STELLUNGNAHME

Berlin, 28. Mai 2024

Deutsche Industrie- und Handelskammer

Entwurf des Bundesministeriums des Innern und für Heimat: Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

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

Wir bedanken uns für die Gelegenheit zur Stellungnahme zu dem o. g. Referentenentwurf. Das Ziel des Gesetzes, ein hohes gemeinsames Sicherheitsniveau sicherzustellen, unterstützt die DIHK ausdrücklich. Das Ziel kann aber nur erreicht werden, wenn die Maßnahmen und bürokratischen Pflichten angemessen sind. Denn letztgenannte binden Kapazitäten in den Unternehmen, die wiederum zielgerichteter für die eigentliche Umsetzung von Cybersicherheitsmaßnahmen eingesetzt werden könnten. Zudem sollte das Miteinander von Staat und Wirtschaft, insbesondere der Informationsrückfluss aus den zusätzlichen Meldepflichten einer größeren Anzahl von Unternehmen, konkretisiert und gemeinsam an den Bedarfen der Unternehmen ausgerichtet werden.

A. Anmerkungen der DIHK in Kürze:

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

- mehr echte Kooperation
  - zwischen Unternehmen, Politik und Verwaltung,
  - innerhalb der Wirtschaft, damit auch kleinere und mittlere Unternehmen voneinander lernen und so ihre Resilienz erhöhen können,
  - auf europäischer bzw. internationaler Ebene,
- ein passgenaues Lagebild, auf dessen Basis sie ihre knappen Ressourcen priorisiert und effizient einsetzen können.

Im Gegensatz dazu wünschen sich die Unternehmen NICHT:

- Überregulierung, inkonsistente Regulierung und bürokratische Hürden.

Unsere Kritikpunkte zum Referentenentwurf zusammengefasst:

- Es sollte ein umfassender Ansatz verfolgt werden, der grundlegende Fragen der Cybersicherheitsarchitektur beantwortet, digitale und analoge Sicherheit gemeinsam adressiert und neben der Wirtschaft auch die öffentliche Hand insgesamt einbezieht.
- Zusammenarbeitsprozesse der Behörden untereinander und zwischen Behörden und Unternehmen sollten von Beginn an klar definiert und umgesetzt werden.
- Lageinformationen und unterstützende Handlungsempfehlungen zu analogen und digitalen Bedrohungen sollten den betroffenen Unternehmen aus einer Hand zielgerichtet zugänglich gemacht werden. Die konkrete Umsetzung des Information Sharing Portal sollte gemeinsam mit der Wirtschaft so schnell wie möglich ausgestaltet werden.
- Doppelregulierungen sollten vermieden und bürokratische Belastungen so gering wie möglich gehalten werden. Registrierungs- und Meldepflichten sollten durchgängig digital und so effektiv wie möglich erfolgen.
- Unternehmen benötigen Rechtssicherheit. Die schleppende politische Diskussion wirkt kontraproduktiv. Die betroffenen Unternhemen benötigen eine zeitliche Roadmap und Klarheit über ihre Betroffenheit. Dafür sind Umsetzungshilfen zur Verfügung zu stellen.

B. Allgemeine Anmerkungen

Staat und Wirtschaft sind gemeinsam gefordert, die Sicherheit grundlegender Infrastrukturen und Anlagen zu gewährleisten. Das NIS2UmsuCG adressiert dieses Anliegen. Es soll die Cyber-Sicherheit und Resilienz von Betreibern kritischer Infrastrukturen und weiterer für das Funktionieren der Wirtschaft und des Gemeinwesens bedeutsamen Unternehmen und deren Einrichtungen stärken. Zudem setzt es die EU NIS2-Richtlinie um und führt zusätzliche Maßnahmen und Pflichten zum Risiko- und Krisenmanagement für Unternehmen sowie Melde- und Nachweispflichten ein.

Mit der starken Ausweitung des Umsetzungsbereichs verlässt der Gesetzgeber den bisherigen Ansatz, insbesondere kritische Infrastruktur zu regulieren. Wir befürchten, dass es der Akzeptanz des Gesetzes nicht dienlich ist, wenn sich ein nennenswerter Teil der Unternehmen nicht als Teil der Zielgruppe versteht. Hier ist Kommunikations- und Vermittlungsarbeit zu leisten, insbesondere gegenüber den mittelständisch geprägten Unternehmen bis 250 Beschäftigten.

Gesamtkonzept erforderlich

Erforderlich wäre ein Gesamtkonzept, das analoge und digitale Sicherheit von Staat, Wirtschaft und Gesellschaft umfassend und gleichermaßen adressiert und in die europaweiten Aktivitäten eingebettet ist. Die Erarbeitung einer aktuellen Cyber-Sicherheitsstrategie steht noch immer aus.

Rechtssicherheit und konsistente Regelungen gewährleisten

Ein konsistenter Ordnungsrahmen muss den Unternehmen verlässliche Orientierung geben und größtmögliche Transparenz über die rechtlichen Verpflichtungen herstellen. Es wäre wünschenswert gewesen, die Referentenentwürfe zum NIS2UmsuCG und zum KRITIS-Dachgesetz aufgrund der inhaltlichen Zusammenhänge zumindest parallel zur Diskussion zu stellen. Sinnvoller wäre ein gemeinsames Gesetzgebungsverfahren gewesen. Auf jeden Fall ist eine vollständige Harmonisierung der Regelungen (auch branchenspezifischer Verpflichtungen) nötig – im Hinblick auf die verwendeten Begriffe und Definitionen, auf die Umsetzungsprozesse und in Bezug auf die Kompetenzen der beteiligten Behörden. Die parallelen Gesetzesvorschläge führen zu einer komplexen Vorgabesystematik, deren wechselseitige Abhängigkeiten und Zuständigkeiten der einzelnen Behörden eine Umsetzung für Unternehmen unnötig erschweren. Die Aufteilung in zwei getrennte Gesetzgebungsverfahren erschwert es den Unternehmen zusätzlich, die eigene Betroffenheit festzustellen, die jeweils relevanten Anforderungen abzuleiten und rechtskonform umzusetzen.

Effektives Zusammenspiel der Behörden für mehr Cybersicherheit der Unternehmen

Insbesondere vor dem Hintergrund, dass mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zwei unterschiedliche Aufsichtsbehörden für die Umsetzung des KRITIS-Dachgesetz und des NIS2UmsuCG verantwortlich zeichnen, die sich wiederum mit weiteren sektorspezifischen Aufsichtsbehörden und Behörden der Länder vernetzen müssen, sollten die Prozesse der Zusammenarbeit zwischen den Behörden klar definiert werden. Nur so lassen sich Doppelaufwand für die Unternehmen, z. B. durch Mehrfachmeldungen, verhindern und effektive Warnhinweise an die Unternehmen gewährleisten. Alle Maßnahmen müssen darauf hinwirken, das Schutzniveau der Unternehmen zu verbessern und deren eigene Sicherheitsbemühungen zu unterstützen. Eine angemessene personelle Ausstattung der Behörden ist dafür eine weitere Voraussetzung.

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 Meldungen an das BSI sollte deshalb ein effektiver Rückkanal in die Unternehmen etabliert werden, etwa indem Lageinformationen mit entsprechenden Handlungsempfehlungen zielgerichtet ausgetauscht werden. Es gilt, diesen kooperativen Ansatz zwischen Staat und Wirtschaft, der in Teilen, z. B. mit dem UP KRITIS im Bereich der kritischen Infrastrukturen oder in der Allianz für Cybersicherheit, bereits etabliert ist, zu skalieren und im Sinne eines echten Unterstützungsnetzwerkes weiter auszubauen. Das geplante Information Sharing Portal ist ein guter Ansatz, der zeitnah mit Leben gefüllt werden muss.

Insbesondere die mittleren Unternehmen sollten bei ihren Sicherheitsvorkehrungen unterstützt werden. Dazu sollten das BSI bzw. weitere Institutionen Umsetzungshilfen, Vorlagen, Muster und Leitfäden bereitstellen.

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 für die 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.

Transparenz über Umsetzungsfristen herstellen

Durch die aktuelle zeitliche Verzögerung des Gesetzgebungsverfahrens ist zu erwarten, dass das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz nicht fristgerecht zum 17.10.2024 umgesetzt werden kann. Für Unternehmen ist wichtig zu wissen, was ab wann verpflichtend nötig ist. Die Zweifel, ob der Termin für das Umsetzungsgesetz und die begleiteten Verordnungen gehalten werden kann, müssen ausgeräumt werden, oder die Unternehmen sollten über eine ggf. geänderte Umsetzungsfrist informiert werden.

EU-weite Harmonisierung gewährleisten

Mit der NIS2-Richtlinie beabsichtigt der EU-Gesetzgeber eine EU-weite Harmonisierung der Cybersicherheit. Der deutsche Gesetzgeber entfernt sich bei der Umsetzung von der Struktur der NIS2-Richtlinie, was die Anwendung für grenzüberschreitend tätige Unternehmen unnötig komplex macht.

Einbeziehung der öffentlichen Hand

Für die öffentliche Hand sind abseits der Bundesverwaltung derzeit keine Verpflichtungen vorgesehen. Viele Unternehmen äußern Unverständnis darüber, dass Kommunen entsprechend dem Beschluss des IT-Planungsrates 2023/39 keinen vergleichbaren Verpflichtungen wie die Unternehmen unterworfen werden sollen.

Für die Unternehmen ist wichtig, dass sie sich auf funktionierende Prozesse mit der Verwaltung verlassen können. Wesentliche Unternehmensprozesse, beispielsweise Planungs- und Genehmiungsverfahren, 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. Hier wären dringend Regelungen erforderlich, die ein bundesweit einheitliches Sicherheitsniveau auch auf kommunaler und Landesebene (ggf. zeitlich abgestuft) gewährleisten. Bisherige Vereinbarungen unterhalb der Gesetzesebene haben in der Praxis nicht hinreichend gewirkt. Auch Behörden und Organisationen mit Sicherheitsaufgaben sollten ein entsprechendes Sicherheitsniveau gewährleisten, um deren Reaktionsfähigkeit z. B. in plötzlich auftretenden Krisensituationen jederzeit sicherzustellen. Dies auch vor dem Hintergrund, dass die Unternehmen sich auch dann auf die Funktionsfähigkeit des Staates verlassen können müssen, wenn sie selber von einem Cybersicherheitsvorfall oder anderen Krisensituationen betroffen sind.

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.

Wir erwarten, dass die steigende Nachfrage nach IT-Sicherheitsdienstleistungen und IT-Sicherheitsfachkräften Preissprünge bewirken wird. Deshalb gehen wir davon aus, 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 Kosten, die auf die Unternehmen zukommen, sind insbesondere die bürokratischen Aufwände für Melde- und Nachweispflichten möglichst bürokratiearm auszugestalten.

Begriffsbestimmungen und Rechtsverordnung (BSIG § 2)

An einigen Stellen des Entwurfes wird das Schutzziel Authentizität weiterhin adressiert (z. B. BSIG § 2 Abs 1 Nr 22 und BSIG § 30 Abs 2 Nr 10). Dieses sollte im Schutzziel Integrität inkludiert sein.

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)

Auf die IT-Sicherheit von Unternehmen wirkt sich insbesondere der Umstand aus, dass das BMI mit dem BSI eine Behörde beheimatet, die IT-Sicherheit fördern soll, und zugleich auch Behörden, für deren Arbeit auch IT-Schwachstellen genutzt werden. Zugleich ist der staatliche Umgang mit Schwachstellen in Hard- und Software ungeklärt. Das Gesetz sollte auch dazu genutzt werden, diese Themen im Sinne einer besseren Kooperationsfähigkeit von Staat und Wirtschaft zu adressieren. Dazu gehört auch, das BSI – wie im Koalitionsvertrag angekündigt – unabhängiger aufzustellen und mit den entsprechenden Ressourcen auszustatten.

Informationsaustausch (BSIG § 6)

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

Eine effektive Entgegennahme und Aufbereitung sowie die zielgerichtete Ausgabe von darauf basierenden Lageinformationen an Unternehmen ist wesentliche Voraussetzung für eine konstruktive Zusammenarbeit von Staat und Wirtschaft zur Verbesserung des Cybersicherheitsniveaus insgesamt. Die Diskussion über entsprechende Ansätze sollten 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 uns 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. automatisierte Schnittstelle zur Abfrage aktuell schadhafter Hardware- und Softwarekomponenten.

Der Betrieb eines Informations Sharing Portals, das wirklich einen Mehrwert für die Unternehmen generiert, verursacht großen personellen Aufwand, der im BSI abgebildet werden muss. Das Bundesamt muss sich zeitnah um das entsprechedne Fachpersonal bemühen, damit dieser Mehrwert für die Unternehmen entwickelt werden kann. Aufbauend auf bereits erfolgten Austauschformaten (z. B. über von BDI und DIHK durchgeführte Umfragen und Workshops im Rahmen der Allianz für Cybersicherheit) sollten Unternehmen viel enger als bisher in den Umsetzungsprozess eingebunden werden, um nutzerorientierte Angebote zu schaffen.

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.

Empfehlungen zum Einsatz bestimmter Sicherheitsprodukte(BSIG § 13)

Das BSI darf Sicherheitsmaßnahmen und Einsatz bestimmter Sicherheitsprodukte empfehlen.

Diese Empfehlungen dürfen nicht verpflichtend sein, da sie ansonsten als wettbewerbsverzerrend anzusehen wären.

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.

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.

Beispielsweise werden kleinste „Anbieter öffentlicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze“ zu Verpflichteten. Hier sollte klargestellt werden, was z. B. „Betreiber öffentlicher Telekommunikationsnetze“ sind. Fallen etwa Anbieter öffentlicher WLAN-Hotspots darunter? Der Passus kann bei sehr weiter Auslegung den Kreis der Betroffenen deutlich vergrößern.

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. So betreiben Stadtwerke (KRITIS-Unternehmen) beispielsweise Mobilitätsplattformen (Online-Marktplatz, über den auch Services Dritter vermittelt werden) als Mehrwertdienst zum eigentlichen Service ÖPNV. Eine Anwendung der NIS2-Regularien auf derartige Service wäre eine unnötige zusätzliche bürokratische Belastung.

Risikomanagementmaßnahmen besonders wichtiger Einrichtungen 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 und enthält einige Beispiele.

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 könnten weitergehende Empfehlungen zu angemessener Dokumentation hilfreich sein.

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 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.

Zu den konkreten Maßnahmen gehört auch „Sicherheit der Lieferkette“ (BSIG § 30 Abs 2 Nr 4). Spätestens hier wären dann voraussichtlich mehr als die vom Gesetzgeber ermittelten ca. 30.000 Unternehmen indirekt betroffen. Kleinere Unternehmen in der Lieferkette werden durch die immer professionelleren Cyberangriffe und die immer aufwendigeren Sicherheitsmaßnahmen zunehmend überfordert. Deshalb muss das BSI ausdrücklich dazu verpflichtet werden, geeignete, zielgruppengerecht aufbereitete Informationen, Unterstützungsmaßnahmen für KMU und Warnsysteme allgemeinzugänglich bereitstellen. Dies sollte im BSI-Gesetz explizit geregelt werden.

Die Verpflichtung zur Nutzung von zertifizierten Komponenten und Prozessen (BSIG § 30 Abs 6) darf nicht zu Beschaffungsengpässen und zur Bildung von Oligopolen führen. Wir bitten, die Regelung daraufhin zu prüfen.

Auch das in den sicherheitskritischen Bereichen der Unternehmen eingesetzte Personal muss besonders vertrauenswürdig sein. Hier wünschen sich die Unternehmen mehr staatliche Unterstützung bei Sicherheitsüberprüfungen.

Meldepflichten (BSIG § 32)

Besonders wichtige und wichtige Einrichtungen werden verpflichtet, dem BSI bei erheblichen Sicherheitsvorfällen bis zu 5 Meldungen zu übermitteln. Bisher mussten Unternehmen eine Meldung abgeben. Die Ausgestaltung des Meldeverfahrens kann das BSI festlegen.

Mit den Meldungen sind erst einmal Aufwände für die Unternehmen verbunden, die sich bei einem erheblichen Sicherheitsvorfall in einer Ausnahmesituation befinden und alle Kräfte auf die Vorfallsbearbeitung konzentrieren müssen. Die Unternehmen wollen eine klare und

effektive Ausgestaltung des Meldeverfahrens, die Doppelmeldungen und unnötige Statusaktualisierungen (BSIG § 32 Abs 1 Nr 3) vermeidet. Alle Meldepflichten (nach NIS2UmsuCG und KRITIS-Dachgesetz) sollten möglichst einfach, digital und im Idealfall nur einmal erfolgen. In Bezug auf die zu meldenden Fälle sollte das NIS2UmsuCG nicht über den Wortlaut der NIS2-Richtlinie hinausgehen.

Für bereits verpflichtete Kritis-Unternehmen bleibt es bei Dopplungen. Telekommunikationsunternehmen unterliegen beispielsweise einer doppelten Meldepflicht von Vorfällen sowohl an das BSI als auch an die BNetzA (vgl. Artikel 23 § 168 Abs 1 TKG). Dies führt zu einem erheblichen Aufwand und zu Doppelregulierungen.

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.

Die kleinen und mittleren Unternehmen hingegen, insbesondere diejenigen aus dem produzierenden Gewerbe und mit geringer Datenintensität, sind mit kurzen Fristen eher überfordert, insbesondere in den Zeiten der Betriebsruhe und an Wochenenden.

Im übrigen verweisen wir auf die oben stehenden Anmerkungen zum Mehrwert aus den Meldungen sowie auf unsere 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.

In der Unternehmerschaft bestehen in Bezug auf die Frage, ob sie vom Gesetz betroffen sind, aktuell die größten Unsicherheiten. Ein gemeinsames digitales Portal für die Registrierung nach KRITIS-Dachgesetz als auch nach NIS2UmsuCG ist auf jeden Fall hilfreich.

Das Portal sollte auch Prüfmöglichkeiten enthalten, anhand derer die Unternehmen ihre Betroffenheit bereits vor der Registrierung als Self-Service einfach selber 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.

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. Wir bitten auch darum, den Entwurf nochmals daraufhin zu überprüfen, dass keine Unklarheiten und Doppelmeldungen bei der Registrierung und der Benennung einer Kontaktstelle auftreten.

Bestehende Registrierungen nach BSIG sollten für die Registrierungen nach § 6 Entwurf KRITIS-Dachgesetz ohne erneute Registrierung anerkannt und bedarfsgerecht übernommen werden.

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

Unklar bleibt, inwiefern Registrierung und Zugang zum Information Sharing Portal 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 vorn herein sichergestellt sein, dass ausreichend Kapazitäten im BSI für dieses – grundsätzlich ausdrücklich erwünschte Angebot – zur Verfügung stehen.

Es muss absolut sicher gestellt werden, dass Meldungen an das BSI nicht per Presse, Social Media oder über andere Kanäle an die Öffentlichkeit gelangen, da so ggf. der Unternehmenswert stark beeinflusst werden kann.

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 in jedem Fall erfolgen. Diese hätten sicherlich einen Mehrwert, der in den Lagebericht 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 grundsätzlich richtig – aber nicht erforderlich.

BSIG § 38 Abs 1 ist von der allgemeinen Organisationsverantwortung bereits gedeckt und insofern nicht notwendig. Die DIHK regt eine Streichung des BSIG § 38 Abs 2 an, der einen Verzicht der Einrichtung bzw. einen Vergleich ausschließt. Eine entsprechende Regelung ist in der NIS2-Richtlinie nicht enthalten, und auch hier sollte man sich an allgemeinen Grundsätzen orientieren.

Einzelne Unternehmen weisen darauf hin, dass es zuweilen unklar sein könnte, wo die Herstellerhaftung aufhört und die Betreiberhaftung beginnt. So sind immer mehr Geräte mit dem Internet verbunden. Beispielsweise könnten Zulieferer von Komponenten von den Regelungen betroffen sein, wenn ein großes Krankenhaus Solaranlagen verbaut. Wenn die Ansteuerung der Solaranlage über Handy-App erfolgen kann, steigt die Komplexität. So könnten unter Umständen von den Regelungen dann auch Hersteller betroffen sein, die nicht damit gerechnet haben, dass Betreiber die Geräte im Zusammenhang mit sicherheitskritischer Infrastruktur einsetzen. Hier besteht Unsicherheit bei den Unternehmen, wie weit genau Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen reichen. Siehe dazu auch unsere oben stehenden Anmerkungen zum Anwendungsbereich BSIG § 28.

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 sollte geprüft werden, ob eine Ausweitung der Nachweispflichen für Betreiber kritischer Anlagen über die allgemeinen Aufsichts- und Durchsetzungsmaßnahmen des BSI nach BSIG § 65 hinaus wirklich erforderlich ist.

Sollten die Nachweispflichten Bestand haben, sollten auch hier Unklarheiten im Hinblick auf die Verhältnismäßigkeit beseitigt werden. Es sollte zumindest eindeutig klargestellt werden, dass die Risikomanagementmaßnahmen und Nachweispflichten nur abgegrenzte kritische Anlagen einer besonders wichtigen oder wichtigen Einrichtung umfassen, nicht auch sonstige Dienstleistungen der Einrichtungen.

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)

Das BSI soll Meldungen zu Schwachstellen aufnehmen und analysieren.

Viele Unternehmen fragen sich, was anschließend mit den Schwachstellen passiert und inwieweit das BSI Informationen zu Schwachstellen an andere Sicherheitsbehörden weiterleitet, statt auf eine schnelle Schließung derselben hinzuwirken. Meldungen zu Schwachstellen sind den betroffenen Unternehmen – nicht nur wie vorgesehen den Betreibern kritischer Anlagen, sondern beispielsweise auch Herstellern – zuerst mitzuteilen, so dass diese die Möglichkeit haben, die Sicherheitslücken zu schließen. Sie dürfen keinesfalls für die Tätigkeit anderer staatlicher Akteure offengehalten bzw. genutzt werden.

Bei der Entgegennahme, der Analyse und der vertrauensvollen Adressierung von Schwachstellen sollten bestehende nicht-staatliche Strukturen durch die Ausweitung der BSI-Aufgaben zumindest nicht beeinträchtigt, besser noch einbezogen werden.

Einsatz kritischer Komponenten (BSIG § 41)

Das bestehende Prüfverfahren zu den kritischen Komponenten wurde in den BSIG § 41 überführt.

Insgesamt stellt sich die Frage, wie die Überführung der bisherigen Regelung, die hauptsächlich auf den Telekommunikationsbereich angewendet wurde, auf alle Betreiber kritischer Anlagen skalieren soll. Berichten aus der Telekommunikationsbranche zufolge gestaltet sich das bisherige Verfahren lang und kompliziert. Unternehmen aus dem Telekommunikationsbereich äußern Unverständnis darüber, warum die Regelung bezüglich der einzuholenden Garantieerklärungen von Herstellern kritischer Komponenten nach BSIG § 41 Abs 3 aufgenommen wurde, obgleich das Bundesministerium des Innern und für Heimat bereits im Oktober 2022 die entsprechende Allgemeinverfügung für den Telekommunikationssektor widerrufen hatte.

Einige Unternehmen schlagen ein White-/Blacklisting (vergleichbar Datenschutz) vor, um den Rechercheaufwand bei der Einführung neuer kritischer Komponenten zu vereinfachen. Auf der Whitelist müssten sich die Zertifikate, welche nach BSIG § 54 erteilt wurden, und solche Komponenten, welche nach BSIG § 41 anerkannt wurden, wiederfinden. Auf der Blacklist müssten dementsprechend solche Komponenten enthalten sein, deren Einsatz untersagt wurden.

Rechtsverordnungen (BSIG § 58)

Die Betreiber müssen selber feststellen, ob sie kritische Anlagen betreiben und deshalb unter die gesetzlichen Vorgaben fallen. Die Anlagenarten, Schwellenwerte etc. sollen durch eine

Verordnung konkretisiert werden (BSIG § 58 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 tatsächlich für beide o. g. Gesetze gelten.

Aufsichts- und Durchsetzungsmaßnahmen (BSIG § 65)

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

In Bezug auf BSIG § 65 Abs 10 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.

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 28. Mai 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.