21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)058
vom 6. Oktober 2025

Schriftliche Stellungnahme

der Deutschen Industrie- und Handelskammer vom 30. September 2025

zu dem Gesetzentwurf der Bundesregierung

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

BT-Drucksache 21/1501

STELLUNGNAHME

Berlin, 30. September 2025

Deutsche Industrie- und Handelskammer

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

Das vorliegende Gesetz 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. Der nun vorgelegte Regierungsentwurf basiert auf diesen Vorarbeiten und enthält einige Änderungen, die Unternehmen betreffen – etwa in Bezug auf den Anwendungsbereich. **Unsere bisherigen Anmerkungen haben weiterhin Bestand.**

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 diese nicht überfordern.

Zusammenarbeitsprozesse der Behörden untereinander und zwischen Behörden und Unternehmen sollten von Beginn an klar definiert und einheitlich umgesetzt werden. Eine effektive

Cybersicherheitsarchitektur und eine angemessene Ausstattung der Sicherheitsbehörden sind Voraussetzung, um Unternehmen sowohl präventiv als auch im Schadensfall zu unterstützen. Insofern besteht weiterer Klärungsbedarf im Hinblick auf wesentliche Fragen, etwa den Umgang mit Schwachstellen.

Unternehmen benötigen vor allem Planungs- und Rechtssicherheit. 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 unnötiger Komplexität führen. Meldefristen, Meldeinhalte und Prozesse sollten mit dem KRITIS-Dachgesetz und relevanten Fachgesetzen harmonisiert werden. Dies sollte nun endlich im Bundestag umgesetzt werden, indem NIS2-Umsetzungsgesetz und KRITIS-Dachgesetz zusammen beraten und synchronisiert werden. Jede Abweichung oder Unklarheit führt in der Praxis zu erhöhten Dokumentations- und Prüfaufwänden für Unternehmen.

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.

B. Konkrete Bewertung des Entwurfs

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 selbst binden oder externe Rechtsberatung erforderlich machen – was mit erheblichen Kosten verbunden ist.

Auch in der Lieferkette entstehen zusätzliche Kosten. Besonders mittlere 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.

Selbst einfache Informationspflichten verursachen bereits spürbare Aufwände. Die Annahmen und Berechnungsgrundlagen 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)

Der Entwurf enthält Abweichungen von der EU-Richtlinie, etwa bei der Definition „wichtige Einrichtungen“ oder den „vernachlässigbaren Tätigkeiten“. Dies kann die rechtskonforme Umsetzung erschweren und ggf. zu weiteren Verzögerungen in der Umsetzung führen. Grundsätzlich ist sicherzustellen, dass einheitliche Begriffe sowohl in Bezug zur EU-NIS2-Richtlinie als auch zum KRITIS-Dachgesetz verwendet werden.

Im Gesetzentwurf 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.

Klärungsbedarf besteht im Hinblick auf „kritische Anlagen“. Diese sollen durch Rechtsverordnung nach § 56 Abs. 4 näher bestimmt werden. Unternehmen fragen sich, ob sich dadurch der Anwendungsbereich erweitert.

Informationsaustausch (BSIG § 6)

Der Entwurf sieht vor, dass das BSI eine Online-Plattform für den Informationsaustausch zwischen Unternehmen und Einrichtungen der Bundesverwaltung betreibt (Information Sharing Portal).

Das Information Sharing Portal stellt eines der Kernelemente des Gesetzes dar und wird von der DIHK ausdrücklich befürwortet. Eine effektive Entgegennahme und Aufbereitung von Meldungen sowie die zielgerichtete Information von Unternehmen sind wesentlich für eine konstruktive Zusammenarbeit von Staat und Wirtschaft. Die Vorteile für die Unternehmen sollten transparent und greifbar gemacht werden, damit ein gelebtes vertrauensvolles Miteinander entstehen kann.

Das Information Sharing Portal sollte 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. Auch Unternehmen in der Lieferkette sollten am Informationsaustausch teilhaben können, sofern übergeordnete Bedenken nicht entgegenstehen.

Anwendungsbereich (BSIG § 28)

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

Unternehmen benötigen erst einmal Klarheit über ihre Betroffenheit. Trotz der inzwischen geschaffenen und ständig weiterentwickelten Informationsangebote des BSI ergeben sich jedoch noch immer viele Fragen im Hinblick auf die konkrete Betroffenheit der Unternehmen. Klare und verständliche Formulierungen sollten es den Unternehmen so einfach wie möglich machen, ihre Betroffenheit zu bestimmen. Dafür und für die konkrete Umsetzung sind rechtssichere und praxistaugliche Umsetzungshilfen zur Verfügung zu stellen. Im Falle von zusätzlicher Betroffenheit durch branchenspezifische Sicherheitsvorgaben sind diese Regelungen zu harmonisieren.

Die Regelung zum Anwendungsbereich in § 28 Abs. 3 „Bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 können solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind“ führt zu Verunsicherung bei den Unternehmen. Es ist grundsätzlich sinnvoll, dass unwichtige oder nur am Rand liegende Geschäftstätigkeiten eines Unternehmens bei der Prüfung einer NIS2-Pflicht außen vorbleiben. Der Ansatz, sogenannte „vernachlässigbare“ Anwendungen von der Bewertung auszunehmen, zeugt vom Bestreben, bürokratische Lasten für Unternehmen in Grenzen zu halten. Eine Konzentration des Anwendungsbereiches auf die zentralen Geschäftsprozesse ist sinnvoll, damit Aufwand und Nutzen in einem sinnvollen Verhältnis bleiben. Die NIS2-Richtlinie enthält keine ausdrückliche Regelung, dass nicht relevante Geschäftstätigkeiten bei der Betroffenheitsprüfung automatisch ausgeschlossen werden können. Die 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 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. Unternehmen benötigen Rechtsklarheit.

Mit der starken Ausweitung des Anwendungsbereichs muss eine verstärkte Kommunikations- und Vermittlungsarbeit einher gehen, insbesondere gegenüber den mittelständisch geprägten Unternehmen bis 250 Beschäftigten.

Einrichtungen der Bundesverwaltung (BSIG § 29)

Nach dem Entwurf finden für Einrichtungen der Bundesverwaltung 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. Die Einrichtungen der Bundesverwaltung sollten ein einheitlich hohes Cybersicherheitsniveau haben.

In Bezug auf eine Anwendung auf Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen erscheint aus unserer Sicht die Lösung einer Einzelfallentscheidung angemessen. Dass die Entscheidung des BSI nur im Einvernehmen mit der Rechtsaufsicht getroffen werden können soll, ist sachgerecht, da diese das Erfordernis und die Auswirkungen einer Anwendungserstreckung am besten beurteilen kann.

Risikomanagementmaßnahmen besonders wichtiger und wichtiger Einrichtungen (BSIG § 30, § 31; EnWG § 5c Abs. 4)

Bei den im Entwurf vorgesehenen 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.

Unsere bisherigen Erfahrungen 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 des BSI 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 Gesetzentwurf enthält gegenüber der europäischen NIS2-Richtlinie 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 Entwurf 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.

Zentrale Melde- und Anlaufstelle (BSIG § 40)

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

Unternehmen sollten von Doppelmeldungen entlastet werden, und die Meldungen sollten so einfach wie möglich erfolgen. Das BSI als zentrale Meldestelle sollte geeignete Prozesse etablieren, um Meldewege zu vereinheitlichen. Beispielsweise sollten eingehende Meldungen der Unternehmen direkt an die Datenschutzaufsichtsbehörden weitergeleitet werden, sofern der Vorfall datenschutzrechtlich relevant ist.

Unternehmen müssen sicher gehen können, dass bekannt gewordene Schwachstellen grundsätzlich geschlossen werden. Die konkreten Verfahren zum Umgang mit Schwachstellen sollten gesetzlich definiert werden.

Untersagung des Einsatzes kritischer Komponenten (BSIG § 41)

Betreiber kritischer Infrastrukturen müssen nach dem Gesetzentwurf 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.

Speicherpflicht und Zugangsgewährung zu DNS-Registrierungsdaten (BSIG § 49, § 50, § 51)

Die Begründung zu § 51 BSIG 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 Registrare droht sogar ein Verlust der Daten.

§ 2 Abs. 2 beschränkt den Zugang auf wenige nationale Behörden. Dies widerspricht der NIS2-Richtlinie, die in diesem Punkt offengehalten ist. Rechteinhaber blieben nach dem NIS2UmsuCG außen vor, es besteht die Gefahr, dass die Durchsetzung zivilrechtlicher Ansprüche erheblich erschwert wird.

Eine Nachbesserung ist erforderlich, um den Zugang zu WHOIS-Daten praktikabel, rechtssicher und europarechtskonform zu gestalten. Der Kreis der berechtigten Zugangsnachfrager sollte entsprechend der NIS2-Richtlinie weiter gefasst werden. Beispielsweise sollten Rechteinhaber wie von der Kommission im Rahmen der „Toolbox against Counterfeiting“ empfohlen als zugangsberechtigt anerkannt werden, wie etwa auch im belgischen Umsetzungsgesetz vorgesehen.

Rechtsverordnungen (BSIG § 56)

Die bisherige Praxis der Anhörung der Wirtschaft im Bereich des IT-Sicherheitsrechts sollte unbedingt fortgesetzt werden, um rechtliche Vorgaben praxistauglich zu gestalten.

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.

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

Nach dem Entwurf 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, deren Marktanteile 80 Prozent außerhalb der EU liegen.

Die Einbeziehung von Betreibern sogenannter digitaler Energiedienste unterstreicht die Bedeutung des Energiesystems für die Sicherheit des Wirtschaftsstandorts Deutschland. Dabei ist eine Balance zwischen Schutzniveau einerseits und damit einhergehende Kostensteigerungen für die Breite der Wirtschaft andererseits zu berücksichtigen. Zu berücksichtigen ist insbesondere, dass zusätzliche Bürokratie und Auflagen für die Betriebe vermeiden werden und kleine und mittlere Unternehmen nicht zusätzlich belastet werden. Vor diesem Hintergrund ist ein hoher IT-Sicherheitsstandard für alle Energiedienstleister grundsätzlich sinnvoll und kann bei Neu- oder Umbauten entsprechend berücksichtigt werden. Eine kurzfristige Umrüstung bestehender Systeme wird hingegen von Betrieben kritisch bewertet. Allerdings sollte klargestellt werden, dass nicht jeder IT-Dienst im Energiebereich automatisch ein „digitaler Energiedienst“ im regulierungsrelevanten Sinne ist. Entscheidend ist, dass eine Kritikalität für den Energiesektor tatsächlich gegeben ist. Möglich wäre beispielsweise eine Bagatellgrenze und Ausnahmen für Betreiber digitaler Energiedienste unterhalb einer Mindestgröße aufzunehmen, um kleinere Betriebe nicht unverhältnismäßig zu belasten sowie die Energiewende nicht zu behindern. Dabei wäre jedoch sicherzustellen, dass etwaige Ausnahmetatbestände nicht die Gesamtheit des Sicherheitsniveaus unterlaufen.

Darüber hinaus sollte nicht nur ein angemessenes Schutzniveau der IT-Systeme in den Blick genommen werden, sondern auch die Diversifizierung von Bezugsländern. Dabei ist anzumerken, dass die unklare Definition digitaler Energiedienste die ohnehin große regulatorische Komplexität verstärkt – eine Ausweitung ist daher nicht zielführend.

Nach dem Entwurf soll das BSI 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.

Aus der Perspektive der Wirtschaft erscheint es richtig, das BSI und dessen Kompetenzen beim Thema Cybersicherheit verstärkt einzubeziehen. Daher ist ein mehr an Mitspracherecht durch das BSI sinnvoll. Alternativ müsste die BNetzA eigene Cybersicherheitskompetenz aufbauen, was zu ineffizienten Kosten und Doppelstrukturen für die Wirtschaft führen könnte. Wichtig

ist, dass eine klare Arbeitsaufteilung zwischen den Behörden erfolgt, die eine effizienten Schutz und Niveau an Cybersicherheit ermöglicht.

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 30. September 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.