GESELLSCHAFT
FÜR INFORMATIK

Berlin, 28. Mai 2024

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

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

(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

GESELLSCHAFT
FÜR INFORMATIK

Am 07. Mai 2024 hat das Bundesministerium des Innern und für Heimat (*BMI*) den Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (*NIS2UmsuCG*) veröffentlicht und Fachverbände und Interessensvertreter*innen zur Stellungnahme aufgefordert.

Grundsätzliche Einschätzung

Die Gesellschaft für Informatik e.V. (*GI*) begrüßt die Bestrebungen zur Umsetzung der NIS-2-Richtlinie durch den aktuellen Entwurf des NIS2UmsuCG. Folgende positive Aspekte möchten wir hervorheben:

- Die Einbeziehung zahlreicher Bundesstellen und nicht nur der Bundesministerien *(§ 29 Abs. 2*) ist ein wichtiger Schritt zur umfassenden Stärkung der Cybersicherheit innerhalb der Bundesverwaltung. Dies erweitert den Schutzbereich erheblich und sorgt dafür, dass auch andere zentrale Bundesstellen angemessen abgesichert werden.
- Die verpflichtende Bestellung von Informationssicherheitsbeauftragten (*§ 45*) ist eine unerlässliche Maßnahme, um Sicherheitsstandards in den jeweiligen Institutionen kontinuierlich und professionell zu überwachen uns umzusetzen.
- Die Möglichkeit für KRITIS-Unternehmen, eigene branchenspezifische Sicherheitsstandards (*B3S*) vorzulegen *(§ 30 Abs. 9*), ist ein positiver Schritt. Dies ermöglicht eine maßgeschneiderte und effektive Sicherheitsstrategie, die auf die spezifischen Anforderungen und Risiken der jeweiligen Branchen eingeht.
- Wir begrüßen es ausdrücklich, dass unsere Anregungen bzgl. der Definition von Sicherheitsvorfällen im KRITIS-DachG-E berücksichtigt wurden und im vorliegenden Entwurf von „Vorfällen“ und nicht mehr von „Störungen“ gesprochen wird.

Trotz der positiven Aspekte des Entwurfs sehen wir auch dringenden Verbesserungsbedarf in verschiedenen Bereichen. Wir schlagen folgende Verbesserungen vor:

1) Stärkung des BSI als zentrale Meldestelle

Die GI wiederholt Kernforderung aus ihrer Stellungnahme zum KRITIS-DachG-E: Das Bundesamt für Sicherheit in der Informationstechnik (*BSI*) muss als die zentrale Meldestelle für IT-Sicherheitsschwachstellen und Sicherheitsvorfälle gestärkt werden. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sollte lediglich an relevanten Schnittstellen einbezogen werden, um die CER-Richtlinie abzudecken. Diesem Anspruch tragen die Bestimmungen des § 4 Abs. 1 (*„Das Bundesamt ist die zentrale Meldestelle für die Zusammenarbeit der Einrichtungen der Bundesverwaltung*

in Angelegenheiten der Sicherheit in der Informationstechnik“) oder § 5 Abs. 1 (*„[…] Das Bundesamt ist dabei der nationale Koordinator für die Zwecke einer koordinierten Offenlegung von Schwachstellen*“) nicht hinreichend Rechnung.

2) Meldepflichten regulatorisch vereinfachen

Komplexität ist der Feind von Sicherheit. Dies betrifft nicht nur die technische Ebene von IT-Sicherheit, sondern auch auf das regulatorische Framework zu den Anforderungen an die IT-Sicherheit und gilt insbesondere bei Meldepflichten. Regularien sollten miteinander abgestimmt und Verantwortlichkeiten klar und zentral geregelt werden.

3) Berücksichtigung des Sicherheitsziels Authentizität

Das Sicherheitsziel Authentizität fehlt bisher im Entwurf. Neben den drei häufig genannten Sicherheitszielen Vertraulichkeit, Integrität und Verfügbarkeit ist das Sicherheitsziel Authentizität jedoch ebenso unverzichtbar und sollte berücksichtigt werden.

4) Den Erfüllungsaufwand für IT-Sicherheit realistisch ansetzen

Investitionen in IT-Sicherheit lohnen und schützen vor meist viel größeren wirtschaftlichen und gesellschaftlichen Schäden. Gerade in kritischen Bereichen ist es entscheidend, angemessene Ressourcen bereitzustellen, um ein hohes Sicherheitsniveau zu gewährleisten. Eine realistische Einschätzung der tatsächlichen finanziellen Bedarfe fehlt im vorliegenden Entwurf.

5) Begriffe präzise definieren und verwenden

Wichtige Begriffe im Gesetzesentwurf sind im Gegensatz zur NIS-2-Richtlinie unbestimmt. Klare und präzise Definitionen sind jedoch notwendig, um Missverständnisse zu vermeiden und eine einheitliche Umsetzung zu gewährleisten.

Im Folgenden gehen wir jeweils detailliert auf diese fünf Aspekte ein.

Anmerkungen im Detail

1) Stärkung des BSI als zentrale Meldestelle für IT-Sicherheit

Das BSI sollte mit dem NIS2UmsuCG weiter gestärkt werden, so wie es andere Regularien vorsehen.

Den Grundstein der KRITIS-Regulierung in Deutschland bildet das BSI-Gesetz (*BSIG*). § 8b BSIG definiert das BSI als zentrale Meldestelle für KRITIS-Betreiber. § 4 BSIG legt das BSI als zentrale Meldestelle für Bundesbehörden fest, § 4b BSIG definiert es als zentrale allgemeine Meldestelle für Sicherheit in der IT. Das BSI darf zur Abwehr von Gefahren Informationen sammeln und auswerten sowie sich mit anderen Behörden austauschen.

Anderslautend § 33 Abs. 1 des vorliegenden Entwurfs. In diesem Paragraphen werden besonders wichtige Einrichtungen dazu verpflichtet, Informationen an eine Meldestelle des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (*BBK*) zu richten.

Für das BSI spricht außerdem eine beinahe zehnjährige Erfahrung als zentrale Meldestelle für Sicherheitsvorfälle sowie ihre dessen Kompetenzen in IT-Sicherheit, die in dem Ausmaß keine weitere Aufsichtsbehörde verfügt (*mit Außnahme der Bundes- und Landesdatenschutzbehörden auf dem Gebiet der Meldung von Datenpannen gemäß Art. 33 / 34 DSGVO*).

2) Meldepflichten regulatorisch vereinfachen

a. Harmonisierung der Nomenklatur zwischen DORA und NIS2

Das NIS2UmsuCG sowie der sich in der Umsetzung befindende Digital Operational Resilience Act (*DORA*) weisen Bezüge zueinander auf, denen nicht gründlich nachgekommen wird.

Die Bafin regelt die Umsetzung von DORA sowie das Incident-Meldewesen zu (schwerwiegenden) IKT-bezogenen Vorfällen. Finanzunternehmen melden im bestehenden Entwurf zu DORA sogenannte „*IKT-bezogene Vorfälle*“ direkt an die BaFin. Im vorliegenden Entwurf zu NIS2 wird jedoch anderslautend von „*Sicherheitsvorfällen*“ geschrieben. Eine gegenseitige Anpassung der Nomenklatur ist wünschenswert.

Es verwirrt, dass der vorliegende Entwurf zu NIS2 Vorgaben für Finanzunternehmen enthält, die eigentlich mit DORA geregelt werden sollten (*vgl. „Unterrichtungspflichten“ in § 35 Abs. 2*). Vorgaben, die Finanzunternehmen betreffen, sollten direkt über die zuständige Aufsicht – die BaFin – kanalisiert werden. Dies dient dem Bürokratieabbau, mehr Transparenz und damit letztendlich auch der Sicherheit.

b. Vermeidung von Komplexität bei Meldepflichten durch klare Regelungen

Die Meldepflichten von Unternehmen müssen klar geregelt werden. Dem steht eine Diversifizierung von Gesetzen und Regelungen für Meldungen von Sicherheitsvorfällen entgegen, zu denen das NIS2UmsuCG leider beiträgt.

Während die Meldepflichten bzgl. Datenpannen gemäß Art. 33 DSGVO relativ stabil in ihren Anforderungen bleiben, verhält es sich mit den Meldepflichten für

Sicherheitsvorfälle eher umgekehrt: Meldepflichten wurden zuerst mit dem IT-Sicherheitsgesetzes 2.0 (*ITSiG 2.0*) und darauffolgenden Anpassungen geregelt. Anschließend gab es neue Regelungen im KRITIS-DachG, wonach eine zusätzliche Meldeinstanz neben der zentralen Meldestelle, dem BSI, etabliert werden sollte (*vgl. Regelungen zu § 12 Meldewesen für Vorfälle , § 3 - Zentrale Anlaufstelle; Zuständigkeiten; behördliche Zusammenarbeit oder § 6 – Registrierung der kritischen Anlage und Ansprechpartner; Geltungszeitpunkt KRITIS-DachG-E*).

Nun regeln wiederum die §§ 33 ff. des vorliegenden Entwurfs zu NIS2 weitere Meldepflichten für Sicherheitsvorfälle, während im § 5 Abs. 2 von der Entgegennahme von „*Informationen zu Schwachstellen, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen sowie zu Sicherheitsvorfällen, Cyberbedrohungen und Beinahevorfällen*“ durch das BSI gesprochen wird.

Die GI schlägt vor, die Regelungen nicht komplexer zu gestalten, sondern stattdessen Prozesse zu vereinfachen. Unser Vorschlag ist, eine Schnittstelle zu den bestehenden Verfahren und Meldesystemen beim BSI einzurichten, an die für das BBK interessanten und relevanten „Vorfälle“, Schwachstellen etc. gemeldet werden. Damit würden auch die Anforderungen der CER-Richtlinie sowie DORA erfüllt werden.

c. Ausnahmen in der Meldepflicht vermeiden

§ 37 Abs. 2 definiert Ausnahmen von Meldepflichten, etwa für Bereiche der nationalen und öffentlichen Sicherheit oder von für ausgewählte Behörden. Angesichts der international sehr hohen Gefährdungslage sind solche Ausnahmen nicht zielführend. Die Sicherheit der genannten Einrichtungen sollte ebenso auf hohem Niveau geregelt werden.

Sollte ein anderes Gesetz diese Ausnahmen regulieren, ist zwecks Transparenz ein Verweis auf das entsprechende Gesetz an dieser Stelle notwendig.

d. Vorschlag zur Anpassung der Meldepflichten an bewährte DSGVO-Verfahren

Auf S. 96 wird im Entwurf argumentiert, dass die Einführung eines dreistufigen Melderegimes den bürokratischen Aufwand für die Einrichtungen im Rahmen des Umsetzungsspielraums minimiere. Es ist nicht nachvollziehbar, wie bzw. für wen sich hier Aufwände reduzieren würden.

Die GI schlägt vor, die Meldepflichten für Sicherheitsvorfälle stattdessen nach Art. 33 / 34 DSGVO zu gestalten. Es handelt sich dabei um ein erprobtes und seit mehreren Jahren optimiertes Verfahren.

1) Berücksichtigung des Sicherheitsziels Authentizität

Das Sicherheitsziel Authentizität fehlt bisher im Entwurf und sollte hinzugefügt werden.

Authentizität stellt die Echtheit und Vertrauenswürdigkeit von Identitäten und Daten sicher. Sie gewährleistet, dass nur befugte Personen oder Systeme auf Informationen zugreifen. Eine wesentliche Ursache für den Erfolg von Ransomware-Angriffen liegt in der Missachtung dieses Sicherheitsziels. Das gilt gleichermaßen für einen Teil der beobachtbaren Supply-Chain-Angriffen.

Für ein wirksames Gesetz ist es daher von zentraler Bedeutung, das Sicherheitsziel Authentizität angemessen zu berücksichtigen. Die GI empfiehlt, Authentizität an folgenden Stellen als zusätzliches Ziel aufzunehmen:

1) § 2 Abs. 1 Nr. 1
2) § 2 Abs. 1 Nr. 16
3) § 2 Abs. 1 Nr. 38
4) § 2 Abs. 1 Nr. 39
5) § 16 Abs. 2
6) § 30 Abs. 1
7) § 41 Abs. 3 (zweifach)
8) § 41 Abs. 5 Nr. 5
9) § 41 Abs. 5 Nr. 6

3) Den Erfüllungsaufwand für IT-Sicherheit realistisch ansetzen

Das NIS2UmsuCG weist keine realistische Einschätzung der finanziellen für die Umsetzung von IT-Sicherheit auf.

Der in der Begründung zur Einhaltung des Mindestniveaus an IT-Sicherheit für besonders wichtige und wichtige Einrichtungen angegebene Erfüllungsaufwand (S. 106 ff.) ist gering angesetzt, da neben der Funktion eines Informationssicherheits-beauftragten insbesondere auch Stellen zur operativen Informationssicherheit einzurichten sind. Die angesetzten 1,5 Vollzeitäquivalente und 60.000 € Sachmittel reichen nicht aus, um die Anforderungen aus der NIS-2-Richtlinie wirksam umzusetzen. Die GI schätzt die erforderlichen Kosten auf mindestens das Doppelte.

4) Begriffe präzise definieren und verwenden

Die GI stellt im Entwurf eine Reihe unklarer oder unvollständiger Definitionen oder Formulierungen fest. Für diese werden im Folgenden Empfehlungen zur Präzisierung bzw. Vervollständigung gegeben:

a) § 2 Abs. 1 Nr. 10 lit. a: Ergänzende Kriterien aus ErwG 101 der NIS-2-Richtlinie fehlen

Hinsichtlich der Bestimmung, was unter schwerwiegenden Betriebsstörungen nach § 2 Abs. 1 10 lit. a fällt, fehlen die ergänzenden und erläuternden Kriterien aus ErwG 101 der NIS-2-Richtlinie, welche soweit mit einem eingeschobenen Relativsatz eingefügt werden sollten.

b) § 11 Abs. 7: „Herausgehobenen Fall" klarer definieren

Es ist unklar, warum ein herausgehobener Fall bereits dann vorliegen soll, wenn gemäß § 11 Abs. 7 *„eine Stelle eines Landes betroffen*" ist. Die Kriterien in § 11 Abs. 2 setzen entweder eine besondere technische Qualität des Angriffs oder ein besonderes öffentliches Interesse an der zügigen Wiederherstellung voraus. Diese Regelung könnte dazu führen, dass Länderinteressen vor Bundesinteressen gestellt werden.

Nicht jeder erfolgreiche Angriff gegen eine Landesstelle erfordert zwingend ein unverzügliches Handeln einer Bundesbehörde. Sollten solche Regelungen gewollt sein, muss das BSI über zusätzliche Befugnisse verfügen. Deren Erteilung wäre zustimmungspflichtig und würde Anpassungen im Grundgesetz erfordern. Eine einzelgesetzliche Verankerung erscheint daher schwierig.

Eine angemessenere Regelung wäre, wenn mehrere Stellen eines oder mehrerer Länder betroffen sind. Dann könnte von einem systematischen Angriff ausgegangen werden.

c) § 30 Abs. 1: Verluste in Risiko-Definition einbeziehen

Risiken werden im § 30 Abs. 1 des NIS2UmsuCG nur unvollständig erfasst. Im Gegensatz zu Art. 6 Nr. 9 NIS-2-Richtlinie bezieht § 30 Abs. 1 des vorliegenden Entwurfs keine Verluste im Risikomanagement mit ein. (Damit werden Verluste nicht als Ergebnis von Störungen angesehen.) Für eine adäquate Umsetzung von Art. 21 Abs. 1 i.V.m. Art. 6 Nr. 9 NIS-2-Richtlinie sollte der erste Satz (unter Einbeziehung des zusätzlich gebotenen Sicherheitsziels) lauten:

> *„Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen* ***als auch Verluste*** *der Verfügbarkeit, Integrität und Vertraulichkeit* ***sowie der Authentizität*** *der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.*"

d) § 39 Abs. 1: Verpflichtung zur Wirksamkeitsprüfung klarer definieren

Von den Verpflichteten nach der NIS-2-Richtlinie wird eine wirksame Umsetzung der Maßnahmen verlangt. Davon haben sich unabhängige Prüfer*innen zu vergewissern. Der vorliegende Entwurf des NIS2UmsuCG erwähnt keine solche Verpflichtung. Wenn das BSI bei der Überprüfung von Nachweisen die Dokumentation nach § 39 Abs. 1 verlangt, folgt daraus, dass für die durchgeführte Wirksamkeitsprüfung eine entsprechende Aufzeichnung nötig ist. Zur besseren Klarheit sollte die Verpflichtung damit entsprechend aufgenommen werden.

e) Sonstiges

§ 28 Abs. 6 ist unbestimmt, da eine (kritische) Anlage offensichtlich immer Einfluss auf die eigene (kritische) Anlage hat. Hier sollte daher der letzte Teilsatz wie folgt lauten: *„... bestimmenden Einfluss auf eine **andere** oder mehrere kritische Anlagen ausübt“*.

§ 61 Abs. 1 und § 61 Abs. 2 Nr. 7 sind identisch, was auf einen Darstellungsfehler hinweist.

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.