Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)749

STELLUNGNAHME

Berlin, 26. Februar 2021

Deutscher Industrie- und Handelskammertag

Gesetzentwurf der Bundesregierung: Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

Daten, Systeme und Infrastrukturen – die Digitalisierung insgesamt – werden immer wesentlicher für die Wettbewerbsfähigkeit und gar generell den Fortbestand von Unternehmen. Aufgrund der starken Abhängigkeit der gewerblichen Wirtschaft von sicheren digitalen Infrastrukturen und Anwendungen setzt sich der DIHK für geeignete Rahmenbedingungen ein, um die Daten- und Informationssicherheit in der Breite der Wirtschaft zu verbessern. Er nimmt wie folgt zu ausgewählten zentralen wirtschaftsbezogenen Aspekten des vorliegenden Entwurfes Stellung:

Unternehmen sind grundsätzlich selbst für das Handling der Risiken in ihrem eigenen Verantwortungsbereich verantwortlich. Jeder Unternehmer muss – im Rahmen der gesetzlichen Vorgaben – entscheiden, welche eigenen Daten, Informationen und Infrastrukturen besonders schützenswert sind und die erforderlichen Schutzmaßnahmen treffen. Unseren Erfahrungen nach haben Unternehmen in den letzten Jahren in der Regel entsprechende technische und organisatorische Vorkehrungen getroffen. Individuelle Datensicherheit ist zugleich aber auch ein Beitrag zur gemeinschaftlichen Resilienz. Wo besondere Risiken bestehen, müssen andere Marktteilnehmer durch spezielle rechtliche Vorgaben geschützt werden – so geschehen etwa mit den Regelungen des ersten IT-Sicherheitsgesetzes zu kritischen Infrastrukturen.

Der Gesetzgeber hat mit dem ersten IT-Sicherheitsgesetz Meldepflichten für IT-Sicherheitsvorfälle und Mindestsicherheitsstandards für die Betreiber kritischer Infrastrukturen wie Energie, Wasser, Gesundheit oder Telekommunikation eingeführt, die erst nach und nach in der Umsetzung ankommen. Mit dem vorliegenden Entwurf eines IT-Sicherheitsgesetzes 2.0 werden zusätzliche gesetzliche Anforderungen an weitere Unternehmen im besonderen öffentlichen Interesse vorgesehen, bevor evaluiert wurde, inwiefern die bisherigen Verpflichtungen zu einem höheren IT-Sicherheitsniveau beitragen. Wir empfehlen, bei künftigen Gesetzgebungsvorhaben konkrete Evaluierungen vorzusehen und diese verbindlich in den Gesetzgebungsprozess einfließen zu lassen, um auf Basis dieser Erkenntnisse eventuellen zusätzlichen Regelungsbedarf der Unternehmensrealität anzupassen. Bei der Ausweitung gesetzlicher Vorgaben sollten konkrete Umsetzungserfordernisse in den Unternehmen von Beginn an in die Betrachtungen einbezogen werden. Eine solche vollzugssensitive Regulierung sollte von vornherein das Verhältnis der damit

DIHK | Deutscher Industrie- und Handelskammertag e.V.
Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Postanschrift: DIHK | 11052 Berlin

Tel. 030-20308-0 | Fax 030-20308-1000 | Internet: www.dihk.de

verbundenen Belastungen und den konkreten Nutzen einer Regelung für die Unternehmen in den Blick nehmen.

Dem vorliegenden Entwurf zufolge entsteht der Wirtschaft für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein einmaliger Aufwand in Höhe von ca. 40.000 Euro sowie laufende Aufwände in Höhe von rund 21 Millionen Euro. Die Ermittlung des Erfüllungsaufwands für die Wirtschaft ist laut Entwurf „nur unter hoher Unsicherheit quantifizierbar“ und sind „somit als Mindestwerte zu verstehen“. Der tatsächliche Aufwand in den Unternehmen dürfte wesentlich höher liegen, so sind beispielsweise etwaige Folgekosten nicht erfasst, die in der Anwendung des Gesetzes entstehen, etwa bei einer möglichen Rückbauanordnung. Insbesondere vor diesem Hintergrund sollte den betroffenen Unternehmen durch das Gesetzesvorhaben nicht nur Aufwand, sondern vor allem ein unmittelbarer Gewinn an IT-Sicherheit entstehen. Ein konkreter Mehrwert durch die Erfüllung zusätzlicher Verpflichtungen, insbes. Meldepflichten, sollte im Gesetzentwurf deutlicher herausgearbeitet werden. Hilfreich für die Unternehmen könnte beispielsweise ein aktuelles Lagebild inkl. branchenspezifischer Handlungsempfehlungen sein, aber auch Unterstützung durch die Mobile Incident Response Teams.

Im Fokus des Gesetzentwurfs stehen vor allem (End)Nutzer, große Unternehmen sowie Unternehmen mit kritischer Infrastruktur. Wünschenswert wäre eine stärkere Fokussierung auch auf pragmatische Unterstützungsleistungen – nicht zusätzliche regulatorische Belastungen – insbesondere kleinerer und mittlerer Unternehmen bei der Erhöhung ihrer Daten- und Informationssicherheit. Diese sollten als relevante Zielgruppe stärker benannt werden, ggf. wäre bei den betreffenden Regelungen der Begriff „Anwender“ statt „Verbraucher“ treffender. Die folgenden Ausführungen nehmen daher die Auswirkungen des Entwurfes auf Anwender im Sinne von Unternehmen in den Fokus und beziehen sich nicht auf den Verbraucherbegriff im Sinne des BGB. Sofern kleine und mittlere Unternehmen in den Anwendungsbereich des Gesetzes fallen, sind selbst die o. g. Aufwände nicht darstellbar. Hier ist mehr Augenmaß bei der Gesetzgebung und eine Orientierung an den unternehmerischen Realitäten gefragt.

Insgesamt ist ein systematisches, gesamtheitliches Vorgehen zum Schutz der Wirtschaft erforderlich. Dieses sollte darauf ausgerichtet sein, Daten- und Informationssicherheit in der Unternehmerschaft im Sinne eines breiten Resilienzstandards umzusetzen. Das Sicherheitsniveau sollte durch verschiedene Maßnahmen (rechtliche Vorgaben, Informations- und Unterstützungsleistungen, Förderung etc.) schrittweise erhöht werden. Erforderlich dafür ist ein übergreifendes Gesamtkonzept, das das Zusammenspiel freiwilliger und verpflichtender Vorhaben transparent macht, Lösungen im europäischen Kontext und einen konkreten Umsetzungsplan beinhaltet. Das IT-Sicherheitsgesetz ist ein Teil dieses Gesamtkonzepts und sollte eine entsprechende Einordnung finden. Insbesondere weisen wir darauf hin, dass zentrale Begriffe des Entwurfs im Einklang mit europäischen Regelungen erfolgen sollten, – insbes. zur europäischen Richtlinie zur Erhöhung der Netz- und Informationssicherheit (sog. NIS-Richtlinie), die gerade überarbeitet wird – um Rechtsunsicherheiten für die Unternehmen zu vermeiden.

Im Einzelnen:

Ausweitung von Pflichten sollte mit konkreten Sicherheitsgewinnen einhergehen

Für die Betreiber von kritischen Infrastrukturen bestehende Meldepflichten und Verpflichtungen zur Gewährleistung eines Mindestsicherheitsstandards sollen auf weitere Teile der Wirtschaft ausgeweitet werden. Hierunter fallen insbes. solche Unternehmen, an deren Funktionsfähigkeit ein „besonderes öffentliches Interesse“ besteht, worunter nach § 2 Absatz 14 Nr. 2 BSIG-E unter anderem Unternehmen zu verstehen sind, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind. Entsprechende Unternehmen sollen durch Rechtsverordnung bestimmt werden, in der „abstrakt-generelle Kriterien verbindlich vorgegeben“ werden, „nach denen Unternehmen selbst feststellen können, ob sie Unternehmen im besonderen öffentlichen Interesse“ sind. Dabei soll man sich am Gutachten der Monopolkommission orientieren, in dem „die einhundert größten Unternehmen Deutschlands nach inländischer Wertschöpfung ermittelt“ werden.

Aus Gründen der Sachnähe und Flexibilität ist es zwar sinnvoll, nicht jedes kleinste Detail durch Gesetz zu regeln, Unternehmen benötigen aber frühzeitig Rechtssicherheit darüber, wen genau die neuen Regelungen betreffen und was sie zu tun haben. Mithin erscheinen die Maßstäbe zur Bestimmung des Adressatenkreises zu unbestimmt – auf europäischer Ebene sind keine vergleichbaren Regelungen im Rahmen der NIS-Richtlinie vorgesehen. Doppelregulierungen und Widersprüche sind zu vermeiden. Um die Bürokratielast nicht unnötig zu vergrößern, sollte die Ausweitung des Kreises der Unternehmen, denen die aufwändigen Zusatzpflichten auferlegt werden, auf ein notwendiges Maß begrenzt sein.

Die Einbeziehung von wichtigen Unternehmen über den KRITIS-Kernbereich hinaus ist für diese mit Aufwand verbunden, der laut Entwurf nur „unter hoher Unsicherheit quantifizierbar“ ist. Für die betroffenen Unternehmen sollte aber nicht nur Aufwand, sondern vor allem ein unmittelbarer Gewinn an IT-Sicherheit entstehen, wenn sie zusätzliche Verpflichtungen erfüllen müssen. Ein solcher könnte sich etwa durch ein aktuelles Lagebild mit entsprechenden Handlungsempfehlungen oder durch Unterstützung im Schadensfall ergeben. Dafür sollte sichergestellt sein, dass auch das entsprechende Fachpersonal im BSI verfügbar ist.

Mehr Kompetenzen des BSI nur in Verbindung mit mehr Transparenz und konkretem Mehrwert für die Unternehmen

Das BSI erhält zahlreiche zusätzliche Befugnisse. Eingeführt werden soll eine Bestandsdaten-auskunft für Anbieter von Telekommunikationsdiensten. Diese Informationen sollen verwendet werden, um Betreiber kritischer Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse und Anbieter digitaler Dienste über die dazugehörigen Cyber-Angriffe zu informieren und bei der Angriffsabwehr zu unterstützen. Darüber hinaus kann das BSI bei den genannten Institutionen aktive Detektionsmaßnahmen durchführen sowie generell Produkte und Systeme untersuchen und

die Ergebnisse veröffentlichen. Auch dafür müssen die verpflichteten Unternehmen Informationen bereitstellen. Zur Gefahrenabwehr soll nach dem Entwurf das BSI Maßnahmen für Diensteanbieter anordnen können. Es wird eine Registrierungspflicht für Betreiber kritischer Infrastrukturen und für Unternehmen im besonderen öffentlichen Interesse eingeführt, und das BSI soll Cybersicherheitszertifikate für Systeme, Komponenten und Produkte ausstellen, wofür es vorab den sog. Stand der Technik festlegen soll.

Die Entwicklung und Veröffentlichung von sicherheitstechnischen Anforderungen an IT-Produkte durch das BSI darf nicht in einen nationalen Alleingang münden, und es sollten keine Parallelstrukturen aufgebaut werden. Der Stand der Technik sollte wie bisher auf Basis anerkannter Normen und Standards ausgelegt werden, an deren Erarbeitung die betroffenen Unternehmen und Normungsorganisationen beteiligt sind.

Angesichts des geplanten umfangreichen Ausbaus der Aufgaben und Kompetenzen des BSI stellt sich die Frage nach der Erhöhung der Akzeptanz für diese zusätzlichen Befugnisse, insbesondere vor dem Hintergrund der geplanten zusätzlichen Detektions-, Kontroll- und Anordnungsbefugnisse und der engen Zusammenarbeit zwischen BSI und Sicherheitsbehörden. 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. Viele Unternehmen fragen sich, inwieweit das BSI aufgedeckte Schwachstellen an andere Sicherheitsbehörden weiterleitet, statt auf die Schließung dieser Lücken hinzuwirken, die auch von anderen Staaten und organisierter Kriminalität genutzt werden und damit erhebliche Schäden bei betroffenen Unternehmen verursachen können.

Das in § 7 Abs. 2 BSIG-E formulierte eigene Ermessen als Grundlage, Sicherheitslücken zu publizieren, erscheint insofern zu unspezifisch. Hier sollte klargestellt werden, dass das BSI derartiges Wissen und auch darüber hinaus bekanntgewordene Erkenntnisse mit der Wirtschaft teilen muss, um ein schnelles und sachgerechtes Schließen von Sicherheitslücken auch in anderen Bereichen kritischer Infrastrukturen zu ermöglichen. Insbesondere darf das BSI-Gesetz kein Einfallstor für die Aufweichung von Verschlüsselung durch sog. Backdoors werden.

Eine getrennte Fachaufsicht über defensive (BSI) und offensive Sicherheitsbehörden könnte zudem ein Mindestmaß an Grundvertrauen in der Wirtschaft schaffen. Von einer ernsthaften Befassung der Bundesregierung mit diesem Thema würde die Cyber- und IT-Sicherheit der Unternehmen profitieren. Denn das BSI kann seinem Auftrag – die IT-Systeme in Deutschland sicherer zu machen – nur in vertrauensvoller Zusammenarbeit mit den Marktakteuren effektiv nachkommen.

Das Bestandsdatenauskunftsverlangen richtet sich an denjenigen, „der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt". Damit könnte jeder Anbieter umfasst sein, gleich welcher Größenordnung. Zudem wird aus dem Entwurf nicht deutlich, wie Diensteanbieter sich gegen Anordnungen des BSI zu Umleitungen des Datenverkehrs an eine vom BSI benannte Anschlusskennung (sog. Sinkhole-Server zur Verminderung der Gefahren von

Botnetzen) verwehren können. Dies scheint eine unzulässige Vermengung der BSI-Anordnungen zur allgemeinen Sicherheitserhöhung mit Verfahren der Strafverfolgung.

Für Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse besteht künftig eine Registrierungspflicht beim BSI – unabhängig von der bereits bestehenden Regstrierungspflicht für eine Kontaktstelle. Es ist für Unternehmer bereits jetzt schwierig, den Überblick zu behalten, wo sie sich überall registrieren oder eintragen lassen müssen. Wird eine Registrierung nicht oder nicht rechtzeitig vorgenommen, handelt es sich um eine Ordnungswidrigkeit, die mit einer Geldbuße geahndet werden kann. Im Hinblick auf eine ebenfalls geplante Registrierungspflicht im Rahmen der NIS-Richtlinie sollte von vorn herein sichergestellt werden, dass nicht mit Inkrafttreten der NIS-Richtlinie erneute Registrierungspflichten auf die Unternehmen zukommen.

Das BSI soll zentrale Meldestelle für die Sicherheit in der Informationstechnik werden. Hierfür soll es Informationen über Sicherheitsrisiken in der Informationstechnik (z. B. zu Sicherheitslücken, Schadprogrammen, Angriffen) entgegennehmen, diese auswerten und verarbeiten. Die Verarbeitung umfasst die Weitergabe unternehmerischer Daten durch die Information Dritter, die Warnung der Öffentlichkeit und die Unterrichtung von Betreibern Kritischer Infrastrukturen. Es sollte klargestellt werden, dass bei Meldungen generell bereits etablierte Meldewege genutzt werden und kein zusätzlicher Kanal bedient werden muss. Zudem bedarf es einer Konkretisierung des dadurch für die Unternehmen entstehenden Mehrwerts – detailliertes Lagebild und Handlungsempfehlungen.

Geprüft werden sollte deshalb auch, inwieweit die erlangten Informationen über den Kreis der Betreiber kritischer Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse und Anbieter digitaler Dienste hinaus auch anderen betroffenen Unternehmen möglichst zielgenau zur Verfügung gestellt werden können, etwa den Partnern der Allianz für Cybersicherheit. Eine Aufbereitung der Informationen je nach Adressatenkreis ist dabei notwendig. Meldungen zu Schwachstellen sind 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.

Insgesamt sollte bei den einzelnen Verpflichtungen stärker darauf geachtet werden, inwieweit die Maßnahmen von den Unternehmen, insbesondere auch von kleinen und mittleren Unternehmen, aus wirtschaftlichen Erwägungen leistbar sind und mit welchem zusätzlichen Sicherheitsgewinn jeweils faktisch zu rechnen wäre. Entsprechende Eingrenzungen des Anwendungsbereichs scheinen insbesondere mit Blick auf die angepassten Bußgeldvorschriften erforderlich.

Infrastrukturen innovationsoffen und sicher gestalten – geeignete Rahmenbedingungen auf europäischer Ebene schaffen

Eine zentrale Regelung des Entwurfs betrifft den Einsatz besonders kritischer Komponenten im Bereich der kritischen Infrastrukturen. Dieser soll künftig unter bestimmten Voraussetzungen

untersagt werden können. Vorgesehen ist ein mehrstufiges Verfahren, in dem vor Einsatz der Komponenten die technische Zuverlässigkeit geprüft, zertifiziert und von den Betreibern eine Garantieerklärung der Hersteller der kritischen Komponenten vorgelegt werden muss. Anschließend erfolgt eine Prüfung, ob dem Einsatz der Komponenten überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange entgegenstehen. Darüber entscheiden die betreffenden Ressorts der Bundesregierung.

Die Sicherheit von Daten und Informationen aller Anwenderunternehmen hängt davon ab, ob (Vor)Produkte, Komponenten und Infrastrukturen sicher sind. Spezifische IT-Sicherheits-Vorgaben sind für sicherheitsrelevante Produktkategorien erforderlich. Mit einer entsprechenden Regelung kann mehr Transparenz geschaffen und den Anwenderunternehmen die Nutzung von geprüft sicheren Infrastrukturen zumindest erleichtert werden. Auf der anderen Seite werden den Betreibern kritischer Infrastrukturen wesentliche Belastungen auferlegt – von der Einholung der Garantieerklärung für kritische Komponenten bis hin zum Umbau der Systeme bei einer eventuellen Untersagung eines Komponenteneinsatzes, ohne dass im Entwurf Schadensersatzleistungen oder Umsetzungszeiträume geregelt wären.

Bei einem solch vielschichtigen Problem wird eine rein nationale Lösung langfristig nicht weiterhelfen. Fraglich ist, ob ein nationales Vorpreschen hier nicht allein nationale Anbieter benachteiligt. Innerhalb der EU sollten keine künstlichen Marktverzerrungen kreiert werden. Die Bundesregierung ist deshalb gefordert, gemeinsam mit den anderen EU-Mitgliedstaaten eine nachhaltige, zukunftsoffene Lösung auf europäischer Ebene zu finden. Mittelfristig sollte die EU die Rahmenbedingungen dafür schaffen, die europäischen Kräfte in Hochtechnologiebereichen und kritischen Infrastrukturen besser zu bündeln, und in diesem Zuge die Wettbewerbsfähigkeit und digitale Sicherheit der gewerblichen Wirtschaft in einer digitalisierten Welt auch europaweit zu gewährleisten.

Eine Erklärung des Herstellers über seine Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur (Garantieerklärung), die sich über die gesamte Lieferkette des Herstellers erstreckt, ist im Zeitalter von internationalen Zulieferern und Open-Source-Software kaum verbindlich leistbar und auch nicht durch den Betreiber überprüfbar. Es ist nicht zu erwarten, dass einzelne Hersteller eine solche Erklärung nicht abgeben würden. Von daher erscheint die Aussagekraft einer solchen von vorn herein sehr beschränkt. Der Fokus sollte vielmehr auf Prozesse zur Stärkung der Sicherheit gelegt werden.

Ferner bedeutet eine drohende Untersagungsanordnung für den Betreiber ein nahezu unbeherrschbares über den gesamten Lebenszyklus einer Komponente andauerndes Risiko. Dadurch erfolgt ein massiver nachträglicher Eingriff in bereits in der Vergangenheit auf Basis geltenden Rechts getroffene Investitionsentscheidungen sowie in grundgesetzlich geschützte Rechtspositionen. Im Falle einer Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller sollten zumindest bestandssichernde Regelungen zur Aufrechterhaltung der kritischen Geschäftsprozesse getroffen werden.

Zudem ist eine Definition materiell nachprüfbarer Gründe im Gesetz erforderlich, die der Vertrauenswürdigkeit entgegenstehen. Eine Untersagung muss für den Betreiber nachvollziehbar und materiell begründbar sein. Dabei sind weitere Wechselwirkungen (u.a. Ausbauverpflichtungen, Betriebskontinuität) zu berücksichtigen, um im Einvernehmen mit den Verpflichteten die Funktionsfähigkeit der Infrastrukturen als solcher zu gewährleisten.

Dies gilt insbesondere für bereits im Einsatz befindliche kritische Komponenten. Eine grundlegende Definition kritischer Kernkomponenten leistet der Gesetzentwurf indes nicht. Die Entscheidung, welche Komponenten dem Regime des IT-Sicherheitsgesetzes unterworfen werden, obläge damit allein dem Verordnungsgeber. Den möglichen, insbesondere erheblichen wirtschaftlichen Folgen für die Betreiber wird dies nicht gerecht, so dass eine Konkretisierung im Gesetz erforderlich ist.

Der neue § 10 Abs. 6 BSIG-E sieht vor, dass das BMI unter Beteiligung von Verbänden und des BMWi durch Rechtsverordnung die Offenlegung von Schnittstellen und die Einhaltung etablierter technischer Standards bestimmen kann. Diese allgemeine Anordnungsbefugnis zur Offenlegung von Schnittstellen, Einhaltung etablierter technischer Standards und Interoperabilität wird in der Unternehmerschaft kontrovers diskutiert. Auf der einen Seite wird gewürdigt, dass das Potenzial von Interoperabilität zur langfristigen Steigerung der IT-Sicherheit und digitalen Souveränität im Gesetzestext explizit aufgeführt wird. Andere Marktvertreter hingegen führen an, dass durch die Offenlegung von Schnittstellen zusätzliche Sicherheitsrisiken geschaffen werden, weil sensible, für den Schutz der Netzwerke relevante Informationen, in die Hände böswilliger Akteure fallen könnten. Eine abschließende Bewertung ist aufgrund der fehlenden Gesetzesbegründung und einer europarechtlichen Einordnung derzeit nicht möglich. Zu diesem Aspekt sehen wir im politischen Verfahren weiteren Diskussionsbedarf. In die Beratungen sollten die betroffenen Unternehmen eng eingebunden werden.

IT-Sicherheitskennzeichnung EU-weit einheitlich gestalten

Eine spezielle IT-Sicherheitskennzeichnung kann zu mehr Transparenz über die Sicherheitseigenschaften und zu einer Sensibilisierung auch der kleineren geschäftlichen Anwender für sicherere IT-basierte Produkte beitragen. Dieser Mehrwert ist mit der vorgesehenen nationalen Regelung jedoch nicht gegeben. Die Akzeptanz einer IT-Sicherheitskennzeichnung wird umso höher sein, je besser die Nutzer dessen Aussagegehalt verstehen. Ein IT-Sicherheitskennzeichen wird nur dann einen Mehrwert haben, wenn es europaweit einheitlich ausgestaltet ist.

Bei der Einführung eines freiwilligen IT-Sicherheitskennzeichens sollte darauf geachtet werden, dass die zusätzlichen Belastungen gerade für kleine und mittlere Hersteller möglichst geringgehalten werden. Sinnvoll ist ein abgestuftes Vorgehen je nach erforderlichem Sicherheitsniveau der Produkte. Die Sicherheitsanforderungen der jeweiligen Produktklassen und die Prüftiefe sollten verhältnismäßig sein und gemeinsam mit den betroffenen Unternehmen (insbesondere kleine und mittlere Unternehmen und Startups) auf Basis EU-weiter und internationaler Standards erarbeitet werden. Ein solches Kennzeichen kann nur dann eine Wirkung entfalten, wenn es durch entsprechende Kommunikationsmaßnahmen begleitet wird.

Unterstützungsangeboten für KMU mehr Raum geben

Um auch im Digitalen sicher wirtschaften zu können, benötigen Unternehmen weitere konkrete Unterstützungsangebote, die im vorliegenden Entwurf nicht explizit aufgegriffen werden, z. B.:

- Lotsen- bzw. Anlaufstellen für Fragen zur Prävention und für akute IT-Sicherheitsvorfälle. Dort sollten Unternehmen alle relevanten Informationen erhalten,
- eine stärkere Sensibilisierung und Kompetenzaufbau in Unternehmen durch Kampagnen, Informationsangebote und Vermittlung von IT-Sicherheits-Knowhow von der Schule an,
- Ausbau der Fördermöglichkeiten für KMU-Aktivitäten für mehr IT-Sicherheit.

Sofern das Bundesamt für Sicherheit in der Informationstechnik (BSI) hier Unterstützung leisten kann, sollte dies rechtlich verankert und mit einer entsprechenden Personalausstattung hinterlegt sein.

Umsetzungsfristen angemessen gestalten

Für die technische Implementierung der Vorgaben sind angemessene Übergangsfristen vorzusehen.

Wer wir sind

Unter dem Dach des Deutschen Industrie- und Handelskammertags (DIHK) haben sich die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich der 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.

Grundlage dieser Stellungnahme sind die dem DIHK bis zur Abgabe der Stellungnahme am 09. Dezember 2020 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.

Ansprechpartnerin im DIHK

Dr. Katrin Sobania, sobania.katrin@dihk.de