[redacted]

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Herrn Prof. Dr. Lars Castellucci
Platz der Republik 1
11011 Berlin

[redacted]

Per E-Mail an innenausschuss@bundestag.de

Neckarsulm, 30.10.2024

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

Sehr geehrter Herr Abgeordneter,

beiliegende Stellungnahme zu dem oben genannten Gesetzentwurf übersende ich Ihnen mit der Bitte, diese an die Berichterstattenden der Fraktionen und Mitglieder des Ausschusses weiterzuleiten.

Mit freundlichen Grüßen

[redacted]

[redacted]

Stellungnahme

[redacted]

zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
Drucksache 20/13184

[redacted]

1. Grundsätzliche Anmerkungen

Ziel der NIS2-Richtlinie ist die Einführung verbindlicher Maßnahmen für Verwaltung und Wirtschaft, mit denen in der gesamten Europäischen Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll. Dies trägt zur Stärkung der europaweiten Harmonisierung der Cybersicherheitsregulierung bei – ein richtiger Schritt im Kontext der angespannten Bedrohungslage im Cyberraum. Auch kritische Infrastrukturen, die öffentliche Hand und Politik stehen immer stärker im Zentrum von Cyberangriffen. Dies stellt eine bedeutsame Bedrohung des Gemeinwesens dar. Auf Grund der Abhängigkeit einzelner Unternehmen von funktionierenden Lieferketten, Infrastruktur und Behörden, ist die übergreifende Definition und Durchsetzung eines Mindestsicherheitsniveaus begrüßenswert und notwendig.

NIS2 umfasst gegenüber der NIS1 sinnvolle Verbesserungen. Hierbei sind im Besonderen hervorzuheben: Die Konkretisierung der geforderten Absicherungsmaßnahmen sowie Fokussierung auf ein aktives Management zur Behandlung von Cyberrisiken.

Die geforderten Absicherungsmaßnahmen sind angemessen und folgen Best-Practices, welche im Wesentlichen von Unternehmen und Organisationen ohnehin aus Eigeninteresse zum Schutz gegen Cyberbedrohungen, getroffen werden sollten.

2. Kongruenz mit dem KRITIS-Dachgesetz

Das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) und das KRITIS-Dachgesetz sollten stärker aufeinander abgestimmt werden (insb. bei den definierten Sektoren und zuständigen Behörden). Sowohl das NIS2UmsuCG wie auch das KRITIS-Dachgesetz zielen auf den Schutz kritischer Infrastrukturen ab. Im Besonderen bei hybriden Angriffsszenarien ist eine klare Abgrenzung des Schutzes des physischen Raums und des Cyberraums oft nicht eindeutig möglich. Insofern ist auch auf gesetzlicher Ebene ein ganzheitliches, aufeinander abgestimmtes Schutzkonzept erforderlich. Unternehmen, die von beiden gesetzlichen Regelwerken betroffen sind, können vor verschiedenen Herausforderungen stehen, wie z.B. doppelte Meldepflichten an unterschiedliche Behörden (aktuell Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Bundesamt für Sicherheit in der Informationstechnik (BSI) und andere sektorale Aufsichtsbehörden). Während die NIS2-Richtlinie auf eine Harmonisierung auf EU-Ebene abzielt, könnten parallele Regelungen wie das KRITIS-Dachgesetz zu Lücken oder Überschneidungen führen. Dies kann für unnötige Bürokratie, Effizienzverluste und Unsicherheiten bei den betroffenen Unternehmen sorgen. Es gilt daher mit dem NIS2UmsuCG und dem KRITIS-Dachgesetz ein einheitliches Verständnis darüber zu entwickeln, wie physische Sicherheit und Cybersicherheit gemeinsam umgesetzt werden können. Dies umfasst auch die abgestimmte Operationalisierung von Anforderungen aus beiden Gesetzen wie z.B. Risikomanagementmaßnahmen, Bewältigung von Sicherheitsvorfällen oder Notfall- und Krisenmanagement.

Die in § 32 definierte gemeinsame Meldestelle für das BSI sowie das BBK ist hierbei eine positive Entwicklung.

3. Europaweit einheitliche Nachweis-, Melde- und Registrierungspflichten

Die definierten Nachweis-, Melde- und Registrierungspflichten können zu einer besseren präventiven Absicherung sowie einer besseren Reaktion auf Cyberangriffe auf nationaler und europäischer Ebene sowie in einzelnen Organisationen führen. Jedoch können unterschiedliche Umsetzungen der jeweiligen Mitgliedsstaaten bei den geforderten Nachweis-, Melde- und Registrierungspflichten für EU-weit agierende Unternehmen eine Herausforderung darstellen und effektive Reaktionen auf Cyberangriffe erschweren.

So muss ein Sicherheitsvorfall, der in mehreren Mitgliedstaaten Auswirkungen auf die Erbringung der kritischen Dienstleistung haben kann, jeweils an die jeweiligen Computer Security Incident Response Teams (CSIRT) der Mitgliedsstaaten gemeldet werden. Hier wären eine weitere Konkretisierung und Vereinfachung der Meldepflichten auf EU-Ebene begrüßenswert.

Gleiches gilt für in Teilen unterschiedliche Anforderungen der Mitgliedsstaaten hinsichtlich der Nachweispflichten. Dies kann zu Mehrfachprüfungen der gleichen Infrastruktur bei EU-weit agierenden Unternehmen führen.

[redacted]

Ein möglicher Lösungsansatz ist Nachweis-, Melde- und Registrierungspflichten auf den Mitgliedsstaat zu beschränken, in dem die jeweilige IT-Infrastruktur maßgeblich (physisch und damit lokal vor Ort in einem Mitgliedsstaat) betrieben wird.

4. Überprüfung Risikomanagementmaßnahmen

Neben dem Fokus auf reaktive Risikomanagementmaßnahmen, wie die Erkennung und Bewältigung von Sicherheitsvorfällen oder Krisenreaktion, ist auch die Berücksichtigung von präventiven Sicherheitsmaßnahmen wie z.B. die Identifikation von durch Angreifer ausnutzbare Sicherheitslücken oder Fehlkonfigurationen von IT-Systemen wichtig und hervorzuheben, um erfolgreiche Angriffe bestmöglich zu vermeiden. Hierbei ist im Besonderen bei weiteren Konkretisierungen wie z.B. im Rahmen von Durchführungsverordnungen der EU zu beachten, dass die Technologieoffenheit gewahrt bleibt und Unternehmen weiterhin die Möglichkeit haben die identifizierten Risiken auf die jeweilige Situation angepasst nach aktuellen Best Practices zu mitigieren.

Auf Grund der stetigen Veränderung des Angreiferverhaltens im Cyberraum, der technischen Innovationen im Kontext der Digitalisierung sowie der Automatisierung von Verteidigungsmaßnahmen, sollten die konkreten Anforderungen an nicht-technische Maßnahmen und eingesetzte Technologien von den Gesetzgebungsprozessen entkoppelt werden. Darüber hinaus sollten die technischen Anforderungen und Maßnahmen regelmäßig überprüft und bei Bedarf angepasst werden.

5. Wichtigkeit der Rolle des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Während unter der vorherigen Regulierung eine mittlere vierstellige Anzahl an Unternehmen von Cybersicherheitsmindestanforderungen und Meldepflichten betroffen waren, erhöht sich diese Anzahl auf rund 29.500 Unternehmen, bei gleichzeitiger Kürzung des BSI-Haushalts für 2025[1]. Das BSI ist zentrale Anlaufstelle aller betroffenen oder potenziell betroffenen Unternehmen in Bezug auf das NIS2UmsuCG und der Umsetzung der darin enthaltenen Risikomanagementmaßnahmen, Registrierungs- und Meldepflichten. Durch die Bereitstellung geeigneter Tools, wie der NIS-2-Betroffenheitsprüfung, das Erstellen von Orientierungshilfen oder FAQs, das Versenden von IT-Tageslageberichten oder die Teilnahme an Themenarbeitskreisen sowie Branchenarbeitskreisen, leistet das BSI einen wesentlichen Beitrag, um in gemeinsamer Zusammenarbeit das Cybersicherheitsniveau auf nationaler, aber auch internationaler Ebene nachhaltig zu erhöhen. Eine eingeschränkte Arbeits-/Leistungsfähigkeit des BSI könnte der effektiven Umsetzung des NIS2UmsuCG bei den betroffenen Unternehmen entgegenstehen.

Meldungen der von NIS2UmsuCG betroffenen Unternehmen entfalten nur dann die gewünschte Wirkung, wenn diese zeitnah und fachgerecht durch das BSI (CSIRT) verarbeitet werden und abgeleitete Informationen und Berichte an die Unternehmen weitergegeben werden.

Die gute Zusammenarbeit zwischen Unternehmen und dem BSI ist ein wesentlicher Erfolgsfaktor für die Verbesserung der Cybersicherheit in Deutschland und sollte daher weiter gestärkt und ausgebaut werden.

6. Cybersicherheit ist eine gesamtgesellschaftliche Aufgabe

Ein effektives Cybersicherheitsniveau kann nicht allein durch das BSI oder die jeweiligen Sicherheitsfunktionen in Unternehmen gewährleistet werden. Vielmehr ist dies eine gesamtgesellschaftliche Aufgabe.

Das NIS2UmsuCG erweitert den Anwendungsbereich auf zahlreiche neue unter die Regulierung fallende Unternehmen und wird große Teile der deutschen Wirtschaft betreffen.

Der Ausschluss staatlicher Stellen und Behörden im NIS2UmsuCG ist der falsche Weg und schwächt die staatliche Vorbildfunktion und das einheitliche Cybersicherheitsniveau.

---

[1] BMI-Pressemitteilung 24.07.2024 (Wirtschaft und Staat vor Cyberattacken schützen: Bundesregierung beschließt umfassende Änderung des IT-Sicherheitsrechts) und Entwurf eines Gesetzes über die Feststellung des Bundeshaushaltsplans für das Haushaltsjahr 2025 (Drucksache 20/12400)

[redacted]

Zur Verbesserung der Cybersicherheit im öffentlichen Sektor gehört neben der Stärkung des BSI und weiterer Sicherheitsfunktionen auch die Modernisierung der IT-Infrastruktur nach Stand der Technik und der Bereitstellung des hierfür erforderlichen Budgets bei Bund, Ländern und Kommunen.

Die im Gesetzesentwurf erwähnten geänderten wirtschaftspolitischen und geopolitischen Rahmenbedingungen machen deutlich, dass die Etablierung eines angemessenen Cybersicherheitsniveaus in Europa auch die Stärkung der europäischen Souveränität im Kontext der eingesetzten IT-Infrastruktur umfassen muss.

[redacted]