STELLUNGNAHME

Berlin, 04. Juli 2025

Deutsche Industrie- und Handelskammer

Referentenentwurf des Bundesministeriums des Innern
Gesetz 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. Indirekt betroffen sind auch Unternehmen in der Lieferkette.

Die DIHK hat sich bereits mehrfach zu vorhergehenden Entwürfen geäußert, zuletzt zum Regierungsentwurf der Vorgängerregierung. Der nun vorgelegte Referentenentwurf basiert auf diesen Vorarbeiten und enthält einige Änderungen, die Unternehmen betreffen – etwa in Bezug auf den Anwendungsbereich. **Unsere bisherigen Anmerkungen haben weiterhin Bestand. Diese Stellungnahme bezieht sich insbesondere auf die neu hinzugekommenen Aspekte.**

A. Das Wichtigste in Kürze

Das Ziel des Gesetzes, ein hohes gemeinsames Sicherheitsniveau aufrecht zu halten, unterstützt die DIHK ausdrücklich. Der vorliegende Gesetzentwurf kann nur ein Baustein unter vielen sein, um die Resilienz der Wirtschaft insgesamt auf ein höheres Niveau zu heben. Staat und Wirtschaft sind gemeinschaftlich gefordert. 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 Unternehmen benötigen vor allem Planungs- und Rechtssicherheit. Insofern ist positiv, dass der neue Entwurf zumindest nicht wesentlich von den Vorgängerversionen abweicht. Denn einige Unternehmen haben ungeachtet der Verzögerungen im Gesetzgebungsverfahren bereits damit begonnen, zentrale NIS2-Maßnahmen, insbesondere zum Risikomanagement einzuleiten.

Deshalb ist eine zügige und klare Umsetzung der NIS2-Richtlinie erforderlich. Strikte EU-Konformität ist nicht nur für Unternehmen wichtig, die in mehreren EU-Ländern tätig sind. Der Gesetzentwurf enthält noch immer Definitionen und Kategorien, die zu Interpretationsschwierigkeiten und großer Komplexität führen, etwa bei der Betroffenheitsprüfung. Der neue Referentenentwurf enthält Abweichung von der EU-Richtlinie, etwa bei der Definition „wichtige Einrichtungen“. So stellen z. B. die „vernachlässigbaren Tätigkeiten“ einen Themenkomplex dar, der deutlich von der EU-Vorgabe abweicht, was ggf. zu weiteren Verzögerungen in der rechtskonformen Umsetzung führen kann.

Meldefristen, Meldeinhalte und Prozesse sollten mit den anderen relevanten Gesetzen harmonisiert werden. Besser als mit einem Omnibus-Verfahren im Rahmen des Cyber Security Acts wäre gewesen, dies von vornherein sicherzustellen. Zumindest NIS2UmsuCG und KRITIS-Dachgesetz sollten sowohl einheitliche Begriffe und Definitionen verwenden als auch einheitliche Vorgaben enthalten: Im Hinblick auf die Umsetzungsprozesse, Meldepflichten und in Bezug auf die Kompetenzen der beteiligten Behörden. Jede Abweichung oder Unklarheit führt in der Praxis zu einem erhöhten Dokumentationsaufwand für Unternehmen, die die Erfüllung der Vorgaben nachweisen müssen.

Für die öffentliche Hand sind abseits von Teilen der Bundesverwaltung keine Verpflichtungen vorgesehen. Das stößt bei den Unternehmen weiterhin auf großes Unverständnis. Für die Unternehmen ist wichtig, dass sie sich auf funktionierende Prozesse mit der Verwaltung verlassen können. Bund und Länder sind in der Pflicht, die entsprechenden Voraussetzungen zu schaffen. Unternehmen erwarten zumindest einen verbindlichen Umsetzungsplan mit konkreten Meilensteinen.

B. Konkrete Bewertung des Referentenentwurfs

Erfüllungsaufwand

Nach der neuen Gesetzeslage werden wesentlich mehr Unternehmen als bislang besondere Cyber-Sicherheitsanforderungen umsetzen und nachweisen müssen

Beim einmaligen Erfüllungsaufwand sollte auch berücksichtigt werden, dass viel mehr als die tatsächlich betroffenen Unternehmen erst einmal gefordert sind, mit eigenem oder externem juristischen Fachwissen zu klären, ob sie überhaupt unter das Gesetz fallen. Diese Unsicherheit führt zu zahlreichen Anfragen bei den Industrie- und Handelskammern (IHKs), die oft schwer zu beantworten sind und derzeit viele personelle Ressourcen in den Unternehmen binden – was mit erheblichen Kosten verbunden ist. Selbst einfache Informationspflichten verursachen bereits spürbare Aufwände.

Auch in der Lieferkette entstehen zusätzliche Kosten. Besonders mittelständische Unternehmen, die indirekt vom Gesetz betroffen sind, tragen dabei überproportional hohe Aufwände. Diese Unternehmen sollten gezielt entlastet werden. Zertifizierungen wie ISO 27001, VdS oder TISAX sollten als ausreichender Nachweis für die Einhaltung von Sicherheitsvorgaben in der Lieferkette anerkannt werden. Derzeit müssen Unternehmen, die unter die NIS2-Richtlinie fallen, die Einhaltung der Sicherheitsanforderungen bei ihren Zulieferern selbst überprüfen – selbst dann, wenn diese bereits zertifiziert sind. Das führt zu erheblichem Mehraufwand in der gesamten Lieferkette, da unklar ist, ob eine Zertifizierung die Prüfpflichten erfüllt. In der Praxis bedeutet das: Manche Zulieferer müssen Hunderte unterschiedliche Anfragen beantworten – ein enormer Aufwand, der viel Zeit und Ressourcen kostet. Die Annahmen und Berechnungsgrundlagen im Referentenentwurf sollten realitätsnah angepasst werden. 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)

Es erfolgt eine Klarstellung hinsichtlich der Definition DNS-Diensteanbieter, MSSP und MSP.

Art. 6 Nummer 39 bzw. 40 in der EU-Richtlinie sind hier sehr allgemein gehalten. Eine EU-weit einheitliche Konkretisierung wäre grundsätzlich zu bevorzugen. Allein der Versuch einer Differenzierung in der Gesetzesbegründung des deutschen Umsetzungsgesetzes wird von den Unternehmen nicht als hinreichend erachtet.

Im Entwurf wird der bisherige Begriff „kritische Infrastrukturen“ durch „kritische Anlagen“ ersetzt, ebenso in mehreren Paragrafen des Telekommunikationsgesetzes (TKG). Was diese Änderung konkret bedeutet, ist derzeit noch unklar. Unternehmen fragen sich, ob sich dadurch

der Anwendungsbereich erweitert, ob mit dem neuen Begriff zusätzliche Pflichten verbunden sind, oder ob bestehende Anforderungen wegfallen. Hier besteht Klärungsbedarf.

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. Die ergänzte Regelung zum Anwendungsbereich: Bei der Betroffenheitsprüfung können Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung „vernachlässigbar" sind soll der Begründung zufolge verhindern, dass „eine nur geringfügige Nebentätigkeit zu einer unverhältnismäßigen Identifizierung als wichtige oder besonders wichtige Einrichtung führt."

Praxisbeispiel: Ein Logistikunternehmen betreibt ein internes Ladesäulennetz für E-Fahrzeuge – das bedeutet nicht automatisch, dass es im Sinne von Anlage 2 „Betreiber von Ladeinfrastruktur" ist.

Es ist grundsätzlich sinnvoll, dass unwichtige oder nur am Rand liegende Geschäftstätigkeiten eines Unternehmens bei der Prüfung einer NIS2-Pflicht außen vor bleiben. Der Ansatz, sogenannte „vernachlässigbare" Anwendungen von der Bewertung auszunehmen, zeigt Vertrauen in die Unternehmen und setzt voraus, dass diese ihre IT-Systeme klar trennen – je nachdem, ob sie für das Geschäft relevant oder eher unbedeutend sind. Gerade für mittelständische Unternehmen ist es wichtig, dass die Anforderungen an IT-Sicherheit in einem angemessenen Verhältnis zu den Kosten und dem Aufwand stehen. Eine Konzentration des Anwendungsbereiches auf die zentralen Geschäftsprozesse ist sinnvoll, damit Aufwand und Nutzen in einem sinnvollen Verhältnis bleiben. Die NIS2-Richtlinie enthält demgegenüber keine ausdrückliche Regelung, dass nicht relevante Geschäftstätigkeiten bei der Betroffenheitsprüfung automatisch ausgeschlossen werden können. Der deutsche Gesetzesentwurf geht einen eigenen Weg: Er sieht vor, dass sogenannte „vernachlässigbare" Tätigkeiten nicht berücksichtigt werden müssen. Das könnte jedoch im Widerspruch zur Systematik der EU-Richtlinie stehen. Denn laut NIS2 dienen die Schwellenwerte (z. B. Mitarbeiterzahl, Umsatz) nicht dazu, die Kritikalität eines Unternehmens zu bewerten, sondern sollen eine faire Verteilung der Pflichten

sicherstellen. Diese nationale Sonderregelung könnte den EU-Konsens verlassen und zu unterschiedlichen Umsetzungen in den Mitgliedstaaten führen. Das wiederum birgt rechtliche Unsicherheiten. Vor der endgültigen Verabschiedung sollte daher juristisch geprüft werden, ob diese Einschränkung mit dem Vorrang und der direkten Wirkung von EU-Recht vereinbar ist. Denn nach der Rechtsprechung des Europäischen Gerichtshofs sind nationale Regelungen, die gegen eine EU-Richtlinie verstoßen, nicht anwendbar.

Bei der gesamten Betroffenheitsanalyse sollten es klarere Formulierungen bzw. Abgrenzungen dem Betreiber einfacher machen, seine Betroffenheit zu bestimmen.

Darüber hinaus ist die Mehrfachbetroffenheit für Anlagenbetreiber im Entwurf nicht hinreichend adressiert. Ohne klare und konsistente Vorgaben drohen mehrfach betroffene Unternehmen in einen ineffizienten Nachweisdschungel zu geraten. In der aktuellen Struktur von NIS2 würden betroffene Unternehmen allein für Registrierungs-, Zertifizierungs-, Nachweis- und Meldepflichten – ohne Umsetzung konkreter Maßnahmen – hohe Bürokratiekosten tragen müssen. Eine stärkere Angleichung der Betroffenheitskriterien zwischen KRITIS und NIS2 wäre sinnvoll.

Einrichtungen der Bundesverwaltung (BSIG § 29)

Eine Anwendung auf Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen wird regelmäßig nicht verhältnismäßig sein. Daher erscheint aus unserer Sicht die Lösung einer Einzelfallentscheidung angemessen. Notwendig ist dann jedoch, dass die Rechtsaufsicht der entsprechenden juristischen Personen des öffentlichen Rechts zwingend mitentscheidet, da sie das Erfordernis und die Auswirkungen einer Anwendungserstreckung am besten beurteilen kann. Daher sollte die Entscheidung nur im Einvernehmen mit der Rechtsaufsicht getroffen werden können.

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

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

Bisherige Erfahrungen der IHKs bei der Information der Unternehmen zeigen, dass insbesondere die Anforderungen an Unternehmen in der Lieferkette unterschiedlich interpretiert werden. In Bezug auf die Absicherung der Lieferkette und deren sicherheitsbezogene Aspekte wären weiterführende Hinweise hilfreich, etwa zur Absicherung gemeinsamer/kollaborativer

Systeme, zum Schutz ausgewählter Daten wie Steuerungs- oder Kundendaten, zum Beginn und Ende einer Lieferkette, ggf. nach Instanzen, etc.

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.

Der Referentenentwurf enthält leicht veränderte Formulierungen, so dass die deutsche Umsetzung ggf. von den Umsetzungen anderer EU-Länder abweicht. Aktuell sind keine nachvollziehbaren Gründe für diese Abweichungen erkennbar. Die in der NIS2-Richtlinie formulierten Punkte sollten unverändert übernommen werden.

Speziell sieht die NIS2-Richtlinie „grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit“ vor, der Referentenentwurf hingegen „grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik“. Zwar erscheint dies für Unternehmen leichter verständlich und sollte zu einer Vereinfachung führen. Hingegen führt die Durchführungsverordnung der EU als Bestandteile grundlegender Cyberhygienemaßnahmen unter anderem Zero-Trust-Prinzipien, Gerätekonfiguration, Netzwerksegmentierung sowie Maßnahmen zum Identitäts- und Zugriffsmanagement auf. Ebenso wird die Schulung der Mitarbeitenden zur Sensibilisierung für Cyberbedrohungen (z. B. Phishing oder Social Engineering) explizit genannt.

Der Begriff Cyberhygiene geht unseres Erachtens deutlich über allgemeine „Schulungs- und Sensibilisierungsmaßnahmen“ hinaus. Für international tätige Unternehmen entstehen daraus unterschiedliche Anforderungen und Interpretationsspielraum für die Aufsichtsbehörden.

Nicht nachvollziehbar ist, wieso sich in dem aktuellen Entwurf die gelisteten Maßnahmen für das Risikomanagement unter § 30 Abs. 2 BSIG und unter § 5c Abs. 4 EnWG unterscheiden bzw. sie bei Formulierung und Umfang nicht harmonisiert sind. Dies betrifft insbesondere die Maßnahmen Nr. 5 (Sicherheitsmaßnahmen bei Erwerb, Entwicklung…), Nr. 7 (im Energiegesetz ist weiterhin die Rede von „Cyberhygiene“) und Nr. 9 (Konzepte für Zugriffskontrollen).

Wir empfehlen, in der nationalen Umsetzung für mehr Klarheit und Einheitlichkeit zu sorgen, um Unternehmen eine verlässliche und praxistaugliche Umsetzung zu ermöglichen.

Untersagung des Einsatzes kritischer Komponenten (BSIG § 41)

Betreiber kritischer Infrastrukturen müssen dem Bundesinnenministerium den Einsatz einer kritischen Komponente vorab mitteilen. Das BMI kann den Einsatz innerhalb von zwei Monaten nach Eingang der Anzeige untersagen oder Auflagen erteilen.

Unverhältnismäßig wäre, wenn durch Verbot kritischer Komponenten der Geschäftsbetrieb nicht aufrechterhalten werden könnte. Unternehmen müssen komplexe Prozesse wie Ausschreibungen, Anpassungen, Implementierung, Tests durchlaufen. Generell sollte der Erhalt der Geschäftsfähigkeit und eine potenzielle Gefahr einer anfälligen Sicherheitskomponente besser ins Verhältnis gesetzt werden.

Zugangsgewährung und Kooperationspflicht von DNS-Anbietern (BSIG § 50, § 51)

Die NIS2-Richtlinie sieht einen erleichterten Zugang zu korrekten Domain-Inhaberdaten (WHOIS-Daten) für berechtigte Stellen vor. Das NIS2UmsuCG bleibt hinter dieser Zielsetzung zurück.

Der Entwurf legt nahe, dass Domain-Register keine eigenen vollständigen Inhaberdatenbanken mehr führen dürfen. Dies würde nicht nur eine Abkehr von der gängigen Praxis bedeuten, es würde auch zu einer Fragmentierung der Datenbanken führen, da Inhaberdaten nur noch von den die Registrierungsdaten erhebenden Registraren gespeichert würden. Berechtigte Zugangsnachfrager wären so unter Umständen (selbst bei DE-Domains) auf die Kooperation und schnelle Bearbeitung von außerhalb der EU ansässigen Registraren angewiesen. Bei einer Insolvenz oder technischen Problemen eines der tausenden Registraren droht sogar ein Verlust der Daten.

§ 2 NIS2UmsuCG beschränkt den Zugang auf wenige nationale Behörden. Dies widerspricht der NIS2-Richtlinie, die auch CERTs, CIRTs und private Rechteinhaber einbezieht. Damit ließen sich zivilrechtliche Ansprüche durch Rechteinhaber schwerer durchzusetzen.

Eine Nachbesserung ist erforderlich, um den Zugang zu WHOIS-Daten praktikabel, rechtssicher und europarechtskonform zu gestalten. Der Kreis der berechtigten Zugangsnachfrager sollte demjenigen entsprechen, der in der NIS2-Richtlinie definiert wurde. Insbesondere sollten Rechteinhaber als zugangsberechtigte Stellen anerkannt werden, wie beispielsweise auch im belgischen Umsetzungsgesetz vorgesehen.

Rechtsverordnungen (BSIG § 56)

Die Wirtschaft wird wieder verpflichtend in die Gestaltung der konkretisierenden Verordnungen einbezogen. Die bisherige Praxis der Anhörung im Bereich des IT-Sicherheitsrechts sollte unbedingt fortgesetzt werden, um rechtliche Vorgaben praxistauglich zu gestalten.

Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) wird in der Liste der beteiligten Ministerien bislang nicht genannt – sollte aber unbedingt ergänzt werden. Gerade das BMDS ist durch seine Zuständigkeit für den Ausbau der Telekommunikationsnetze in Deutschland direkt betroffen. Neue Sicherheitsanforderungen für Netzbetreiber oder Infrastruktur können erhebliche Auswirkungen auf den Ausbau von Festnetz und Mobilfunk haben.

Diese möglichen Folgen müssen in die Entscheidungsprozesse der Bundesregierung einfließen, sorgfältig bewertet und bei widersprüchlichen Interessen miteinander in Einklang gebracht werden. Die Schwellenwerte für Kritische Anlagen werden vor allem durch Rechtsverordnungen nach § 56 Abs. 4 BSIG festgelegt. Bereits bestehende sektorspezifische Schwellenwerte in der BSI-Kritis-Verordnung sollten beibehalten werden, wobei Einrichtungen unterhalb dieser Schwellenwerte als besonders wichtige Einrichtungen gewertet werden sollten.

Abstimmung Cybersicherheitskataloge (EnWG § 5c, Abs. 1 und 2)

Das BSI soll mehr Mitspracherechte in Bezug auf die IT-Sicherheit von Energieunternehmen erhalten. Bislang musste die BNetzA, die die Sicherheitsvorgaben für den Energiebereich erstellt, das BSI nur informieren, wenn sie die Sicherheitskataloge ändert. Jetzt ist „Einvernehmen“ vorgesehen.

Die Kompetenz bzgl. Cybersicherheit sollte beim BSI gebündelt werden. Daher ist ein mehr an Mitspracherecht durch das BSI sinnvoll. Sonst müsste die BNetzA eigene Cybersicherheitskompetenz aufbauen.

Die Regeleung könnte auch zu neuen Unklarheiten führen. Besser wäre vielleicht: BSI = Rahmenstandards und Mindestanforderungen, BNetzA = sektorspezifische Konkretisierung innerhalb dieses Rahmens

Die stärkere Einbindung des BSI ist sachgerecht, da hier die Fachexpertise gebündelt ist und eine koordinierte Steuerung der IT-Sicherheit erfolgen kann.

Einbeziehung digitaler Energiedienste (EnWG § 5c, Abs. 3)

Künftig müssen auch Betreiber sogenannter digitaler Energiedienste einen angemessenen Schutz der IT-Systeme vor Bedrohungen gewährleisten – auch in Bezug auf die Anschaffung von Anlagegütern und Dienstleistungen. Bei einem solchen Dienst handelt es sich um eine Anlage, die einen zentralen Zugriff auf die Steuerung von Energieanlagen oder einen Zugriff auf die Steuerung dezentraler Energieverbrauchsanlagen möglich macht, etwa Wechselrichter, die häufig von chinesischen Firmen stammen.

Die Änderung ist nachvollziehbar, da digitale Energiedienste wesentliche Dienstleistungen für die Stabilität der Stromnetze erbringen. Allerdings sollte klargestellt werden, dass nicht jeder IT-Dienst im Energiebereich automatisch ein „digitaler Energiedienst“ im regulierungsrelevanten Sinne ist. Entscheidend ist: Kritikalität für den Energiesektor, Verfügbarkeit des Dienstes für Dritte oder für Versorgungsaufgaben, Systemische Bedeutung (z. B. Steuerung von Netzfrequenz, nicht bloß Visualisierung).

Ein hoher IT-Sicherheitsstandard für alle Energiedienstleister ist grundsätzlich sinnvoll und kann bei Neu- oder Umbauten entsprechend berücksichtigt werden. Eine kurzfristige

Umrüstung bestehender Systeme ist hingegen kritisch zu bewerten. Wichtig ist zudem, dass eine Diversität an Anbietern – insbesondere außerhalb von Ländern wie China – besteht. Dennoch ist anzumerken, dass die unklare Definition digitaler Energiedienste die ohnehin große regulatorische Komplexität verstärkt – eine Ausweitung ist daher nicht zielführend.

Weitere Energiedienste wie Wechselrichter in die Betrachtung zur Absicherung vor digitalen Angriffen einzubeziehen, ist unter dem Aspekt der Digitalen Souveränität essenziell und ein sinnvoller Schritt.

"Der angemessene Schutz nach Satz 1 ist auch durch Berücksichtigung erforderlicher Anforderungen bei der Beschaffung von Anlagengütern und Dienstleistungen sicherzustellen." Ist auch wieder vage. Das soll zwar erarbeitet werden. Aber Rechtssicherheit sieht anders aus. Die Erwähnung von China in der DIHK Mail in diesem Kontext finde ich unglücklich. Sanktionen oder politische Einschränkungen sollten nicht unbedingt in die NIS-2 Umsetzung hineingedichtet werden.

Für Betreiber digitaler Energiedienste sollte eine Mindestgröße (z. B. nach Kapazität oder angeschlossenen Haushalten) festgelegt werden. Kleine Energiegenossenschaften und Betreiber dezentraler Anlagen sollten von den umfassenden Pflichten ausgenommen werden, um die Energiewende nicht zu behindern.

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 4. Juli 2025 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.