Bundesvereinigung der Deutschen ERNÄHRUNGS INDUSTRIE

STELLUNGNAHME

Bundesvereinigung der
Deutschen Ernährungsindustrie e. V.
Claire-Waldoff-Straße 7
10117 Berlin

zum Referentenentwurf des Bundesministeriums des Innern und für Heimat zur Umsetzung der NIS-2-Richtlinie in Deutschland „NIS2UmsuCG“ vom 07.05.2024

Berlin, 28.05.2024

Die Bundesvereinigung der Deutschen Ernährungsindustrie (BVE) dankt dem Bundesministerium des Innern für die Möglichkeit zu dem Referentenentwurf zur Umsetzung der NIS-2-Richtlinie in Deutschland „NIS2UmsuCG“ vom 7. Mai 2024 Stellung nehmen zu dürfen. Die BVE möchte auf notwendige Anpassungen in dem Referentenentwurf für die überwiegend kleinen und mittelständischen Unternehmen der Ernährungsindustrie aufmerksam machen. Die BVE begrüßt grundsätzlich, dass die überarbeitete NIS-Richtlinie 2.0 beabsichtigt die Netz- und Informationssicherheit im EU-Binnenmarkt zu stärken und zu harmonisieren. Eine Umsetzung in das nationale Recht muss jedoch mit Augenmaß erfolgen und sollte vor allem kleine und mittelständische Unternehmen so weit wie möglich entlasten. Auch sollten das NIS2UmsuCG und KRITIS-DachG stärker miteinander abgestimmt und hierbei die Wirtschaft eng einbezogen werden.

Es wird begrüßt, dass besonders wichtige Unternehmen und wichtige Unternehmen, nicht das gleiche Schutzniveau wie Betreiber Kritischer Anlagen in deren Anlagen-Scope erreichen sollen. Hierdurch können nach einem risikobasierten Ansatz angemessene Sicherheitsmaßnahmen implementiert werden. Zur Bürokratievermeidung trägt ebenso bei, dass nur auf Anforderung des BSI eine Nachweiserbringung erfolgen muss, so können Unternehmen die knappen Ressourcen besser dem operativen Schutz der Systeme widmen. Ebenso positiv bewertet wird die Erweiterung des Nachweiszyklus auf die international etablierten 3 Jahre für Betreiber Kritischer Anlagen.

Hingegen sollte bei der Neuregelung der Prüfung von Konformitätsbewertungsprogrammen ein nationaler Alleingang vermieden werden, damit die europäischen Anforderungen möglichst harmonisiert umgesetzt werden, insbesondere in Hinblick auf weitere europäische Regelungen (z.B. den CRA), damit hier nicht nachträglich nachgebessert werden muss. Ein Hindernis und sehr bürokratisch sind jedoch 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. Eine 1:1 Umsetzung des Richtlinientextes in nationales Recht ist vielmehr geboten.

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

Es folgen die wichtigsten Punkte aus Sicht der BVE zusammengefasst:

1. NIS2UmsuCG und KRITIS-DachG sollten stärker miteinander abgestimmt, wesentliche Regelungsinhalte im Sinne des All-Gefahren-Ansatzes harmonisiert und beide Gesetze gleichzeitig in den Bundestag eingebracht werden. Es muss das Prinzip gelten: 1 Vorfall 1 Meldung. Die

behördlichen Abstimmungsprozesse sind entsprechend sicher zu gestalten. In Hinblick auf die Bewältigung terroristischer oder militärischer Bedrohungen kritischer Infrastruktur wird auf die mangels Kompetenz der Betreiber kritischer Anlagen drohende „Resilienz-Lücke“ hingewiesen, die staatlicherseits durch eine bessere Unterstützung geschlossen werden muss.

2. 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. Das 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 wichtige Einrichtungen für die Vorgaben aus 1. bis 10. §30 (2) BSIG orientieren.“

3. Nach der Inkraftsetzung des NIS2UmsuCG werden voraussichtlich etwa 29.000 bis 30.000 Unternehmen betroffen sein. Diese Unternehmen müssen künftig dem BSI erhebliche Sicherheitsvorfälle melden. Das Bundesamt benötigt geeignete Technologien und Prozesse, um diese „Meldeflut“ zu bewältigen (E-Mails oder Portale mit ausschließlich manueller Verarbeitung sind ungeeignet) und, was noch wichtiger ist, relevante Meldungen/Informationen zu identifizieren und an die zuständigen Stellen und die betroffenen Unternehmen weiterzuleiten damit diese ihre eigene Betroffenheit prüfen und gegebenenfalls Maßnahmen ergreifen können.

4. Notwendige Begriffsbestimmung im § 2 Abs. 1 Nr. 10 BSIG (erheblicher Sicherheitsvorfall): Der Wortlaut des Referentenentwurfes 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. Verstärkt wird dies dadurch, dass nach dem Wortlaut des Referentenentwurfes der finanzielle Verlust gar nicht eingetreten sein muss, sondern allein die Möglichkeit des Eintritts ausreicht. 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.

5. Bezüglich § 33 BSIG Registrierungspflicht Abs. 1 Nr. 4: Auflistung der Mitgliedsstaaten der EU, in denen die Dienste erbracht werden, ist klarzustellen, ob hier der Sitz der Kunden in den Mitgliedsstaaten gemeint ist oder tatsächlich der Dienst. Es stellt sich die Frage nach der Definition des Begriffes „Dienste… erbringen“. Bedeutet dies, dass die Dienste in einem Land produziert werden oder genutzt werden können. Hier muss eine praxistaugliche Regelung getroffen werden, da sich hier in den Geschäftsbeziehungen kurzfristig viele Änderungen ergeben können, die nur mit hinreichenden Fristen überhaupt registriert werden können.

6. Klarstellung benötigt auch §34 BSIG Registrierungspflicht für bestimmte Einrichtungsarten: Abs. 1 Nr. 3 (Anschrift der Hauptniederlassung). Die Definition der Hauptniederlassung und die Auswirkung auf die Tochtergesellschaften in einem Konzernkonstrukt ist nach wie vor unklar. Die Verweise sind hier noch anzupassen, insb. in Bezug auf die Hauptniederlassungsfrage für den IT-Betrieb sind die Zuständigkeiten und Anforderungen deutlich zu definieren.

7. In der NIS-2 wird von der Beherrschung von Risiken für die Erbringung der Dienste gesprochen, das NIS2UmsuCG (§30 (1)) spricht jedoch von der Vermeidung von Störungen in informationstechnischen Systemen, Komponenten und Prozesse, die für die Erbringung ihrer Dienste genutzt werden. Hier fehlt ein qualifizierender Faktor, dass die Störung überhaupt Relevanz für die Diensterbringung hat und es somit ein zu beherrschendes Risiko gibt.

8. Das bestehende Prüfverfahren zu den kritischen Komponenten welches in §41 BSIG überführt wurde, sollte entfallen oder durch eine, den KRITIS Betreibern zur Verfügung gestellten, Ausschlussliste ersetzt werden.

9. Die Verpflichtung zur Nutzung von zertifizierten Komponenten und Prozessen §30 (6) BSIG und die Möglichkeit zum Erlass nationaler technischer Spezifizierungen §30 (5) BSIG dürfen nicht zu Beschaffungsengpässen oder Nachteilen im europäischen Wettbewerb führen.

10. Konformitätsbewertung und Konformitätserklärung §55 BSIG wurde ohne entsprechendes Gegenstück in der NIS2 neu aufgenommen. § 55 BSIG ist zu streichen: Eine Regelung, welche eine einzelstaatliche „Konformitätserklärung“ gegen nationale Technischen Richtlinien etabliert, stellt einen Sonderweg dar, welcher die europäischen Harmonisierungsbemühungen (u. a. anderen im Cybersecurity Act (CSA) und Cyber Resilience Act (CRA)) konterkariert. Konformitätsbewertung und die fachliche Qualifikation der Prüfstellen sollten im Sinne der Internationalisierung des nationalen Cybersicherheitsrechts auf Grundlage internationalen Standards erfolgen.

11. Im §58 (4) BSIG wurde, ein für die Wirtschaft sehr wichtiger Punkt, der bisher erfolgreich gelebte Praxis war, gestrichen: Die Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der Wirtschaftsverbände beim Erlass oder Änderung der Verordnung zur Identifizierung von Kritischen Anlagen. Wir empfehlen, dass diese Beteiligung, wie im Erläuterungsteil auf Seite 171 formuliert, wieder aufgenommen wird und im Rahmen der Einführung des KRITIS-DachG weiterhin Anwendung findet.

12. Behördliche Eingriffe in betriebliche Abläufe und Entscheidungen sind geplant, hier bedarf es aber einer Klärung zum Weiterbetrieb und Haftung bei Eingriff in die Geschäftsführung durch das BSI nach § 65 Absatz 10 (2) BSIG oder sonstige Aufsichtsbehörde § 65 (9) BSIG. Auch ist im § 11 (1) BSIG geregelt, dass die für den Betreiber zuständige Behörde bei einem herausgehobenen Fall, dass BSI um Unterstützung ersuchen und den IT-Betrieb übernehmen lassen kann. Gegenwärtig ist nicht geregelt, wer den Betrieb leiten oder führen soll und z.B. für Schäden haftet, die im Zusammenhang mit diesem Eingriff durch das BSI entstehen. Sofern diesbezüglich keine Klärung im Gesetz erfolgt, sollte der Regelungsinhalt ganz entfallen.

13. Nach §13 (1) 2 BSIG darf das Bundesamt Sicherheitsmaßnahmen und den Einsatz bestimmter Sicherheitsprodukte empfehlen. Entweder ist der §13 (1) 2 BSIG zu streichen, oder es sollte zumindest in der Gesetzesbegründung darauf hingewiesen werden, dass es keine Ermächtigung darstellt.

14. Für Rechenzentrumsbetreiber droht eine Überregulierung, die weit über die EU-Anforderungen hinausgeht, da alle benötigten Anlagen und Infrastrukturen, insbesondere die für die Stromverteilung, mit einbezogen werden (§ 2 Abs. 1 Nr. 34 BSIG).

15. Wir begrüßen die Integration des Schutzziels Authentizität im international etablierten Schutzziel Integrität, um hier nicht von internationalen Standards abzuweichen. An einigen Stellen des Entwurfes wird das Schutzziel jedoch weiterhin adressiert (z.B. §2 (22) BSIG und §30 (2) 10 BSIG).

16. Ausnahmetatbestände für Bundesministerien und -Behörden erschließen sich der Wirtschaft nicht, (z.B. in §29 BSIG). Wir empfehlen ergänzend zu dem vorliegenden Referentenentwurf die Wirksamkeit auch im Kontext der Landesbehörden und kommunalen Einrichtungen abzustimmen, da diese Organe wesentlich zur Sicherheit der Bevölkerung beitragen.

In der Ernährungsindustrie erwirtschaften rund 6.000 Betriebe einen jährlichen Umsatz von 233 Mrd. Euro. Mit über 643.000 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: