochen würde. Es bedarf hier solcher Begrifflichkeiten, die auch in der praktischen Umsetzung "funktionieren". Insofern empfehlen sich kurze Begriffe und keine 3-Wort-Zusammenstellungen. Die Praxis der letzten Monate zeigt zudem schon jetzt, dass eine klare begriffliche Fassung wichtig ist. Bespiel sind die "*besonders wichtigen Einrichtungen, die nicht Betreiber einer kritischen Anlage sind*". Diese Gruppe von Gesetzesadressaten gibt es und kann derzeit wohl nicht kürzer bezeichnet werden. Es ist unklar, was es für einen Grund geben soll, die Begrifflichkeiten nicht zu optimieren.

Die "Betreiber kritischer Anlagen" sollten konsequenterweise "kritische Einrichtungen" genannt werden, vgl. NIS2-Richtlinie.

Begrüßenswert ist, dass Anbieter öffentlich zugänglicher Telekommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze, welche die Schwellenwerte des Abs. 1 Nr. 3 nicht erreichen, nun als "wichtige Einrichtungen" vom BSIG-E adressiert werden.

§ 28 Abs. 9 Ziff. 1 und 2 schränken die Anwendbarkeit des Gesetzes aus politischen Gründen unzulässig ein. Technisch ist dies nicht zu begründen. Der TeleTrusT lehnt diese Einschränkung zu Lasten der IT-Sicherheit entschieden ab.

Wenngleich es grundsätzlich positiv ist, dass Stellen des Bundes, Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen auf Bundesebene vom BSIG-E adressiert werden, ist die erfolgte Aufweichung des Anwendungsbereichs scharf zu kritisieren: Die Geschäftsbereiche des Auswärtigen Amts, der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz sollten ebenfalls umfassend zur IT-Sicherheit verpflichtet werden. Hinsichtlich der vom Auswärtigen Amt zu erlassenden Verwaltungsvorschrift ist bei der Verwendung des Begriffs ("ergebnisäquivalente Maßnahmen") fraglich, ob diese zu einem ausreichenden Maß an IT-Sicherheit verpflichten werden.

Auch die Streichung der öffentlichen Unternehmen von der Definition der "Einrichtungen der Bundesverwaltung" ist ein weiterer Schritt in die falsche Richtung. Öffentliche Unternehmen sollten umfassend IT-sicherheitsrechtlich verpflichtet werden, unabhängig von einer Erfassung als "besonders wichtige Einrichtung" oder "wichtige Einrichtung".

7. § 30 BSIG-E, Risikomanagementmaßnahmen

Es wäre wünschenswert, die Maßgaben, nach denen die Einrichtungen Maßnahmen zur IT-Sicherheit i. S. v. § 30 Abs. 1 BSIG-E umsetzen sollen, zu schärfen.

Der Entwurf lässt nach wie vor unklar, was unter dem Begriff der Risikoexposition exakt zu verstehen ist. Auch die weiteren Faktoren, die bei der Auswahl der IT-Sicherheitsmaßnahmen zu berücksichtigen sind, bleiben weiterhin unklar: das betrifft die Umsetzungskosten, die auch nach geltendem Recht berücksichtigt werden dürfen. Hier hat sich bislang keine klare Rechtsmeinung dazu gebildet, wie dies geschehen darf.

Bei den Aspekten der "gesellschaftlichen und wirtschaftlichen Auswirkungen" bleibt noch immer gänzlich unklar, was darunter zu verstehen ist. Aufgrund der schieren Menge möglicher Einflussfaktoren auf eine nicht definierbare Menge von Aspekten, kann ein alleiniger Kausalzusammenhang jedenfalls augenscheinlich nicht genügen. Es stellt sich bereits die Frage, worauf exakt sich das "dabei" (Abs. 1 e. E.) beziehen soll.

TeleTrusT wirbt deshalb dafür, Abs. 1 zu überarbeiten und so zu gestalten, dass er subsumtionsfähig, aber vor allem praktisch anwendbar wird.

In Abs. 2 bleibt unklar, welche Bedeutung den europäischen und internationalen Normen hier zukommen soll. Denn diese beinhalten in der Regel Maßgaben unterhalb des Stands der Technik, also zu den

allgemein anerkannten Regeln der Technik. Insoweit erschließt sich keine eigene Wirkung, die über die Verpflichtung, den Stand der Technik zu berücksichtigen, hinausgeht.

TeleTrusT schlägt vor, in Abs. 2 die Fachkreise/ Expertenkreise der IT-Sicherheit und deren Empfehlungen (abstrakt) aufzunehmen. Die Fachkreise sind der Ort, wo das Technologieniveau "Stand der Technik" mit konkreten Angaben ausgefüllt wird, vgl. TeleTrusT-Handreichung zum Stand der Technik in der IT-Sicherheit.

Der Begriff der Cyberhygiene sollte klarer definiert werden. Bei der bisherigen Beschreibung ist kein methodischer oder systematischer Hintergrund oder Ansatz zu erkennen. Es bleibt unklar, warum bestimmte Maßnahmen/ -kategorien zur Cyberhygiene gehören sollen, andere jedoch nicht.

Zu Abs. 6: TeleTrusT regt an, IT-Produkte, die bereits im Rahmen von VSA für die Verarbeitung von VS-Material zugelassen sind, Produkten, die eine Cybersicherheitszertifizierung aufweisen, rechtlich gleich zu bewerten.

Abs. 9: im Rahmen der branchenspezifischen Sicherheitsstandards sollte klargestellt werden, dass sie Angaben darüber zu enthalten haben, wie konkret mit der Aufrechterhaltung des Stands der Technik umgegangen wird. Hier bestand in der Vergangenheit häufig das Missverständnis, ein B3S sei qua definitionem und unbeachtlich konkreter Angaben "als Ganzes" der Stand der Technik. Leider enthalten die im Einsatz befindlichen B3S zu selten Informationen zum Stand der Technik. Das sollte sich ändern.

Die Erweiterung der zu einem Nachweis Verpflichteten auch auf besonders wichtige und wichtige Einrichtungen im Wege einer allgemeinen Rechenschaftspflicht gem. § 30 Abs. 1 a. E. war der Vorschlag vom TeleTrusT. Wir halten diese aus mitgeteilten Gründen nach wie vor für wesentlich.

8. § 31 BSIG-E, Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

Die Anforderungen an IT-Sicherheitsmaßnahmen an Betreiber kritischer Anlagen stellen aufgrund der Relevanz einen wichtigen Regelungskern des BSIG dar. Dennoch bestimmt der § 31 Abs. 1 BSIG-E keinerlei eigenen materiellen Anforderungen, sondern beschränkt den Gesetzesadressaten lediglich bei dessen wirtschaftlichen Beurteilungsspielraum im Rahmen der Maßnahmenauswahl (gem. § 30 BSIG-E). Dies wiederum nur höchst abstrakt. Es bleibt unklar, was "aufwändigere Maßnahmen" darstellen.

TeleTrusT hält die Norm in der Entwurfsfassung für offensichtlich dysfunktional und rechtlich zu unbestimmt.

9. § 38 BSIG-E

Vergleiche sind gem. § 38 Abs. 2 nunmehr grundsätzlich möglich, soweit sie nicht "in einem groben Missverhältnis zu einer bestehenden Ungewissheit über das Rechtsverhältnis" stehen. Die Begriffe "grobes Missverhältnis" und "bestehende Ungewissheit" sind zu unbestimmt. Gleichzeitig dürfte bereits jetzt klar sein, dass es der Regelfall und nicht die Ausnahme ist, dass bei einem erfolgreichen Cyberangriff eine "Ungewissheit" besteht.

Im Rahmen des gesellschaftsrechtlichen Zulässigen muss ein Vergleich zwischen dem Geschäftsführer und dem Unternehmen stets möglich sein. Die Zulässigkeit bestimmt sich bereits nach der ausdifferenzierten Dogmatik des Gesellschafts-rechts. Der Verweis des § 38 BSIG-E auf den Vergleich sollte daher gestrichen werden.

10. § 43 BSIG-E

Im Gegensatz zu Begriff "Geschäftsleitung" findet sich zum Begriff der "Einrichtungsleitung" keine Legaldefinition.

Zur Herstellung auf Aufrechterhaltung der Informationssicherheit sind nunmehr bedarfsgerechte (a. F.: "angemessene") finanzielle, personelle und Sachmittel einzusetzen. Nach dem BSIG-E a.F. galt der finanzielle Mitteleinsatz als angemessen, wenn er mindestens 20 Prozent der Ausgaben des IT-Betriebs innerhalb der Einrichtung beträgt. Diese Formulierung wurde nun aus der Begründung des § 43 gestrichen. Grundsätzlich ist eine quantitative Betrachtungsweise auch nicht geeignet, um den konkreten Mittelbedarf zu sichern. Allerdings wurde der Passus ersatzlos gestrichen, anstatt qualitative Faktoren miteinzubeziehen, welche bei der Beurteilung, ob es sich um "bedarfsgerechte" Mittel handelt, berücksichtigt werden können. Der Begriff "bedarfsgerecht" ohne nähere Definition oder Beschreibung ist zu ungenau und kann kaum für einen ausreichenden Mitteleinsatz sorgen, zumal im Teil "Allgemeine Begründung", Ziffer 1 ausdrücklich auch für Bundesverwaltung eine erhöhte Gefährdungslage festgestellt wird und zudem konstatiert wird, dass die bisherigen Anstrengungen nicht ausreichend gewesen sind.

11. § 45 BSIG-E, Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung

Im Unterschied zum Informationssicherheitsbeauftragten der Ressorts, der nach § 46 Abs. 2 S. 2 die notwendigen Kenntnisse besitzen muss, kann der Informationssicherheitsbeauftragte dem Wortlaut des § 45 Abs. 2 S. 2 diese noch erwerben.

12. § 46 BSIG-E, Informationssicherheitsbeauftragte der Ressorts

Hervorzuheben ist die Kompetenz des jeweiligen Informationssicherheitsbeauftragten nach Abs. 3 Satz 3, in begründeten Ausnahmefällen, im Benehmen mit dem oder der jeweiligen IT-Beauftragten des Ressorts den Einsatz bestimmter IT-Produkte in Einrichtungen der Bundesverwaltung innerhalb des jeweiligen Ressorts ganz oder teilweise zu untersagen. Die Begründung des Gesetzes führt hierzu aus, das Veto-Recht zum Einsatz bestimmter IT-Produkte diene "dem Zweck, bei Bedarf Informationssicherheitsbelange durchsetzen zu können." Worin diese Belange im Einzelnen bestehen, bleibt indes offen.

13. § 47 BSIG-E, Wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes

Begrüßenswert ist der Ansatz, dass bei wesentlichen Digitalisierungsvorhaben Informationssicherheit schon bei der Planung zu berücksichtigen ist, Abs. 2 S.1 ("security by design"). Welche Inhalte hier genau zu berücksichtigen sind, bleibt indes offen. Hier empfiehlt sich der Rückgriff auf etablierte Handreichungen wie die des TeleTrusT ("2023-TeleTrusT-Handreichung_"Security_by_Design").

14. § 51 Abs. 3 BSIG-E

Satz 1: Soweit hiernach erforderlich ist, explizit auch "*Überprüfungsverfahren"* zur Verifizierung von Angaben vorzunehmen, kann dies für Domain-Name-Registry-Dienstleister zu Mehraufwand führen. Mit dem Wortlaut der Regelung bleibt unklar, welche konkreten Anforderungen an die Verifizierung der jeweils erfassten Daten gestellt werden.

- Welchen Mindeststandard hat ein Domain-Name-Registry-Dienstleister bei der Verifizierung einzuhalten?
- Darf eine Top Level Domain Name Registry die Freischaltung einer Domain verweigern, wenn ein Domain-Name-Registry-Dienstleister nicht alle Mindestangaben aus § 51 Abs. 2 BSIG-E verifiziert hat?
- Oder, muss die Top Level Domain Name Registry sogleich eigene Anstrengungen zur Verifizierung unternehmen?

Satz 2: Ungenau ist auch, in welchem Umfang und in welcher Tiefe die verlangten *"[…] Vorgaben und Verfahren […]"* öffentlich zugänglich zu machen sind. Reichen dazu Zertifizierungen, Prozessbeschreibungen, Erklärungen/ Selbstverpflichtungen?

15. § 52 Satz 1 Nr. 2 BSIG-E

Die Formulierung *"[…] alle Anträge auf Zugang […]"* sollte eine direkte Bezugnahme zu Nr. 1 enthalten, sonst wären auch völlig substanzlosen Anträge binnen 72 Stunden zu beantworten. Zwar ist der Wortlaut des Art. 28 (5) der NIS-2-Richtlinie ebenfalls nicht präziser, hier sollte der nationale Gesetzgeber präziser vorgehen.

In der NIS-2-Richtlinie ist der Inhalt nicht auf 2 Nummern aufgeteilt, sondern im Blockabsatz dargestellt. Vorschlag zur Präzisierung: *"[…]* ***diese*** *Anträge auf Zugang […]"*

Zugang soll nur zu "*bestimmten*" Domänennamen-Registrierungsdaten gewährt werden. Zu welchen aber (mindestens) Zugang zu gewähren ist, wird nicht näher definiert.

16. § 52 Satz 2 BSIG-E

Die Formulierung leidet unter derselben Ungenauigkeit wie oben zu § 51 Abs. 3 Satz 2 BSIG-E dargestellt. In welchem Umfang und in welcher Tiefe die verlangten "Vorgaben und Verfahren" öffentlich zugänglich zu machen sind, ist offen: Zertifizierungen, Prozessbeschreibungen, Erklärungen/ Selbstverpflichtungen?

17. § 61 BSIG-E, Bußgeldvorschriften

Begrüßenswert ist, dass die Neugliederung des § 61 Abs. 5-7 für mehr Übersichtlichkeit bei den Bußgeldern sorgt.

Für Verstöße gegen § 61 Abs. 2 Nr. 13, 14 BSIG-E enthält § 61 Abs. 5 keinen Bußgeldrahmen.

Die Formulierung in § 61 Abs. 8 bedeutet, dass die wichtige oder besonders wichtige Einrichtung nicht zwingend die gesamte zugehörige juristische Person meint, sondern eine solche Einrichtung auch einem "Unternehmen" angehören kann. Dieses Verständnis steht im Widerspruch zum Einrichtungs-Begriff in der NIS-2-Richtlinie (vgl. Art. 3 Nr. 38 NIS-2-Richtlinie). Sofern diese Formulierung auf die Anwendung des unionsrechtlichen Unternehmensbegriffs zurückzuführen ist, wäre eine entsprechende Klarstellung aus Gründen der Rechtsklarheit wünschenswert.

18. § 62 BSIG-E, Zuwiderhandlungen durch Institutionen der sozialen Sicherung

§ 62 BSIG-E- übernimmt den bisherigen § 14a BSIG fast wortgleich. Entsprechend stellen sich bei § 62 BSIG-E die gleichen Kritikpunkte wie bei dem bisherigen § 14a BSIG.

Es wird weiterhin nicht hinreichend klar festlegt, ob die Anwendbarkeit der dem BSI zustehenden Aufsichts- und Durchsetzungsmittel (siehe §§ 65, 66 BSIG-E) sowie die weiteren Befugnisse des BSI (siehe hierzu etwa die §§ 14 ff. BSIG-E) eingeschränkt werden sollen. Die Ratio der Norm (vgl. § 62 S. 4 BSIG-E) spricht eher für eine entsprechende Sperrwirkung. Ein sachlicher Grund für diese wäre allerdings nicht erkennbar. Es wäre wünschenswert, wenn festgelegt wird, ob und inwieweit das BSI in der Ausübung seiner Befugnisse eingeschränkt werden soll.

19. § 64 BSIG-E, Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten

Der Wortlaut von § 64 Abs. 3 und 4 BSIG-E wird zwar fast wortgleich aus der NIS-2-Richtlinie übernommen. Soweit dies aber nicht der Fall ist, werden wichtige Aspekte nicht geregelt. Dies betrifft zum einen die Frage, welche Personen überhaupt als Vertreter agieren dürfen und zum anderen, welche Aufgaben

der Vertreter übernimmt. Beide Punkte werden in Art. 6 Nr. 34 der NIS-2-Richtlinie geregelt. Insoweit empfiehlt es sich daher, die Definition des Vertreters aus Art. 6 Nr. 34 der NIS-2-Richtlinie entweder in § 2 oder § 64 Abs. 3 BSIG-E zu übernehmen.

Auch die Form der Benennung eines Vertreters ist nicht geregelt. Art. 6 Nr. 34 der NIS-2-Richtlinie verlangt eine "ausdrückliche" Benennung des Vertreters. Eine entsprechende Regelung ist in § 64 nicht enthalten. In dem Zusammenhang empfiehlt es sich auch, die Form der Benennung auch dahingehend weiter zu konkretisieren, ob hierfür die Schriftform oder eine andere Form zwingend notwendig ist, um etwaige Unklarheiten zu vermeiden. Die NIS-2-Richtlinie verlangt insofern in ErwGr. 116 eine ausdrückliche *schriftliche* Benennung.

20. § 65 BSIG-E, Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

§ 65 Abs. 3 BSIG-E berechtigt das Bundesamt zur Anforderung von Nachweisen auch von besonders wichtigen Einrichtungen. Die Anforderung von Nachweisen ist sinnvoll und nachvollziehbar. Allerdings sind entsprechende ausdrückliche Nachweispflichten bislang nur in § 39 BSIG-E für Betreiber kritischer Anlagen geregelt, während wichtige und besonders wichtige Einrichtungen lediglich allgemeine Dokumentationspflichten (vgl. § 30 Abs. 1 S. 3 BSIG-E). Aus Gründen der Rechtssicherheit empfiehlt es sich daher, dass in § 65 Abs. 3 BSIG-E klargestellt wird, dass das BSI lediglich die Dokumentation anfordern darf.

21. § 66 BSIG-E, Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen

Es ist weiterhin unklar, wie substantiiert die "Tatsachen" sein müssen, die die Annahme einer nicht oder "nicht richtigen Umsetzung" der Anforderungen aus den §§ 30, 31, 32 BSIG-E, rechtfertigen. Zudem wird eine solche Formulierung gerade nicht in § 65 BSIG-E genutzt. Es ist daher im Zweifel unklar, ob bei der Wahrnehmung der Aufsichts- und Durchsetzungsmaßnahmen gegenüber wichtigen und besonders wichtigen Einrichtungen unterschiedliche materielle Voraussetzungen gelten sollen.

Die Regelung enthält keine Einschränkung dazu, welche Maßnahmen das Bundesamt im Falle der Annahme, dass eine wichtige Einrichtung die Anforderungen aus den §§ 30, 31 und 32 nicht oder nicht richtig umsetzt, ergreifen kann. Dem Bundesamt stünde daher bspw. auch die Möglichkeit offen, von Betreibern wichtiger Einrichtungen nach § 65 Abs. 3 BSIG-E Nachweise i. S. d. § 39 BSIG-E zu verlangen, obwohl diese Pflicht sich nur an Betreiber kritischer Anlagen richtet. Faktisch kann dies somit zu einer Ausweitung der Pflichten über den Gesetzeswortlaut führen könnte. Es wäre daher wünschenswert, wenn klargestellt wird, welche Maßnahmen in § 65 BSIG-E auf wichtige Einrichtungen angewandt werden können sollen.

22. Nr. 6 der Anlage 2 BSIG-E, Anbietereigenschaft im Rahmen des Sektors "Anbieter digitaler Dienste"

Im aktuellen BSIG wird ein "Anbieter digitaler Dienste" nach § 2 Abs. 12 BSIG-E schlicht als "juristische Person, die einen digitalen Dienst anbietet" definiert, im aktuellen BSIG-E nicht.

In das BSIG-E sollte eine Definition des "Anbieters digitaler Dienste" aufgenommen werden, die auf eine hinreichende (technische) Einwirkungsmöglichkeit eines Verantwortlichen auf den digitalen Dienst abstellt. Denkbar ist, dass die Definition gleichlaufend zu den Betreibern wie in § 28 Abs. 6 BSIG-E sein soll. Dann würde diese Definition insbesondere für White-Label-Lösungen zusätzlich für Klarheit sorgen. Bei diesen herrscht derzeit in der Praxis Unsicherheit, wer genau den digitalen Dienst eigentlich anbietet.

23. Anlage 2 Nr. 3 BSIG-E

Im Rahmen des Sektors "Produktion, Herstellung und Handel mit chemischen Stoffen" der Anlage 2 Nr. 3 BSIG-E muss klargestellt werden, wer genau dem Anwendungsbereich des Umsetzungsgesetzes unterfallen soll.

Begrüßenswert ist die Klarstellung, dass nur solche Unternehmen adressiert sein sollen, die in die Abteilung 20 NACE Rev. 2 fallen und damit Hersteller von chemischen Erzeugnissen sind. Vor diesem Hintergrund ist davon auszugehen, dass der Verweis auf Ar. 3 Nr. 11 der Verordnung (EG) 1907/2006 (Importeure) lediglich ein Redaktionsversehen ist und gelöscht werden kann. Insbesondere würde die Regulierung von Importeuren von den Vorgaben der NIS2-Richtlinie abweichen, die dies nicht vorsieht.