GESELLSCHAFT
FÜR INFORMATIK

Berlin, 04. Juli 2025

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

Zum neuen Referentenentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG)

Stand: 24.06.2025

Die Gesellschaft für Informatik e.V. (GI) begrüßt die Fortschritte in dem neuen Referentenentwurf zum NIS2UmsuCG. Die GI verweist auf nach wie vor relevante Punkte aus den Stellungnahmen vom 07.05.2024 und 29.11.2024 zu 1) einer einheitlichen Nomenklatur, 2) Vereinfachung der Meldungen, 3) Ausnahmen von der Meldepflicht sowie 4) Authentizität als eigenes Sicherheitsziel.

Um die IT-Sicherheit in Deutschland zu verbessern, fordern wir eine schnelle Verabschiedung des Gesetzes, nicht jedoch ohne wichtige Fragen unbeantwortet zu lassen.

1) Wichtige Begriffe normenübergreifend einheitlich und klarer definieren

Um spätere Auslegungsschwierigkeiten zu vermeiden, sollten die Begriffsdefinitionen noch klarer gefasst werden. Innerhalb der Formulierungshilfe gilt dies bei der Abgrenzung zwischen einer „erheblichen Cyberbedrohung“ und einem „erheblichen Sicherheitsvorfall“. Die Begriffe sollten auch in weiteren Gesetzen einheitlich verwendet werden: Im aktuellen Entwurf des KRITIS-Dachgesetz *(§ 2 Nr. 9)* wird allgemein von „Vorfällen“, im Digital-Operational-Resilience-Act (EU 2022/2554, kurz: DORA) wiederum von „IKT-bezogenen Vorfällen“ gesprochen. Da DORA bereits im Januar 2025 Geltung erlangte, empfehlen wir, einheitlich das Vokabular von DORA auf nun folgende Normen, Standards und Gesetze zu übertragen.

Außerdem sollten nicht nachvollziehbare Unterschiede zwischen europäischen und nationalen Begriffen, etwa bei „wesentlichen“ und „besonders wichtigen“ Einrichtungen angeglichen werden. Es stellt sich des Weiteren die Frage, ob eine Parallelisierung der (leicht) erweiterten Vorgaben für Betreiber kritischer Anlagen und teilweise sogar Infrastrukturen (Nomenklatur aus dem alten ITSiG), die eine gemeinsame Schnittmenge sowohl mit den besonders wichtigen als auch wichtigen Einrichtungen aufweist, noch mehrwertbringend und sinnvoll ist.

Es stellt sich weiterhin die Frage, inwieweit die Ausnahmeregelungen im § 37 mit dem Ziel eines einheitlichen und vollständigen Lagebildes zur Cybersicherheit dienlich sind. Bestimmte Einrichtungen können demnach im Einvernehmen mit dem zuständigen Ministerium oder im Benehmen mit den Ministerien für Inneres und Justiz der Länder von der Meldepflicht gemäß § 32 befreit werden. Dies unter der Voraussetzung: „sofern die Einrichtung Vorgaben einhält, die den Verpflichtungen nach diesem Gesetz gleichwertig sind“ (vgl. § 37 Abs. 1). Eine solche Ausnahmeregelung könnte zum Entstehen von Parallelstrukturen oder einer Zwei-Klassen-Öffentlichkeit führen und das tatsächliche Lagebild der Cybersicherheit verzerren und gefährden. Notwendig wäre hier ein Kriterienkatalog, der Klarheit, Grenzen und Transparenz über die Anwendung dieser Ausnahmeregelungen schafft.

Sehr zu begrüßen ist eine eindeutige Festlegung der Arten von Rückmeldungen im § 36 Abs. 1, die die meldenden Einrichtungen – auf Ersuchen der Einrichtung – vom BSI erhalten dürfen. Darunter ist auch die „zusätzliche technische Unterstützung" zu begrüßen, die das BSI auf Ersuchen der meldenden Einrichtung leisten darf.

2) Einfachheit bei der Meldung von Sicherheitsvorfällen durchsetzen

Der Entwurf definiert das BSI zwar als „zentrale Meldestelle", fügt hierfür aber Ausnahmen ein. Diese Ausnahmen erhöhen die Komplexität unnötig. Die GI setzt sich weiterhin dafür ein, diese zu verringern.

§ 32 ist mit unnötig viel Bürokratie verbunden, was bereits vielfach kritisiert wurde. Wir empfehlen daher, dem Vorschlag des Bundesrats zu folgen und § 40 Absatz 3 um eine neue Nr. 5 zu ergänzen. Mit diesem würden „geeignete Online-Formulare" zur Meldung eingeführt werden. Vorteil hierbei wäre, dass Datenschutz und IT-Sicherheit (durch eine zeitgleiche Meldung nach Art. 33 DSGVO und § 32 BSIG-E) miteinander verknüpft würden.

Eine weitere Effektivierung würde sich aus der Vereinheitlichung der Meldepflichten für „erhebliche Sicherheitsvorfälle" gemäß § 32 Abs. 1 de NIS2UmsuCG und ebendieser Pflichten aus dem DORA ergeben. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) regelt die Umsetzung und das Vorfallsmeldewesen zu schwerwiegenden „IKT-bezogenen Vorfällen" gemäß Art. 3 Nr. 10 DORA in diesem Sektor. Zur Vermeidung von Doppelmeldungen erfolgt aktuell die Meldung schwerwiegender IKT-Vorfälle direkt an die BaFin. Diese übernimmt die automatisierte Weiterleitung an das BSI, die Europäischen Aufsichtsbehörden (ESAs) sowie, sofern relevant, an weitere Institutionen wie die Deutsche Bundesbank, die Europäische Zentralbank (EZB) oder mittelbar an die European Union Agency for Cybersecurity (ENISA).

Da sich die Anforderungen aus DORA und der NIS-2-Richtlinie teilweise überschneiden, kommt die Lex-specialis-Regelung zum Tragen, wie die BaFin erläutert: „Finanzunternehmen, die unter die NIS-2-Richtlinie fallen, müssen […] künftig nur eine Vorfallsmeldung gemäß DORA bei der BaFin einreichen. Die BaFin stellt die Meldung unverzüglich dem Bundesamt für Sicherheit in der Informationstechnik zur Verfügung."

Im #nis2know-Webinar des BSI am 8. Oktober 2024 wies der Referent darauf hin, dass für Finanzinstitute vorrangig DORA gelte, ungeachtet des NIS-Umsetzungsgesetzes. Zu einer Doppelregulierung komme es nicht, teilte das BSI mit, da nach dem Lex-specialis-Grundsatz DORA Vorrang vor der NIS-2-Richtlinie habe. Dies trifft zweifelsohne zu – allerdings möglicherweise nicht für alle Finanzunternehmen und nicht für alle Mindestanforderungen, die aus der aktuellen EU-Regulierung zu

Cybersicherheit und Resilienz resultieren. BaFin teilt bei Nachfragen dieser Art regelmäßig mit, bei jeder Anfrage als Einzelfall entscheiden zu wollen (nur Anfragen betroffener Finanzunternehmen werden beauskunftet).

3) Entschlossenheit bei der Meldung von Schwachstellen zeigen

Mit § 5 Abs. 3 BSIG wird endlich eine Pflicht zur Weitergabe gemeldeter Schwachstellen eingeführt. Wir begrüßen dies sowie die Ergänzung des § 43, um Einrichtungen der Bundesverwaltung zur Meldung von Schwachstellen an das BSI zu verpflichten. Leider gibt es aber weiterhin Ausnahmen an dieser Verpflichtung, die ein Offenhalten von Schwachstellen ermöglichen und die Wirksamkeit von IT-Sicherheitsmaßnahmen schwächen.

Die GI begrüßt ausdrücklich die Streichung der Ausnahmen für das Auswärtige Amt, die Streitkräfte und den Militärischen Abschirmdienst. Allerdings sollte auch § 5 Absatz 4 Satz 2 gestrichen werden, der eine vage formulierte Ausnahme der Meldung von Schwachstellen „auf Grund von Vereinbarungen mit Dritten“ formuliert.

4) Authentizität als eigenes Sicherheitsziel anerkennen

Integrität und Authentizität sind eigene Sicherheitsziele der IT-Sicherheit und erfordern jeweils entsprechende Sicherheitsstrategien. Im bisher geltenden BSI-Gesetz wird dies noch berücksichtigt, im Referentenentwurf dagegen überraschend und mit unzutreffender Begründung aufgegeben.

Auch im NIS2UmsuCG sollte Authentizität weiterhin als eigenes Sicherheitsziel festgeschrieben werden und nicht als Unterfall der Integrität betrachtet werden. Authentizität stellt die Echtheit von Daten und Identitäten fest. Dies ist beispielsweise wichtig, um Phishing-E-Mails zu erkennen. Authentizität ist daher für die Vertrauenswürdigkeit von digitalen Services von größter Wichtigkeit.

Über die Gesellschaft für Informatik e.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.