Stellungnahme

zum Referentenentwurf des Bundesministeriums des Innern und für Heimat für das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

Angesichts der wachsenden Bedrohung durch Cyberangriffe bietet das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) eine Gelegenheit, die Cyberresilienz von Staat und Wirtschaft zu stärken. Dabei ist es jedoch entscheidend, dass die Vorgaben des Gesetzes effektiv und mit minimalem bürokratischem Aufwand umgesetzt werden. Leider müssen wir feststellen, dass die von uns im Oktober 2023 als kritisch identifizierten Punkte des damaligen Diskussionspapiers in dem nun veröffentlichten Referentenentwurf in nahezu unveränderter Form vorkommen.

Durch die Ausweitung des Anwendungsbereiches der NIS-2-Richtlinie ist die Elektro- und Digitalindustrie deutlich stärker von dem Rechtsakt betroffen als noch unter der ersten NIS-Richtlinie. Für die betroffenen Unternehmen erfordert dies eine intensivere Auseinandersetzung mit dem nationalen Umsetzungsgesetz in Begleitung von mit hohem Ressourcenaufwand verbundenen Anpassungen. Der jetzt vorliegende Referentenentwurf des NIS2UmsuCG wurde weniger als 6 Monate vor Ablauf der Umsetzungsfrist der EU-Richtlinie in die Anhörung gegeben. Umfassende und tiefgreifende Anforderungen – z.B. die Gewährleistung der Sicherheit der Lieferkette (gem. § 30 Abs. 2 S. 4) – konfrontieren insbesondere kleinere Unternehmen mit Herausforderungen, auf die sie heute noch keine adäquaten Lösungen haben. Vor diesem Hintergrund sollte auf eine sensible und praxisnahe Ausgestaltung des NIS2UmsuCG geachtet werden. Betroffenen Unternehmen sollten Orientierungshilfen zur Seite gestellt werden, damit diese ihre begrenzten Ressourcen zielführend einsetzen können.

Zusätzlich sollte EU-weite Einheitlichkeit das oberste Prinzip bei der nationalen Umsetzung der NIS-2-Richtlinie sein. Viele unserer Unternehmen sind mindestens europäisch, wenn nicht international tätig, jegliche Abweichung in den einzelstaatlichen Umsetzungen hat unnötige Mehraufwände zur Konsequenz. Regulatorische Diskrepanzen erfordern Anpassungen, die Ressourcen binden und die deutsche Wirtschaftskraft hemmen. Es ist daher essenziell, dass die Mitgliedstaaten eng zusammenarbeiten, um konsistente und harmonisierte Regelungen zu entwickeln und umzusetzen.

Aus Sicht des ZVEI sind folgende Aspekte für eine effektive Umsetzung des NIS2UmsuCG problematisch:

- **Die aktuell verwendete Definition des „Managed Service Provider“ oder „MSP“ gem. § 2 Abs. 1 S. 30 ist in der Hinsicht problematisch, dass hierrüber Einrichtungen als besonders wichtige Einrichtungen eingestuft werden könnten, deren Einstufung ursprünglich lediglich als wichtige Einrichtungen vorgesehen war.**
- **Die antizipierte Änderung des Energiewirtschaftsgesetzes birgt das Risiko einer Doppelregulierung für bestimmte Einrichtungen. Zudem sollten auch sog. virtuelle Kraftwerke in den Anwendungsbereich aufgenommen werden.**
- **Die Nutzung von CSA-Schemata entsprechend § 30 (6) sollte mit Augenmaß und zielgerichtet erfolgen. Die Festlegung mittels Rechtsverordnungen wirft prinzipielle rechtliche Fragen auf, vor allem, ob eine so umfassende Vorgabe wie ein potenzielles Verwendungsverbot lediglich mittels einer Rechtsverordnung erfolgen sollte.**
- **Die praktische Umsetzung der Meldepflichten gem. § 32 bleibt unklar. Die aktuelle Vorgabe ließe sich so auslegen, dass die 24-Stunden-Frist für Erstmeldungen ab dem Zeitpunkt beginnt, an dem die betroffene Einrichtung von einem Sicherheitsvorfall erfährt, ohne dass diese die Möglichkeit hatte diesen auf seine „Erheblichkeit“ i.S.v § 30 Abs. 1 S. 1 zu prüfen.**
- **Es sollte sichergestellt werden, dass Registrierungspflichten gem. §§ 33 und 34 nur im Land des Hauptsitzes erfolgen müssen. Eine europäisch einheitliche Lösung ist unbedingt national abweichenden Regelungen vorzuziehen.**
- **Die mit § 55 eingeführte nationale Zertifizierung führt zu Unsicherheiten in Folge von inkonsistenten Regelungen im EU-Binnenmarkt.**

Begriffsbestimmungen

Aus unserer Sicht ist die aktuell verwendete Definition des „Managed Service Provider“ oder „MSP“ problematisch:

> *Referentenentwurf:*
>
> *§ 2 (25) „Managed Service Provider“ oder „MSP“ ein Anbieter von Diensten im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten der Kunden oder aus der Ferne;*

Condition Monitoring Services sowie Remote Access sind vielfach Standardfeatures werden vom Großteil der Hersteller angeboten. In der im aktuellen Entwurf vorgenommenen Begriffsbestimmung würden sie als Tätigkeiten von MSP definiert. Gleichzeitig werden MSP unter Punkt 6.1.10 in Anlage 1 explizit als besonders wichtige und wichtige Einrichtungsarten aufgeführt. Je nach Unternehmensgröße, Umsatz und Bilanzsumme, wäre ein Großteil des deutschen Maschinenbaus, sowie die ihn ausrüstenden Komponentenhersteller, mit dieser Formulierung als besonders wichtige Einrichtungen einzustufen.

Hier zeigt sich eine Diskrepanz zwischen dem ursprünglichen Ziel der NIS-2-Richtlinie, den Sektor „Verarbeitendes Gewerbe/Herstellung von Waren“ gem. Punkt 5 in Anlage 2 als „wichtige Einrichtungen“ einzustufen, und der bestehenden Regelung. Die Verantwortung für die Sicherheit der beauftragten IT-Dienstleister und die Berücksichtigung entsprechender Features werden außerdem bereits durch die Lieferkettenverantwortung gemäß § 30 Abs. 2 Nr. 4 adressiert. Der Gesetzgeber sollte hier eine klare und kohärente Regelung schaffen, die Doppelbelastungen für die betroffenen Einrichtungen vermeidet.

Änderung des Energiewirtschaftsgesetzes

In Art. § 28 Abs. (4) Nr. 2 werden Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetz von den §§ 31, 32, 35 und 39 ausgenommen, soweit § 5c EnWG einschlägig ist:

> *Referentenentwurf:*
>
> *§ 28 (4) Die §§ 31, 32, 35 und 39 gelten nicht für: [...]*
>
> *2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 1 des Gesetzes vom 5. Februar 2024 (BGBl. 2024 I Nr. 32) geändert worden ist, soweit sie den Regelungen des § 5c des Energiewirtschaftsgesetzes unterliegen.*

Die mit § 28 Abs. 4 BSI-G aufgehobenen Normen sind im Wesentlichen in § 5c des EnWG (E) „gedoppelt“. Zusätzlich werden mit § 5c Abs. 3 EnWG (E) die Risikomanagementmaßnahmen für wichtige und besonders wichtige Einrichtungen gem. § 30 des BSI-G in das EnWG (E) überführt. Das auf diese Weise antizipierte Konstrukt birgt das Risiko einer Doppelregulierung. Einrichtungen haben keine abschließende Klarheit darüber, welchen Maßnahmenkatalog künftig erfüllen müssen, falls EnWG und BSI-G voneinander divergieren sollten. Soweit an der spezialgesetzlichen Regelung des EnWG für die Energiebranche festgehalten werden soll, wäre es einfacher, auch § 30 BSI-G als vom EnWG verdrängt zu bezeichnen.

§ 5c Abs. 3 EnWG (E) ist inhaltlich nicht identisch mit § 30 Abs. 2 BSI-G. Im EnWG (E) würde gem. § 5c Abs. 3 S. 11 die Verpflichtung zum Einsatz von Angriffserkennungssystemen für alle Betreiber von Energieanlagen, die besonders wichtige oder wichtig Einrichtungen i.S.d. BSI-G sind, gelten. Im § 31 des BSI-G wäre diese Pflicht indes nur den Betreibern kritischer Anlagen vorbehalten. Die Regelung im EnWG (E) geht somit über den BSIG-Entwurf hinaus und ist zudem keine Anforderung der NIS-2-Richtlinie. § 5c Abs. 3 Nr. 11 EnWG ist daher unverhältnismäßig und sollte komplett gestrichen werden.

Insgesamt erscheint die Gesetzgebungstechnik an dieser Stelle unglücklich. Der Rückverweis in § 5c Abs. 6 EnWG (E) auf den „eigentlich verdrängten“ § 32 Abs. 2-5 BSI-G verdeutlicht, dass die Gesetzesanwender künftig zwischen EnWG und BSI-G hin- und herspringen sollen; was die Handhabbarkeit erschwert und zu Unverständlichkeiten führt.

Des Weiteren sollte die Änderung des § 11 Abs. 1g EnWG durch dessen Integration in den § 5c Abs. 9 EnWG zum Anlass genommen werden, um eine maßgebliche Regelungslücke zu schließen und in dieser Vorschrift auch Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung („virtuelle Kraftwerke“) zu erfassen.

Die Stabilität des Stromnetzes wird heute sowohl von einzelnen großen Kraftwerken als auch zu einem immer größeren Teil von vielen kleinen Anlagen erbracht, die gebündelt wie ein großes „virtuelles“ Kraftwerk agieren. Von beiden kann grundsätzliche in gleichem Maße eine Störung für die Sicherheit der Energieversorgung ausgehen. Große Erzeugungsanlagen werden aktuell kaum noch gebaut. Kleine dezentrale Anlagen, die sich zur Bündelung in virtuellen Kraftwerken eignen, dagegen in rasantem Tempo. So wurden im letzten Jahr etwa 5,3 GW Heimspeicher in Deutschland installiert.

Aus diesem Grund werden in Anhang 1 Teil 2 Ziffer 1.1 der KRITIS-Verordnung einzelne Kraftwerke und virtuelle Kraftwerke gleichermaßen als kritische Infrastruktur behandelt, sobald sie den Schwellenwert von 104 MW, bzw. 36 MW in der Regelleistung überschreiten. Das ist zielführend.

Dieser Gleichlauf fehlt bislang in § 5c Abs. 9 (neu) EnWG. Die BNetzA darf kritische Funktionen nur dann regeln, wenn sie von einzelnen großen Erzeugungsanlagen oder Energieversorgungsnetzen übernommen werden. Ein virtuelles Kraftwerk darf dagegen kritische Funktionen übernehmen und könnte sogar ausschließlich aus kritischen Komponenten bestehen und diese wären gegenüber der BNetzA nicht einmal anzeigepflichtig.

Diese Regelungslücke sollte geschlossen werden, indem die Festlegung der BNetzA gemäß § 5c Abs. 9 neben Energieversorgungsnetzen und Energieanlagen auch Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung im Sinne der Ziffer 1.1.2 des Teil 3 Anlage 1 zur KRITISVO erfassen darf.

Nutzung von CSA-Zertifizierungsschemata

> *Referentenentwurf:*
>
> *§ 30 (6) Besonders wichtige Einrichtungen und wichtige Einrichtung dürfen durch Rechtsverordnung nach § 57 Absatz 4 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen.*

Mit diesem Absatz wird die in Art. 24 (1) der NIS-2-Richtlinie gegebene Möglichkeit genutzt wird, die Nutzung von Zertifizierungsschemata des sog. Cybersecurity Acts (CSA) für spezielle IKT-Produkte, -Dienste und -Prozesse verpflichtend vorschreiben zu können. Wir stellen in Frage, ob der hieraus folgende massive Eingriff, lediglich in Form einer Rechtsverordnung erfolgen sollte.

Unseres Erachtens wird die Tragweite dieses Absatzes nicht ausreichend erfasst: Der Gesetzgeber spricht hier von einem Verwendungsverbot für Produkte, die keine Cybersicherheitszertifizierung entsprechend eines CSA-Schemas durchlaufen haben. Dies kann zumindest teilweise zu erheblichen Problemen bei der Umsetzung der Verpflichtungen führen, wenn aus dem Verwendungsverbot eine Abschaltpflicht hergeleitet werden sollte.

Dabei wurden bisher weder ein Bestandsschutz für bereits bestehende Einrichtungen noch Übergangsfristen diskutiert. Würden diese Aspekte in einer Rechtsverordnung nicht ausreichend berücksichtigt, z. B. zumindest in der Form, dass für bereits bestehende Systeme, ein Bestandsschutz möglich ist, bevor Investitionen in neue Technologien gefordert werden, so besteht die Gefahr, dass ganze Installationen „über Nacht“ de facto illegal werden könnten. Ein rechts-konformer Betrieb von besonders wichtigen Einrichtungen, wie z. B. Energieübertragungsnetzen aber auch von betroffenen wichtigen Einrichtungen, hierunter z. B. produzierende Unternehmen, wäre somit ggf. nicht mehr möglich. Zusätzlich sollte außerdem sichergestellt werden, dass die mittels § 30 Abs. (6) zur Anwendung gebrachten Schemata nicht im Widerspruch stehen zu den Branchenstandards entsprechend § 30 Abs. (9).

Außerdem sind wir der festen Überzeugung, dass der Gesetzgeber hier von seinem in Art. 24 (1) gegebenen Auslegungsspielraum Gebrauch machen sollte und die verpflichtende Verwendung auf ausgewählte besonders wichtige Einrichtungen beschränken sollte. Eine Anwendung auf wichtige Einrichtungen schränkt deren Auswahlmöglichkeit vor allem angesichts der vorhandenen Limitierungen des CSA und der entsprechenden Schemes unnötig ein.

Meldepflichten

Referentenentwurf:

§32 (1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, folgende Informationen an eine vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle zu melden:

1. unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

Hierbei bestehen Unklarheiten für die praktische Umsetzung der Meldepflichten. Gemäß § 2 Abs. 1 Satz 10. des Referentenentwurfs ist ein „erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann; oder b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.“

Soweit das Bundesministerium des Inneren und Heimat (BMI) keine weitergehende Begriffsbestimmung (gem. § 2 Abs. 2) vornimmt impliziert der aktuelle Entwurf, dass Einrichtungen zunächst intern prüfen müssen, ob die genannten Kriterien vorliegen, bevor sie eine Erstmeldung an die gemeinsame Meldestelle geben. Die in § 30 Abs. 1Satz 1 gewählte Formulierung könnte indes dahingehend interpretiert werden, dass die 24-Stunden-Frist ab dem Zeitpunkt beginnt, an dem die betroffene Einrichtung von einem Sicherheitsvorfall erfährt, ohne dass diese die Möglichkeit hatte, zu prüfen, ob der Vorfall im Sinne von § 30 Abs. 1 Satz 1 als „erheblich“ einzustufen ist.

Dies könnte zu Situationen führen, bei denen ein Unternehmen am Freitagabend auf einen potenziellen Sicherheitsvorfall aufmerksam gemacht wird, die zuständigen Mitarbeiter aber erst am darauffolgenden Montag wieder im Dienst sind. Gemäß der aktuellen Formulierung könnten Aufsichtsbehörden den Fall so auslegen, dass die 24-Stunden-Frist ab dem Freitagabend liefe, womit die frühestens am darauffolgenden Montag erfolgende Meldung nicht fristgerecht wäre und gegen die Meldepflicht gemäß § 32 verstoßen würde. Ohne eine Klarstellung dieser Passage könnten Unternehmen gezwungen sein, eine dauerhafte Überwachungsinstanz einzurichten, die jederzeit in der Lage ist, Sicherheitsvorfälle auf ihre Relevanz gemäß § 2 Abs. 1 Satz 10 zu prüfen. Die Bindung der dafür erforderlichen Ressourcen und der damit verbundene bürokratische Aufwand würden die deutsche Wirtschaft erheblich belasten.

Grundsätzlich sollte das gemeinsame Meldeportal volldigitalisiert eingerichtet werden und auf einen effizienten und schlanken Meldeprozess geachtet werden.

Registrierungspflichten

Wie eingangs erwähnt, ist der Großteil unserer Mitgliedsunternehmen europaweit bzw. international tätig. Hinsichtlich einer kohärenten Umsetzung der NIS-2-Richtlinie ist es dementsprechend unbedingt notwendig, dass die Bundesregierung in Abstimmung mit ihren europäischen Partnern sicherstellt, dass Nachweispflichten jeweils nur in dem Land erfolgen müssen, in dem eine Einrichtung ihren Hauptsitz hat, da von diesem zumeist die Cybersicherheitsgovernance erfolgt. Zu berücksichtigen ist hierbei, dass die Definition der Hauptniederlassung und die Auswirkung auf die Tochtergesellschaften in einem Konzernkonstrukt nach wie vor unklar ist. Es ist ferner zu klären, welcher Geschäftsführer / welche Geschäftsführerin innerhalb eines Konzernkonstrukts haftet. Auch muss geklärt werden, welcher – im Zweifel national definierte – Stand der Technik in einem Konzernkonstrukt umzusetzen ist, jener der Hauptniederlassung oder jener des Landes, in dem eine Tochtergesellschaft tätig ist. Dies gilt auch für die zentrale Frage, wie Konzerne mit unterschiedlichen Tochtergesellschaften und einer übergeordneten IT-Gesellschaft, die z.B. als konzerninterner IT-Dienstleister fungiert, betrachtet werden kann. Es bleibt offen, ob einzelne Tochtergesellschaften im Anwendungsbereich der NIS-2-Richtlinie sein können, während andere Einheiten nicht betroffen sind.

Eine **europäisch einheitliche Lösung** ist grundsätzlich vorzugswürdig. National abweichende Regelungen, welche über die Anforderungen der NIS-2-Richtlinie hinausgehen, führen zu einer zusätzlichen Belastung für die betroffenen Einrichtungen.

Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen

> *Referentenentwurf:*
>
> *§38 (3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik und die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste zu erwerben.*

Der europäische Gesetzgeber hat die „Managerhaftung“ in der NIS-2-Richtlinie in Art. 20 Abs. 1 allgemein und in Art. 32 Abs. 6 zusätzlich für besonders wichtige Einrichtungen definiert. Diese Differenzierung fehlt in § 38. Der ZVE fordert den Gesetzgeber auf, diese Differenzierung ins nationale Umsetzungsgesetz aufzunehmen und keine über den europäischen Rechtsrahmen hinausgehenden Anforderungen im NIS2UmsuCG festzuschreiben.

Aus unserer Sicht bedarf es einer Klarstellung bezüglich der Möglichkeit zur Delegation der Umsetzung. Insbesondere aus der Perspektive einer Konzernstruktur ist unklar, in welchem Umfang die Delegation von Verantwortlichkeiten auf Konzern- / Unternehmensangehörige im Zusammenhang mit der Einhaltung der Risikomanagement-Vorgaben zur IT-Sicherheit noch möglich ist. Üblicherweise erfolgt die Verteilung von Aufgaben im Zusammenhang mit der IT-Sicherheit auf einzelne Unternehmensabteilungen und damit korrespondierende Führungsfunktionen (auch unternehmensübergreifend innerhalb eines Konzerns; CISO o.Ä.). Es bedarf einer ausdrücklichen Klarstellung, wonach die Umsetzung von Cybersicherheitsmaßnahmen durch Dritte weiterhin möglich ist. Dies würde Rechtssicherheit schaffen. Zudem bedarf es einer raschen Klärung hinsichtlich der inhaltlichen Ausgestaltung der zu belegenden Schulungen.

Ferner sollte Absatz 2 gestrichen werden, da die NIS-2-Richtlinie keine entsprechenden Regelungen hinsichtlich eines Verzichts oder Vergleichs vorsieht. Inwiefern zum Beispiel die jeweiligen Aufsichtsgremien der Einrichtung zur Durchsetzung eines Anspruchs verpflichtet sind, sollte sich nach allgemeinen Grundsätzen bestimmen.

Konformitätsbewertung und Konformitätserklärung

Der im aktuellen Entwurf des NIS2UmsuCG neu eingeführte § 55 beschreibt die freiwillige Konformitätsbewertung von Herstellern, Händlern, Personen, oder IT-Sicherheitsdienstleister mit den Anforderungen von Technischen Richtlinien des Bundesamts für Sicherheit in der Informationssicherheit (BSI). Damit werden neue Optionen der Konformitätsbewertung in den Gesetzestext aufgenommen.

Die Passage sorgt in der deutschen Elektro- und Digitalindustrie für Unsicherheiten. Deutsche Hersteller stehen bereits heute angesichts umfassender und tiefgreifender digitalpolitischer Regulierungen vor großen Herausforderungen. Mit dem sog. Cyber Resilience Act (CRA) steht ein EU-Rechtsakt kurz vor dem Abschluss, der mit einem horizontalen Regulierungsansatz neue Cybersicherheitsanforderungen für Produkte mit digitalen Elementen vorschreibt. Die Anpassungen der Entwicklungs- und Produktionsprozesse an den CRA erfordern beträchtliche Ressourcen und haben bereits heute Auswirkungen auf die betriebliche Effizienz sowie die finanzielle Leistungsfähigkeit der Unternehmen.

Gleichzeitig wurde 2019 mit dem sog. Cybersecurity Act (CSA) ein einheitlicher europäischer Zertifizierungsrahmen für IKT-Produkte, -Dienstleistungen und -Prozesse auf den Weg gebracht, der die Notwendigkeit eines zusätzlichen nationalen Zertifizierungssystems in Frage stellt. Wie eingangs dargelegt, sollten konsistente und einheitliche Regelungen im europäischen Binnenmarkt priorisiert werden. Diese im Referentenentwurf des NIS2UmsuCG aufgeführte nationale Zertifizierung, deren internationale Gültigkeit zudem ungeklärt ist, steht im Widerspruch dazu und sollte aus dem Gesetzestext entfernt werden.

Kontakt

Lennard Kreißl • Manager Cybersecurity • Abteilung Digital- und Innovationspolitik • Bereich Digitalisierung & Recht
Tel.: +49 30 306960 20 • Mobil: +49 162 2664 941 • E-Mail: lennard.kreissl@googlemail.com

ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Charlottenstraße 35/36 • 10117 Berlin
Lobbyregisternr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org

Datum: 28.05.2024