21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)051
vom 19. September 2025

Stellungnahme

des Bundesverbandes IT-Sicherheit e.V.
vom 19. September 2025

zum

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

Bundestagsdrucksache 21/1501

Berlin, 18.09.2025

Stellungnahme

zum

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

Kontakt:
RA Karsten U. Bartels, LL.M.
HK2 Rechtsanwälte
Hausvogteiplatz 11 A
10117 Berlin
-
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. Einleitung

Die folgende Stellungnahme wendet sich an den federführenden Innenausschuss, der den Regierungsentwurf für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (im Folgenden "NIS2UmsG") berät.

Der Entwurf bezweckt die Steigerung der Resilienz von Wirtschaft und Staat, insbesondere gegen Cyberangriffe. Dazu sollen auch die bislang als unzureichend angesehenen Steuerungsinstrumente in der Bundesverwaltung durch wirksamere, verbindliche Vorgaben ersetzt und damit das Sicherheitsniveau flächendeckend angehoben werden. Begründet wird der Handlungsbedarf unter anderem mit dem erheblichen volkswirtschaftlichen Schadensvolumen (2024: EUR 266,6 Mrd.). Der Entwurf beansprucht damit, einen kohärenten, vollzugsfähigen Regelungsrahmen zu schaffen, der die offenkundigen Defizite adressiert.

Die auf den letzten Referentenentwurf vom 23.06.2025 folgende Kritik, die auch in der Verbändeanhörung artikuliert wurde, schlägt sich jedoch nicht im Entwurf der Bundesregierung nieder. Vielmehr befinden sich an zahlreichen Stellen des Entwurfstextes Aufweichungen und nicht berichtigte Fehler, die aufzeigen, dass die Bundesregierung das gesteckte Ziel nicht einhalten kann.

Der Innenausschuss sollte darauf hinwirken, diese Mängel zu beheben.

Im Folgenden werden relevante Änderungen des Regierungsentwurfs im Vergleich zum vorherigen Referentenentwurf beleuchtet und der diesbezügliche Handlungsbedarf für den Innenausschuss festgestellt.

II. Anwendungsbereich, § 28 BSIG-E

Enttäuschend ist zunächst die Beibehaltung des § 28 Abs. 3 BSIG-E. Dieser sieht seinem Wortlaut nach vor, dass bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 solche Geschäftstätigkeiten unberücksichtigt bleiben können, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind. Die Formulierung wurde bereits im Referentenentwurf vom 23.06.2025 eingeführt und in der Verbändeanhörung umfassend als zu unbestimmt und potentiell europarechtswidrig kritisiert.

Indes behielt die Bundesregierung die Formulierung des § 28 Abs. 3 BSIG-E bei und fügte lediglich zwei Absätze in der Begründung zum Entwurf hinzu. Bei der Einordnung einer Geschäftstätigkeit als "vernachlässigbar" können hiernach etwa die Anzahl der in diesem Bereich beschäftigten Mitarbeiter, der Umsatz oder die Bilanzsumme hinzugezogen werden. Hingegen würde eine Nennung im Gründungsdokument des Unternehmens gegen eine Vernachlässigbarkeit des Geschäftsbereiches sprechen. Insgesamt seien das Gesamtbild der betreffenden Geschäftstätigkeit im Lichte der Gesamtgeschäftstätigkeit der Einrichtung unter Berücksichtigung aller relevanten Anhaltspunkte entscheidend.

Die vielfach geforderte Konkretisierung findet man in diesen eigentlich der Erklärung dienenden Sätzen vergeblich. Mit der Begründung stellt die Bundesregierung vielmehr klar, dass sogar rein formelle Aspekte, wie die Nennung im Gesellschaftervertrag, unabhängig von ihrer konkreten Ausgestaltung im Betrieb zu berücksichtigen sind und nicht nur rein materielle Aspekte wie Mitarbeiterzahl, Umsatz und Jahresbilanzsumme. Es ist zu erwarten, dass Unternehmen in Anbetracht dieser enormen Rechtsunsicherheit aus Sorge vor einer fehlerhaften Einordnung und der damit verbundenen Sanktionierungsgefahr tatsächlich vernachlässigbare Geschäftsbereiche eher in den Anwendungsbereich einbeziehen werden.

Unabhängig von den Problemen, die mit der Unbestimmtheit des § 28 Abs. 3 BSIG-E einhergehen, ist diese Bereichsausnahme nicht richtlinienkonform und damit europarechtswidrig. Der NIS-2-Richtlinie liegt ein formeller Einrichtungsbegriff zugrunde, vgl. Art. 6 Nr. 38 der NIS-2-Richtlinie. Für die Eröffnung des Anwendungsbereichs bei bestimmter Unternehmensgröße kommt es nach Art. 2 Abs. 1 der NIS-2-Richtlinie lediglich darauf an, ob die genannten Schwellenwerte durch die Einrichtung insgesamt erreicht bzw. überschritten werden, unabhängig von der konkreten Geschäftstätigkeit. Hinreichend große Unternehmen fallen damit auch dann unter die

NIS-2-Richtlinie, wenn sie nur einen untergeordneten Teil ihrer Tätigkeit in einem der relevanten Sektoren ausüben.

Abweichungen zur Anwendbarkeit des Gesetzes sieht die NIS-2-Richtlinie nach ihrem Erwägungsgrund 16 jedoch nur bei der Miteinbeziehung der Daten verbundener Unternehmen vor, wenn das betrachtete Unternehmen hinreichend unabhängig von seinem Partnerunternehmen ist. Das Abstellen auf einzelne Geschäftstätigkeiten innerhalb einer einzelnen Einrichtung befindet sich außerhalb des Anwendungsbereiches dieser vorgesehenen Einschränkungsmöglichkeit. Ein entsprechender Wille des europäischen Gesetzgebers, weitergehende Einschränkungen des Anwendungsbereichs der NIS-2-Richtlinie zu erlauben, ist nicht erkennbar. Der § 28 Abs. 3 BSIG-E läuft vielmehr dem Ziel der Richtlinie, ein umfassendes und mindestharmonisiertes IT-Sicherheitsniveau herzustellen, zuwider.

Die Europarechtswidrigkeit der Norm würde zunächst nichts an ihrer Anwendbarkeit ändern. Bis zu einer Entscheidung des EuGH können bekanntermaßen Jahre vergehen. Bis dahin können Unternehmen von der Bereichsausnahme Gebrauch machen - jedoch stets unter dem Vorbehalt, dass der § 28 Abs. 3 BSIG-E früher oder später aufgehoben wird. Neben der Rechtsunsicherheit durch die Formulierung der Vorschrift kommt also auch die Unsicherheit über die Beständigkeit der Norm hinzu.

Der Innenausschuss sollte vorschlagen, den § 28 Abs. 3 BSIG-E insgesamt aus dem Entwurf herauszunehmen.

III. Rückausnahme für Betreiber von Energieanlagen, § 28 Abs. 5 S. 4 BSIG-E

Analog zu § 28 Abs. 3 BSIG-E sieht § 28 Abs. 5 S. 4 BSIG-E vor, dass besonders wichtige oder wichtige Einrichtungen, bei denen der Betrieb einer Energieanlage im Hinblick auf die gesamte Geschäftstätigkeit dieser Einrichtung vernachlässigbar ist, nicht von der Ausnahmevorschrift des § 28 Abs. 5 S. 1 BSIG-E erfasst sind. Dieser bestimmt grundsätzlich die Nichtanwendbarkeit von verpflichtenden Vorschriften des BSIG-E für Energieanlagenbetreiber, die den Regelungen der §§ 5c bis 5e EnWG[-E] unterfallen.

§ 5c EnWG-E verpflichtet Betreiber einer Energieanlage, der als wichtige oder besonders wichtige Einrichtung i.S.d. § 28 Abs. 1, Abs. 2 BSIG-E gilt, und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und Datenverarbeitungssysteme zu gewährleisten.

Durch die Rückausnahme soll nach der Begründung zu § 28 Abs. 5 S. 4 BSIG-E sichergestellt werden, dass in den Fällen, in denen der Betrieb einer Energieanlage vernachlässigbar ist, das Unternehmen aber auch zu einer anderen relevanten Einrichtungsart zuzuordnen ist (z.B. im Sektor Wasser), die gesamte Geschäftstätigkeit der Einrichtung sich hinsichtlich der Regulierung nach diesem Hauptsektor (Wasser) richtet. Das wäre nach der Formulierung des § 28 Abs. 5 S. 4 BSIG-E aber rechtlich nicht zutreffend.

§ 5c Abs. 1 Nr. 2 EnWG-E adressiert den Betreiber einer Energieanlage, der (auch) als wichtige oder besonders wichtige Einrichtung i.S.d. § 28 Abs. 1, Abs. 2 BSIG-E gilt. Wenn der Betreiber der Energieanlage wegen seiner Geschäftstätigkeit in einem anderen Sektor als besonders wichtige oder wichtige Einrichtung i.S.d. BSIG-E einzuordnen ist, wird er dem Wortlaut des § 5c EnWG-E nach dennoch vom Anwendungsbereich der § 5c-5e EnWG-E adressiert. Im Fall dieser Überschneidungen sieht § 28 Abs. 5 S. 2, S. 3 BSIG-E grundsätzlich vor, dass hinsichtlich der Energieanlagen die §§ 5c-5e EnWG-E gelten und nicht die §§ 30 ff. BSIG-E, und dass hinsichtlich der weiteren kritischen Anlagen die §§ 30 ff. BSIG-E fortgelten.

Durch die Rückausnahme des § 28 Abs. 5 S. 4 BSIG-E findet der gesamte § 28 Abs. 5 BSIG-E keine Anwendung mehr. Das heißt, dass das Unternehmen insgesamt den §§ 30 ff. BSIG-E unterliegt. Gleichzeitig finden dem Wortlaut des § 5c Abs. 1 Nr. 2 EnWG-E nach die Vorschriften der §§ 5c-5e EnWG-E weiterhin Anwendung - der Wortlaut des § 5c Abs. 1 Nr. 2 EnWG-E differenziert schließlich nicht danach, ob die Einordnung als wichtige oder besonders wichtige Einrichtung an der Tätigkeit des Unternehmens im Energiesektor liegt.

Damit findet in diesem Fall eine Doppelregulierung statt, die § 28 Abs. 5 BSIG-E eigentlich zu verhindern sucht.

Zu lösen wäre dies, indem man dem § 5c Abs. 1 EnWG einen weiteren Satz beifügt, der bestimmt, dass in den Fällen des § 28 Abs. 5 S. 4 BSIG die §§ 5c-5e EnWG keine Anwendung finden.

Der Innenausschuss sollte vorschlagen, eine derartige Formulierung in das NIS2UmsG aufzunehmen, um dem Ziel des Gesetzgebers hinsichtlich § 28 Abs. 5 S. 4 BSIG-E zu entsprechen.

IV. Anwendungsbereich der Einrichtungen der Bundesverwaltung, § 29 Abs. 1 Nr. 3 BSIG-E

Zu begrüßen ist die Beibehaltung der weiteren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihrer Vereinigungen auf Bundesebene im Anwendungsbereich des BSIG-E über § 29 Abs. 1 Nr. 3 BSIG-E. Hiernach gelten diese Einrichtungen als Einrichtungen der Bundesverwaltung, wenn dies durch das BSI angeordnet wird. Die Einrichtungen der Bundesverwaltung unterfallen sodann den §§ 43 ff. BSIG-E. Eine gänzliche Herausnahme dieser Einrichtungen war aufgrund des Klammerzusatzes im Referentenentwurf noch zu befürchten.

Im Regierungsentwurf änderte sich jedoch, dass für die Anordnung des BSI nun ein Einvernehmen und damit die ausdrückliche Zustimmung des jeweils zuständigen Ressorts erforderlich ist. Im Referentenentwurf war noch ein Benehmen des jeweiligen Ressorts ausreichend, also die bloße Beteiligung am Entscheidungsprozess. Es ist zu hoffen, dass die jeweiligen Ressorts von ihrem damit entstandenen Vetorecht keinen umfassenden Gebrauch machen und damit die IT-Sicherheit von Institutionen der Bundesverwaltung unterminieren werden.

Der Innenausschuss sollte vorschlagen, das Einvernehmenserfordernis aus dem Normtext zu streichen oder beraten, welche Instrumente zur Verhinderung eines Missbrauchs der Vetomöglichkeit implementiert werden können.

V. IT-Sicherheitspflichten für Einrichtungen der Bundesverwaltung, §§ 29, 44 BSIG-E

Deutlich zu kritisieren ist auch die finale Aufnahme einer weiteren Ausnahme in § 29 Abs. 2 S. 2 BSIG-E. Hiernach ist die zentrale Pflicht zum Ergreifen von Risikomanagementmaßnahmen nach § 30 BSIG-E nicht auf die Einrichtungen der Bundesverwaltung anzuwenden, außer auf das Bundeskanzleramt und die Bundesministerien.

Der Innenausschuss sollte vorschlagen, auch die sonstigen Einrichtungen der Bundesverwaltung in Hinblick auf § 30 BSIG-E zu verpflichten.

Die IT-Sicherheitsanforderungen für Einrichtungen der Bundesverwaltung ergeben sich nun ausschließlich aus § 44 BSIG-E. Dieser bestimmt, dass alle Einrichtungen der Bundesverwaltung die jeweils geltenden Fassungen der Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards) als Mindestanforderungen erfüllen müssen. Diese werden von dem BSI im Benehmen mit den Ressorts und weiteren obersten Bundesbehörden festgelegt.

Das Bundeskanzleramt und die Bundesministerien müssen als zusätzliche Mindestanforderungen außerdem die BSI-Standards und das IT-Grundschutz-Kompendium des BSI (IT-Grundschutz) erfüllen. Mit der Umsetzung der Mindeststandards und des IT-Grundschutzes wird die Erfüllung der Vorgaben des § 30 grundsätzlich gewährleistet, § 44 Abs. 3 S. 1 BSIG-E. Der Referentenentwurf sah noch vor, dass sämtliche Einrichtungen der Bundesverwaltung auch die höheren Anforderungen des IT-Grundschutzes einhalten müssen.

Die Beschränkung des IT-Grundschutzes auf die Bundesministeriumsebene bei gleichzeitiger Nichtanwendbarkeit des § 30 BSIG-E auf sonstige Einrichtungen der Bundesverwaltung ist in Zeiten, in denen gerade Verwaltungseinrichtungen im Fokus von Cyberangriffen sind, irritierend. Zumal § 44 Abs. 3 S. 1 BSIG-E verdeutlicht, dass nur ein Umsetzen von Mindeststandards und IT-Grundschutz ein Äquivalent zu den Risikomanagementmaßnahmen nach § 30 BSIG-E darstellt, nicht die Erfüllung der Mindeststandards allein. Damit unterliegen Einrichtungen der Bundesverwaltung geringeren IT-Sicherheitspflichten als privatrechtliche wichtige und besonders

wichtige Einrichtungen, obwohl sie ihnen in Hinblick auf die Auswirkungen eines Cyberangriffs in nichts nahestehen - und obwohl die Bundesregierung das gegenwärtige Niveau der IT-Sicherheit in der Bundesverwaltung selbst als unzureichend bezeichnet.

Der Innenausschuss sollte daher vorschlagen, die Verpflichtung zur Einhaltung des IT-Grundschutzes auf sämtliche Einrichtungen der Bundesverwaltung auszuweiten.

Darüber hinaus sieht § 44 Abs. 1 S. 3 BSIG-E die Möglichkeit von Abweichungen von diesen Mindeststandards in sachlich gerechtfertigten Fällen vor, wie es auch gegenwärtig in § 8 Abs. 1 S. 2 BSIG zu finden ist. Die nicht weiter konkretisierte Möglichkeit, sogar von den unzureichenden Mindeststandards abzuweichen, ist als Einfallstor zum Unterlaufen eines dringend benötigten IT-Sicherheitsstandards in der Bundesverwaltung zu kritisieren.

Der Innenausschuss sollte darüber beraten, wie eine Verhinderung des Missbrauchs dieser Abweichungsmöglichkeit erreicht werden kann.

Ebenfalls kritikwürdig ist die Verlängerung der Nachweisfrist für Einrichtungen der Bundesverwaltung auf fünf Jahre nach dem Inkrafttreten des BSIG anstatt der im Referentenentwurf genannten drei Jahre, § 43 Abs. 1 BSIG-E. Hierdurch wird faktisch auch die Umsetzungsdauer ohne Grund in die Länge gezogen.

Der Innenausschuss sollte vorschlagen, die Nachweisfrist wieder auf drei Jahre zu verkürzen.

VI. Fazit

Bei legislaturübergreifender Betrachtung der vielen Gesetzesentwürfe zur nationalen Umsetzung der NIS-2-Richtlinie und der intensiven, wiederholten Befassung aller Stakeholder mit der Regelungsentwürfen ist es außerordentlich bedauernswert, noch immer Aufweichungen und Mängel in den Anwendungsregeln vorzufinden.

Der Innenausschuss sollte die dringend erforderlichen Nachbesserungen vorschlagen.