bitkom

Stellungnahme

Januar 2025

Formulierungshilfen für ein NIS2UmsuCG

Die Bundesregierung hat im Dezember nach einer Einigung zwischen SPD und Grünen eine Formulierungshilfe für Änderungsanträge zum NIS2UmsuCG vorgelegt. Ziel ist es, die Cybersicherheitsvorgaben der EU-Richtlinie noch in dieser Legislaturperiode gesetzlich zu verankern. Angesichts der verbleibenden Sitzungswoche des Bundestages ist der zeitliche Rahmen für die Verabschiedung des Gesetzes sehr eng.

Die vorgelegte Formulierungshilfe enthält neben einer Reihe von Klarstellungen und redaktionellen Änderungen an der Novelle des BSI-Gesetzes auch wesentliche inhaltliche Anpassungen gegenüber dem ursprünglichen Regierungsentwurf. Diese gehen in vielen Bereichen über die Vorgaben der europäischen Richtlinie hinaus und stellen einen deutschen Sonderweg dar, was der gradlinigen und zeitnahen Umsetzung auf deutscher Ebene im Wege steht. Aus Sicht des Bitkom stellt sowohl der Inhalt als auch der Umfang dieser Änderungen ein bedeutendes Novum dar, das eine umfassende und direkte Einbindung der Wirtschaft erfordert hätte.

Eine Verabschiedung des Gesetzes vor der Bundestagswahl ist aus der Perspektive der bereits abgelaufenen Umsetzungsfrist der EU-Kommission im Oktober verständlich. Eine Nichtumsetzung könnte im Rahmen eines Vertragsverletzungsverfahren gegen Deutschland zu Strafzahlungen führen. Zudem würde eine Verabschiedung der Novelle Rechtssicherheit schaffen, damit sich Unternehmen auf die wichtigen, neuen Regelungen zu Cybersicherheit und -resilienz einstellen können. Auf der anderen Seite sprechen jedoch die Einführung von weitreichenden Änderungen, die zum Teil über die europäische NIS2-Richtlinie hinausgehen, gegen eine übereilte Verabschiedung in der vorliegenden Form. Insbesondere § 41 BSIG in der Fassung der Formulierungshilfe sollte im Falle einer Verabschiedung durch das NIS2UmsuCG nicht zugestimmt werden. Zudem sind noch viele Punkte offen, insbesondere die Abstimmung mit dem KRITIS-Dachgesetz, die noch nicht abgeschlossen ist und mit mehr Zeit in der kommenden Legislaturperiode erfolgen könnte.

Umso wichtiger ist es, dass die Perspektiven der Digitalwirtschaft in dieser entscheidenden Phase des Gesetzgebungsprozesses Berücksichtigung finden. Mit diesem Papier möchte der Bitkom dazu beitragen, die Interessen und Anforderungen der Branche zu adressieren und eine ausgewogene sowie praxisgerechte Umsetzung der NIS2-Richtlinie zu unterstützen.

§ 1 BSIG: Bundesamt für Sicherheit in der Informationstechnik
Überschrift 2, möglicherweise auch mehrzeilig

Eine größere fachliche Unabhängigkeit des BSI wurde erreicht. Es bleibt zwar eine nachgeordnete Behörde des BMI, soll aber selbstständig sein und seine Aufgaben fachlich unabhängig wahrnehmen. Das BMI übt die Aufsicht über das Bundesamt aus, indem beide Behörden jährlich eine Zielvereinbarung abschließen. Über den Inhalt der Zielvereinbarung und deren Erfüllung hat das BMI dem zuständigen Ausschuss jährlich zu berichten.

Die Richtung dieser Regelung ist grundsätzlich zu begrüßen. Inwieweit dies langfristig sinnvoll ist, hängt jedoch davon ab, ob es nach der Wahl ein Digitalministerium geben wird und wie dann die Anbindung des BSI in diesem Zusammenhang gestaltet wird. Entscheidend muss bleiben, dass Schritte unternommen werden, das BSI auch zu einer Zentralstelle auszubauen. Dies muss von der nächsten Bundesregierung in der kommenden Legislaturperiode angegangen werden.

§ 7 BSIG: Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte

Das BSI erhält auch in seiner Rolle als CISO Bund (vgl. § 46) erweiterte Kontroll- und Zugriffsrechte. Nach dem neuen Entwurf darf das BSI die Kommunikationstechnik des Bundes, ihre Komponenten und technischen Infrastrukturen auch mittels Penetrationstests überprüfen. Das BSI darf also aktiv versuchen, in die IT einer Bundesbehörde einzudringen. Damit wurde aus Sicht des Bitkom eine verbesserte Kontrollmöglichkeit für das BSI geschaffen.

§ 28 BSIG: Besonders wichtige Einrichtungen und wichtige Einrichtungen

Anhaltende Cyberangriffe auf Kommunen und Behörden mit weitreichenden Folgen für Wirtschaft und Gesellschaft unterstreichen die Dringlichkeit, die öffentliche Verwaltung auf allen Ebenen des föderalen Staates in den Anwendungsbereich des NIS2UmsuCG einzubeziehen. Neben Bundesbehörden sollten auch Landes- und Kommunalbehörden als besonders wichtige Stellen definiert und damit in den Anwendungsbereich des NIS2UmsuCG einbezogen werden.

Hinsichtlich der Definition von wichtigen Einrichtungen sollte eine klare Differenzierung zwischen Herstellern und Anbietern im Sinne der europäischen NIS2-Richtlinie vorgenommen werden. Eine solche Unterscheidung trägt dazu bei, die Vorgaben der Richtlinie 1:1 umzusetzen, ohne zusätzliche nationale Sonderanforderungen einzuführen.

§ 29 BSIG: Einrichtungen der Bundesverwaltung

Der Bitkom hat weiterhin starke Bedenken hinsichtlich der vorgesehenen Regelungen für die IT-Sicherheit in der Bundesverwaltung. Der vorliegende Entwurf verpflichtet weiterhin ausschließlich die Bundesministerien und das Bundeskanzleramt zur Einhaltung des IT-Grundschutzes, während für die übrigen Einrichtungen der Bundesverwaltung lediglich Mindeststandards gelten sollen. Diese Mindeststandards bleiben hinter dem IT-Grundschutz zurück, obwohl der Umsetzungsplan Bund die obersten Bundesbehörden bereits seit 2017 zur Anwendung des IT-Grundschutzes verpflichtet.

Der Verzicht auf die Ausweitung des IT-Grundschutzes auf die gesamte Bundesverwaltung im Rahmen des NIS2UmsuCG führt faktisch zu einer Absenkung des Cyber-Sicherheitsniveaus innerhalb der Bundesverwaltung. Diese Entscheidung steht nicht nur im Widerspruch zu Forderungen, die unter anderem im Rahmen der öffentlichen Anhörung des Bundestages erhoben wurden, sondern sendet auch problematische Signale an die Wirtschaft. Unternehmen, die durch die Umsetzung des NIS 2 Umsetzungsgesetzes erheblich belastet werden, könnten das Fehlen einer Vorbildfunktion der öffentlichen Hand als Glaubwürdigkeitsdefizit wahrnehmen.

Besonders kritisch ist, dass auch sicherheitsrelevante Behörden wie das BKA und das BSI von der Einhaltung des IT-Grundschutzes ausgenommen bleiben sollen. Angesichts der sensiblen Daten, die diese Institutionen verwalten, und ihrer unverzichtbaren Funktionalität im Krisenfall wäre eine höhere Sicherheitsanforderung dringend geboten.

Die Begründung, eine Ausweitung des IT-Grundschutzes sei aus Kostengründen nicht realisierbar, erscheint nicht überzeugend. Die nun notwendigen Maßnahmen hätten bereits vor Jahren umgesetzt werden sollen, sodass die anfallenden Kosten eher als technische Schulden zu betrachten sind. Zudem ist allgemein bekannt, dass die Folgekosten von Cybervorfällen die Ausgaben für Prävention bei weitem übersteigen. Bitkom appelliert daher eindringlich, den IT-Grundschutz für die gesamte Bundesverwaltung verbindlich vorzuschreiben, um ein hohes Sicherheitsniveau nachhaltig sicherzustellen.

§30 BSIG: Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Die Formulierungen „Erbringung ihrer Dienste“ im Gesetzestext sowie in den Erläuterungen bleiben weiterhin unklar und bedürfen einer Konkretisierung (vgl. hierzu die Bitkom-Stellungnahme vom Juli 2024). Es wird empfohlen, die Definition auf IT-Systeme und -Komponenten zu beschränken, die spezifisch für die Erbringung der Dienste in den jeweiligen Einrichtungsarten gemäß Anlage 1 oder 2 eingesetzt werden.

§ 31 BSIG: Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

Die geplante Änderung in Absatz 2 sieht vor, dass kritische „Komponenten und Prozesse“ der Angriffserkennung unterliegen sollen. Insbesondere bei Prozessen erscheint dies jedoch nicht praktikabel, da „Komponenten und Prozesse“ nicht direkt an eine Angriffserkennung angeschlossen werden können. Eine solche Maßnahme ist technisch nur bei „Systemen“ umsetzbar.

§ 32 BSIG: Meldepflichten

Auch hinsichtlich der Meldefristen im Zusammenhang mit der Meldung von Sicherheitsvorfällen gibt es weiterhin offene Fragen. Die auf europäischer Ebene festgelegte Frist für die erste Meldung innerhalb von 24 Stunden wird als zu kurz erachtet, insbesondere für kleinere und mittlere Unternehmen, die von NIS2 betroffen sind. Diese Frist kann leider nicht mehr geändert werden, weshalb es nunmehr notwendig ist, zumindest klarzustellen, dass die 24-Stunden-Frist entweder ab dem Zeitpunkt gilt, an dem das betroffene Unternehmen tatsächlich Kenntnis von dem Vorfall erlangt oder - noch sinnvoller - ab dem Zeitpunkt, an dem das betroffene Unternehmen tatsächlich die Signifikanz des Vorfalls, die zu einer Meldepflicht führt, festgestellt hat.

Diese Klarstellung ist für kleinere und mittlere Unternehmen von zentraler Bedeutung, da sie andernfalls gezwungen wären, einen IT-Service rund um die Uhr bereitzustellen, was für viele Unternehmen im Anwendungsbereich der vorliegenden Richtlinie nicht praktikabel ist. Im Fall eines Angriffs, der beispielsweise an einem Wochenende oder an Feiertagen stattfindet, wäre es für diese Unternehmen unmöglich, die Meldepflichten innerhalb von 24 Stunden zu erfüllen. Bitkom fordert daher eine präzise Regelung, die sicherstellt, dass die Frist zur Meldung erst zu einem der o.g. Zeitpunkte zu laufen beginnt, um die praktische Umsetzbarkeit für alle Unternehmen zu gewährleisten.

Zudem sollte der Gesetzgeber sicherstellen, dass die Anforderungen im Meldewesen so effizient und digital wie möglich umgesetzt werden. Hierzu sollte ein vollständig digitalisiertes Meldeportal eingerichtet werden, das über effiziente Schnittstellen zur Automatisierung verfügt, Mehrfachmeldungen vermeidet und eine zentrale Anlaufstelle bietet. Unternehmen sollte zudem die Möglichkeit eingeräumt werden, Meldungen in englischer Sprache einzureichen, um den internationalen Anforderungen gerecht zu werden. Zwischenmeldungen sollten auf das notwendige Minimum reduziert werden, um den administrativen Aufwand und die Belastung der Ressourcen zu minimieren.

§ 33 BSIG: Registrierungspflicht

Die im zweiten und fünften Absatz eingeführte Verpflichtung zur Registrierung von „Typen von kritischen Komponenten“ führt zu einem erheblichen zusätzlichen Aufwand, der in der Praxis schwer umzusetzen ist. Um die Umsetzbarkeit sicherzustellen und unnötige Bürokratie zu vermeiden, sollten diese Ergänzungen gestrichen werden.

§ 41 BSIG: Untersagung des Einsatzes kritischer Komponenten

Es gibt starke Bedenken hinsichtlich der Änderungen in § 41 BSIG, die dem BMI die Befugnis einräumt, nur im Benehmen mit den jeweiligen Fachministerien die Verwendung kritischer Komponenten zu untersagen. Die Formulierung würde dem BMI alleinige Entscheidungsbefugnis verleihen und die bisherige Abstimmung mit anderen Ressorts ersetzen, was die Grundlage für ausgewogene Entscheidungen gefährdet. Die Expertise der Aufsichtsbehörden wie BSI und BNetzA würde dadurch nicht mehr berücksichtigt werden. Für eine Untersagung kritischer Komponenten soll es gemäß der Formulierungshilfe zudem genügen, wenn diese vom BMI im Wege einer Allgemeinverfügung im Bundesanzeiger bekannt gegeben wird. Gleichzeitig sieht der Entwurf vor, die aufschiebende Wirkung von Widersprüchen oder Klagen betroffener Unternehmen gesetzlich auszuschließen. Dies bedeutet, dass selbst im Falle einer späteren gerichtlichen Feststellung der Unrechtmäßigkeit einer Untersagung der entstandene Schaden für die Unternehmen bereits eingetreten wäre.

Vor dem Hintergrund des öffentlich-rechtlichen Vertrags zwischen den Mobilfunknetzbetreibern und der Bundesregierung aus dem Juli 2024 erscheint es weder sinnvoll noch notwendig, die bestehende Regelung in § 9b BSIG durch eine Neuregelung im NIS 2 Umsetzungsgesetz zu ersetzen. Das geplante Vorgehen hätte stattdessen gravierenden Auswirkungen auf die Infrastrukturversorgung, die wirtschaftliche Stabilität und strategische Ziele wie die Gigabit- und Digitalisierungsstrategie. Die Möglichkeit, Verbote ohne aufschiebende Rechtsmittel per Allgemeinverfügung durchzusetzen, schafft erhebliche Planungsunsicherheit für Unternehmen, die Milliarden in die TK-Infrastruktur investieren. Dabei stellt sich insbesondere die Frage, wie die Kostenträgerschaft im Falle des Rückbaus bereits verbauter Technologie geregelt werden soll. Zudem bleibt unklar, wie die Anwendung von §41 mit der zwingend vorgegebenen Durchführung von Vergabeverfahren für öffentliche Unternehmen in Einklang zu bringen ist.

Es ist außerdem zu kritisieren, dass nie eine Konsultation oder Anhörung der betroffenen Branchen, die eine wesentliche Änderung betrifft, stattgefunden hat. Wir empfehlen generell, dass jegliche Anpassungen der bestehenden Konzepte nur mit der gesamten Industrie, Forschung und betroffenen Unternehmen in transparenten Beteiligungsverfahren durchgeführt werden.

Angesichts der aktuellen wirtschaftlichen Herausforderungen könnte der vorliegende Entwurf zu erheblichen negativen Folgen für den Netzausbau und die Digitalisierung in Deutschland führen. Es muss daher gegen die Änderung des §9b/41 BSIG gestimmt

werden. Das BMI sollte auch künftig in der Lage sein, kritische Funktionen und Komponenten für neue Bereiche per Rechtsverordnung zu bestimmen, jedoch weiterhin im Einvernehmen mit den jeweiligen Fachministerien. Zudem sollten BNetzA und BSI weiterhin den Prozess zur technischen Festlegung kritischer Funktionen und Komponenten im Sicherheitskontext durchführen.

§ 43 BSIG: Informationssicherheitsmanagement

Wir begrüßen grundsätzlich, dass das BSI verpflichtet wird, gemeldete Schwachstellen unverzüglich an die verantwortlichen Hersteller oder Produktverantwortlichen zur Behebung weiterzuleiten, sofern diese nicht bereits öffentlich bekannt sind. Ebenso wird die Verpflichtung der Ministerien zur Meldung von Schwachstellen positiv aufgenommen.

Allerdings führen die vorgesehenen Ausnahmen für Sicherheitsbehörden und Vereinbarungen mit „Dritten“ weiterhin zu erheblichen Sicherheitsrisiken. Insbesondere fehlt die notwendige Transparenz darüber, mit welchen „Dritten“ das BSI entsprechende Vereinbarungen trifft und welche gemeldeten Schwachstellen davon betroffen sind. Der aktuelle Entwurf lässt somit Schwachstellen bestehen, was die Sicherheit von nationalen Systemen und Netzwerken nachhaltig gefährdet.

Der Entwurf sollte dahingehend überarbeitet werden, dass Schwachstellen bedingungslos und zeitnah von allen Stellen an die Hersteller gemeldet werden. Nur auf diesem Weg kann die IT-Sicherheit umfassend gestärkt und das Risiko von Cyberangriffen signifikant reduziert werden.

Wir begrüßen grundsätzlich, dass das BSI verpflichtet wird, gemeldete Schwachstellen unverzüglich an die verantwortlichen Hersteller oder Produktverantwortlichen zur Behebung weiterzuleiten, sofern diese nicht bereits öffentlich bekannt sind. Ebenso wird die Verpflichtung der Ministerien zur Meldung von Schwachstellen positiv aufgenommen.

Allerdings führen die vorgesehenen Ausnahmen für Sicherheitsbehörden und Vereinbarungen mit „Dritten“ weiterhin zu erheblichen Sicherheitsrisiken. Insbesondere fehlt die notwendige Transparenz darüber, mit welchen „Dritten“ das BSI entsprechende Vereinbarungen trifft und welche gemeldeten Schwachstellen davon betroffen sind. Der aktuelle Entwurf lässt somit Schwachstellen bestehen, was die Sicherheit von nationalen Systemen und Netzwerken nachhaltig gefährdet.

Der Entwurf sollte dahingehend überarbeitet werden, dass Schwachstellen bedingungslos und zeitnah von allen Stellen an die Hersteller gemeldet werden. Nur auf diesem Weg kann die IT-Sicherheit umfassend gestärkt und das Risiko von Cyberangriffen signifikant reduziert werden.

§ 46 BSIG: Informationssicherheitsbeauftragte der Ressorts

Wir begrüßen die im Gesetzentwurf vorgesehenen Regelungen zur Rolle des CISO Bund, der für die Steuerung der IT-Sicherheit des Bundes verantwortlich ist und beim BSI angesiedelt ist. Die derzeitige Wahrnehmung dieser Rolle durch Claudia Plattner sowie die Unterstützung durch einen stellvertretenden CISO werden als positive Maßnahmen hervorgehoben.

Positiv bewertet wird auch die Verpflichtung, dass der CISO Bund einmal jährlich dem Haushaltsausschuss über die durchgeführten Kontrollen zu berichten hat, wobei der Bericht spätestens am 30. Juni vorliegen muss. Diese Transparenz fördert eine kontinuierliche Kontrolle und Verbesserung der IT-Sicherheit auf Bundesebene. Zudem wird die Regelung unterstützt, dass der oder die CISO Bund anzuhören ist, wenn der Bundestag Gesetze beschließen möchte, die die Informationssicherheit betreffen. Diese Maßnahme stärkt das BSI weiter und trägt zur Sicherstellung eines hohen Standards in der IT-Sicherheit und dem Datenschutz bei. Bitkom begrüßt daher diese Anpassungen.

§56 Ermächtigung zum Erlass von Rechtsverordnungen

Die Aufnahme der Beteiligung zivilgesellschaftlicher Akteure bei der Erstellung der Rechtsverordnungen im Gesetzestext wird grundsätzlich begrüßt. Jedoch gibt der Entwurf dem BMI gemäß Abs. 7 künftig die Möglichkeit, eigenständig festzulegen, welche Komponenten als kritisch anzusehen sind, und erlaubt es, die Nutzung dieser Komponenten weitgehend im Alleingang zu untersagen. Das Fehlen einer ausgewogenen Entscheidungsstruktur erhöht das wirtschaftliche Risiko für Betreiber kritischer Infrastrukturen und birgt Gefahren für die Digital-, Außen-, Wirtschafts- und Technologiepolitik.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Bereichsleiter Sicherheitspolitik
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik