

Berlin, 18. Dezember 2024

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

Zur neuen Formulierungshilfe
zum NIS-2-Umsetzungs- und
Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

Stand: 29.11.2024



Die Gesellschaft für Informatik e.V. (GI) begrüßt die Fortschritte in der neuen Formulierungshilfe zum NIS2UmsuCG. Nachbesserungen wie die Stärkung des BSI als „fachlich unabhängige“ Behörde, sehen wir positiv. Um das Gesetz noch wirksamer zu gestalten, fordern wir letzte Änderungen vor der hoffentlich noch vor der Bundestagswahl stattfindenden Verabschiedung des Gesetzes.

1) Wichtige Begriffe einheitlich und klarer definieren

Um spätere Auslegungsschwierigkeiten zu vermeiden sollten die Begriffsdefinitionen noch klarer gefasst werden. Innerhalb der Formulierungshilfe gilt dies etwa bei der Abgrenzung zwischen einer „erheblichen Cyberbedrohung“ und einem „erheblichen Sicherheitsvorfall“. Die Begriffe sollten auch in weiteren Gesetzen einheitlich verwendet werden – leider ist dies nicht der Fall, stattdessen verwirren sie mit weiteren Begriffen: Im aktuellen Entwurf des KRITIS-Dachgesetz (§ 2 Nr. 9) wird allgemein von „Vorfällen“, in der DORA-Verordnung wiederum von „IKT-bezogenen Vorfällen“ gesprochen . Da DORA bereits im Januar 2025 Geltung erlangt, empfehlen wir, einheitlich das Vokabular von DORA zu verwenden.

Weiterhin sollte die „Informationssicherheit“ durch zentrale technisch-organisatorischer Schutzziele ergänzt und damit weiter präzisiert werden. Außerdem sollten nicht nachvollziehbare Unterschiede zwischen europäischen und nationalen Begriffen, etwa bei „wesentlichen“ und „besonders wichtigen“ Einrichtungen, angeglichen werden.

2) Einfachheit bei der Meldung von Sicherheitsvorfällen durchsetzen

Die Formulierungshilfe des NIS2UmsuCG definiert das BSI zwar als „zentrale Meldestelle“, fügt hierfür aber Ausnahmen ein. Diese Ausnahmen erhöhen die Komplexität unnötig und sollten daher abgeschafft werden.

Der § 32 ist mit unnötig viel Bürokratie verbunden, was bereits vielfach kritisiert wurde. Wir empfehlen daher, dem Vorschlag des Bundesrats zu folgen und den § 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.

3) Entschlossenheit bei der Meldung von Schwachstellen zeigen

Mit § 5 Abs. 3 BSI-G wird endlich eine Pflicht zur Weitergabe gemeldeter Schwachstellen eingeführt. Wir begrüßen dies sowie die Ergänzung des § 43 um den neuen Absatz 7, der auch Einrichtungen der Bundesverwaltung zur Meldung von Schwachstellen an das BSI verpflichtet. Leider gibt es aber weiterhin Ausnahmen an dieser Verpflichtung, die ein Offenhalten von Schwachstellen ermöglichen und die Wirksamkeit von IT-Sicherheitsmaßnahmen schwächen.

Wir fordern, dass § 5 Absatz 4 Satz 2 gestrichen wird, der eine vage formulierte Ausnahme der Meldung von Schwachstellen „auf Grund von Vereinbarungen mit Dritten“ formuliert. Außerdem fordern wir die Streichung der Ausnahmen für das Auswärtige Amt, die Streitkräfte und den Militärischen Abschirmdienst.

4) Authentizität als eigenes Sicherheitsziel anerkennen

Integrität und Authentizität sind eigene Sicherheitsziele der IT-Sicherheit und erfordern jeweils entsprechende Sicherheitsstrategien. Bereits im bisher geltenden BSI-Gesetz wird dies nicht berücksichtigt. Mit dem NIS-2-Umsetzungsgesetz sollte Authentizität endlich als eigenes Sicherheitsziel festgeschrieben werden. Dies ist nötig, um unternehmerische Maßnahmen zu motivieren, die Daten und Identitäten auf Echtheit überprüfen und somit zum Beispiel Phishing-E-mails als solche aufspüren.

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.