STELLUNGNAHME

Berlin, 20. Oktober 2023

Deutsche Industrie- und Handelskammer

Diskussionspapier des Bundesministeriums des Innern und für Heimat: Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland

Wir bedanken uns für die Gelegenheit zur Stellungnahme zu dem o. g. Diskussionspapier zum BSI-Gesetz im Vorfeld der eigentlichen Verbändebeteiligung zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG). Daten, Systeme und Infrastrukturen – die Digitalisierung insgesamt – werden immer wesentlicher für die Wettbewerbsfähigkeit von Unternehmen. Aufgrund der starken Abhängigkeit der gesamten gewerblichen Wirtschaft von sicheren digitalen Infrastrukturen und Unternehmen, die wesentliche Dienste erbringen, setzt sich die DIHK für geeignete Rahmenbedingungen zur Verbesserung der Daten- und Informationssicherheit insbesondere in diesen Bereichen ein, die die Funktionsfähigkeit der Wirtschaft insgesamt beeinflussen.

A. Das Wichtigste in Kürze

Das Ziel des Gesetzes, ein hohes gemeinsames Sicherheitsniveau sicherzustellen, unterstützt die DIHK ausdrücklich. Das Ziel kann aber nur erreicht werden, wenn die Maßnahmen angemessen sind und den Unternehmen nicht zusätzliche bürokratische Pflichten auferlegt werden. Denn diese binden unnötig Kapazitäten, die wiederum zielgerichteter für die eigentliche Umsetzung von Cybersicherheitsmaßnahmen in den Unternehmen 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.

Positiv hervorzuheben ist, dass der Anwendungsbereich direkt im Gesetz präzisiert wird und die Begrifflichkeiten aus der NIS2-Richtlinie übernommen werden.

Anpassungsbedarf sieht die DIHK insbesondere in den folgenden Bereichen:

- Registrierungs- und Meldepflichten sollten durchgängig digital abgewickelt werden, und ohne Doppelerfassungen erfolgen.
- Lageinformationen und unterstützende Handlungsempfehlungen zu analogen und digitalen Bedrohungen sollten den betroffenen Unternehmen aus einer Hand zielgerichtet zugänglich gemacht werden.

DIHK | Deutsche Industrie- und Handelskammer
Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Postanschrift: DIHK | 11052 Berlin
Tel. 030-20308-0 | Internet: www.dihk.de

- Effektive Zusammenarbeitsprozesse der Behörden sollten von Beginn an klar definiert und umgesetzt werden.
- Es sollte ein umfassender Ansatz verfolgt werden, der auch die öffentliche Hand insgesamt einbezieht. Ländern und insbesondere Kommunen sollten entsprechende Risikomanagementmaßnahmen und Meldungen abverlangt werden.

B. Allgemeine Anmerkungen

Staat und Wirtschaft sind gemeinsam gefordert, die Sicherheit der Netze und (besonders) wichtiger Anlagen zu gewährleisten. Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), dessen wirtschaftsbezogene Regelungen im BSI-Gesetz das Bundesministerium des Innern und für Heimat zur Diskussion stellt, 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.

Nach der neuen Gesetzeslage werden wesentlich mehr Unternehmen als bislang besondere Cyber-Sicherheitsanforderungen umsetzen und nachweisen müssen. Damit einher geht ein signifikanter Erfüllungsaufwand für die Unternehmen. Umso wichtiger ist es deshalb, dass die Erfüllung der zusätzlichen Pflichten möglichst bürokratiearm erfolgt und dass die Unternehmen einen 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 weitergegeben 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, etwa mit Hilfestellungen und konkreten Unterstützungsleistungen – präventiv und im Schadensfall. Die Diskussion über entsprechende Ansätze sollten parallel zum Gesetzgebungsverfahren auf den Weg gebracht werden, damit die Vorteile für die Unternehmen transparent und greifbar gemacht werden und ein gelebtes vertrauensvolles Miteinander entstehen kann. Dazu gehört auch, das BSI – wie im Koalitionsvertrag angekündigt – unabhängiger aufzustellen und vor allem mit den entsprechenden Ressourcen auszustatten.

Eine abschließende Beurteilung ist noch nicht möglich, weil wesentliche Paragrafen mit unmittelbarer Relevanz für die Wirtschaft im Diskussionspapier nicht enthalten sind. Dazu zählt insbesondere § 41, der die Untersagung des Einsatzes kritischer Komponenten in kritischen Infrastrukturen regelt.

Zudem äußern viele Unternehmen Unverständnis darüber, dass kommunale Eigenbetriebe richtiger Weise den Verpflichtungen unterliegen, die Kommunen selber aber nicht. Gleiches gilt für die Länder. Für die Unternehmen ist wichtig, dass sie sich auf funktionierende Prozesse

mit der Verwaltung verlassen können. Insbesondere die kommunale Ebene war in den letzten Jahren häufig von Cyberangriffen betroffen und zum Teil länger handlungsunfähig. Für die öffentliche Hand sind abseits der Bundesverwaltung derzeit keine Verpflichtungen vorgesehen. Hier wären aber dringend Regelungen erforderlich, die ein bundesweit einheitliches Sicherheitsniveau auch auf kommunaler und Landesebene gewährleisten. Wesentliche Unternehmensprozesse, insbesondere im Bereich von Planungs- und Genehmiungsverfahren, in denen die öffentliche Hand Teil der Wertschöpfungskette ist, müssen jederzeit funktionieren. 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. Gesamtkonzept erforderlich

Alle Unternehmen haben das Ziel, ihre Geschäftstätigkeit aufrecht zu erhalten. Dabei sind unter anderem Aspekte wie die Cybersicherheit, Verhaltensregeln für Mitarbeitende, robuste analoge Ersatzprozesse und Schadensminimierung im Angriffsfall bis zur Herstellung einer dauerhaften und hinreichenden Robustheit aller relevanten unternehmensinternen und -übergreifenden Prozesse gesamtheitlich im Blick zu behalten.

Vor diesem Hintergrund weisen wir darauf hin, dass ein Gesamtkonzept erforderlich wäre, das analoge und digitale Sicherheit von Staat, Wirtschaft und Gesellschaft umfassend und gleichermaßen adressiert und in Bezug auf die Belastungen der betroffenen Unternehmen dem Angemessenheitsprinzip Rechnung trägt. Im Moment stehen auf nationaler Ebene IT-Sicherheitsgesetz und Nationale Cybersicherheitsstrategie einerseits und KRITIS-Dachgesetz und Nationale Sicherheitsstrategie andererseits nebeneinander. Ein gesamtheitlicher Ansatz sollte die Prozess- und Leistungssicherheit von Infrastrukturen und kritischen Anlagen, Unternehmen, Staat und Gesellschaft ganzheitlich adressieren und in die europaweiten Aktivitäten eingebettet sein.

Ein konsistenter Ordnungsrahmen wäre hilfreich. Er kann den Unternehmen verlässliche Orientierung geben und größtmögliche Transparenz über die rechtlichen Verpflichtungen herstellen. Es wäre wünschenswert gewesen, die Referentenentwürfe zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) und zum KRITIS-Dachgesetz aufgrund der inhaltlichen Zusammenhänge zumindest parallel zur Diskussion zu stellen. Sinnvoller wäre ein gemeinsames Gesetzgebungsverfahren, auf jeden Fall ist eine Harmonisierung der Regelungen dringend notwendig – im Hinblick auf die verwendeten Begriffe und Definitionen, auf die Umsetzungsprozesse und in Bezug auf die Kompetenzen der beteiligten Behörden. Mit der parallelen Behandlung physischer und cybersicherheitsrelevanter Verpflichtungen in zwei unterschiedlichen Gesetzgebungsverfahren besteht die Gefahr von Doppelregulierung und Inkonsistenzen. Die parallelen Gesetzesvorschläge führen zu einer komplexen Vorgabesystematik,

deren wechselseitige Abhängigkeiten und Zuständigkeiten der einzelnen Behörden eine Umsetzung für Unternehmen unnötig erschweren. Dabei sollten – im Gegenteil – Dokumentationsaufwand und zusätzliche bürokratische Belastungen minimiert werden, um nicht unnötig Kapazitäten zu binden, die die Unternehmen in die Verbesserung ihrer Sicherheitsvorkehrungen investieren könnten. Die Aufteilung in zwei getrennte Gesetzgebungsverfahren erschwert es den Unternehmen zusätzlich, die eigene Betroffenheit im Vorfeld überhaupt festzustellen und die jeweils relevanten Anforderungen abzuleiten und rechtskonform umzusetzen.

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. Dazu sollten konkrete Angaben im Gesetz gemacht werden.

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

Schätzungen gehen von ca. 30.000 betroffenen Unternehmen aus, die in einer zertifizierten Form Nachweise über die Erfüllung des NIS2UmsuCG beibringen müssen. In Deutschland gibt es nach Angaben von Statista derzeit weniger als 2.000 Unternehmen, die nach ISO 27001 zertifizierte Informationssicherheits-Managementsysteme vorweisen können. Daher ist zu erwarten, dass viele Unternehmen Schwierigkeiten haben werden, der Umsetzung der NIS-2-Richtlinie nachzukommen. Auch externe Dienstleister werden sehr ausgelastet und schwer zu engagieren sein.

Insbesondere die Einbeziehung der Lieferkette in die Risikomanagementmaßnahmen in Verbindung mit den vorgesehenen Haftungsansprüchen führt zu enormer Verunsicherung in den Unternehmen. Zu erwarten ist, dass die nach NIS2UmsuCG verpflichteten Unternehmen im Rahmen ihres Risikomanagements entsprechende Anforderungen an ihre Lieferanten und Partner weitergeben werden. Angesichts des Fachkräftemangels steht zu befürchten, dass kleinere Unternehmen die Anforderungen schwer stemmen können. Es ist sehr wahrscheinlich, dass kleinere Anbieter in der Lieferkette Wettbewerbsnachteile erleiden. Da die meisten, insbesondere kleinere Unternehmen keine IT-Sicherheitsexperten sein können, sollten die Unternehmen bei ihren Sicherheitsvorkehrungen unterstützt werden. Dazu sollte das BSI (oder

angegliederte Einrichtungen wie z. B. die Allianz für Cybersicherheit oder Transferstelle für Cybersicherheit im Mittelstand) Umsetzungshilfen, Vorlagen, Muster und Leitfäden sowie eine Anlaufstelle bereitstellen. Auch für die direkt verpflichteten Unternehmen sollten geeignete Unterstützungsangebote auf den Weg gebracht werden.

Insgesamt wird durch die zunehmende Zahl an gesetzlich vorgegebenen Sicherheitsanforderungen an immer mehr Unternehmen (der Cyber Resilience Act muss demnächst auch noch umgesetzt werden, so dass dann noch viel mehr Fachkräfte benötigt werden) der 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 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. Dies gilt insbesondere im Hinblick auf die öffentliche Hand, wenn diese umfassender einbezogen werden sollte.

D. Konkrete Bewertung des Diskussionspapiers

Informationsaustausch (§ 6)

Das BSI stellt ein Online-Portal für den Informationsaustausch der Unternehmen untereinander zur Verfügung. Unverständlich ist, dass im Diskussionspapier § 5 zu den Aufgaben des BSI als allgemeine Meldestelle zu Sicherheitsrisiken nicht enthalten ist. Wie dargestellt, ist die effektive Entgegennahme und Aufbereitung sowie die zielgerichtete Ausgabe von darauf basierenden Lageinformationen an Unternehmen wesentliche Voraussetzung für eine konstruktive Zusammenarbeit von Staat und Wirtschaft zur Verbesserung des Cybersicherheitsniveaus insgesamt.

Insofern ist die Ausgestaltung des sog. Information Sharing Portal als reine Austauschplattform der Verpflichteten untereinander deutlich zu kurz gesprungen. Aktuelle Lageinformationen helfen den Unternehmen, schnell auf Bedrohungen zu reagieren bzw. rechtzeitig Vorsorge zu treffen. Für viele insbesondere kleine und mittlere Unternehmen stellt es eine große Herausforderung im Hinblick auf Ressourcen und Kompetenzen dar, sich die relevanten Informationen zur Bedrohungslage aus den unterschiedlichsten Quellen zusammenzusuchen. Dies bindet enorme Ressourcen, die wiederum nicht für die eigentliche Umsetzung von Sicherheitsmaßnahmen in den Unternehmen zur Verfügung stehen. Das Information Sharing Portal sollte deshalb auch aktuelle Lageinformationen der öffentlichen Hand, über das BSI gebündelt, verfügbar machen – zeitnah, verständlich aufbereitet für die unterschiedlichen Zielgruppen mit konkreten Handlungsempfehlungen zu analogen und digitalen Bedrohungsszenarien gleichermaßen. Zumindest sollte im Gesetz verankert werden, wie die Zurverfügungstellung der

Lageinformationen konkret ausgestaltet werden soll. Aufbauend auf bereits erfolgten Austauschformaten (z. B. über von BDI und DIHK durchgeführte Umfragen und Workshops im Rahmen der Allianz für Cybersicherheit) sollten Unternehmen weiterhin eng in den Umsetzungsprozess eingebunden werden, um hier wirklich nutzerorientierte Angebote zu schaffen.

Der sichere Zugang zum Portal sollte über bestehende Mechanismen abgebildet werden. Hier bietet sich das Unternehmenskonto der öffentlichen Hand an, wenn es in allen Funktionalitäten (inkl. Baustein 5: OZG-PLUS Postfach und Baustein 6: Rechte- und Rollenverwaltung) verfügbar ist.

Unterstützung bei der Wiederherstellung in herausgehobenen Fällen (§ 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.

Anwendungsbereich (§ 28)

Gut ist, dass die besonders wichtigen Einrichtungen und die wichtigen Einrichtungen inkl. der Größenangaben nun direkt im Gesetzestext spezifiziert werden. Auch die Auflistung einschlägiger Einrichtungsarten in den zwei neuen Anhängen dürfte dazu beitragen, Rechtsunsicherheiten für die Unternehmen zu verringern.

Es ergeben sich jedoch noch immer Fragen im Hinblick auf die konkrete Betroffenheit der Unternehmen. Im weiteren Verfahren sollte sichergestellt werden, dass insbesondere die „kritischen Anlagen“ im KRITIS-Dachgesetz und im NIS2UmsuCG einheitlich definiert werden.

In Bezug auf die Hinzurechnung von Daten verbundener Unternehmen zu Mitarbeiterzahl, Jahresumsatz und Jahresbilanz nach § 28 Abs. 3 liegt die Beweislast für die Nichtberücksichtigung der Daten verbundener Unternehmen aktuell bei den Einrichtungen statt beim BSI. Die DIHK regt eine Beweislastumkehr an. Die Formulierung „sind nicht hinzuzurechnen, wenn das Unternehmen… unabhängig von seinem Partner oder verbundenen Unternehmen ist“ sollte wie folgt angepasst werden: „dürfen nur hinzugerechnet werden, wenn das Unternehmen… abhängig von seinem Partner oder verbundenen Unternehmen ist“.

Auch im Hinblick auf die Verhältnismäßigkeit der Maßnahmen bestehen Unsicherheiten. Nach dem Entwurf ist davon auszugehen, dass die Risikomanagementmaßnahmen und Nachweispflichten nur abgegrenzte kritische Anlagen einer besonders wichtigen oder wichtigen Einrichtung umfassen. Dies sollte deutlich klargestellt werden.

Im Hinblick auf die Einbeziehung von Ländern und Kommunen verweisen wir auf unsere oben stehenden Ausführungen. Diese sollten neben der „Zentralregierung“ ebenfalls den Regelungen des NIS2UmsuCG unterfallen, da ihre Dienstleistungen eine wesentliche Grundlage für eine funktionsfähige Wirtschaft sind.

Maßnahmen zum Risikomanagement (§ 30, § 31)

Bei den geforderten Maßnahmen zum Risikomanagement übernimmt das Diskussionspapier den Katalog aus der NIS2-Richtlinie der EU und verankert dabei den Verhältnismäßigkeitsgrundsatz sowie einen gefahrenübergreifenden Ansatz.

Die Anforderungen stellen für viele Unternehmen zusätzlichen Aufwand dar. Insofern unterstützt die DIHK die explizite Orientierung an der Verhältnismäßigkeit und den risikobasierten Ansatz 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 stehen. Hier ist Augenmaß und eine Orientierung an den unternehmerischen Realitäten gefragt.

Zu den konkreten Maßnahmen gehört auch „Sicherheit der Lieferkette" (§ 30 Abs 2 Nr. 4). Spätestens hier wären dann voraussichtlich mehr als die vom Gesetzgeber ermittelten ca. 30.000 Unternehmen betroffen. Klargestellt werden sollte zumindest, dass sich die Maßnahmen auf das Risikomanagement der besonders wichtigen und wichtigen Einrichtungen im Hinblick auf die Lieferkette beziehen.

Eine gesonderte Regelung zu den Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen nach § 31 erscheint nicht erforderlich, da § 30 Abs. 1 bereits einen risikobasierten Ansatz vorsieht.

Meldepflichten (§ 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 (§ 32 Abs. 1 Nr. 3) vermeidet. Alle Meldepflichten (nach NIS2UmsuCG und KRITIS-Dachgesetz) sollten möglichst einfach, digital und im Idealfall nur einmal erfolgen.

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. Das NIS2UmsuCG sollte explizit erlauben, Meldungen in deutscher oder englischer Sprache abzugeben, die vom BSI an die betreffenden EU-Länder weitergegeben werden.

Um Klarheit und Konsistenz zu gewährleisten sollten die unterschiedlichen Fristen für Störungsmeldungen in KRITIS-Dachgesetz (24 Stunden/1 Monat) und NIS2UmsuCG (24

Stunden/72 Stunden/1 Monat) vereinheitlicht werden. Insbesondere die Erstmeldungsfrist von 24 Stunden erscheint im Vergleich zu 72 Stunden in vergleichbaren kritischen Sektoren wie dem Flugbetrieb nicht verhältnismäßig.

Im übrigen verweisen wir auf die oben stehenden Anmerkungen zum Mehrwert aus den Meldungen sowie auf unsere Anmerkungen zu § 36.

Registrierungspflichten (§ 33)

Die betroffenen Unternehmen sollen sich über ein Online-Meldeportal beim BSI registrieren und eine Kontaktstelle bzw. Ansprechperson benennen, die jederzeit erreichbar ist.

Für die Unternehmen ist häufig ein größerer Rechercheaufwand erforderlich, um ihre Betroffenheit durch das KRITIS-Dachgesetz als auch durch das NIS2UmsuCG festzustellen. Ein gemeinsames digitales Portal für die Registrierung ist auf jeden Fall hilfreich. 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 digital verfügbare Meldeportal sollte Once only-Standards entsprechen und eine Anmeldung mit dem Organisationskonto der öffentlichen Hand ermöglichen. Das Portal sollte auch Prüfmöglichkeiten enthalten, anhand derer die Unternehmen ihre Betroffenheit vor der Registrierung als Self-Service einfach selber überprüfen können, bzw. über entsprechende Prüfroutinen bei der Dateneingabe verfügen. Zusem sollte das Portal – oder entsprechende Prüfmöglichkeiten – so rechtzeitig vor Inkrafttreten des Gesetzes zur Verfügung stehen, dass die Unternehmen ihre Betroffenheit möglichst zeitnah feststellen können, um die entsprechenden Umsetzungsmaßnahmen einleiten zu können.

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 § 8 KRITIS-Dachgesetz ohne erneute Registrierung anerkannt und bedarfsgerecht übernommen werden.

Rückmeldungen des BSI gegenüber den Unternehmen (§ 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 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.

Billigungs-, Überwachungs- und Schulungspflichten der Geschäftsleitung (§ 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. Dem Entwurf zufolge scheint das BMI davon auszugehen, dass Haftungsfragen der Geschäftsleitung durch bestehende Regelungen im Gesellschaftsrecht abgedeckt sind. Dem schließt sich die DIHK grundsätzlich an (in Bezug auf den bereits gestrichenen Absatz 2 des Referentenentwurfs vom Juli 2023). Auch Absatz 1 ist von der allgemeinen Organisationsverantwortung bereits gedeckt und insofern nicht erforderlich. Die DIHK regt eine Streichung des § 38 Abs. 2 im Diskussionspapier 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 aber zuweilen unklar sein könnte, wo die Herstellerhaftung aufhört und die Betreiberhaftung beginnt. Immer mehr Geräte sind 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.

Nachweispflichten (§ 39)

Betreiber kritischer Anlagen sollen nach § 39 die Erfüllung der Pflichten erstmals zu einem noch zu bestimmenden Zeitpunkt frühestens drei Jahre nach Inkrafttreten des Gesetzes mittels Audits, Prüfungen oder Zertifizierungen nachweisen. Anschließend müssen Nachweise regelmäßig alle drei Jahre erbracht werden.

Die Verlängerung der Fristen für die Erbringung von Nachweisen gegenüber dem BSI von 2 auf 3 Jahre ist ein Ansatz, der in der Praxis eher umsetzbar scheint als der bisher angedachte Zeitraum von 2 Jahren. Zusätzliche Dokumentations- und Nachweispflichten binden jedoch 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 ernsthaft geprüft werden, ob eine Ausweitung der Nachweispflichen für Betreibr kritischer Anlagen über die allgemeinen Aufsichts- und Durchsetzungsmaßnahmen des BSI nach § 64 Referentenentwurf vom Juli 2023 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 Risikomanagementmaßnahmen und Nachweispflichten nur abgegrenzte kritische

Anlagen einer besonders wichtigen oder wichtigen Einrichtung umfassen, nicht auch sonstige Dienstleistungen der Einrichtungen.

Zentrale Melde- und Anlaufstelle (§ 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 müssen den betroffenen Unternehmen 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. Für ein vertrauensvolles Miteinander von Staat und Wirtschaft ist essenziell, dass sich die Unternehmen darauf verlassen können, dass auf die Schließung der von ihnen gemeldeten Schwachstellen hingewirkt wird, damit diese nicht von anderen Staaten und organisierter Kriminalität genutzt werden können und so Schäden von den Unternehmen abgewendet werden.

Im Übrigen verweisen wir auf unsere Ausführungen zu § 6.

Einsatz kritischer Komponenten (§ 41)

Die Regelung zum „Einsatz kritischer Komponenten; Verordnungsermächtigung“ ist im Entwurf noch nicht enthalten.

Da es sich hier um eine wesentliche Regelung handelt, die die Geschäftstätigkeit der Unternehmen maßgeblich tangiert, sollte hierzu schnellstmöglich eine Regelung zur Diskussion gestellt werden, um Rechts- und Planungssicherheit herzustellen.

Rechtsverordnungen (§ 57)

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 (§ 57 Abs. 4), die noch nicht vorliegt. Die Rechtsverordnung soll für das KRITIS-Dachgesetz und das NIS2UmsuCG gleichermaßen gelten.

Die Unternehmen benötigen frühzeitig Rechtssicherheit. Die – lediglich weiter 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.

Sanktionsvorschriften (§ 60)

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. Bei den Obergrenzen der Bußgelder sollte nicht über die EU-Vorgaben hinausgegangen werden.

E. 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 20. Oktober 2023 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 und Europapolitischen 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.