Bundesvereinigung der Deutschen ERNÄHRUNGS INDUSTRIE

STELLUNGNAHME

Bundesvereinigung der
Deutschen Ernährungsindustrie e. V.
Claire-Waldoff-Straße 7
10117 Berlin
Telefon +49 30 200786-0
cheng@ernaehrungsindustrie.de
www.ernaehrungsindustrie.de

zum Referentenentwurf des
Bundesministeriums des Innern
für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)

Berlin, 01.07.2025

Die Bundesvereinigung der Deutschen Ernährungsindustrie (BVE) dankt dem Bundesministerium des Innern für die Möglichkeit, kurzfristig zu dem überarbeiteten Referentenentwurf zur Umsetzung der NIS-2-Richtlinie in Deutschland „NIS2UmsuCG“ vom 23. Juni 2025 Stellung nehmen zu dürfen. Die BVE möchte auf notwendige Anpassungen in dem Referentenentwurf für die überwiegend kleinen und mittelständischen Unternehmen der Ernährungsindustrie aufmerksam machen.

Hierbei verweisen wir auf unsere Stellungnahme zu vorhergehenden Referentenentwürfen vom 28. Mai 2024 und 1. Juli 2024. Die BVE begrüßt grundsätzlich die Absicht, die Netz- und Informationssicherheit im EU-Binnenmarkt zu stärken und zu harmonisieren. Eine Umsetzung in das nationale Recht sollte jedoch ohne Erweiterungen bzw. Verschärfungen erfolgen.

Nach der Inkraftsetzung des NIS2UmsuCG werden voraussichtlich etwa 29.000 bis 30.000 Unternehmen betroffen sein. Gerade KMUs sind aus unserer Sicht noch nicht ausreichend auf die Umsetzung des NIS2UmsuCG vorbereitet und benötigen gezielt Unterstützung. Aus unserer Sicht sollten vor allem kleine und mittelständische Unternehmen so weit wie möglich entlastet werden. Wir plädieren hierbei dafür nur die rechts-systematisch notwendigen Anpassungen vorzunehmen.
Seit jeher plädieren wir daher im Sinne von „Ein Vorfall eine Meldung“ im Zusammenhang mit der anstehenden Umsetzung der CER-Richtlinie und dem Cyber Resilience Act für effiziente und einfache Meldeprozesse sowie entsprechende Antwortkanäle zu den Unternehmen, die aufgebaut werden müssen, damit diese ihre eigene Betroffenheit prüfen und gegebenenfalls Maßnahmen ergreifen können.
Nach wie vor sollten das NIS2UmsuCG und die Umsetzung der CER-Richtlinie (Kritis-Dachgesetz) stärker miteinander abgestimmt und hierbei die Wirtschaft eng miteinbezogen werden. Wesentliche Regelungsinhalte sollten im Sinne des All-Gefahren-Ansatzes harmonisiert und beide Gesetze gleichzeitig in den Bundestag eingebracht werden.

Ein Hindernis und sehr bürokratisch bleiben die geplanten Regelungen zum zukünftigen Komponenten- bzw. Produkteinsatz in den Unternehmen. Diese zu hohen Anforderungen können die Entscheidungsspielräume der Unternehmen empfindlich einschränken und damit auch die Sicherheit der Infrastruktur schädigen statt schützen. Insbesondere darf die Verpflichtung zur Nutzung von zertifizierten Komponenten und Prozessen gemäß §30 Absatz 6 und die Möglichkeit zum Erlass nationaler technischer Spezifizierungen gemäß §30 Absatz 5 nicht zu Beschaffungsengpässen, zur Bildung von Oligopolen oder Nachteilen im europäischen Wettbewerb führen. Der Einsatz von ausschließlich zertifizierten Komponenten ist für die Aufrechterhaltung eines Regelbetriebs aufgrund Ersatzbeschaffung sehr problematisch und kann im worst-case zum Stillstand der KRITIS führen. Besonders das angedachte Prüfverfahren zu den kritischen Komponenten nach § 41 NIS2UmsuCG sollte entfallen oder muss zumindest durch ein öffentliches, EU-weit abgestimmtes Blacklisting ergänzt werden. Rückwirkende Verbote (Ausbau von Komponenten) bergen aus unserer Sicht häufig mehr Risiken als Sicherheitsgewinn. Gleichzeitig können rückwirkende Verbote im Widerspruch zu anderen europäischen Regelungen wie dem Vergaberecht stehen.

Die Registrierungspflichten gemäß § 33 und § 34 sind aus unserer Sicht unklar und sollten mit § 26 NISUmsCG abgestimmt werden. Hier werden eindeutige Vorgaben für die Wirtschaft benötigt.

Das für besonders wichtige und wichtige Einrichtungen ein anderes Schutzniveau angedacht ist als für Betreiber Kritischer Infrastrukturen wird an einigen Stellen im Gesetzesentwurf klar, jedoch nicht an allen. Dass besonders wichtige Einrichtungen sich einen, ihrem Schutzniveau entsprechenden branchenspezifischen Sicherheits-Standard beim Bundesamt als geeignet anerkennen lassen können hilft diesen Unternehmen zur Orientierung bei Ihrer Auswahl von geeigneten Sicherheitsmaßnahmen. Um auch wichtigen Einrichtungen eine Orientierung zu geben, sollte in der Gesetzesbegründung folgendes aufgenommen werden: „Wichtige Einrichtungen können sich angemessen und risikobasiert an den zukünftigen Branchensicherheitsstandards der besonders wichtigen Einrichtungen für die Vorgaben aus 1. bis 10. §30 Absatz BSIG orientieren."

Aus unserer Sicht darf die Ermächtigung des BSI zur Ausgestaltung des Verfahrens von Prüfungen und der Erbringung von Nachweisen für Betreiber kritischer Anlagen nicht dazu führen, dass international anerkannte Normen und Verfahren sowie auch national etablierte Prüfverfahren, wie z. B. die Branchensicherheitsstandards, nach dem Stand der Technik nicht mehr möglich sind.

Die Aussage der „Vernachlässigbarkeit" in § 28 Abs. 3 und die Aussage in § 30 Abs. 1 zur „Erbringung ihrer Dienste" sollten konkretisiert werden, da beide Punkte in der aktuellen Formulierung Rechtsunsicherheiten schaffen könnten.

Weiter bleibt es notwendig die Begriffsbestimmung im § 2 Nr. 11 BSIG (erheblicher Sicherheitsvorfall) zu konkretisieren. Der Wortlaut kann so verstanden werden, dass jeder nur mögliche finanzielle Verlust, ganz gleich wie groß er ist, zu einem erheblichen Sicherheitsvorfall führt. Da jeder Sicherheitsvorfall allein durch die Behebung zu einem finanziellen Verlust führt, wäre somit diese Regelung uferlos und unverhältnismäßig. Deshalb sollten „finanziellen Verluste" durch „… oder erhebliche finanzielle Verluste für die betreffende Einrichtung, die im Risikomanagement der Einrichtung als relevant eingestuft werden, verursacht hat oder gesichert verursachen kann;" in dem Gesetzestext Ersetzung finden. Grundsätzlich sollte im Hinblick auf die hiermit verbundenen Pflichten stärker nach Art des Sicherheitsvorfalls ausdifferenziert werden, um eine Fehlallokation von Ressourcen zu vermeiden.

Überdies kann der Wortlaut von § 2 Nr. 11 b) so ausgelegt werden, dass auch jeder Datenschutzvorfall mit erheblichen Schäden (Anwendung der Begriffe siehe allgemein gültige Beschreibungen zum Datenschutz nach DSGVO) zusätzlich als „erheblicher Sicherheitsvorfall" betrachtet werden und an das BSI gemeldet werden müsste. Damit erfolgt eine Doppelbehandlung eines Vorfalls mit entsprechendem Mehraufwand für das Unternehmen. Insbesondere ergeben sich in solchen Fällen Mehraufwendungen, da die zeitliche Meldefrist bei Datenschutzvorfällen mit 72h benannt ist und die für Sicherheitsvorfälle auf 24h begrenzt werden soll. Hier sollte deutlicher abgegrenzt werden, wann 11 b) wirklich greifen soll.

Abschließend bewerten wir das Eingriffsrecht des BSI nach § 61 Abs. 9 Nr. 2 BSIG kritisch und zu weitgehend. Die Untersagung der Tätigkeit der Geschäftsleitung sollte, auch wenn diese nur vorübergehender Natur ist, ersatzlos gestrichen werden.

Die BVE möchte als Mitglied des UP KRITIS auch auf dessen Positionspapier verweisen und dessen Unterstützung explizit unterstreichen.

In der Ernährungsindustrie erwirtschaften rund 6.000 Betriebe einen jährlichen Umsatz von 218,5 Mrd. Euro. Mit 637.000 Beschäftigten ist diese Branche der viertgrößte Industriezweig

Deutschlands. Dabei ist die Branche klein- und mittelständisch geprägt: 90 Prozent der Unternehmen der deutschen Ernährungsindustrie gehören dem Mittelstand an. Die Exportquote von 35 Prozent zeigt, dass Kunden auf der ganzen Welt die Qualität deutscher Lebensmittel schätzen.

Für Rückfragen wenden Sie sich bitte an:

Kim Cheng
Geschäftsführerin
Tel: +49 30 200786-143
E-Mail: cheng@ernaehrungsindustrie.de