STELLUNGNAHME

Der Mittelstand.
BVMW e.V.
Bundesverband

Zusammenfassung Stellungnahme NIS2UmsuCG:

Mittelstand begrüßt Harmonisierung des Regulierungsrahmens

Ein einheitliches Cybersicherheitsniveau kann den fairen und resilienten Wettbewerb in der EU fördern und positiv zu einem grenzüberschreitenden Wirtschaftsverhältnis beitragen. Bei der Umsetzung in Deutschland sollten die Anforderungen allerdings nicht zusätzlich nach oben geschraubt werden, da dies zu einem Standortnachteil für deutsche Unternehmen führen kann.

Bei Nachweisfristen an realen Möglichkeiten von KMU orientieren

Die Änderungen im Diskussionspapier sind im Vergleich zu den ersten geleakten Entwürfen ein Fortschritt. Für besonders wichtige und wichtige Unternehmen schlagen wir einen Zeitraum von vier bis fünf Jahren vor, bis Nachweise durch das BSI angefragt werden können. Denn neu betroffene Unternehmen haben nicht die jahrelange Vorlaufzeit durch vorangegangene Gesetze gehabt, um entsprechende Maßnahmen einzuführen.

Risikomanagement & Berichtspflichten: Unternehmen in der Lieferkette unterstützen

Klarheit für die Betroffenheit in der Lieferkette schaffen. Aus den bisherigen Entwürfen ist es vielen Unternehmen noch nicht klar, welche Maßnahmen Zulieferer für betroffene Unternehmen leisten müssen. Da hier auch kleinere Unternehmen betroffen sind, ist mehr Genauigkeit bei den Vorgaben für eine bessere Planbarkeit wünschenswert. Der BVMW sieht hier die Gefahr, dass viele Geschäftsbeziehungen unnötig gestört werden.

Bußgelder für mittlere Unternehmen anpassen und transparent gestalten

Bei der Höhe der Bußgelder befürchten wir, dass diese bei vielen KMU zu Unsicherheit führen und deren finanzielle Tragfähigkeit übersteigen. Dies kann zu einem Rückzug aus betroffenen Geschäftsfeldern oder einem Vermeiden des Wachstums über den Schwellenwert von 50 Beschäftigten oder 10 Mio. € Umsatz führen. Deswegen fordern wir die EU-Vorgaben nicht zu überschreiten und wenn möglich Transparenz zu schaffen, wann welche Strafen drohen.

Melde- und Dokumentationspflichten effizient umsetzen

Durch die sehr frühen Vorgaben zur Meldung von Vorfällen und auch der engen Taktung (nach 24h, 72h und einem Monat) fordern wir eine unbürokratische und praxisnahe Möglichkeit, um Meldungen durchzuführen. Die Meldestelle sollte „Ende-zu-Ende“ digitalisiert sein und die Meldung nach dem „Once-Only“ Prinzip nur einmal bei einer zentralen Stelle im BSI nötig sein.

Unterstützung von staatlicher Seite für KMU

Zur Unterstützung wären Informationsangebote mit rechtssicheren Informationen wie zum Beispiel Leitfäden zur Implementierung der Maßnahmen notwendig. Diese können ohne große bürokratische Anträge wertvolle Informationen liefern. Gleichzeitig sollte man auch darüber nachdenken, bestehende Förderinstrumente gerade für betroffene Unternehmen knapp über der Schwelle von 50 Beschäftigten oder 10 Mio. € Umsatz, bzw. auch knapp darunter finanziell zu unterstützen. Denn gerade diese Unternehmen haben oft größere finanzielle und personelle Beschränkungen.

Stand: November 2023

STELLUNGNAHME

Der Mittelstand. BVMW e.V. Bundesverband

Stellungnahme zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

Standpunkte zum NIS2UmsuCG

- **Mittelstand begrüßt Harmonisierung des Regulierungsrahmens**
- **Bei Nachweisfristen an realen Möglichkeiten von KMU orientieren**
- **Risikomanagement & Berichtspflichten: Unternehmen in der Lieferkette unterstützen**
- **Melde- und Dokumentationspflichten effizient umsetzen**
- **Unterstützung von staatlicher Seite für KMU**
- **Bußgelder für mittlere Unternehmen anpassen und transparent gestalten**

Allgemeines

Nachdem die „Network and Information Systems 2.0 Directive“ (NIS-2 Richtlinie) in der EU beschlossen wurde, muss Deutschland diese in nationales Recht umwandeln. Dabei soll die Resilienz gegenüber Angriffen aus dem digitalen Raum gestärkt und auch das gesamte Cybersicherheitsniveau in den EU-Mitgliedsstaaten erhöht werden. Als Frist für die Umsetzung der NIS-2 Richtlinie wurde der 17. Oktober 2024 festgelegt. Mit dem Diskussionspapier des Bundesministeriums des Inneren und für Heimat zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) folgt nun ein erster Schritt in die Umsetzung in nationales Recht. Mit dem NIS2UmsuCG sind Unternehmen mit mehr als 50 Beschäftigten oder 10 Mio. € Umsatz aus bestimmten Sektoren (siehe Anhang 1 und 2 des Diskussionspapiers[1]) betroffen. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Gefährdungslage bei Cybersicherheitsattacken so hoch wie nie[2]. Nicht nur deswegen sieht Der Mittelstand. BVMW e. V. Cybersicherheit auch als ein sehr wichtiges Thema an. Dementsprechend engagiert sich der Verband auch in geförderten Projekten, wie z.B. der Transferstelle Cybersicherheit oder im Projekt „mIT Standard sicher“, bei dem ein praxisnaher Standard für Unternehmen mit weniger als 50 Beschäftigten als Einstieg, u. a. mit dem BSI, entwickelt wurde.

Jedoch sieht Der Mittelstand. BVMW e. V. gemischt auf den Referentenentwurf des NIS2UmsuCG. Grundsätzlich begrüßt der BVMW die Stärkung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als nationale Institution im Bereich Cybersicherheit. Denn die Bündelung der Aufsicht zur Erfüllung und der Überwachung der erforderlichen Maßnahmen sowie die Funktion als Meldestelle für Cybersicherheitsvorfälle soll laut dem Diskussionspapier beim BSI liegen. Damit kann es für Unternehmen einfacher werden, die Meldestelle für Registrierungs- oder Meldepflichten zu finden. Außerdem wird eine unterschiedliche Auslegung der Regeln, z. B. durch verschiedene Behörden, potenziell vermieden. Negativ sehen wir die Verzögerungen in der Gesetzgebung. Der Oktober 2024 rückt immer näher. Betroffene Unternehmen sollten frühzeitig Klarheit darüber bekommen, welche Pflichten auf sie zukommt.

Mittelstand begrüßt Harmonisierung des Regulierungsrahmens in der EU

Um den Wettbewerb in der EU zwischen den verschiedenen Mitgliedstaaten zu stärken und ihn fair zu gestalten, begrüßt der BVMW die Harmonisierung bestehender Regelungen. Gerade für den staatsübergreifenden Wettbewerb kann dies zu einer Erleichterung für Unternehmen führen, wenn sie nicht auf unzählige verschiedene gesetzliche Rahmenbedingungen achten müssen.

Bei der Umsetzung in nationales Recht sollte darauf geachtet werden, die Anforderungen im NIS2UmsuCG gegenüber den Anforderungen aus der europäischen NIS-2-Richtlinie nicht noch weiter zu erhöhen, um zusätzliche Belastungen am Standort Deutschland zu vermeiden. Sonst würde man wieder dem

1 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/diskussionspapier-NIS-2-umsetzung.html
2 Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2022 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410)

Ziel einer Harmonisierung des Rechtsrahmens innerhalb der EU entgegenwirken. Die Anforderungen für KMU sind ohnehin schon hoch, weswegen eine weitere Erhöhung der Anforderungen, die Lage weiter verschärfen würde.

Bei Nachweisfristen (§39) an realen Möglichkeiten von KMU orientieren

Als Mittelstandsverband möchten wir hier die Belange und Perspektive der mittelständischen Unternehmen verdeutlichen. Gerade für KMUs ist die Umsetzung der erforderlichen Maßnahmen eine große Aufgabe und Belastung. Insbesondere die knappen Fachkräfte in diesem Bereich stellen ein Problem bei der Umsetzung dar. Das beginnt intern in Unternehmen, geht aber darüber hinaus bei externen Beratern weiter. Besonders mittlere Unternehmen und durch die Lieferkette indirekt betroffene kleinere Unternehmen haben durch fehlende Fachabteilungen oft nicht das entsprechende interne Wissen. Dafür muss dann meist auf externe Unterstützung durch Beratungen zurückgegriffen werden. Durch die Abhängigkeit von externer Beratung kommen auch finanzielle Beschränkungen hinzu. Denn nicht jedes mittlere Unternehmen oder kurz vor der Schwelle zur Betroffenheit stehende Unternehmen hat die notwendigen finanziellen Ressourcen, um dies schnellstmöglich umzusetzen.

Deswegen sollte zur Umsetzung der Maßnahmen bei mittleren Unternehmen, bzw. wichtigen und besonders wichtigen Einrichtungen genug Zeit eingeplant werden. Der Vorschlag im Diskussionspapier geht dabei in die richtige Richtung. Eine Nachweispflicht alle drei Jahre für Betreiber kritischer Anlagen und auf Anfrage für besonders wichtige und wichtige Einrichtungen ist im Vergleich zu den „inoffiziellen Referentenentwürfen“ ein Fortschritt. Offen bleibt jedoch, ab wann Nachweise durch das BSI abgefragt werden können. Hier sollte eine zeitliche Orientierung klar kommuniziert und im Gesetz festgehalten werden. Realistisch für mittlere Unternehmen wären hier mindestens vier besser allerdings fünf Jahre. Grundsätzlich sieht der BVMW die Abstufung nach Unternehmensgröße und Kritikalität der Einrichtungen als ein geeignetes Maß an.

Risikomanagement & Berichtspflichten: Unternehmen in der Lieferkette unterstützen

Gerade als mittelständischer Verband ist es uns wichtig, dass die Anforderungen an die Unternehmen in der Lieferkette (§ 30 (4) 4.) sinnvoll gestaltet werden. Denn hier werden voraussichtlich auch Unternehmen betroffen sein, die kleiner sind als mittlere Unternehmen mit 50 Beschäftigten oder 10 Millionen € Umsatz. Aktuell ist es allerdings für viele Unternehmen noch unklar, welche Maßnahmen sie umsetzen müssen und inwiefern Sie als Teil der Lieferkette betroffen sind.

Hier sollte frühzeitig Klarheit geschaffen werden. Die Anforderungen an Unternehmen in der Lieferkette sollten frühzeitig bekanntgegeben werden. Außerdem sollten auch relativ genau angegeben werden, welche Maßnahmen erforderlich sind. Es sollten auch, wie in Punkt eins erwähnt, keine strikteren Vorgaben im Vergleich zur EU-Ebene eingeführt werden. Der Gesetzgeber sollte hier auch an eine Unterstützung indirekt betroffener Unternehmen denken und bereits getroffene Maßnahmen wie z.B. ISMS-Zertifizierungen nach Möglichkeit anerkennen.

Melde- und Dokumentationspflichten effizient umsetzen

Innerhalb von 24 Stunden nach Kenntnisnahme eines Sicherheitsvorfalls muss eine erste Meldung als Frühwarnung bei den zuständigen Behörden eingehen. In dieser wird angegeben, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist. Innerhalb von 72 Stunden muss dann ein weiterer Bericht ausgehändigt werden, der die sogenannten „Indicators of Compromise“ beschreibt und der ohne dediziertes Security-Know-how zu einer fast unlösbaren Aufgabe wird. Spätestens einen Monat nach dem Vorfall ist schließlich noch ein Abschlussbericht fällig, der mindestens eine ausführliche Beschreibung des Sicherheitsvorfalls, seines Schweregrads und seiner Auswirkungen sowie Angaben zur Art der Bedrohung und den getroffenen Abhilfemaßnahmen beinhalten muss.

Der BVMW sieht KMU und insbesondere auch wachsende Unternehmen, die kurz davor sind, 50 Beschäftigte zu überschreiten vor großen Problemen. Zur Meldung in der kurzen Zeit fehlen hier in der Regel das Personal und das Wissen sowie die finanziellen Mittel, um weiteres Personal einzustellen. Um die Meldepflichten möglichst praxistauglich zu gestalten, sollten sie einfach und unbürokratisch umgesetzt werden. Auch sollte es im Nachhinein noch möglich sein, die Berichte bei geänderter Lage oder zusätzlichen gewonnener Informationen anzupassen. Zu begrüßen ist es, dass es mit dem BSI lediglich eine Meldestelle vorgesehen ist. Das BSI sollte nach dem Once-Only-Prinzip bei Bedarf Informationen an weitere Behörden weitergeben können, um zusätzliche Angaben und Anträge zu vermeiden.

Unterstützung von staatlicher Seite für KMU

In den zuvor genannten Punkten wurden bereits einige Probleme identifiziert. Generell sehen wir große Probleme bei der Umsetzung, gerade bei neu betroffenen kleinen und mittleren

Unternehmen. Die Unklarheit für Unternehmen in der Lieferkette, aber auch die Anforderungen an neu betroffene Unternehmen sind keine leichten Aufgaben. Deswegen wäre es gut, wenn Maßnahmen zur Umsetzung durch rechtsverbindliche Hilfsangebote wie Leitfäden unterstützt werden. Aber auch die finanzielle Förderung von Maßnahmen in diesem Bereich ist ein sinnvoller Weg, um Unternehmen bei Maßnahmen zu unterstützen.

Auf Bundesebene könnte das Förderprogramm „Digital Jetzt" genutzt werden. Allerdings würden die zusätzlichen Ausgaben durch die Anforderungen an die NIS-2 Richtlinie das bereits vorhandene Budget übersteigen. Deswegen wäre hier eine Aufstockung bezogen auf Maßnahmen zur Umsetzung des NIS2UmsuCG notwendig. Schon jetzt muss man feststellen, dass die Nachfrage das Angebots in diesem Programm schon sehr übersteigt. Für ein spezifisches Förderangebot wäre auch ein bürokratiearmes Programm ähnlich der Förderlinie Digitale Sicherheit des Programms Mittelstand Innovativ & Digital in Nordrhein-Westfalen mit einer speziellen Förderlinie für die Umsetzung der Maßnahmen in der NIS-2 Richtline in direkt und indirekt betroffenen Unternehmen denkbar.

Bußgelder an mittlere Unternehmen anpassen und transparent gestalten

Das Diskussionspapier sieht in § 60 (5) einen Stufenansatz bei allgemeinen Tatbeständen vor. Hier wird auch nicht zwischen den Betreibergruppen unterschieden. Die Strafen von bis zu 100.000€ über bis zu 500.000€ bis zu zwei oder 20 Millionen €[3] in der höchsten Kategorie sind dabei sehr beträchtlich und gehen über die Grenzen in der NIS-2 Richtlinie hinaus (Art. 34 Abs. 4 und 5)[4]. Darüber hinaus sind für weitere Tatbestände (z.B. eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gemacht) bei wichtigen Einrichtungen (§ 60 (6)) Bußgelder bis zu 7 Millionen € oder 1,4 Prozent des Umsatzes definiert. Bei besonders wichtigen Einrichtungen (§ 60 (7)) kann dies sogar bis zu 10 Millionen € oder 2 Prozent des Umsatzes bedeuten. Ansonsten gleichen sich die Höhe der Bußgelder an den Stufen der allgemeinen Tatbestände.

Wenn die oben genannten Sanktionen auch in der Höhe umgesetzt werden, kann dies dazu führen, dass die finanzielle Tragfähigkeit von Unternehmen, insbesondere von mittelständischen Unternehmen, stark gefährdet wird. Um mittelständische Unternehmen nicht zu überlasten und zu verunsichern, sollte bei den allgemeinen Tatbeständen eine weitere Differenzierung über das Stufenmodell hinaus stattfinden. Hier kann man sich an § 60 (6) und (7) orientieren und eine Abstufung einführen. Auch sollte Transparenz hergestellt werden, an welchen Maßstäben die Höhe der Bußgelder bemessen wird. Dazu ist mit dem Stufenmodell schon ein Anfang gelungen. Allerdings sind detailliertere Informationen dazu für Unternehmen hilfreich, damit Unsicherheit gar nicht erst entsteht.

Ein kooperativer Ansatz zur Durchsetzung der Maßnahmen hilft unserer Meinung nach das Cybersicherheitsniveau nachhaltig zu erhöhen. Denn wenn Unternehmen ermöglicht wird aus ihren Fehlern zu lernen, ist dies aus unserer Sicht nachhaltiger als eine Sanktionierung mit Bußgeldern. Denn wie bereits erwähnt sehen wir die Vorgaben als sehr umfangreich und aufgrund bereits genannter Probleme als schwierig umsetzbar an.

---

3 Hier werden im Gesetzestext zwei Millionen € als höchste Stufe und in der Begründung (auf Seite 53) zwanzig Millionen € erwähnt. Der Unterschied in beiden Texten sollte geklärt werden.

4 Richtlinie des europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (vom 14.12.2022)

Kontakt
Der Mittelstand. BVMW e.V.
Bereich Politik und Volkswirtschaft
Potsdamer Straße 7, 10785 Berlin
Telefon: + 49 30 533206-0, Telefax: +49 30 533206-50
E-Mail: politik@bvmw.de; Social Media: @BVMWeV