STELLUNGNAHME

Berlin, 9. Dezember 2020

Deutscher Industrie- und Handelskammertag

Diskussionsentwurf des Bundesministeriums des Innern, für Bau und Heimat eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme
(Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

Wir bedanken uns für die Gelegenheit, zu dem o. g. Entwurf kurzfristig Stellung zu nehmen. Unsere Anmerkungen beziehen sich ebenso auf den am 9. Dezember vorgelegten Referentenentwurf, sofern die darin enthaltenen Regelungen nicht bereits die von uns genannten Aspekte aufgreifen.

Daten, Systeme und Infrastrukturen – die Digitalisierung insgesamt – sind immer wichtiger für den Fortbestand von Unternehmen. Aufgrund der starken Abhängigkeit der gesamten deutschen 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. Aufgrund der Kürze der Stellungnahmefrist nimmt er 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 entscheiden, welche eigenen Daten, Informationen und Infrastrukturen besonders schützenswert sind und die erforderlichen Schutzmaßnahmen treffen. 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 und aktuell mit weiteren Vorgaben im vorliegenden Entwurf des IT-Sicherheitsgesetzes 2.0.

Der Gesetzgeber hat mit dem ersten IT-Sicherheitsgesetz Meldepflichten für IT-Sicherheitsvorfälle und Mindestsicherheitsstandards für die Betreiber besonders gefährdeter 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 vorgesehen, bevor evaluiert wurde, inwiefern die bisherigen Verpflichtungen zu einem höheren IT-Sicherheitsniveau beitragen.

Wir empfehlen, die Ergebnisse der Evaluierung in den Gesetzgebungsprozess einfließen zu lassen, um auf Basis dieser Erkenntnisse den zusätzlichen Regelungsbedarf der Unternehmensrealität

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

anzupassen. Bei der Ausweitung gesetzlicher Vorgaben sollten konkrete Umsetzungserfordernisse von Beginn an in die Betrachtungen einbezogen werden. Eine solche vollzugssensitive Regulierung sollte von vornherein das Verhältnis des Nutzens einer Regelung und die damit verbundenen Belastungen für die Unternehmen in den Blick nehmen.

Im Fokus des Diskussionsentwurfs stehen vor allem (End)Nutzer, große Unternehmen sowie Unternehmen mit kritischer Infrastruktur. Wünschenswert wäre eine stärkere Fokussierung auch auf die Erhöhung der Sicherheit insbesondere kleinerer und mittlerer Unternehmen gewesen. 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 Diskussionsentwurfes auf Anwender im Sinne von Unternehmen in den Fokus und beziehen sich nicht auf den Verbraucherbegriff im Sinne des BGB.

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 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.

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. Anlaufstelle für Fragen zur Prävention und für akute IT-Sicherheitsvorfälle. Dort sollten Unternehmen alle relevanten Informationen finden und an die richtigen hilfreichen Ansprechpartner vermittelt werden,
- eine stärkere Sensibilisierung und Kompetenzaufbau in Unternehmen durch Kampagnen, Informationsangebote und Vermittlung von IT-Sicherheits-Knowhow von der Schule an,
- Förderung und Angebote zur Unterstützung der IT-Sicherheit in KMU.

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

Dem vorliegenden Entwurf zufolge entsteht der Wirtschaft für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein Aufwand von einmaligen Personalkosten in Höhe von ca. 69.654 Euro, jährlichen Personalkosten in Höhe von ca. 2.913.022 Euro und jährlichen Sachkosten in Höhe von rund 6 Millionen Euro. Die Ermittlung des Erfüllungsaufwands für die Wirtschaft ist laut Entwurf „von deutlichen Unsicherheiten geprägt", „da zu einer Reihe von Vorschriften noch untergesetzliche Ausführungen erforderlich sind und die von der Wirtschaft genutzte IT nur in Teilen bekannt ist". Insbesondere vor diesem Hintergrund sollte den betroffenen Unternehmen durch das Gesetzesvorhaben nicht nur Aufwand, sondern vor allem ein unmittelbarer Gewinn an IT-Sicherheit entstehen.

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

Im Einzelnen:

Mehr Kompetenzen des BSI nur in Verbindung mit mehr Transparenz

Das BSI erhält zahlreiche zusätzliche Befugnisse, etwa zu sog. Portscans zur Detektion von Sicherheitsrisiken und Angriffsmethoden und zum Einsatz sog. Honeypots zur Anlayse von Angriffsmustern, zur Warnung der Nutzer informationstechnischer Systeme, in der Cybersicherheitszertifizierung etc.

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 den 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.

Zumindest sollten die zusätzlichen Kompetenzen des BSI einer umfassenden Transparenz und Kontrolle unterliegen. Eine getrennte Fachaufsicht über defensive (BSI) und offensive Sicherheitsbehörden könnte 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.

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.

Zwar wurden die Begriffe der „Infrastruktur im besonderen öffentlichen Interesse“ und „sons-tige Unternehmen mit Relevanz für die IT-Sicherheit (Cyberkritikalität)“ begrüßenswerter Weise gestrichen und damit bisherige Kritik aus der Wirtschaft aufgegriffen. Geplant ist dafür nun die Einführung des Begriffs der „Unternehmen im besonderen öffentlichen Interesse“, 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 festgelegt

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

wird, welche wirtschaftlichen Kennzahlen bei der Berechnung der inländischen Wertschöpfung heranzuziehen sind, mit welcher Methodik die Berechnung zu erfolgen hat und welche Schwellenwerte maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland gehört.

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 noch immer zu unbestimmt – auf europäischer Ebene sind keine vergleichbaren Adressatenkreise im Rahmen der NIS-Richtlinie vorgesehen. Doppelregulierungen sind zu vermeiden.

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 die geplanten Portscans durch das BSI oder durch schnelle Hilfe im Schadensfall durch die Mobile incident response Teams ergeben. Dafür sollte sichergestellt sein, dass auch das entsprechende Fachpersonal im BSI zeitnah verfügbar ist.

Bestandsdatenauskunft, Untersuchungen, Detektion, Anordnungen und weitere Verpflichtungen verhältnismäßig und adressatenorientiert gestalten

Eingeführt werden soll eine Bestandsdatenauskunft für Anbeiter 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 Hersteller Informationen bereitstellen. Zur Gefahrenabwehr darf das BSI Maßnahmen für Diensteanbieter anordnen.

Das Bestandsdatenauskunftsverlangen richtet sich an denjenigen, „der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt". Damit wäre jeder Anbieter umfasst, gleich welcher Größenordnung. Die Formulierung "eine unmittelbare Kontaktaufnahme durch das Bundesamt mit ihm als erforderlich erscheinen lassen" öffnet das Auskunftsverlangen zudem in beliebigen Fällen. Hier sollte noch einmal geprüft werden, inwieweit die Auskunftspflicht insbesondere auch durch kleine und mittlere Unternehmen leistbar ist und ggf. den Anwendungsbereich anpassen.

Geprüft werden sollte 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 notwendig.

Das BSI ist künftig zur Durchführung von Portscans zur Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden befugt. Auch wenn nach wie vor kein aktives Eindringen in IT-Systeme vorgesehen ist, sollte eine Vorankündigung der Detektionsmaßnahmen gesetzlich verankert werden.

Generell erscheint das Auskunftserlangen zu Produkten sehr weit gefasst. Mit der vorliegenden Formulierung kann das BSI die Auskünfte für jedes beliebige Produkt am Markt verlangen.

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. Eine vorgeschaltete Frist zur Stellungnahme wäre insbesondere für kleine Anbeiter sinnvoll.

Das BSI soll zentrale Meldestelle für die Sicherheit in der Informationstechnik werden. Hierfür soll es Informationen über Sicherheitsrisiken in der Informationstechnik 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. Als Kritikpunkt ist hier hervorzuheben, dass zwar Betriebs- und Geschäftsgeheimnisse Dritter geschützt werden, nicht jedoch die des betroffenen Unternehmens selbst.

Für Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse besteht künftig eine Registrierungspflicht beim BSI. Es ist für Unternehmer bereits jetzt schwierig, den Überblick zu behalten, wo sie sich überall registrieren oder eintragen lassen müssen (z B. Eintragung des wirtschaftlich Berechtigten im Transparenzregister). Wird eine Registrierung nicht oder nicht rechtzeitig vorgenommen, handelt es sich um eine Ordnungswidrigkeit, die mit einer Geldbuße geahndet werden kann.Wünschenswert ist „zweistufiges Vorgehen“: Zunächst ein Hinweis bei einem Verstoß gegen die Registrierungspflicht und erst bei Missachtung des Hinweises die Ahndung mit einer Geld-buße.

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.

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

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.

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. Im Falle einer Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller sollten zumindest Regelungen zur Aufrechterhaltung der kritischen Geschäftsprozesse, angemessene Übergangsfristen und sonstige unterstützende Regelungen für die Betreiber vorgesehen werden.

IT-Sicherheitskennzeichen 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. Ein IT-Sicherheitskennzeichen wird sich nur durchsetzen, wenn es europaweit einheitlich ist, und wenn die Nutzer dessen Aussagegehalt verstehen. Unklar ist das Verhältnis zum freiwilligen Cybersicherheits-Zertifikat, das durch den EU Cybersecurity Act einführt wurde. Um einen unnötigen Mehraufwand und eine Überforderung insbesondere kleinerUnternehmen angesichts einer Vielzahl von Gütesiegeln zu verhindern, wäre auch hier ein einheitliches europäisches Vorgehen sinnvoller als eine rein nationale Regelung.

Bei der Einführung eines IT-Sicherheitskennzeichens sollte zudem 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 durch das BSI sollten verhältnismäßig sein und gemeinsam mit den betroffenen Unternehmen (insbesondere kleine und mittlere Unternehmen und Startups) erarbeitet werden.

Umsetzungsfristen angemessen gestalten

Für die technische Implementierung der Vorgaben sind angemessene Übergangsfristen vorzusehen.

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

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