VOICE - Bundesverband der IT-Anwender e.V. | Invalidenstraße 91 | 10115 Berlin

per E-Mail

Bundesministerium des Innern
Referat CI 1
Alt-Moabit 140
10557 Berlin

VOICE
Bundesverband der IT-Anwender e.V.

Büro Berlin:
Invalidenstraße 91
10115 Berlin

Büro München:
Riedenburger Str. 2
81677 München

+49 (0) 30 20 84 9 64 70
voice-info@voice-ev.org
www.voice-ev.org

Berlin, den 02.07.2025

Kommentierung des Referentenentwurfs des BMI für ein NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Sehr geehrte Damen und Herren,

herzlichen Dank für die Gelegenheit zur Stellungnahme.
In der Anlage finden Sie die Hinweise unserer Mitglieder zum vorliegenden Referentenentwurf.

Unsere Mitgliedsunternehmen legen großen Wert auf eine praxistaugliche Umsetzung gesetzlicher Vorgaben. Vor diesem Hintergrund bitten wir nachdrücklich darum, Dokumentationspflichten und Meldeverfahren so weit wie möglich zu verschlanken. Insbesondere international tätige Unternehmen berichten, dass sie Meldungen und Nachweise in jedem EU-Mitgliedstaat einzeln und in der jeweiligen Landessprache bereitstellen müssen – ein erheblicher Aufwand.

Wir würden uns freuen, wenn unsere Anmerkungen Berücksichtigung finden, und stehen für Rückfragen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Digital unterschrieben von Robin Kaufmann
Datum: 2025.07.04 00:32:01 +02'00'

Robin Kaufmann
Geschäftsführer VOICE – Bundesverband der IT-Anwender e.V.

Bankverbindung:
Deutsche Bank Privat- und Geschäftskunden AG
BIC: DEUTDEBBXXX IBAN: DE03 1007 0000 0299 0992 00

Geschäftsführer: Robin Kaufmann
Vorsitzende des Präsidiums: Dr. Bettina Uhlich
VR 31149B AG Charlottenburg
USt-Id Nr.: DE 281638339

Stellungnahme zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
(Stand: 23.6.2025)

Der Referentenentwurf ist gegenüber der Fassung vom Herbst 2024 weitgehend unverändert. Artikel 1 beschreibt nach wie vor die umfangreichen Rechte und Pflichten des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Rahmen des BSI-Gesetzes (BSIG). Die notwendigen Anpassungen und Erweiterungen des IT-Sicherheitsgesetzes 2.0 (IT-SIG 2.0) ergeben sich aus der europäischen NIS2-Richtlinie.

Ergänzend werden kleinere Korrekturen und Anpassungen an den damit verbundenen gesetzlichen Rahmenbedingungen vorgenommen, wie in den folgenden Kapiteln näher ausgeführt.

Fragen und Aspekte, die ausschließlich den Bund betreffen, werden in dieser Stellungnahme nicht behandelt.

Anmerkungen zu einzelnen Kapiteln bzw. Abschnitten

Übernahme der Mindestsicherheitsanforderungen gemäß Artikel 21 Absatz 2 der NIS-Verordnung

Die Ausdifferenzierung der Maßnahmen nach dem Prinzip der Verhältnismäßigkeit führt in der Praxis – insbesondere bei kleinen und mittleren Unternehmen (KMU) – zu erheblicher Unsicherheit hinsichtlich des tatsächlich erforderlichen Erfüllungsaufwands.

Hilfreich wäre hier eine zeitnahe begleitende Stellungnahme oder eine praxisorientierte Erläuterung im Sinne einer Best Practice – idealerweise in kompakter Form im Rahmen des geplanten neuen BSI-Grundschutzes.

Die DVO (EU) 2024/2690 sowie die „Implementing Guidelines“ der ENISA bieten hierfür eine gute Grundlage und sollten im Gesetz oder in einem Anhang ausdrücklich referenziert werden.

Verantwortung der Geschäftsleitung

Die Thematik wird an mehreren Stellen im Entwurf adressiert. In Teil 1, § 2 Punkt 13 erfolgt zunächst die Definition der Geschäftsleitung. Unklar bleibt dabei, auf welches Gesetz sich die Ausnahme für „Leiterinnen und Leiter der Bundesverwaltung nach § 29“ bezieht – diese gelten demnach nicht als Geschäftsleitung.

Welche praktischen Konsequenzen ergeben sich aus dieser Ungleichbehandlung? Insbesondere stellt sich die Frage, ob für öffentliche Einrichtungen des Bundes somit keine persönliche Haftung greift.

Ergänzend dazu wird in Teil 3, Kapitel 1, § 38 die Umsetzungs-, Überwachungs- und Schulungspflicht der Geschäftsleitung geregelt. Dieser Abschnitt ist im Hinblick auf mögliche persönliche Haftung besonders relevant.

Bankverbindung:
Deutsche Bank Privat- und Geschäftskunden AG
BIC: DEUTDEBBXXX IBAN: DE03 1007 0000 0299 0992 00

Geschäftsführer: Robin Kaufmann
Vorsitzende des Präsidiums: Dr. Bettina Uhlich
VR 31149B AG Charlottenburg
USt-Id Nr.: DE 281638339

Ob jedoch eine vierstündige Schulung tatsächlich ausreicht, um die Geschäftsleitung in die Lage zu versetzen, ihre Pflichten angemessen zu erfüllen, erscheint fraglich. Eine verbindliche Darstellung der Inhalte und Anforderungen einer solchen Schulung wäre daher wünschenswert.

Teil 2, Kapitel 1, §3 – Aufgaben des Bundesamtes bzw. §6 Informationsaustausch

Aus unserer Sicht ist es entscheidend, dass die weitere Vorgehensweise klar kommuniziert wird – insbesondere im Hinblick auf die technische Verfügbarkeit einer entsprechenden Lösung, etwa einer zentralen Online-Plattform zur Erfüllung der Melde- und Nachweispflichten.

Teil 2, Kapitel 1 §15 – Detektion von Angriffsmethoden und von Sicherheitsrisken für die IT- und Netzsicherheit

Welcher Umgang ist konkret geplant?

Schwachstellen, die über einen längeren Zeitraum im Internet sichtbar bleiben, können als fahrlässiger Umgang mit IT-Sicherheitsrisiken gewertet werden. In diesem Zusammenhang stellt sich die Frage, wie mit Fällen umgegangen wird, in denen besonders wichtige oder kritische Einrichtungen nur geringe oder unzureichende Prüftätigkeiten nachweisen können.

Kann dies künftig als Anlass für vertiefte Untersuchungen oder gar Sanktionen dienen?

Zudem wird im Entwurf mehrfach auf den „Stand der Technik“ verwiesen, insbesondere im Hinblick auf geeignete Schutzmaßnahmen. Welche konkreten Veröffentlichungen und anerkannten Standards werden hier zur Auslegung des Standes der Technik herangezogen (z. B. BSI-Empfehlungen, DIN-Normen, ISO-Standards)?

Eine Klarstellung wäre aus Sicht der Praxis wünschenswert, um Rechtssicherheit für die verpflichteten Unternehmen zu schaffen.

Teil 3, Sicherheit in der Informationstechnik von Einrichtungen

Verwendung von Produkten mit Sicherheitszertifizierungen

Die verpflichtende Nutzung von Produkten mit Sicherheitszertifizierungen ist grundsätzlich zu begrüßen. Allerdings sollte zwingend eine realistische Übergangsfrist vorgesehen werden. In vielen Bereichen stehen derzeit noch keine entsprechend zertifizierten Produkte oder Dienstleistungen zur Verfügung – insbesondere für bestimmte Branchenlösungen oder Spezialanwendungen.

Ohne eine solche Frist drohen praxisferne Anforderungen, die Unternehmen faktisch nicht erfüllen können. Eine stufenweise Einführung oder Übergangsregelung wäre hier sinnvoll und notwendig.

Bankverbindung:
Deutsche Bank Privat- und Geschäftskunden AG
BIC: DEUTDEBBXXX IBAN: DE03 1007 0000 0299 0992 00

Geschäftsführer: Robin Kaufmann
Vorsitzende des Präsidiums: Dr. Bettina Uhlich
VR 31149B AG Charlottenburg
USt-Id Nr.: DE 281638339

Teil 5, Zertifizierung, Konformitätserklärung und Kennzeichen

Unklarheiten bei notwendigen Produktzertifizierungen - die Verpflichtung, in kritischen Bereichen ausschließlich zertifizierte Produkte und Dienstleistungen einzusetzen, wirft erhebliche praktische Fragen auf – insbesondere dann, wenn entsprechende zertifizierte Angebote am Markt noch nicht verfügbar sind. Für betroffene Unternehmen stellt sich die Frage nach einer realistischen und rechtssicheren Übergangslösung.

Zudem besteht die Gefahr von Lock-in-Effekten und Marktverzerrungen: Einzelne Anbieter könnten ihre Marktmacht ausnutzen, indem sie nur überteuerte Lizenzmodelle oder Produkt-Bundles mit Zertifizierung anbieten. Dies würde den Wettbewerb einschränken und insbesondere kleinere Anbieter und Anwenderunternehmen benachteiligen.

Eine klare Regelung zur Übergangsphase sowie flankierende Maßnahmen zur Vermeidung marktbeherrschender Strukturen sind daher aus unserer Sicht dringend erforderlich.

Teil 6, §56 – Ermächtigung zum Erlass von Rechtsverordnungen, Absatz 4

Bestimmung kritischer Dienste und kritischer Anlagen - die Kriterien zur Einstufung kritischer Dienste und Anlagen bleiben im Entwurf teilweise unklar. Eine beispielhafte Auflistung oder Beschreibung im Anhang – differenziert nach Branchen – wäre hilfreich, um Unternehmen mehr Orientierung zu geben.

Zudem stellt sich die Frage: Wie genau werden betroffene Unternehmen über ihre Einstufung informiert? Betrifft dies ausschließlich Unternehmen, die bereits unter die KRITIS-Regulierung fallen, oder sind auch andere Organisationen erfasst, etwa durch die Ausweitung im Rahmen der NIS2-Umsetzung?

Eine frühzeitige und verbindliche Kommunikation der Einstufungskriterien sowie der betroffenen Unternehmen ist aus Sicht der Praxis unerlässlich.

Begründung, Allgemeiner Teil, Pkt. 3 Haushaltsaufgaben

Bei den dargestellten Haushaltsansätzen fehlt es an Transparenz in Bezug auf die zugrunde liegenden Kostenarten. Eine nachvollziehbare Aufschlüsselung ist nicht erkennbar.

Für eine fundierte Bewertung wäre eine detaillierte Darstellung der einzelnen Kostenarten sowie deren jeweilige Begründung notwendig. Nur so lässt sich die Angemessenheit und Verhältnismäßigkeit der vorgesehenen Mittel beurteilen.

Begründung, Allgemeiner Teil, Pkt. 4. Erfüllungsaufwand für die Wirtschaft

Die im Entwurf angegebene Erhöhung des jährlichen Erfüllungsaufwands für die Wirtschaft ist aus Sicht der Praxis kaum nachvollziehbar und tendenziell deutlich zu niedrig angesetzt. Die angenommenen durchschnittlichen Mehrkosten von 76.000 Euro pro Unternehmen und Jahr (basierend auf 2,3 Mrd. Euro Gesamtkosten und 30.000 betroffenen Unternehmen) erscheinen unrealistisch.

Bankverbindung:
Deutsche Bank Privat- und Geschäftskunden AG
BIC: DEUTDEBBXXX IBAN: DE03 1007 0000 0299 0992 00

Geschäftsführer: Robin Kaufmann
Vorsitzende des Präsidiums: Dr. Bettina Uhlich
VR 31149B AG Charlottenburg
USt-Id Nr.: DE 281638339

Schon bei Unternehmen mit rund 500 Mitarbeitenden liegen allein die Kosten für Managed Service Provider-Leistungen (MSP) in vielen Fällen deutlich über diesem Betrag. Auch die zugrunde gelegten Personalkosten für externe Zukaufleistungen weichen erheblich von marktüblichen Konditionen ab.

Zudem bleiben wichtige Kostenfaktoren unberücksichtigt:

- Neue Technologiekomponenten (z. B. SIEM, XDR, Zero Trust, IAM)
- Indirekte Kosten innerhalb der Lieferkette
- Wechselwirkungen mit anderen regulatorischen Anforderungen wie dem Cyber Resilience Act (CRA)
- Langfristige SaaS-Abhängigkeiten mit potenziell jährlich steigenden Kosten

Das ENISA-Dokument *„NIS-Investments 2024“* zeigt eine deutlich realistischere Kostenstruktur auf und macht zugleich auf das insgesamt noch niedrige Investitionsniveau im Bereich Cybersicherheit in Europa aufmerksam.

(https://www.enisa.europa.eu/publications/nis-investments-2024)

Viele Security-Produktkategorien sind heute nur noch als SaaS verfügbar. Daraus ergeben sich dauerhafte Lizenzkosten und Abhängigkeiten, die Fragen der digitalen Souveränität und Kostenkontrolle aufwerfen – insbesondere bei fehlenden europäischen Alternativen.

Die Aussage auf Seite 122 des Entwurfs, „es ist nicht klar, wer zur Geschäftsleitung zählt“, ist nicht nachvollziehbar. In anderen Gesetzen ist diese Frage eindeutig geregelt (z. B. Vorstand, Geschäftsführung, Aufsichtsrat). Eine Klarstellung im Gesetzestext ist dringend erforderlich, um Rechtsunsicherheit und persönliche Haftungsfragen zu vermeiden.

Im Entwurf wird angeführt, dass nur 17 % der Unternehmen bislang ausreichende Investitionen im Bereich Cybersicherheit getätigt haben. Dies steht im klaren Widerspruch zur Annahme eines relativ geringen Mehraufwands und unterstreicht die Notwendigkeit, die tatsächliche Investitionslücke realistisch abzubilden.

Keine Erfüllungspflicht für Kommunen

Die getroffenen Aussagen zur Rolle kommunaler Akteure sind nicht nachvollziehbar. Insbesondere Kommunen erbringen bereits heute substanzielle Vorleistungen für den Ausbau kritischer Infrastrukturen – beispielsweise durch die Verlegung von Lichtwellenleitern im Rahmen von Tiefbaumaßnahmen.

Diese Beiträge sollten im Gesetzesentwurf ausdrücklich anerkannt und bei der weiteren Ausgestaltung berücksichtigt werden – auch im Hinblick auf Förderlogiken, Zuständigkeiten und Kooperationsmodelle.

Abschnitt Kommentare:

Der Aussage, es entstünden „keine Kosten auf Länder- und Kommunenebene“, ist entschieden zu widersprechen. Die Realität zeigt ein anderes Bild: Schadensfälle der vergangenen Jahre – etwa durch Ransomware-Angriffe auf kommunale Verwaltungen –

Bankverbindung:
Deutsche Bank Privat- und Geschäftskunden AG
BIC: DEUTDEBBXXX IBAN: DE03 1007 0000 0299 0992 00

Geschäftsführer: Robin Kaufmann
Vorsitzende des Präsidiums: Dr. Bettina Uhlich
VR 31149B AG Charlottenburg
USt-Id Nr.: DE 281638339

belegen eindrücklich die erheblichen finanziellen und organisatorischen Folgen unzureichender Sicherheitsmaßnahmen.

Hinzu kommen Opportunitätskosten, etwa durch Ausfallzeiten, Wiederherstellungsaufwand, Reputationsschäden oder verschobene Digitalisierungsprojekte. Diese indirekten, aber realen Kosten dürfen nicht ignoriert werden.

Eine realistische Einschätzung der Kostenbelastung auf Länder- und Kommunalebene ist daher unerlässlich, um angemessene Maßnahmen, Ressourcen und Förderprogramme ableiten zu können.

Nachweispflicht bei nur 24 Unternehmen

Die bisherigen Erfahrungen zeigen deutlich: Ohne wirksame Kontrolle und Durchsetzung führen gesetzliche Vorgaben häufig nicht zu einer proaktiven Umsetzung in den Unternehmen.

Ein höheres Maß an regelmäßigen und risikobasierten Überprüfungen würde nicht nur die Umsetzung deutlich verbessern, sondern auch helfen, potenzielle Schadensfälle frühzeitig zu verhindern. Dies wäre nicht nur im Interesse der betroffenen Unternehmen, sondern volkswirtschaftlich insgesamt sinnvoll und nachhaltig.

Weitere Anmerkungen / Fragestellungen:

Generelle Hinweise zur Gesetzesumsetzung und Verzahnung

- Zeitgleiche Umsetzung weiterer gesetzlicher Regelungen:
  Es ist unklar, ob und wie die geplanten Anpassungen zeitlich mit anderen relevanten Gesetzesinitiativen abgestimmt werden. Eine parallele Umsetzung ist aus Sicht der Unternehmen wichtig, um Widersprüche, Doppelregulierungen und Unsicherheiten zu vermeiden.

- Abhängigkeiten mit weiteren Regelwerken:
  Die wechselseitigen Abhängigkeiten zu anderen Gesetzen – etwa dem Cyber Resilience Act (CRA), dem KRITIS-Dachgesetz oder bestehenden Sicherheitsvorgaben – müssen transparent dargestellt und harmonisiert werden. Andernfalls droht ein unkoordinierter Regulierungsrahmen mit erheblichem Mehraufwand für Unternehmen.

- B3S-Standards und Mindestanforderungen:
  Es wäre sehr hilfreich, wenn branchenbezogene Sicherheitsstandards (B3S) sowie konkrete Mindestanforderungen aktiv durch Behörden veröffentlicht und regelmäßig aktualisiert würden – idealerweise mit beispielhaften Umsetzungshilfen. Dies würde zur Rechtssicherheit beitragen und insbesondere KMU bei der Umsetzung unterstützen.

Nicht funktionierende Links im Dokument an mehreren Stellen (Beispiel):

Bankverbindung:
Deutsche Bank Privat- und Geschäftskunden AG
BIC: DEUTDEBBXXX IBAN: DE03 1007 0000 0299 0992 00

Geschäftsführer: Robin Kaufmann
Vorsitzende des Präsidiums: Dr. Bettina Uhlich
VR 31149B AG Charlottenburg
USt-Id Nr.: DE 281638339

tenfreie Angebote, die es bereits heute gibt, zurückgegriffen wird (vgl. BSI, IT-Grundschutz-Schulungen, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/it-grundschutzschulung_node.html). Unter den dargestellten Annahmen entsteht bei einem Lohnsatz von 37,10 Euro je Stunde (Lohnkosten der Gesamtwirt-

Zur weiteren Information fügen wir Ausschnitte aus der bereits erfolgten ersten Stellungnahme von 2024 hinzu:

Teil2 – Kapitel 2 - §30 bis §38

Diese Abschnitte beinhalten die meisten allgemeingültigen Regelungen und sind insbesondere bereits vor Inkraftsetzung des NIS2 Gesetzes entsprechend zu betrachten, um kurzfristige und hoch zu priorisierende Maßnahmen abzuleiten.

Nachfolgend werden nur einige Beispiel (Überschriften) angeführt:

Diese Punkte falle auch klar in den Verantwortungsbereich der Geschäftsführung, um ein entsprechendes Programm aufzusetzen, die Zuständigkeiten zu regeln und eine wirksame Überwachung der Maßnahmenumsetzung zu gewährleisten!

- Konzepte in Bezug auf Risikoanalyse und die Informationssicherheit; in der Praxis erfordert dies jedoch die Vorbereitung und Umsetzung verschiedener Prozesse, Richtlinien und den Einsatz entsprechender Tools (Managementkomponenten gemäß COBIT)
- Die Bewältigung von Sicherheitsvorfällen setzt einen Überblick über kritische Assets und Services (BIA – Business Impact Analyse), entsprechende Notfall- und BCM (Business Continuity Pläne), klare Verantwortungen und ausreichend Ressourcen sowie auch Übungen voraus, die insbesondere in vielen kleineren Mittelstandsunternehmen noch nicht immer gegeben sind.
- Bei der Sicherheit der Lieferkette fehlt in Deutschland ein einheitlicher und anerkannter Mindeststandard. Dies führt für viele Unternehmen zu offenen Fragestellungen zu einer konkreten Vorgehensweise. Ein möglicher Ansatz ist hier die Orientierung an in anderen Ländern bereits festgelegten Mindeststandards (z.B. Cyber Risk Rating in Österreich). Vergleichbare Ansätze in Deutschland werden vor allem durch größere Unternehmen durch die Orientierung an anderen Standards abgebildet (z.B. Auszüge „Cloud Security Alliance““ oder „VdS10000“). Diese wurden jedoch aus anderen Gesichtspunkten ursprünglich erstellt und fokussieren zu wenig auf einen in der Praxis auch leistbaren Umfang!
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Informationstechnik. Es sind entsprechende Regelungen und Prozesse in Abstimmung mit anderen Unternehmensbereichen (Recht, Einkauf) zu gestalten. Indirekt ergeben sich große Auswirkungen auf Themenstellungen wie „Produkte mit digitalen Komponenten“ => CRA oder Herausforderungen durch die verstärkte IT/OT Integration – z.B. Fernwartung von Komponenten, Verpflichtungen zu Sicherheitsupdates usw.
- Grundlegende Verfahren im Bereich der Cyberhygiene; während hier einige Aspekte auch klar bereits im Gesetzesentwurf geregelt sind (z.B. Backup / Recovery) sind

Bankverbindung:
Deutsche Bank Privat- und Geschäftskunden AG
BIC: DEUTDEBBXXX IBAN: DE03 1007 0000 0299 0992 00

Geschäftsführer: Robin Kaufmann
Vorsitzende des Präsidiums: Dr. Bettina Uhlich
VR 31149B AG Charlottenburg
USt-Id Nr.: DE 281638339

andere Bereiche nur allgemein definiert und risikobasiert zu betrachten. Wenn man die weiterführenden Informationen von BSI-Dokumenten (z.B. Handreichungen, Stand der Technik usw.) betrachtet, ergibt sich eine mögliche Konkretisierung. Die Umsetzung dieser Maßnahmen wird in vielen Unternehmen in priorisierter Reihenfolge durch mehrjährige Programme erfolgen müssen (auch wegen Ressourcenrestriktionen).

- Weitere Punkte wie Kryptographie und Multi-Faktor-Authentifizierung sind ebenfalls entsprechend umzusetzen
- Schulung der Geschäftsführung. Hier zeichnet sich ein Mindestumfang von 4 bis 8 Stunden ab. Naturgemäß kann dies nur ein rascher Überblick sein, der in Zukunft zu verschiedenen Themen zu vertiefen ist. Besonderes Augenmerk muss auch auf die technologische Entwicklung wie Cloud Computing oder AI (Artificial Intelligence) und ständig umfangreichere Complianceanforderungen gelegt werden. Diese führen zu neuen Risikobereichen und einer ständigen Vergrößerung der Angriffsoberflächen!

Bankverbindung:
Deutsche Bank Privat- und Geschäftskunden AG
BIC: DEUTDEBBXXX IBAN: DE03 1007 0000 0299 0992 00

Geschäftsführer: Robin Kaufmann
Vorsitzende des Präsidiums: Dr. Bettina Uhlich
VR 31149B AG Charlottenburg
USt-Id Nr.: DE 281638339