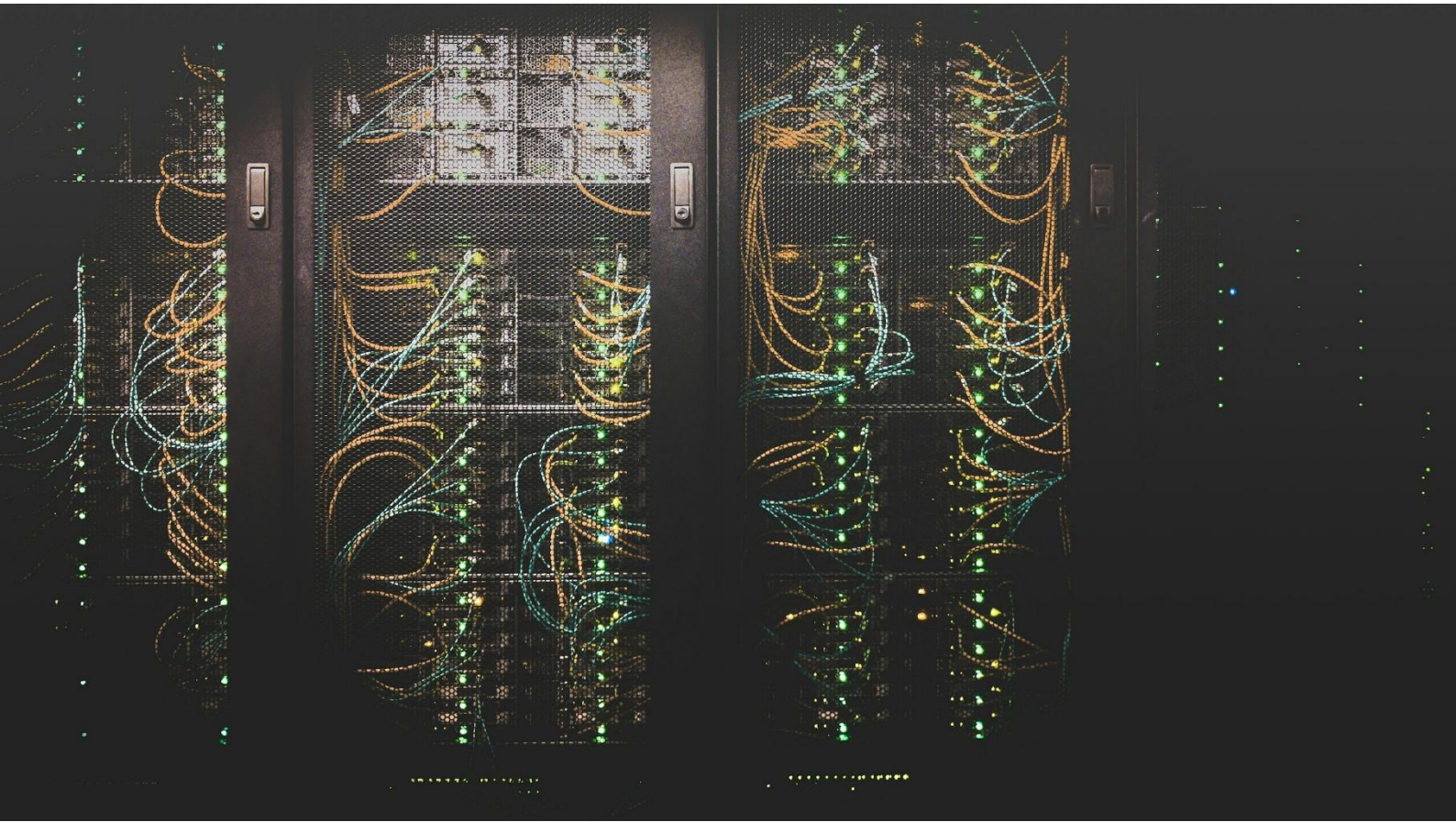
TÜV VERBAND

Berlin
2. Juli 2025

Stellungnahme

zum Referentenentwurf zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheits-managements in der Bundesverwaltung (NIS2UmsuCG)

vom 23.06.2025



Kernforderungen

1. **Unternehmen ganzheitlich betrachten**
   § 28 (3) BSIG-E erlaubt Unternehmen, sich bei der Feststellung der Art von Einrichtungen auf Unternehmensteile zu beschränken. In der NIS-2-Richtlinie ist dies nicht vorgesehen und sie erfordert zudem eine ganzheitliche Betrachtung.

2. **Nachweispflichten ausweiten**
   Der TÜV-Verband kritisiert, dass § 39 BSIG-E nur stichprobenartige Nachweise für „besonders wichtige" Einrichtungen vorsieht und fordert regelmäßige Nachweise und gezielte Überprüfungen.

3. **Nachweiszyklen auf zwei Jahre festlegen**
   Die Verlängerung des Nachweiszyklus auf drei Jahre betrachtet der TÜV-Verband als unangemessen.

4. **Mindestmaßnahmen im Risikomanagement definieren**
   Der TÜV-Verband empfiehlt deshalb, die Mindestmaßnahmen im Gesetzestext so zu konkretisieren, dass die mit dem ehemals verwendeten Begriff der „Cyberhygiene" verbundenen grundlegenden Sicherheitspraktiken verpflichtend verankert bleiben.

5. **Aufsichts- und Durchsetzungsmaßnahmen stärken**
   Der TÜV-Verband bemängelt die eingeschränkte Handlungsfähigkeit des BSI in § 61 BSIG-E und fordert die Wiedereinführung der Benennung eines Überwachungsbeauftragten.

6. **Vertrauen schaffen durch akkreditierte unabhängige Zertifizierungsstellen**
   Der TÜV-Verband fordert verbindliche Zertifizierungen durch qualifizierte Drittstellen, um Vertrauen in die Umsetzung von Cybersicherheitsanforderungen zu schaffen.

7. **Praxishilfe zur Absicherung der Lieferkette**
   Der TÜV-Verband fordert detaillierte Handreichungen zur Gestaltung der Maßnahmen zur Absicherung der Lieferkette, um betriebswirtschaftliche Erwägungen und Interpretationsspielräume zu klären.

8. **Regulatorische Konsistenz herstellen**
   Die Änderungen bei den Mindestmaßnahmen zum Risikomanagement gemäß § 30 (2) BSIG-E sollten im § 5c (4) EnWG-E entsprechend angeglichen werden.

Stellungnahme zum NIS2UmsuCG

Referentenentwurf vom 23.06.2025

Am 24.06.2025 hat das Bundesministerium des Innern und für Heimat (BMI) einen aktualisierten Referentenentwurf zur Umsetzung der NIS-2-Richtlinie in Deutschland vorgelegt. Der TÜV-Verband begrüßt das mit dem NIS-2-Umsetzungsgesetz verbundene Ziel, die Resilienz der digitalen Infrastruktur in Deutschland und Europa zu stärken. Die Notwendigkeit dazu trifft auf große Zustimmung - gemäß der im Sommer 2025 vom TÜV-Verband gemeinsam mit dem BSI veröffentlichten Cybersecurity-Studie sprechen sich auch 56% der befragten Unternehmen für verbindliche Vorgaben zur Cybersicherheit aus.

Der Verband dankt für die Gelegenheit, hierzu Stellung zu nehmen, und möchte folgende Punkte kommentieren:

Einschränkung auf Unternehmensteile

Der TÜV-Verband begrüßt zwar, dass der aktuelle Entwurf die frühere Möglichkeit streicht, durch Herausrechnen von Unternehmensteilen unter die Schwellenwerte der NIS-2-Richtlinie zu fallen. Allerdings wirft die neu eingeführte Ausnahme für „vernachlässigbare" Geschäftstätigkeiten erhebliche Fragen auf. Der Begriff ist unbestimmt und wird im Gesetz nicht näher definiert. Es bleibt unklar, nach welchen Kriterien eine Tätigkeit als vernachlässigbar gelten soll – etwa Umsatz, Personalaufwand oder andere Faktoren. Ohne präzise Vorgaben besteht die Gefahr uneinheitlicher Auslegung und einer Rechtsunsicherheit für Unternehmen. Zudem könnte diese nationale Sonderregelung zu einem faktischen Ausschluss regulierungspflichtiger Tätigkeiten führen, die nach den Vorgaben der NIS-2-Richtlinie eigentlich erfasst sein sollten. Der TÜV-Verband sieht daher die Gefahr, dass der deutsche Gesetzgeber mit dieser Öffnungsklausel vom europarechtlich vorgegebenen Mindestharmonisierungsziel abweicht und fordert eine eindeutige, klar nachvollziehbare und EU-rechtskonforme Ausgestaltung dieser Ausnahme.

Nachweispflichten

Im vorgelegten Diskussionspapier zum NIS2UmsuCG sind in § 39 BSIG-E Nachweispflichten nur für Betreiber von kritischen Anlagen vorgesehen. Damit ist keine regelmäßige Nachweispflicht zumindest für

„besonders wichtige" Einrichtungen vorgesehen, auch wenn das BSI entsprechende Nachweise gemäß § 61 (3) BSIG-E von „besonders wichtigen" Einrichtungen verlangen kann. Somit bleibt diese Nachweispflicht in der Praxis eine Einzelfallanordnung im Rahmen von Stichproben.

Der TÜV-Verband sieht hier eine Abweichung von der Intention der NIS-2-Richtlinie. In der NIS-2-Richtlinie wird in Artikel 32 „Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf „besonders wichtige Einrichtungen", Absatz (2) Punkt b) gefordert, dass Mitgliedsstaaten sicherstellen, dass zuständige Behörden befugt sind, folgende Maßnahmen umzusetzen: „(...) regelmäßige und gezielte Sicherheitsprüfungen, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden." Als TÜV-Verband sehen wir den Ansatz von „regelmäßigen und gezielten Sicherheitsprüfungen" im vorliegenden Diskussionspapier noch nicht konsequent verankert.

Auf Seite 123 des Referentenentwurfs wird geschätzt, „dass das BSI pro Jahr von rund 24 (besonders) wichtigen Einrichtungen Nachweise verlangen wird." Bezogen auf die geschätzt 8.250 besonders wichtigen Einrichtungen ist das ein jährlicher Anteil von nicht einmal 0,3%. Diese Stichprobe ist offensichtlich viel zu gering. Die NIS2-Richtlinie fordert in Artikel 32 Absatz (1), dass Aufsichts- und Durchsetzungsmaßnahmen „wirksam, verhältnismäßig und abschreckend" sein sollen.

Weiterhin gibt der TÜV-Verband aus der Erfahrung seiner Mitglieder und vieler sektorübergreifender Prüfungen zu Bedenken, dass erst durch regelmäßige Prüfungen sichergestellt wird, dass rechtliche Anforderungen auch vollumfänglich umgesetzt werden. Deshalb regt der Verband an, regelmäßige Nachweisprüfungen verbindlich vorzusehen. Weiterhin ist es zwingend notwendig, eine regelmäßige Nachweispflicht nicht nur für Betreiber kritischer Anlagen zu fordern, sondern diese auch für „besonders wichtige Einrichtungen" vorzusehen.

Verlängerung des Nachweiszyklus

Im vorgelegten Diskussionspapier zum NIS2UmsuCG sind in § 39 BSIG-E Nachweispflichten geregelt. Darin ist vorgesehen, dass betroffene Unternehmen (derzeit nur Betreiber kritischer Einrichtungen) alle drei Jahre einen Prüfnachweis vorlegen müssen. Im Vergleich zur gegenwärtigen Regulierung nach IT-SiG 2.0 ist das eine Verlängerung des Nachweiszyklus um ein Jahr. Diese Verlängerung des Nachweiszyklus auf drei Jahre sieht der TÜV-Verband aufgrund der dynamischen Entwicklung im Bereich der Cybersicherheit als nicht sachgerecht an.

Mindestmaßnahmen im Risikomanagement konkretisieren

Im aktuellen Entwurf wurde der Begriff „Cyberhygiene" aus den Mindestmaßnahmen zum Risikomanagement gemäß § 30 Absatz 2 BSIG-E gestrichen. Zwar war dieser Begriff bislang nicht

eindeutig definiert und inhaltlich scharf konturiert, dennoch stellte er eine wichtige Klammer für grundlegende, präventive Sicherheitsmaßnahmen dar. Die ENISA verbindet auf ihrer Webseite damit zum Beispiel Maßnahmen den Einsatz von starken Passwörtern, Zwei-Faktor-Authentifizierung, regelmäßigen Software-Updates, Vorsicht beim Öffnen von E-Mails und Links, Datensicherungen, sicheren WLAN-Netzwerken, Antiviren- und Anti-Malware-Software, Weiterbildung und Sensibilisierung, Zurückhaltung beim Teilen persönlicher Informationen sowie Überwachung von Konten und Geräten.

Mit dem ersatzlosen Wegfall dieser Anforderung droht eine Absenkung des Schutzniveaus gegenüber den Vorgaben der NIS-2-Richtlinie. Der TÜV-Verband empfiehlt deshalb, die Mindestmaßnahmen im Gesetzestext so zu konkretisieren, dass diese grundlegende Sicherheitspraktiken verpflichtend verankert bleiben und Unternehmen eine klare Orientierung erhalten.

Aufsichts- und Durchsetzungsmaßnahmen

In § 61 BSIG-E sind die Aufsichts- und Durchsetzungsmaßnahmen des BSI dargestellt. Aus Sicht des TÜV-Verbands wurde die Handlungsfähigkeit des BSI hier eingeschränkt, da einige Maßnahmen nur noch im Benehmen mit der jeweils zuständigen Aufsichtsbehörde verhängt werden können bzw. nur durch die jeweils zuständige Aufsichtsbehörde selbst. Der TÜV-Verband sieht hier die Gefahr, dass es dem BSI somit durch notwendige Abstimmungsprozesse und bürokratische Hürden zusätzlich erschwert wird, diese Maßnahmen in der Praxis effizient und wirkungsvoll durchzusetzen.

Darüber hinaus ist für den TÜV-Verband nicht nachvollziehbar, weshalb die Notwendigkeit für die Maßnahme zur Benennung eines Überwachungsbeauftragten im vorliegenden Entwurf nicht gesehen wird. Diese Maßnahme war im bereits zuvor kommentierten Diskussionspapier des BMI vorgesehen und wird in Artikel 32 Absatz (4) Buchstabe g der NIS2-Richtlinie explizit gefordert. Deshalb empfiehlt der TÜV-Verband eindringlich, diese Maßnahmen im Gesetzentwurf wiederaufzunehmen.

Einvernehmen der BNetzA mit dem BSI

Betreiber von Energieanlagen werden im Referentenentwurf u.a. im Rahmen des neuen § 5c EnWG-E reguliert. Positiv bewertet der TÜV-Verband die Anpassung im neuen § 5c EnWG-E, wonach die Bundesnetzagentur zukünftige IT-Sicherheitskataloge nur noch im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik erlassen darf. Diese Änderung stärkt die Rolle des BSI im Energiesektor erheblich und stellt sicher, dass die notwendige sicherheitstechnische Expertise bei der Festlegung branchenspezifischer Anforderungen verbindlich einfließt.

Vertrauen schaffen durch akkreditierte unabhängige Zertifizierungsstellen

Nur bei Einbindung unabhängiger Dritter ist aus Sicht des TÜV-Verbands sichergestellt, dass das notwendige Vertrauen in die Umsetzung von Cybersicherheitsanforderungen geschaffen werden kann. Deshalb regt der TÜV-Verband an, Zertifizierungen durch akkreditierte und unabhängige Konformitätsbewertungsstellen verbindlich in dem Prozess der Nachweiserbringung (§ 39 BSIG-E) durch die Hersteller vorzusehen.

Absicherung der Lieferkette

Mit Blick auf die weitgefassten Formulierungen zur Absicherung der Lieferkette ist es erforderlich den Unternehmen eine Handreichung und Orientierungshilfe zur Gestaltungstiefe der Maßnahmen zur Absicherung der Lieferkette an die Hand zu geben. In diesem Sinne ist beispielsweise die Forderung „Security by Design" recht vage und bedarf weiterer Detaillierungen. Eine Orientierungshilfe kann sowohl Mindestmaßnahmen aufzeigen als auch Interpretations- und Auslegungsspielräume reduzieren und leistet somit einen Beitrag zur Erhöhung der Klarheit und Handlungssicherheit der Verpflichteten.

Klarstellungen zur Interessensabwägung bei den Unterrichtungspflichten

Der TÜV-Verband empfiehlt, den letzten Satz in § 35 Absatz 2 deutlicher zu fassen und damit für mehr Rechtssicherheit und Transparenz bei den betroffenen Einrichtungen zu sorgen. Insbesondere sollte eindeutig beschrieben werden, welche Interessen hier als „berechtigt" anerkannt werden können. Dazu gehört auch die Frage, ob potenzielle Imageschäden und damit verbundene finanzielle Folgekosten ebenfalls als abzuwägende Interessen einzustufen sind und wie gewichtig diese gegenüber dem Interesse des Empfängers geltend gemacht werden können.

Autor und Ansprechpartner

Marc Fliehe
Fachbereichsleiter Digitalisierung & Bildung
E-Mail: marc.fliehe@tuev-verband.de
Tel. +49 30 760095 460
www.tuev-verband.de

Als TÜV-Verband e.V. vertreten wir die politischen Interessen der TÜV-Prüforganisationen und fördern den fachlichen Austausch unserer Mitglieder. Wir setzen uns für die technische und digitale Sicherheit sowie die Nachhaltigkeit von Fahrzeugen, Produkten, Anlagen und Dienstleistungen ein. Grundlage dafür sind allgemeingültige Standards, unabhängige Prüfungen und qualifizierte Weiterbildung. Unser Ziel ist es, das hohe Niveau der technischen Sicherheit zu wahren, Vertrauen in die digitale Welt zu schaffen und unsere Lebensgrundlagen zu erhalten. Dafür sind wir im regelmäßigen Austausch mit Politik, Behörden, Medien, Unternehmen und Verbraucher:innen.

Herausgeber
TÜV-Verband e. V.
Friedrichstraße 136
10117 Berlin

Tel.: +49 30 760095-400
Fax: +49 30 760095-401
E-Mail: berlin@tuev-verband.de
www.tuev-verband.de