STELLUNGNAHME

Berlin, 12. Dezember 2024

Deutsche Industrie- und Handelskammer

Gesetzentwurf der Bundesregierung

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

(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, NIS2UmsuCG)

Das NIS2UmsuCG setzt die EU NIS2-Richtlinie auf nationaler Ebene um. Es führt zusätzliche Maßnahmen und Pflichten zum Risiko- und Krisenmanagement sowie Melde- und Nachweispflichten für eine erheblich größere Anzahl an Unternehmen als bislang ein.

A. Anmerkungen der DIHK in Kürze:

Insgesamt sollte ein umfassender Ansatz verfolgt werden: Dieser sollte digitale und analoge Sicherheit gemeinsam adressieren, auf Arbeitsteilung von Staat und Wirtschaft basieren und prinzipiell auf die Eigenverantwortung der Unternehmen setzen.

Lageinformationen und Unterstützungsangebote für Unternehmen: Informationen zu analogen und digitalen Bedrohungen sollten den betroffenen Unternehmen aus einer Hand zielgerichtet und aktuell zugänglich gemacht werden. Handreichungen für die Umsetzung des NIS2UmsuCG sollten schnellstmöglich in verständlicher Form sowie eine zentrale Ansprechstelle für Unternehmen bereitgestellt werden. Das geplante Information Sharing Portal ist ein guter Ansatz, der zeitnah mit Leben gefüllt werden muss. Unternehmen wünschen sich darüberhinausgehende konkrete Unterstützungsangebote, z. B. bei (freiwilligen) Vertrauenswürdigkeitsüberprüfungen von Personal.

Doppelregulierungen vermeiden und bürokratische Belastungen so gering wie möglich halten, klare Orientierung am Angemessenheitsprinzip: Je mehr rechtliche Verpflichtungen aus unterschiedlichsten Gesetzen Unternehmen prüfen und erfüllen müssen, desto weniger Spielräume bleiben fürs eigentliche Geschäft und echte Cybersicherheitsmaßnahmen. Registrierungs- und Meldepflichten im Rahmen des NIS2UmsuCG sollten durchgängig digital und so effektiv wie

möglich erfolgen. Die 24-Stunden-Frist für Erstmeldungen von Vorfällen sollte im Hinblick auf kleinere Unternehmen geprüft werden. (z. B. Leistbarkeit durch die Unternehmen, Verarbeitungskapazitäten beim BSI und Mehrwert für beide Seiten).

Transparente und effektive Sicherheitsarchitektur gewährleisten: Zusammenarbeitsprozesse der Behörden untereinander und zwischen Behörden und Unternehmen sollten von Beginn an klar definiert und umgesetzt werden. Eine effektive Cybersicherheitsarchitektur und eine angemessene Ausstattung der Sicherheitsbehörden sind Voraussetzung, um Unternehmen sowohl präventiv wie im Schadensfall zu unterstützen.

Umfassende Aufnahme der öffentlichen Verwaltung in den Anwendungsbereich: Neben Bundesbehörden sollten auch Behörden der Länder und Kommunen die gleichen Verpflichtungen wie die Unternehmen umsetzen, denn sie sind Teil der Wertschöpfungsketten der Unternehmen. Die Bundesländer sind aufgefordert, dafür einen entsprechenden rechtlichen Rahmen sowie weitere Voraussetzungen für die Umsetzung zu schaffen.

B. Allgemeine Anmerkungen

Für Unternehmen ist Cyber-Sicherheit schon aus eigenem Interesse ein extrem wichtiges Thema. Sie wünschen sich zur Erhöhung der (Cyber)sicherheit insbesondere:

- Ein arbeitsteiliges Vorgehen, das prinzipiell auf die Eigenverantwortung der Unternehmen setzt, praxisorientierte Unterstützungsangebote und ein passgenaues Lagebild, auf dessen Basis Unternehmen ihre knappen Ressourcen priorisiert und effizient einsetzen können,
- dass die öffentliche Hand sich selber schützt und handlungsfähig bleibt,
- Schutz der Unternehmen durch staatliche Behörden und eine intensive und nachhaltige Strafverfolgung – national, europäisch und international.

Im Gegensatz dazu wünschen sich die Unternehmen **NICHT**:

- **Überregulierung**, inkonsistente Regulierung und bürokratische Hürden, die sie daran hindern, ihre begrenzten Kapazitäten für die konkrete Verbesserung ihrer Sicherheit und Resilienz zu nutzen. Deshalb ist ein engmaschiges Monitoring erforderlich, ob die zusätzlichen Verpflichtungen für Unternehmen tatsächlich zu einem erhöhten Sicherheitsniveau führen, und ggf. korrigiert werden.

Das Ziel des Gesetzes, ein hohes gemeinsames Sicherheitsniveau sicherzustellen, unterstützt die DIHK ausdrücklich. Staat und Wirtschaft sind gemeinschaftlich gefordert, die Sicherheit grundlegender Infrastrukturen und Anlagen und der Wirtschaft insgesamt zu gewährleisten. Angesichts der zunehmenden Gefährdungslage und der durch die Digitalisierung bedingten immer breiteren Angriffsfläche ist ein fähigkeitsbezogener Ansatz erforderlich, der Kapazitäten bündelt und gerade kleinere Unternehmen nicht überfordert. Das gemeinsame Ziel sollte in

erster Linie durch praxistaugliche Unterstützungsangebote und aktuelle, relevante, zielgerichtete und konkret an den Bedarfen der Unternehmen ausgerichtete Lageinformationen und Umsetzungshilfen angestrebt werden. Darüberhinausgehende Verpflichtungen sowie zusätzliche Nachweis- und Meldepflichten für die Unternehmen sollten klar dem Angemessenheitsprinzip folgen und gerade kleinere Unternehmen nicht überfordern.

Die DIHK weist an dieser Stelle ausdrücklich darauf hin, dass in den letzten Jahren sehr viele digitalpolitische Gesetze verabschiedet wurden. Die neuen Richtlinien und Verordnungen aus den Bereichen Daten, Cybersicherheit, Plattformökonomie und KI decken einen Großteil des digitalen Marktes und der digitalen Technologien ab und entfalten teils tiefgreifende Auswirkungen auf europäische Unternehmen. Während dies in einigen Fällen zu besseren Wettbewerbsbedingungen und mehr Rechtssicherheit führen wird, zeigen sich viele Unternehmen – insbesondere KMUs – von der Menge an neuen Regulierungen überfordert und entscheiden sich gegen wichtige Investitionen in digitale Zukunftstechnologien. Hinzu kommen zahlreiche Regelungen aus anderen Sachbereichen wie Lieferketten, Corporate Social Responsibility etc., die die Unternehmen zusätzlich belasten. Dadurch verliert der Wirtschaftsstandort Europa an Wettbewerbsfähigkeit. Deutschland ist besonders betroffen. Die hohe Zahl an kleinen und mittleren Unternehmen inklusive der hohen Zahl an mittelgroßen Weltmarktführern in Nischenmärkten gilt europäisch und international als einzigartig. Wenn auf europäischer Ebene Regulierungen beschlossen werden, treffen diese die deutsche Wirtschaft in der Gesamtbetrachtung stärker als die Wirtschaft andere europäische Länder, weil sie den deutschen Mittelstand überproportional belasten. Wenn angesichts der geopolitischen Lage die Sicherheit der Gesamtwirtschaft höchste Priorität hat, sollte sich der Staat bei anderen Auflagen zurückhalten und die Unternehmen aktiv bei der Erhöhung der gesamtwirtschaftlichen Resilienz unterstützen.

Alle Beteiligten sollten gemeinsam im Blick behalten, dass der vorliegende Gesetzentwurf nur ein Baustein unter vielen sein kann, um die Resilienz der Wirtschaft insgesamt auf ein höheres Niveau zu heben. Vor allem aktive Unterstützungsmaßnahmen und eine zeitgemäße Aufstellung der öffentlichen Hand – sowohl im Hinblick auf die eigene Cybersicherheit als auch im Hinblick auf ein effektives Zusammenspiel der Sicherheitsbehörden, die Cybersicherheitsarchitektur – sollten im Fokus von Politik, Verbänden, Kammern bleiben und kontinuierlich und kooperativ weiterentwickelt werden. Die IHK-Organisation trägt gern ihren Teil bei, um die Angebote in die Breite der Unternehmerschaft zu tragen und die Betriebe konkret zu unterstützen.

Gesamtkonzept erforderlich

NIS2UmsuCG, KritisDachG, Wirtschaftsschutzstrategie, Nationale Sicherheitsstrategie und andere Ansätze stehen aktuell nebeneinander. Digitale Identitäten für natürliche und juristische Personen und Dinge – eine der Grundvoraussetzungen für ein vertrauensvolles Miteinander in

der digitalen Welt – sind konzeptionell nicht verzahnt und kommen seit Jahren nicht in die breite Anwendung.

Erforderlich wäre ein Gesamtkonzept, das analoge und digitale Sicherheit von Staat, Wirtschaft und Gesellschaft umfassend und gleichermaßen adressiert, bürokratische Verpflichtungen für Unternehmen auf ein absolutes Minimum begrenzt und in die europaweiten Aktivitäten eingebettet ist. Dieses muss zeitnah in der anstehenden Legislaturperiode auf den Weg gebracht werden.

Rechts- und Planungssicherheit für Unternehmen schaffen

Im Sinne eines All-Gefahren-Ansatzes wäre wünschenswert gewesen, die Referentenentwürfe zum NIS2UmsuCG und zum KRITIS-Dachgesetz zumindest parallel zur Diskussion zu stellen. Die parallelen Gesetzesvorschläge führen im Hinblick auf die verwendeten Begriffe und Definitionen, auf die Umsetzungsprozesse und in Bezug auf die Kompetenzen der beteiligten Behörden zu einer komplexen Vorgabesystematik, deren wechselseitige Abhängigkeiten und Zuständigkeiten der einzelnen Behörden eine Umsetzung für Unternehmen unnötig erschweren. Prinzipiell könnte eine Reduzierung der Vorgaben zu mehr Transparenz und Planungssicherheit beitragen.

Der Gesetzentwurf selber enthält noch immer Definitionen und Kategorien, die zu Interpretationsschwierigkeiten und zu großer Komplexität führen, etwa bei der Betroffenheitsprüfung. Eine klarstellende Verordnung sollte parallel erarbeitet werden, ein Entwurf liegt noch nicht vor, bzw. ist der DIHK nicht bekannt.

Erforderlich ist ein konsistenter Ordnungsrahmen, der den Unternehmen verlässliche Orientierung gibt und größtmögliche Transparenz über die rechtlichen Verpflichtungen herstellt.

EU-weite Harmonisierung gewährleisten

Mit der NIS2-Richtlinie beabsichtigt der EU-Gesetzgeber eine EU-weite Harmonisierung der Cybersicherheit. Die Bundesregierung sollte die Anforderungen der NIS-2-Richtlinie daher 1:1 in nationales Recht umsetzen. Europaweit harmonisierte Anforderungen sind insbesondere für EU-weit agierende Unternehmen von entscheidender Bedeutung, da sie sonst in jedem EU-Mitgliedsstaat abweichende Lösungen implementieren müssen.

Umsetzungsfristen pragmatisch anpassen

Insgesamt wird durch die zunehmende Zahl an gesetzlich vorgegebenen Sicherheitsanforderungen an immer mehr Unternehmen der bereits sehr hohe Bedarf an IT-Sicherheitsfachkräften in den kommenden Jahren noch weiter zunehmen. Unternehmen müssen ihre internen Prozesse überprüfen beziehungsweise Prozesse neu etablieren, Meldewege bedienen, Erreichbarkeiten sicherstellen, Schulungen organisieren etc. Dies kostet nicht nur

Ressourcen bei den Mitarbeitenden in den Unternehmen, es müssen zum Teil zusätzliche IT-(Sicherheits-)Fachkräfte gewonnen werden. Unternehmen berichten sehr häufig, dass sie die dafür erforderlichen Fachkräfte nicht rekrutieren können. Dies trifft gleichermaßen auf den Aufbau von Organisationsstrukturen und Beschäftigten bei den Kontrollbehörden zu.

Eine risikobasierte zeitliche Streckung der Umsetzungsfristen könnte dazu beitragen, die bereits bestehenden Fachkräfteengpässe zumindest nicht weiter zu verschärfen und die Umsetzungskosten nicht unnötig nach oben zu treiben.

Sichtbaren Sicherheitsgewinn ermöglichen und Unternehmen unterstützen

Die Unternehmen sollten konkreten Mehrwert aus der engeren Interaktion mit dem Staat und seinen Sicherheitsbehörden generieren können. Aus den zusätzlichen Meldepflichten gegenüber dem BSI sollte deshalb ein effektiver Rückkanal in die Unternehmen etabliert werden. Etwa indem Informationen zu analogen und digitalen Bedrohungen und konkrete Warnungen mit entsprechenden Handlungsempfehlungen zielgerichtet ausgetauscht werden. Das geplante Information Sharing Portal ist ein guter Ansatz, der zeitnah mit Leben gefüllt werden muss.

Insbesondere die Unternehmen, die neu in den Anwendungsbereich fallen, benötigen entsprechende Unterstützungsangebote für die Umsetzung. Die erforderlichen Kapazitäten beim BSI müssen über den Haushalt abgebildet werden. Alle Maßnahmen müssen darauf hinwirken, das Schutzniveau der Unternehmen zu verbessern und deren eigene Sicherheitsbemühungen zu unterstützen.

Effektive Cybericherheitsarchitektur und angemessene Ausstattung des BSI für mehr Cybersicherheit in der Wirtschaft

Mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zeichnen zwei unterschiedliche Aufsichtsbehörden für die Umsetzung des KRITIS-Dachgesetzes und des NIS2UmsuCG verantwortlich. Diese müssen sich wiederum mit weiteren sektorspezifischen Aufsichtsbehörden und Behörden der Länder vernetzen. Die Prozesse der Zusammenarbeit zwischen den Behörden sollten effektiv organisiert und Aufgaben und Informationsströme klar definiert bzw. ermöglicht werden. Doppelaufwand für die Unternehmen, z. B. durch Mehrfachmeldungen, gilt es zu verhindern.

Dem BSI werden mit dem Gesetz viele neue Aufgaben zugewiesen. Die Zahl der zu betreuenden Unternehmen erhöht sich drastisch. Die zahlreich zu erwartenden Meldungen müssen ausgewertet und in praxistaugliche Hinweise für die Unternehmen übersetzt werden, Angriffsmethoden müssen detektiert, Unterstützungsleistungen zur Verfügung gestellt, die Verpflichtungen gegenüber der Verwaltung wahrgenommen werden etc. Dafür wird entsprechend qualifiziertes Fachpersonal beim BSI benötigt. Das BSI sollte als Zentralstelle in Hinblick auf Budget

und Befugnisse so aufgestellt sein, dass es den Ansprüchen der Unternehmen auch gerecht werden kann. Die staatliche Cybersicherheitsarchitektur sollte angesichts der sich verschärfenden Gefährdungslage und Angriffsfläche adäquat weiterentwickelt werden. Schwachstellen sollten prinzipiell schnell geschlossen werden. Dafür braucht es geordnete, rechtlich geregelte Verfahren.

Umfassende Einbeziehung der öffentlichen Hand

Für die öffentliche Hand sind abseits der Bundesverwaltung derzeit keine Verpflichtungen vorgesehen. Und selbst große Teile der Bundesverwaltung und sind von vornherein vom Anwendungsbereich ausgenommen. Kommunen sollen entsprechend dem Beschluss des IT-Planungsrates 2023/39 keinen vergleichbaren Verpflichtungen wie die Unternehmen unterworfen werden.

Das stößt bei den Unternehmen auf Unverständnis. Für die Unternehmen ist wichtig, dass sie sich auf funktionierende Prozesse mit der Verwaltung verlassen können. Wesentliche Unternehmensprozesse, beispielsweise Planungs- und Genehmigungsverfahren, in denen die öffentliche Hand Teil der Wertschöpfungskette ist, müssen jederzeit funktionieren. Insbesondere die kommunale Ebene war in den letzten Jahren häufig von Cyberangriffen betroffen und zum Teil länger handlungsunfähig. Bisherige Vereinbarungen unterhalb der Gesetzesebene haben in der Praxis nicht hinreichend gewirkt. Hier wären dringend Vorgaben für ein angemessenes, bundesweit einheitliches Sicherheitsniveau auch auf Seiten der öffentlichen Hand erforderlich. Insbesondere die Bundesländer sind hier in der Pflicht, die entsprechenden Voraussetzungen zu schaffen. Unternehmen erwarten zumindest – etwa im Rahmen des o. g. Gesamtkonzeptes – einen verbindlichen Umsetzungsplan mit konkreten Meilensteinen.

Genauso sollte innerhalb der Bundesverwaltung ein einheitliches Sicherheitsniveau sichergestellt werden. Dafür sollte eine umfassende Einbeziehung der Bundesbehörden in den Anwendungsbereich erfolgen.

C. Konkrete Bewertung des Referentenentwurfs

Erfüllungsaufwand

Nach der neuen Gesetzeslage werden wesentlich mehr Unternehmen als bislang besondere Cyber-Sicherheitsanforderungen umsetzen und nachweisen müssen. Nach Berechnungen des Gesetzgebers entstehen neue Pflichten für mehr als 25.000 Unternehmen, insgesamt umfasst der Anwendungsbereich nahezu 30.000 Unternehmen direkt. Zusätzlich ergeben sich abgeleitete Sicherheitsanforderungen für Unternehmen entlang der Lieferkette. Mit den Anforderungen geht für die Unternehmen nach Berechnungen des Gesetzgebers ein signifikanter Erfüllungsaufwand von geschätzt 2,2 Mrd. Euro jährlich und einmalig 2,1. Mrd. Euro für Prozessanpassungen und Bürokratieaufwände einher.

An dieser Stelle ein grundsätzlicher Hinweis: Beim einmaligen Erfüllungsaufwand sollte auch berücksichtigt werden, dass viel mehr als die tatsächlich betroffenen Unternehmen erst einmal gefordert sind, mit eigenem oder extern eingekauftem juristischen Sachverstand festzustellen, ob sie unter die Regelungen des Gesetzes fallen. Die vielen Fragen der Unternehmen dazu, die die IHKs erreichen, sind häufig nicht einfach zu klären und binden aktuell sehr viele Kapazitäten in den Unternehmen – ein nicht unerheblicher Kostenfaktor.

Die DIHK erwartet, dass die steigende Nachfrage nach IT-Sicherheitsdienstleistungen und IT-Sicherheitsfachkräften Preissprünge bewirken wird. Deshalb ist davon auszugehen, dass der tatsächliche Aufwand für die Unternehmen noch höher ausfallen wird. Insbesondere für die Unternehmen, die erstmalig die vorgesehenen Maßnahmen umsetzen müssen.

Angesichts der enormen Aufwände, die auf die Unternehmen zukommen, sind insbesondere Melde-, Dokumentations- und Nachweispflichten möglichst bürokratiearm und digital auszugestalten.

Begriffsbestimmungen und Rechtsverordnung (BSIG § 2)

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 (BSIG § 2 Abs 1 Nr. 34).

Aufgaben des Bundesamtes (BSIG § 3)

Nach § 3 Abs 1 Nr. 20 darf das BSI nur „Einrichtungen der Bundesverwaltung sowie Hersteller, Vertreiber und Anwender“ beraten informieren und warnen. Diese Aufzählung erscheint zu eng und umfasst nicht alle relevanten Gruppen, z. B. Länder- und Kommunalverwaltungen.

Informationsaustausch (BSIG § 6)

Das BSI betreibt eine Online-Plattform für den Informationsaustausch zwischen Unternehmen und Einrichtungen der Bundesverwaltung (Information Sharing Portal).

Eine effektive Entgegennahme und Aufbereitung von Meldungen sowie die zielgerichtete Information von Unternehmen sind wesentliche Voraussetzungen für eine konstruktive Zusammenarbeit von Staat und Wirtschaft bei der Verbesserung des Cybersicherheitsniveaus. Die Diskussion über entsprechende Ansätze sollte parallel zum Gesetzgebungsverfahren geführt werden, damit die Vorteile für die Unternehmen transparent und greifbar gemacht werden und ein gelebtes vertrauensvolles Miteinander entstehen kann. Das Information Sharing Portal stellt eines der Kernelemente des Gesetzes dar und wird von der DIHK ausdrücklich befürwortet. Über die konkrete Umsetzung liegen aber noch zu wenige Informationen vor.

Das Information Sharing Portal sollte (neben den in der Begründung genannten Informationen) auch aktuelle Lageinformationen der öffentlichen Hand verfügbar machen – zeitnah, verständlich aufbereitet für die unterschiedlichen Zielgruppen mit konkreten Handlungsempfehlungen zu analogen und digitalen Bedrohungsszenarien gleichermaßen. Dazu gehören auch Hilfestellungen und die Möglichkeit, auf konkrete Unterstützungsleistungen zuzugreifen, z. B. eine automatisierte Schnittstelle zur Abfrage aktuell schadhafter Hardware- und Softwarekomponenten. Sowohl für die Registrierung als auch für die Nutzung des Information Sharing Portals sollte das Organisationskonto der öffentlichen Hand (inkl. der Bausteine Rechte und Rollen sowie erweitertes Postfach) mitgenutzt werden können.

Der Betrieb eines Informations Sharing Portals mit Mehrwert bedingt personellen Aufwand im BSI. Das Bundesamt muss sich zeitnah um das entsprechende Fachpersonal bemühen, damit dieser Mehrwert für die Unternehmen entwickelt werden kann. Dafür benötigt es verbindliche Budgetzusagen.

Unterstützung bei der Wiederherstellung in herausgehobenen Fällen (BSIG § 11)

Eine Unterstützung des BSI in herausgehobenen Fällen ist hilfreich.

Allerdings sollte vorher das Einverständnis der betroffenen Unternehmen eingeholt werden, wenn das BSI dabei Dritte kostenpflichtig hinzuzieht. Klargestellt werden sollte, wer für eventuelle Schäden haftet, die im Zusammenhang mit diesem Eingriff durch das BSI entstehen könnten.

Anwendungsbereich (BSIG § 28)

Die besonders wichtigen Einrichtungen und die wichtigen Einrichtungen inkl. der Größenangaben werden direkt im Gesetzestext spezifiziert. Die Auflistung betroffener Einrichtungsarten erfolgt in den Anlagen 1 und 2.

Unternehmen benötigen erst einmal Klarheit über ihre Betroffenheit. Dafür und für die konkrete Umsetzung sind rechtssichere und praxistaugliche Umsetzungshilfen zur Verfügung zu stellen. Mit der starken Ausweitung des Umsetzungsbereichs muss eine verstärkte Kommunikations- und Vermittlungsarbeit einher gehen, insbesondere gegenüber den mittelständisch geprägten Unternehmen bis 250 Beschäftigten.

Es ergeben sich jedoch noch immer viele Fragen im Hinblick auf die konkrete Betroffenheit der Unternehmen bzw. Unternehmensteile und Einrichtungen. Einfache Tools zum Selbstcheck bereits vor dem Inkrafttreten des Gesetzes würden den Unternehmen die erforderliche Sicherheit bei der Umsetzung vermitteln.

Nach dem Entwurf ist davon auszugehen, dass die Risikomanagementmaßnahmen und Nachweispflichten nur abgegrenzte kritische Anlagen einer besonders wichtigen oder wichtigen

Einrichtung umfassen. Dies sollte deutlicher klargestellt werden. Fragen ergeben sich beispielsweise im Hinblick auf Vertriebsinfrastrukturen wie Online-Marktplätze.

Einrichtungen der Bundesverwaltung (BSIG § 29)

Für Einrichtungen der Bundesverwaltung finden grundsätzlich die Regelungen für "besonders wichtige Einrichtungen" Anwendung, jedoch z. B. nicht die in § 30 aufgeführten Risikomanagementmaßnahmen (lediglich für Bundeskanzleramt und die Bundesministerien).

Dies erscheint unverständlich. Es stellt sich die Frage, an welchen Maßstäben sich die Einrichtungen der Bundesverwaltung dann orientieren sollen. Diese sollten ein einheitlich hohes Cybersicherheitsniveau haben.

Risikomanagementmaßnahmen besonders wichtiger und wichtiger Einrichtungen (BSIG § 30, § 31)

Bei den geforderten Maßnahmen zum Risikomanagement wird der Katalog aus der NIS2-Richtlinie der EU übernommen und der Verhältnismäßigkeitsgrundsatz sowie ein gefahrenübergreifender Ansatz verankert. Die Umsetzung muss dokumentiert werden. Dazu verweist die Gesetzesbegründung auf vergleichbare Anforderungen aus der Datenschutzgrundverordnung.

Unternehmen befürchten, dass bereits die Mindest-Dokumentationspflicht hohe bürokratische Aufwände generieren könnte. Abwägungen und Entscheidungen des Risikomanagements zu dokumentieren, ist grundsätzlich – auch zum Vergleich für künftige Risikoanalysen – sinnvoll. Der Aufwand sollte aber auf das notwendige Maß begrenzt werden. Hier wären weitergehende Empfehlungen des BSI hilfreich.

Die Anforderungen stellen insbesondere für die neu verpflichteten Unternehmen zusätzlichen Aufwand dar. Insofern unterstützt die DIHK den risikobasierten Ansatz und die explizite Orientierung an der Verhältnismäßigkeit ausdrücklich. Die geforderten betrieblichen Maßnahmen entsprechen im Grundsatz üblichen Anforderungen an ein Informationssicherheitsmanagementsystem. Die Herausforderung wird in der Bewertung der „Angemessenheit“ der Maßnahmen einerseits durch das Unternehmen und andererseits durch das BSI bestehen. Hier sind Augenmaß und eine Orientierung an den unternehmerischen Realitäten gefragt. Hilfreich für die verpflichteten Unternehmen wären auch hierzu Hinweise zur Umsetzung durch das BSI. Diese sollten zeitnah vorliegen, damit sich die Unternehmen vorbereiten können.

Zu den konkreten Maßnahmen gehört auch die „Sicherheit der Lieferkette“ (BSIG § 30 Abs 2 Nr 4). Spätestens hier wären dann voraussichtlich mehr als die vom Gesetzgeber ermittelten, ca. 30.000 Unternehmen auch betroffen. Kleinere Unternehmen in der Lieferkette werden durch die immer professionelleren Cyberangriffe und die immer aufwendigeren

Sicherheitsmaßnahmen zunehmend überfordert. Diesen muss das BSI geeignete, zielgruppengerecht aufbereitete Informationen und Unterstützungsangebote allgemein zugänglich bereitstellen.

Und auch hier ergeben sich für die betroffenen Unternehmen Herausforderungen, wenn sie beispielsweise zur Nutzung von IT-Lösungen der öffentlichen Hand **verpflichtet** sind. So scheint für Apotheken bei der Verarbeitung der E-Rezepte die Telematik-Infrastruktur ein Problem zu sein. Diese erfüllt – zumindest aktuell – nicht immer Anforderungen an die Hochverfügbarkeit. Darauf haben die einzelnen Apotheken keinerlei Einfluss.

Die Verpflichtung zur Nutzung von zertifizierten Komponenten und Prozessen (BSIG § 30 Abs 6) darf nicht zu Beschaffungsengpässen und zur Bildung von Oligopolen führen. Sie wird außerdem nicht von der NIS-2-Richtlinie gefordert.

Es stellt sich die Frage, ob BSIG § 31 überhaupt erforderlich ist, der strengere Risikomanagementanforderungen an Betreiber kritischer Infrastrukturen definiert, da bereits in BSIG § 30 der Grundsatz der Verhältnismäßigkeit der Maßnahmen adressiert wird.

Auch das in den sicherheitskritischen Bereichen der Unternehmen eingesetzte Personal muss besonders vertrauenswürdig sein. Hier wünschen sich die Unternehmen mehr staatliche Unterstützung. Eine freiwillige Vertrauenswürdigkeitsüberprüfung sollte – analog zur Sicherheitsüberprüfung und zur Zuverlässigkeitsüberprüfung – durch staatliche Stellen erfolgen.

Meldepflichten (BSIG § 32)

Besonders wichtige und wichtige Einrichtungen werden verpflichtet, dem BSI bei erheblichen Sicherheitsvorfällen bis zu fünf Meldungen (bisher eine Meldung) zu übermitteln.

Die DIHK weist an dieser Stelle nochmals ausdrücklich darauf hin, dass aus den Meldungen konkreter Mehrwert für die Unternehmen entstehen muss. Wichtig ist ein effektiver Rückkanal in die Unternehmen. Diese benötigen aktuelle, konkrete und passgenaue Informationen zu analogen und digitalen Bedrohungen und konkrete Warnungen mit entsprechenden Handlungsempfehlungen. Das geplante Information Sharing Portal ist ein guter Ansatz, der gemeinsam mit den Unternehmen nutzerorientiert ausgestaltet werden muss.

Mit den Meldungen sind für die Unternehmen, die sich bei einem erheblichen Sicherheitsvorfall in einer Ausnahmesituation befinden und alle Kräfte auf die Vorfallsbearbeitung konzentrieren müssen, erst einmal zusätzliche Aufwände verbunden. Die Unternehmen wollen eine klare und effektive Ausgestaltung des Meldeverfahrens, die Doppelmeldungen und unnötige Statusaktualisierungen (BSIG § 32 Abs 1 Nr 3) vermeidet.

Alle Meldungen (nach NIS2UmsuCG und KRITIS-Dachgesetz) sollten möglichst einfach und digital an die zentrale Meldestelle erfolgen.

Vor allem kleinere Unternehmen, u. a. aus dem produzierenden Gewerbe und mit geringer Datenintensität, sind mit der kurzen 24h-Frist für eine Erstmeldung überfordert, insbesondere in Zeiten der Betriebsruhe und an Wochenenden. Fraglich ist, inwiefern aus den frühen Erstmeldelungen überhaupt schnelle konkrete Warnhinweise an andere Unternehmen durch das BSI generiert werden können. Gleiches gilt für Zwischenmeldungen kleinerer Unternehmen. Hier sollten praxistaugliche Regelungen gefunden werden, die die Unternehmen nicht überfordern.

EU-weit tätige Unternehmen sehen sich vor die Herausforderung gestellt, ggf. in mehreren Ländern und Sprachen melden zu müssen. Hier sollte sichergestellt werden, dass diese ihren Meldepflichten nur in einem Mitgliedstaat nachkommen müssen.

Im Übrigen verweist die DIHK auf die auf die Anmerkungen zu BSIG § 36.

Registrierungspflichten (BSIG § 33)

Die betroffenen Unternehmen sollen sich über ein Online-Portal beim BSI registrieren und eine Kontaktstelle bzw. Ansprechperson benennen, die jederzeit erreichbar ist. Geplant ist ein gemeinsames digitales Portal für die Registrierung nach KRITIS-Dachgesetz als auch nach NIS2UmsuCG.

In der Unternehmerschaft bestehen in Bezug auf die Frage, ob sie vom Gesetz betroffen sind, aktuell die größten Unsicherheiten. Viele Detailfragen, etwa zur Berechnung der Anzahl der Mitarbeitenden oder Abgrenzungsfragen bei verbundenen Unternehmen, lassen sich selbst mit rechtlicher Beratung kaum eindeutig beantworten. Entsprechend groß ist die Verunsicherung. Die auf Basis der Unternehmensanfragen laufend weiterentwickelten FAQ des BSI sind ein guter Ansatz, werden in vielen Fällen aber nicht ausreichen.

Das Portal sollte auch Prüfmöglichkeiten enthalten, anhand derer die Unternehmen ihre Betroffenheit bereits vor der Registrierung als Self-Service einfach selbst überprüfen können. Entsprechende Möglichkeiten sollten so rechtzeitig vor Inkrafttreten des Gesetzes zur Verfügung stehen, dass die Unternehmen ihre Betroffenheit möglichst zeitnah und rechtssicher feststellen können. Alternativ könnte das BSI im Zweifel und auf Anfrage den Unternehmen mitteilen, ob sie in den Anwendungsbereich fallen.

Die DIHK setzt sich seit langem dafür ein, dass Unternehmen einen einheitlichen digitalen Zugang für ihre Verfahren mit der öffentlichen Hand erhalten und nicht ihre Daten mehrfach hinterlegen müssen. Das digitale Registrierungsportal sollte Once-Only-Standards entsprechen und eine Anmeldung mit dem Organisationskonto der öffentlichen Hand ermöglichen. Die DIHK bittet auch darum, den Entwurf nochmals daraufhin zu überprüfen, dass keine Unklarheiten und Doppelmeldungen bei der Registrierung und der Benennung einer Kontaktstelle auftreten.

Die Meldung der zuständigen Aufsichtsbehörden nach § 33 Abs 5 durch die Unternehmen könnte das BSI automatisiert im Nachgang zur Registrierung selbst tun, alternativ sollte zumindest eine Liste der Aufsichtsbehörden beim Registrierungsvorgang hinterlegt sein, aus der die Unternehmen die jeweiligen Behörden auswählen können.

Registrierung und Zugang zum Information Sharing Portal sollten verknüpft werden.

Rückmeldungen des BSI gegenüber den Unternehmen (BSIG § 36)

Die DIHK bewertet es grundsätzlich positiv, dass das BSI zeitnah Feedback zu einer Vorfallsmeldung gibt. Auch das vorgesehene Unterstützungsangebot ist vorteilhaft. Das BSI hat auch in der Vergangenheit bereits angeboten zu unterstützen.

Auf Basis der Erfahrungen aus der Vergangenheit und angesichts der nun viel größeren Zahl der verpflichteten Unternehmen haben viele Unternehmen Zweifel, dass die verfügbaren Ressourcen beim BSI ausreichen werden. Insofern muss von vornherein sichergestellt sein, dass angemessene Kapazitäten im BSI für dieses – grundsätzlich ausdrücklich erwünschte Angebot – zur Verfügung stehen.

Eine Verpflichtung, die Öffentlichkeit auf Anordnung des BSI über bedeutende Vorfälle zu informieren, ist nicht durch die NIS-2-Richtlinie vorgeschrieben und sollte gestrichen werden.

Ausnahmebescheid (BSIG § 37)

Das Bundesministerium des Innern und für Heimat kann auf Eigeninitiative oder auf Vorschlag anderer Ministerien besonders wichtige oder wichtige Einrichtungen ganz oder teilweise von den Pflichten des Gesetzes befreien.

Vor dem Hintergrund, dass aus Föderalismuserwägungen bereits wesentliche Teile des Gemeinwesens aus dem Anwendungsbereich herausfallen, die nach unserem Dafürhalten gleichwertigen Verpflichtungen unterliegen sollten (z. B. Kommunen, Medien, Bildung), sollten insbesondere Vorfallsmeldungen erfolgen und beim BSI zusammenlaufen. Diese hätten einen Mehrwert, der in Lageberichte für die Unternehmen einfließen sollte.

Billigungs-, Überwachungs- und Schulungspflichten der Geschäftsleitung (BSIG § 38)

Die Pflicht zur ordnungsgemäßen Unternehmensleitung umfasst grundsätzlich auch Maßnahmen zur Cybersicherheit. Insofern ist die Verankerung der Verantwortung für die Cybersicherheit in der Unternehmensführung im Gesetzentwurf nicht erforderlich.

Unklar ist, wie die neuen Schulungspflichten praxistauglich umgesetzt und dokumentiert werden können, ohne die Unternehmen mit zusätzlichen bürokratischen Pflichten zu belasten.

Nachweispflichten für Betreiber kritischer Anlagen (BSIG § 39)

Betreiber kritischer Anlagen sollen die Erfüllung der Pflichten kontinuierlich etwa alle drei Jahre mittels Audits, Prüfungen oder Zertifizierungen nachweisen. Anschließend müssen Nachweise regelmäßig alle drei Jahre erbracht werden. Bei Sicherheitsmängeln kann das BSI die Vorlage eines Mängelbeseitigungsplanes und Nachweise über die erfolgte Beseitigung der Mängel verlangen.

Zusätzliche Dokumentations- und Nachweispflichten binden Kapazitäten in den Unternehmen, die bei der konkreten Umsetzung von Cybersicherheitsmaßnahmen fehlen. Die vom Grundsatz her unterstützenswerten Ziele des Gesetzes dürfen nicht durch zusätzliche bürokratische Belastungen ausgehebelt werden. Die DIHK weist an dieser Stelle auf die Anforderungen der NIS2-Richtline hin, über die im Sinne einheitlicher europäischer Wettbewerbsbedingungen nicht hinausgegangen werden sollte. Vor dem Hintergrund des Angemessenheitsprinzips stellt sich die Frage, ob starre proaktive Nachweispflichten für Betreiber kritischer Anlagen über die allgemeinen Aufsichts- und Durchsetzungsmaßnahmen des BSI nach BSIG § 61 hinaus wirklich erforderlich sind.

Sollten die Nachweispflichten Bestand haben, sollten auch hier Unklarheiten im Hinblick auf die Verhältnismäßigkeit beseitigt werden. Es sollte zumindest eindeutig klargestellt werden, dass die Nachweispflichten nur abgegrenzte kritische Anlagen umfassen.

Da die begleitenden Rechtsverordnungen die konkreteren Erwartungen aufzeigen, sollten Fristen erst ab der Gültigkeit dieser Rechtsverordnungen gelten. Erst dann können die Betreiber genau einschätzen, was erwartet wird.

Zentrale Melde- und Anlaufstelle (BSIG § 40)

Es ist vorgesehen, dass das BSI Meldungen zu Schwachstellen aufnehmen, analysieren und Hersteller informieren soll.

Die konkreten Verfahren zum Umgang mit Schwachstellen sollten gesetzlich definiert werden.

Rechtsverordnungen (BSIG § 56)

Die Betreiber müssen selbst feststellen, ob sie kritische Anlagen betreiben und deshalb unter die gesetzlichen Vorgaben fallen. Die Anlagenarten, Schwellenwerte etc. sollen durch eine Verordnung konkretisiert werden (BSIG § 56 Abs 4), die noch nicht vorliegt. Die Rechtsverordnung soll für das KRITIS-Dachgesetz und das NIS2UmsuCG gleichermaßen gelten.

Die Unternehmen benötigen frühzeitig Rechtssicherheit. Die konkretisierende Rechtsverordnung sollte unter Einbeziehung der betroffenen Sektoren (nicht nur der jeweiligen Ressorts) erarbeitet, zeitnah verabschiedet werden und dann einheitlich für beide o. g. Gesetze gelten.

Aufsichts- und Durchsetzungsmaßnahmen (BSIG § 61)

Angesichts der Tatsache, dass Unternehmen bereits ein erhebliches Eigeninteresse daran haben, dass ihre Systeme und ihr Geschäft geschützt sind, sollte hier mit viel Augenmaß agiert werden.

In Bezug auf BSIG § 61 Abs 9 Nr 2 sollten Klarstellungen zum Weiterbetrieb und zur Haftung bei Eingriff in die Geschäftsführung durch das BSI erfolgen. Gegenwärtig ist nicht geregelt, wer den Betrieb leiten soll und 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.

Bußgeldvorschriften (BSIG § 65)

Das Sanktionsregime wurde verschärft, insbesondere wurden die Strafen deutlich erhöht.

Die Vorschriften sollten sowohl im Hinblick auf die EU-rechtlichen Vorgaben als auch im Hinblick auf ihre Verhältnismäßigkeit überarbeitet werden.

D. Ansprechpartnerin

Dr. Katrin Sobania, Bereich Digitalisierung, Infrastruktur, Regionalpolitik (DIR), Leiterin des Referats Informations- und Kommunikationstechnologie, E-Government, Postdienste, Daten- und Informationssicherheit, sobania.katrin@dihk.de

Wer wir sind:

Unter dem Dach der Deutschen Industrie- und Handelskammer (DIHK) sind die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich die DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein.

Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zu gemeinsamen Positionen der Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Darüber hinaus koordiniert die DIHK das Netzwerk der 140 Auslandshandelskammern, Delegationen und Repräsentanzen der Deutschen Wirtschaft in 92 Ländern.

Grundlage dieser Stellungnahme sind die dem DIHK bis zur Abgabe der Stellungnahme am 12. Dezember 2024 eingegangenen Äußerungen der IHKs sowie Diskussionen mit Verbänden, Wissenschaftlern und Unternehmen. Diese Stellungnahme basiert auf einem Beschluss des DIHK-

Vorstands vom 17. Juni 2020 „Digitale Ökosystem als Fundament für den wirtschaftlichen Erfolg gesamtheitlich gestalten“ und auf den Wirtschaftspolitischen Positionen der IHK-Organisation. Sollten dem DIHK noch weitere in dieser Stellungnahme noch nicht berücksichtigte relevante Äußerungen zugehen, wird der DIHK diese Stellungnahme entsprechend ergänzen.