

STELLUNGNAHME

zum „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) des Bundesministeriums des Innern und für Heimat

Berlin, 28. Mai 2024

Mit der Veröffentlichung der NIS-2-Richtlinie im europäischen Gesetzblatt im Dezember 2022 wurde der Grundstein für die nationale Umsetzung gelegt. Nach der Vorstellung des Referentenentwurfs für ein Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG) im Juli 2023 und in dem im September 2023 vorgelegten Diskussionspapier für „wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland“ hat das Bundesministerium des Innern und für Heimat (BMI) zentrale Debattenpunkte aufgenommen und adressiert. Den lang erwarteten Referentenentwurf zum NIS2UmsuCG hat das BMI am 7. Mai 2024 veröffentlicht und die Verbändebeteiligung gestartet.

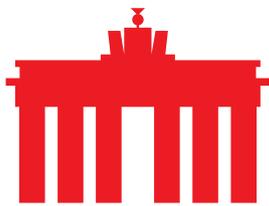
Für die Internetwirtschaft sind die Veränderungen im Bereich der IT-Sicherheitsregulierung gravierend, wird mit den vorgenommenen Vorgaben doch der Anwendungsbereich deutlich ausgeweitet.

Aus Sicht der Internetwirtschaft sind folgende Aspekte für das weitere Gesetzgebungsvorhaben relevant:

Allgemeine Anmerkungen

Die Strukturen und Vorgaben zur Gestaltung von IT-Sicherheit wurden in den vergangenen Jahren wiederholt überarbeitet und angepasst. Mit den ursprünglichen Vorgaben der NIS-Richtlinie und des IT-Sicherheitsgesetzes von 2015 und 2016 wurden so genannte kritische Infrastrukturen (KRITIS) definiert und zentrale Vorgaben für die betroffenen Sektoren geschaffen und mit dem [NIS-Anpassungsgesetz](#) aus dem Jahr 2017 an die Vorgaben weiter angepasst. Das deutsche IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) hat den Anwendungsbereich für KRITIS-Vorgaben ausgeweitet und zusätzliche Regelungen geschaffen. Insgesamt existiert im Bereich der IT-Sicherheit mittlerweile ein gut ausgearbeitetes und strukturiertes Regulierungsgefüge.

Dieses wurde mit der europäischen NIS2-Richtlinie, die seit 16. Januar 2023 in Kraft ist, noch einmal grundlegend überarbeitet. Der Ansatz der bisher definierten KRITIS-Sektoren wurde durch einen neuen Ansatz ersetzt, bei dem die bisherigen kritischen Einrichtungen als wesentliche Einrichtungen erfasst wurden und dazu



ergänzend so genannte wichtige Einrichtungen ergänzt wurden, die ebenfalls bedeutend für das Zusammenleben sind, ohne aber den Charakter der wesentlichen Einrichtungen zu besitzen.

Mit dem im Juli 2023 bekannt gewordenen Entwurf eines NIS2 Umsetzungs- und Anwendungsgesetzes (NIS2UmsuCG) und dem Diskussionspapier des BMI vom September 2023 und dem vor Kabinettsbeschluss befindlichen KRITIS-DachG wurde diese Systematik aufgegriffen und weiterentwickelt.

Aus Sicht der Internetwirtschaft wäre es sinnvoll und begrüßenswert, wenn sich die Definitionen in allen Gesetzgebungsvorhaben an den europäischen Richtlinien orientieren und diese möglichst vollständig übernehmen. Auf die Schaffung zusätzlicher eigener Kategorien von Anlagen oder Einrichtungen nationaler Ebene sollte verzichtet werden. In jedem Fall sollte auch geklärt werden, in welchem Verhältnis KRITIS-DachG und NIS2UmsuCG zueinanderstehen. Dies wird, auch wenn inzwischen zahlreiche Unklarheiten bereinigt wurden, nach wie vor nicht abschließend geklärt. Unternehmen sind allerdings auf überschneidungs- und widerspruchsfreie Vorgaben in beiden Gesetzen angewiesen. Zudem sollten Überschneidungen mit Cybersicherheitsvorgaben im Fachrecht (z.B. TKG) vermieden werden.

Insgesamt sollte bei der Erarbeitung und Ausgestaltung des weiteren Gesetzes darauf geachtet werden, dass die Auflagen für die Wirtschaft verhältnismäßig, transparent und nachvollziehbar sind. Die Schaffung neuer Kategorien und Sektoren im Rahmen der Umsetzung in Deutschland jenseits des von der EU vorgezeichneten Rahmens sind dabei nicht hilfreich. Aus Sicht der Internetwirtschaft muss der vorliegende Entwurf für das NIS2UmsuCG noch einmal überarbeitet und angepasst werden.

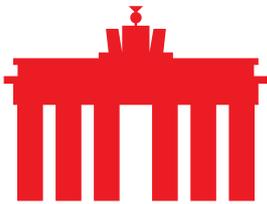
Zu den Regelungen im Einzelnen

I. Zu Artikel 1 Teil 1: Allgemeine Vorschriften

I.1. Zu § 2 Begriffsbestimmungen:

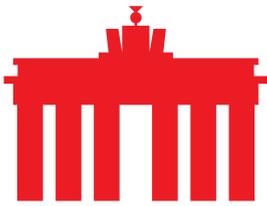
Die in Paragraph 2 aufgeführten Definitionen sind im Wesentlichen mit denen der NIS2-Richtlinie deckungsgleich. eco – Verband der Internetwirtschaft begrüßt diese Kongruenz mit der europäischen Gesetzgebung, da sie die Grundlage für eine einheitliche Anwendung der europäischen Vorgaben darstellen. Im Einzelnen verdienen aus Sicht der Internetwirtschaft die folgenden Definitionen eine genauere Betrachtung.

- Die im NIS2UmsuCG neu eingeführte Definition der „Bodeninfrastruktur“, die in dieser Form nicht in der NIS2-Richtlinie enthalten ist, deckt augenscheinlich den Sektor „Weltraum“ ab. Aus Sicht der Internetwirtschaft wäre es begrüßenswert, wenn hier klargestellt werden könnte, dass Telekommunikationsinfrastrukturen, sofern sie über Bodeninfrastrukturen angeboten werden, grundsätzlich über die Auflagen des Sektors Telekommunikation abgedeckt sind und die vorliegenden Auflagen nur gelten, wenn entsprechende Bodeninfrastrukturen noch nicht an



anderer Stelle geregelt sind. Es sollte bei den Bodeninfrastrukturen außerdem darauf geachtet werden, dass die Regelungen sinnvoll neben die Vorgaben des ebenfalls in Beratung befindlichen KRITIS-DachG gesetzt sind, welches diesen Themenbereich ebenfalls aufgreift.

- Die Definition eines Cloud-Computing-Dienstes entspricht zwar im Wesentlichen der Definition der NIS2-Richtlinie. Es sollte jedoch aus Sicht der Internetwirtschaft klarer herausgearbeitet werden, wie sich ein Cloud-Computing-Dienst von einem Rechenzentrumsdienst abgrenzt. Die vorliegende Definition ist aus Sicht der Internetwirtschaft nicht zweifelsfrei ausreichend, um diese Klarheit herzustellen.
- Die Definition eines Content Delivery Netzwerks (CDN) sollte entsprechend der Definition in der NIS2-Richtlinie formuliert werden, um eine einheitlich EU-weite Harmonisierung sicherzustellen. Bei der Definition des Domain-Name-Registry-Dienstleisters wäre es aus Sicht der Internetwirtschaft wünschenswert, die Terminologie an die der deutschen Sprachfassung der NIS2-Richtlinie anzupassen und von „Einrichtungen, die Domännennamen-Registrierungsdienste erbringen“ zu sprechen. Der Begriff „Domain-Name-Registry-Dienstleister“ suggeriert, dass es sich um einen Dienstleister für die Registry handelt, was insbesondere bei generischen Top Level Domains irreführend ist, wo die Registrare keinesfalls als Dienstleister für eine Registry auftreten.
- Der Begriff der „kritischen Anlage“ wurde im Vergleich zu dem im Herbst vergangenen Jahres vorgestellten Diskussionspapier konkretisiert und „kritische Anlagen“ beziehen sich nun auf eine Rechtsnorm im NIS2UmsuCG-E. eco sieht darin eine positive Entwicklung, da die zuvor eröffnete Definition einen breiten Interpretationsspielraum zuließ und für Unklarheit in Bezug auf den rechtlichen Status sorgte. Problematisch ist jedoch aus Sicht der Internetwirtschaft, dass durch die generelle Aufnahme der Kategorie „kritische Anlage“, die nicht in der NIS2-Richtlinie verankert ist, das bestehende Regelungsgefüge der europäischen Regelung aufgebogen wird, was deren Intention und dem Bestreben der Internetwirtschaft, eine möglichst einheitliche europäische Regulierung anzustreben abträglich sein wird. Weitere Probleme ergeben sich aus dem für die Definition relevanten § 28. Sie werden an anderer Stelle separat gewürdigt.
- Die Definition so genannter „kritischer Komponenten“ entspricht abzüglich der Anpassung der Verweise auf entsprechende Paragraphen der aus dem IT-Sicherheitsgesetz 2.0. eco begrüßt, dass die bestehende Regelung an dieser Stelle beibehalten wurde und keine zusätzliche Rechtsunsicherheit durch Anpassungen geschaffen wurde. In diesem Kontext begrüßt eco außerdem, dass der Begriff der „kritischen Dienstleistung“ ebenfalls klargestellt wurde.
- eco begrüßt, dass der Begriff des „Rechenzentrumsdienstes“ durch den überarbeiteten Gesetzesentwurf nachgeschärft wurde. Die vorliegende Definition ist geeignet um, Rechenzentren von TK-Knotenpunkten besser abgrenzen zu können. Allerdings ist in der vorliegenden Konstellation nicht gänzlich ersichtlich, wie sich ein Rechenzentrumsdienst von einem Cloud-Computing Dienst oder einem CDN nach demselben Gesetz sinnvoll voneinander abgrenzen lässt. Aus diesem Grund wäre es aus Sicht der Internetwirtschaft



sinnvoll, die vorliegenden Definitionen noch einmal kritisch zu hinterfragen und zu überprüfen.

- Der Begriff der „weltraumgestützten Dienste“ ist in der NIS2-Richtlinie in der Form nicht angelegt. Zudem ergeht sich in der vorliegenden Beschreibung des Begriffs nicht, wie genau sich die unterstellte Kritikalität der „weltraumgestützten Dienste“ zu den hier beschriebenen Kaskadeneffekten im Verhältnis zur Kritikalität des Dienstes verhält. Aus Sicht der Internetwirtschaft müsste dies klarer herausgearbeitet werden oder der Begriff sollte gestrichen werden, da er in der NIS2-Richtlinie kein passendes Gegenstück hat.

II. Zu Artikel 1 Teil 2: Das Bundesamt

II.1. Zu § 6: Informationsaustausch

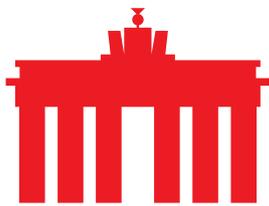
eco begrüßt, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) kollaborative Ansätze zur Gewährleistung oder Wiederherstellung von Cybersicherheit verfolgt und hofft darauf, dass die Ausgestaltung der Online-Plattform zum Informationsaustausch sinnvoll und angemessen erfolgt und diese mit ausreichenden Mitteln ausgestattet wird. Aus unserer Sicht ist es dringend geboten, dass das BSI zukünftig mehr verwertbare Informationen über Cyberbedrohungen mit der Wirtschaft teilt, um auf diese Weise einen Beitrag zu einem verbesserten Lagebild zu leisten.

II.2. Zu § 12: Bestandsdatenauskunft

Der Vorschlag für die Regelung einer Bestandsdatenauskunft für das BSI sollte aus Sicht der Internetwirtschaft noch einmal genau geprüft werden. Es bestehen Zweifel daran, dass die hier dargelegten Gründe für die Abfrage sowohl in ihrer Präzision als auch in ihrer Angemessenheit tatsächlich ausreichend sind, um eine Bestandsdatenabfrage zu begründen. Es sollte zudem geprüft werden, inwieweit für die Erteilung entsprechender Auskünfte zusätzlich Richtervorbehalte erforderlich sein sollten, wenn es sich bspw. um Informationen handelt, mit denen auf Endgeräte zugegriffen werden kann/soll.

II.3. Zu § 15: Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

Aus Sicht der Internetwirtschaft könnte es sich als problematisch erweisen, wenn Maßnahmen zur Detektion von Schwachstellen an Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchgeführt werden, die nicht vorher mit den entsprechenden Einrichtungen oder Netzbetreibern abgesprochen sind, da diese ansonsten eventuell durch Gegenmaßnahmen gegen Angriffe die Verfügbarkeit von Diensten oder Produkten einschränken. Daher wäre es aus Sicht der Internetwirtschaft wichtig, den vorliegenden Passus dahingehend abzuändern, dass entsprechende Abfragen, insbesondere solche, die Angriffe simulieren, nur in Absprache mit den Betreibern von Einrichtungen und Netzen erfolgen.



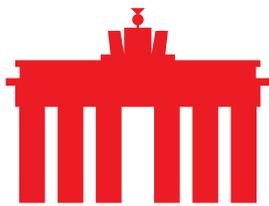
II.4. Zu § 18: Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten

Aus Sicht der Internetwirtschaft sind die hier getroffenen Formulierungen zu unpräzise, um Rechtsklarheit für die Hersteller von IKT-Produkten zu schaffen. Wünschenswert wären sowohl eine Klarstellung wie weit diese Mitwirkungspflichten zur Behebung von Sicherheitslücken und Störungen sich erstrecken, als auch eine Klarstellung dahingehend, dass die Mitwirkungspflichten des Herstellers sich im Rahmen des wirtschaftlich Zumutbaren bewegen sollten. Unklar ist zudem, in welchem Verhältnis die hier geschaffenen Auflagen zu anderen gesetzlichen Regelungen wie bspw. dem „Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen ([BGBL 2021, Teil 1, Nr. 37](#))“ oder der anstehenden nationalen Umsetzung des Cyber Resilience Act der Europäischen Union stehen, die ebenfalls proaktives Handeln von Herstellern von Software und Komponenten vorsehen. Impliziert die hier aufgestellte Mitwirkungspflicht eine über die ohnehin bestehenden gesetzlichen Maßgaben, hinausgehende Verpflichtung für die Internetwirtschaft, so ist aus der Sicht von eco die hier geschaffenen Auflagen unverhältnismäßig und müssten gestrichen werden. Sind sie auf dem Niveau der ohnehin bestehenden Regelungen, stellt sich die Frage nach der Notwendigkeit des § 18 in der bestehenden Form.

III. Zu Artikel 1 Teil 3: Sicherheit in der Informationstechnik von Einrichtungen

III.1. Zu § 28: Besonders wichtige Einrichtungen und wichtige Einrichtungen

Wie bereits in der Kommentierung zum Diskussionspapier zu den wirtschaftsbezogenen Regelungen der NIS2-Richtlinie sieht eco bei § 28 zwei zentrale Herausforderungen. Zum einen werden die Begriffe und Definitionen der NIS2-Richtlinie nicht korrekt übernommen. Die Richtlinie spricht von wesentlichen und wichtigen Einrichtungen. Das NIS2UmsuCG-E hingegen verweist auf besonders wichtige und wichtige Einrichtungen. Diese Abweichungen in der Terminologie sorgen bei den Unternehmen für Rechtsunsicherheit. Zum anderen weicht der Zuschnitt der verschiedenen Einrichtungen von den europäischen Vorgaben ab. So werden an dieser Stelle die Betreiber kritischer Anlagen, die nicht durch die allgemeinen Regelungen des NIS2UmsuCG-E erfasst werden, durch die Formulierungen von § 28 (1) Nr. 1 speziell aufgegriffen. Das Regulierungsgefüge der NIS2-Richtlinie wird damit erheblich verschoben. Zwar hat das BMI nun endlich eine halbwegs plausible Definition für „kritische Anlagen“ vorgelegt, allerdings bleibt es bei der dahinterstehenden grundsätzlichen Problematik, dass das europäische Regulierungsgefüge dadurch beeinträchtigt wird. Das erschwert grenzüberschreitend tätigen Unternehmen die Umsetzung des europäischen Rechtsrahmens erheblich und widerspricht dem mit der NIS2 verfolgten Zielsetzung europaweit harmonisierter Regelungen im Bereich der Cybersicherheit in den Mitgliedstaaten zu etablieren. Aus Sicht der Internetwirtschaft ist dieser Ansatz daher problematisch.



Zuletzt möchte eco darauf hinweisen, dass die rechtliche Sonderstellung für Einrichtungen von Bundesländern gem. § 28 (9) nicht nachvollziehbar ist. Diese Einrichtungen sind genau wie alle anderen ebenfalls Cyberangriffen ausgesetzt, stellen laut Medienberichten sogar sehr häufig Ziele dar. Es ist daher nicht nachvollziehbar, warum diese aber aus der Regulierung und dem Anwendungsbereich des Gesetzes ausgenommen werden sollen. Aus Sicht der Internetwirtschaft wird unter Berufung auf Föderalismus und Konnexitätsregelungen nicht nur ein schlechtes Beispiel für alle Beteiligten geschaffen, sondern auch das Regelungsziel konterkariert.

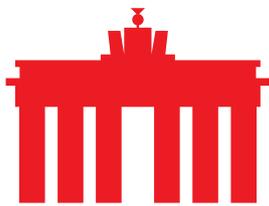
Zuletzt sei an dieser Stelle auf den ebenfalls sehr wichtigen Punkt hingewiesen, dass auch mit den überarbeiteten Definitionen in § 2 Rechenzentrumsbetreiber, die mehr oder minder exklusiv für Telekommunikationsnetze arbeiten, ohne gleichzeitig die Kriterien eines CDN oder eines IXP zu erfüllen, immer noch dem Risiko einer Doppelregulierung unterliegen.

III.2. Zu § 30: Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Aus Sicht der Internetwirtschaft sind in dem vorliegenden § 30 gleich mehrere Probleme eingeschlossen, auf die eco bereits in der Kommentierung des Diskussionspapiers im Oktober vergangenen Jahres hingewiesen hatte. Zum einen wird die Unterscheidung zwischen wichtigen und besonders wichtigen Einrichtungen durch die vorliegenden Maßgaben aufgehoben. Es ist nicht mehr ersichtlich, wie die Regelungen für die jeweiligen Kategorien sinnvoll auseinandergelassen und abgegrenzt werden sollen oder können. Erschwerend kommt hinzu, dass so genannte kritische Anlagen, die gem. § 2, 28 NIS2UmsuCG-E ebenfalls als besonders wichtige Einrichtungen eingestuft sein sollen, am Ende dennoch ein komplett eigenes Regulierungsfeld erhalten und eigene Auflagen, was die ursprüngliche Einsortierung nicht nachvollziehbar macht. Aus Sicht der Internetwirtschaft wäre hier dringend mehr Struktur und Kohärenz geboten, um die Auflagen und Regulierungsansätze der NIS2-Richtlinie für die deutsche Wirtschaft handhabbar und verhältnismäßig nachzubilden.

III.3. Zu § 31: Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

Die in § 31 geschaffenen Auflagen für Betreiber kritischer Anlagen im Verhältnis zu den sonstigen Betreibern besonders wichtiger Einrichtungen unterstreichen, dass das Regelungsgefüge der NIS2-Richtlinie in Deutschland auseinandergefallen ist. Die künstlich in die Kategorie besonders wichtiger Einrichtungen aufgenommenen „kritischen Anlagen“ werden im vorliegenden Paragraphen besonderen Auflagen unterworfen, die wiederum über die Auflagen für besonders wichtige Einrichtungen gem. § 30 hinausgehen, was die Frage aufwirft, warum diese Anlagen überhaupt in diese Kategorie einsortiert werden. Der hier vom Gesetzgeber eingeschlagene Weg sorgt für Verunsicherung bei allen Beteiligten. Insbesondere aber auch bei denjenigen die zwar als besonders wichtige Einrichtung verpflichtet sind,



Maßnahmen umzusetzen, dann aber als Betreiber kritischer Anlagen darüber hinausgehend noch zusätzliche Auflagen erfüllen müssen.

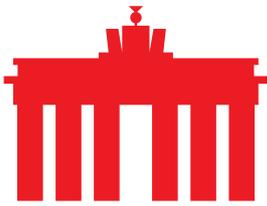
III.4. Zu § 32 Meldepflichten

Aus Sicht der Internetwirtschaft ist es begrüßenswert, dass die Meldepflichten gem. KRITIS-DachG und NIS2UmsuCG möglichst stringent und harmonisch umgesetzt werden und doppelte Berichts- bzw. Meldepflichten entfallen. Mit dem Vorschlag für § 32 ist hierzu ein sinnvoller Beitrag geleistet. Es sollte allerdings sichergestellt sein, dass die Meldepflichten rein digital erbracht werden können. Kritikwürdig bleibt indes, dass der NIS2UmsuCG-E an den starren Vorgaben der NIS2-Richtlinie für die Erstmeldung innerhalb von 24 Stunden und einer ordentlichen Meldung innerhalb von 72 Stunden festhält. Gleiches gilt für die sektorspezifische Parallelnorm des § 168 Abs. 1 TKG der in Artikel 23 NIS2UmsuCG geändert wird. Auch hier bleiben die starren Vorgaben der NIS2-Richtlinie bestehen. Aus Sicht der Internetwirtschaft sind die gesetzten starren Zeitfenster ungeeignet und erzeugen für Unternehmen zusätzlichen organisatorischen Aufwand, ohne tatsächlich zur Beseitigung der Störung beizutragen. Es sollte aus diesem Grund an der in der bisherigen deutschen Gesetzgebung etablierten Form der „unverzöglichen“ Meldung festgehalten werden, die Unternehmen die Möglichkeit eröffnet, sinnvoll auf die bestehende Situation einzugehen. Unternehmen benötigen zudem Klarheit, welche Meldewege im Falle von Sicherheitsvorfällen bei Tochtergesellschaften mit Sitz im EU-Ausland eingehalten werden müssen.

Darüber hinaus bleibt es für Telekommunikationsunternehmen bei einer nicht nachvollziehbaren doppelten Meldepflicht von Vorfällen sowohl an das BSI als auch an die BNetzA (vgl. § 168 Abs. 1 TKG).

III.5. Zu § 41: Untersagung des Einsatzes kritischer Komponenten

Die Auflagen zum Einsatz kritischer Komponenten wirken aus Sicht der Internetwirtschaft nachvollziehbar und orientieren sich an den Auflagen aus dem IT-SiG 2.0. eco begrüßt, dass hier keine weiteren willkürlichen Maßgaben gesetzt wurden, die zusätzliche Unsicherheit bei Unternehmen und insbesondere Netzbetreibern erzeugen. Als weiterhin erklärungsbedürftig ist aus Sicht der Internetwirtschaft, was unter einem schwerwiegenden Fall mangelnder Vertrauenswürdigkeit zu verstehen ist, der die Untersagung sämtlicher kritischer Komponenten eines Herstellers begründet. Außerdem sollte in diesem Zusammenhang auch genauer betrachtet werden, wie entsprechende kritische Komponenten zusammengestellt werden und in welchem Umfang entsprechende Nachweise für Bauteile erbracht werden können. Ferner bleibt unklar, warum die Regelung bzgl. der einzuholenden Garantieerklärungen von Herstellern kritischer ITK-Komponenten aufgenommen wurde, obgleich das Bundesministerium des Innern und für Heimat bereits im Oktober 2022 die entsprechende Allgemeinverfügung für den TK-Sektor widerrufen hatte.



IV. Zu Artikel 1 Teil 4: Datenbanken der Domain-Name-Registrierungsdaten

IV.1. Zu § 51: Pflicht zum Führen einer Datenbank

Die NIS2-Richtlinie verpflichtet die Normadressaten, eine eigene Datenbank für Registrierungsdaten zu betreiben. Diese Anforderung ist insofern unklar, als dass sie dahingehend verstanden werden kann, dass nicht nur die an einer Domainregistrierung beteiligte Registry, der Registrar, etwaiger Reseller und Privacy- und Proxyservicebetreiber eine Datenbank zu unterhalten haben, sondern dass darüber hinaus auch diese Datenbank noch verschieden sein muss von den ansonsten geführten Datenbanken, in denen Registrierungsdaten verarbeitet werden. Eine Klarstellung im Gesetz wäre daher wünschenswert.

Die Auflage, die Datenbank „im Einklang mit dem Datenschutzrecht in Bezug auf personenbezogene Daten“ zu führen und zu pflegen, sorgt bei Registries und Registraren für Verunsicherung, da diese im Unklaren über den Umgang mit Unternehmensdaten sind, wenn diese auch Personenbezug aufweisen, wie beispielsweise E-Mailadressen. Wünschenswert wäre eine gesetzliche Grundlage dafür, dass für juristische Personen alle Datenelemente veröffentlicht werden dürfen. Dies bringt für die Anbieter die erforderliche Rechtssicherheit und kommt dem gesetzgeberischen Wunsch nach der Verfügbarkeit dieser Daten nach.

eco [bekräftigt](#) noch einmal, dass er den gewählten Ansatz für nicht sinnvoll hält und darin keinen Mehrwert für die Steigerung der IT-Sicherheit sieht. Der Umgang mit Registrierungsdaten in einem globalen Ökosystem wie bspw. whois sollte im Rahmen des Multi-Stakeholder Ansatzes erarbeitet werden.

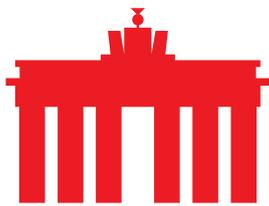
IV.2. Zu § 52: Verpflichtung zur Zugangsgewährung

Der § 52 stellt klar, dass ausschließlich so genannte „berechtigte Zugangsnachfrager“ befugt sind, entsprechende Informationen aus den Datenbanken abzufragen. Aus Sicht der Internetwirtschaft wäre es begrüßenswert, dass diese Zugangsnachfrager klarer beschrieben werden. Auch sollte der Begriff der Zugangsgewährung geprüft werden, da er den Eindruck erweckt, dass Anfragenden Zugriff auf die Datenbank der Registrierungsdaten gewährt wird. Es sollten allerdings lediglich berechtigte Anfragen durch den Anbieter beauskunftet werden müssen. Ein Zugang ist dabei nicht zu gewähren.

Wünschenswert wäre auch eine Klarstellung, dass eine Beauskunftung nach dieser Vorschrift auf den Zweck der Sicherheit, Stabilität und Resilienz des Domain Name Systems beschränkt ist.

IV.3. Zu § 53: Kooperationspflicht

In Bezug auf die in § 53 vorgesehene Kooperationspflicht besteht aus Sicht der Internetwirtschaft Unsicherheit. Die Anforderung an den nationalen Gesetzgeber, die Normadressaten zur Kooperation zu verpflichten, dürfte dem Prinzip der Datenminimierung geschuldet sein, auf das in Erwägungsgrund 51 hingewiesen wird. Daher wäre eine Klarstellung hilfreich, dass in dem Fall, in dem eine



Kooperation zwischen den Beteiligten besteht, auch nur der im Rahmen der Kooperation als für die Erledigung einer bestimmten Aufgabe benannte Akteur die Aufgabe zu erledigen hat.

Unklarheit besteht dabei vor allem bei nicht in der EU ansässigen Registries, da eine Verpflichtung aller, die Daten vorhalten zu müssen, zu internationalen Transfers personenbezogener Daten führen würde, die nicht in allen Fällen durch Angemessenheitsbeschlüsse abgedeckt sind oder durch SCCs rechtmäßig abgewickelt werden können.

Wünschenswert wäre zudem eine Übergangsfrist, binnen derer die erforderlichen Kooperationen verabredet und die Anforderungen aus den §§ 51-53 umgesetzt werden müssen.

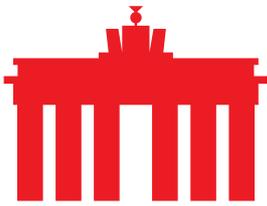
V. Zu Artikel 1 Teil 5: Zertifizierung und Kennzeichen

V.1. Zu § 54 Zertifizierung

Aus Sicht der Internetwirtschaft sind die im Bereich der Zertifizierung gewählten Ansätze nur begrenzt praktikabel. Insbesondere die Möglichkeit des BMI, Zertifizierungen trotz erfüllter Kriterien zu verweigern, wenn dies "überwiegenden öffentlichen Interessen" zuwiderlaufe. Hier wird insbesondere für Betreiber besonders wichtiger Einrichtungen und kritischer Anlagen eine zusätzliche Hürde eingezogen, die den Einsatz insbesondere von kritischen Komponenten deutlich erschwert, ohne dass der klassische Weg der Untersagung des Einsatzes beschritten wird. Aus Sicht der Internetwirtschaft ist dieser Schritt kritikwürdig. Zu diskutieren wäre, ob es sinnvoll ist, dem BSI die Aufsicht über die Zertifizierung zuzuweisen und so zu gewährleisten, dass Zertifizierung strikt auf Grundlage technischer und wissenschaftlicher Erkenntnisse erfolgt.

V.2. Zu § 55 Konformitätsbewertung und Konformitätserklärung

Aus Sicht der Internetwirtschaft ist der hier gewählte Weg einer weiteren Konkretisierung und Formalisierung der Konformitätserklärung für IT-Dienste und IT-Produkte in Bezug auf Technische Richtlinien des BSI problematisch. Ein niedrigschwelliger Ansatz, der gerade kleinen und mittelständischen Unternehmen möglichst einfach und unbürokratisch ermöglicht, IT-Sicherheit nachzuweisen und zu überprüfen, wird durch starre Vorgaben für diese Unternehmen zum Hemmnis. Aus Sicht der Internetwirtschaft sollte insbesondere bei Konformitätserklärungen ein möglichst einfacher und unbürokratischer Ansatz gewählt werden. Formalisierte Abläufe sollten Zertifizierungsvorhaben vorbehalten bleiben. Auch wird bei dem hier gewählten Weg nicht deutlich, wie genau diese Form der Konformitätsbewertung mit weiteren europäischen Gesetzgebungsvorhaben, namentlich dem Cyber Resilience Act interagiert oder diesen Rechnung trägt.



V.3. Zu § 64: Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten

Die Umsetzung des Artikel 26 aus der NIS2-Richtlinie in die nationale Gesetzgebung sollte aus Sicht der Internetwirtschaft mit weiterer Orientierung und Unterstützung für die betroffenen Einrichtungen dahingehend, wie genau festzustellen ist, wo das Cybersicherheitsrisikomanagement durchgeführt wird oder wo realistischerweise anzunehmen ist, dass darüber entschieden wird. Aus Sicht von eco bedarf es hier weiterer Klarstellung, um Unternehmen bei der Gestaltung ihres Cybersicherheits- und Risikomanagements zu unterstützen und zu klären mit welchen Aufsichtsbehörden sie sich jeweils abstimmen sollen. Es ist davon auszugehen, dass durch den § 64 zahlreiche Unternehmen nicht mehr durch das BSI sondern durch andere europäische Behörden beaufsichtigt werden. Es wäre daher insbesondere zu klären, wie die Zusammenarbeit von Aufsichtsbehörden in Bezug auf die betroffenen Unternehmen geregelt ist und zusätzliche Bürokratie vermieden werden kann.

VI. Zu Artikel 1 Teil 7: Sanktionsvorschriften und Aufsicht

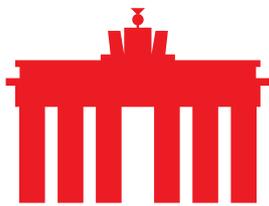
VI.1. Zu §§ 63/64 Zuständigkeiten

§ 63 legt die Zuständigkeit des Bundesamtes für die Einhaltung der Vorschriften aus Teil 3 (§§ 28-50) für wichtige Einrichtungen und besonders wichtige Einrichtungen aber auch für kritische Anlagen in Deutschland fest. Mit § 64 wird diese Zuständigkeit bei IT-Dienstleistungen auf Unternehmensteile oder Beteiligungen in EU-Mitgliedsstaaten erweitert, wenn der Hauptsitz des Unternehmens/Konzerns in Deutschland liegt. Das hätte in der jetzigen Formulierung die Konsequenz, dass das deutsche rechtliche Konzept der „kritischen Anlagen“ auch im europäischen Ausland gelten würde, wenn der Hauptsitz des Betreibers in Deutschland liegt. Dies führt zum Export der erhöhten deutschen KRITIS-Anforderungen in das europäische Ausland. Dies gilt es zu vermeiden, weil es über die eigentlichen Anforderungen der NIS2 hinausgeht und in anderen EU-Mitgliedsstaaten nicht umsetzbar wäre

VII. Zu Artikel 23: Änderung des Telekommunikationsgesetzes

VII.1. Zu 4. § 168 TKG

Die Neufassung des § 168 des TKG sieht eine Meldepflicht für Netzbetreiber an die Bundesnetzagentur und an das BSI vor. Aus Sicht der Internetwirtschaft besteht hier unbeschadet von der bereits bei § 32 vorgetragenen Kritik an dem gestuften Meldeverfahren mit 24 Stunden und 72 Stunden zusätzlich das Problem, dass die doppelte Meldepflicht an das BSI und die BNetzA bestehen bleibt, die entsprechendem Mehraufwand bei Betreibern von TK-Diensten und Netzen verursacht. Aus Sicht der Internetwirtschaft sollte eine zentrale Anlaufstelle geschaffen werden, die die Meldungen entgegennimmt und doppelte Meldepflichten vermieden werden.



Zusammenfassung und Fazit

Aus Sicht der Internetwirtschaft werden mit dem vorliegenden Gesetzentwurf viele bewährte Formen der IT-Sicherheitsregulierung sinnvoll fortgeschrieben, beispielsweise beim Umgang mit kritischen Komponenten. Problematisch erweist sich beim NIS2UmsuCG-E insbesondere das unklare Regulierungsgefüge im Hinblick auf die verschiedenen Kategorien von Einrichtungen, die bei der nationalen Umsetzung im deutschen Gesetz nicht sinnvoll zusammengefügt werden und so eine starke regulatorische Schiefelage und Unsicherheiten in Bezug auf den Anwendungsbereich bzw. die Betroffenheit von bestimmten Regelungen des NIS2UmsuCG erzeugen. Die Kategorien der wichtigen Einrichtungen, der besonders wichtigen Einrichtungen und der kritischen Anlagen bleibt sowohl im Verhältnis zur NIS2-Richtlinie, als auch im Verhältnis zum KRITIS-DachG nicht nachvollziehbar und aus Sicht der Internetwirtschaft unschlüssig. Aus Sicht der Internetwirtschaft ist dies nicht nachvollziehbar und sollte dringend korrigiert werden. Nicht zuletzt für grenzübergreifend tätige Unternehmen könnten Besonderheiten in der nationalen Regulierung ein Problem durch einen auseinanderfallenden Rechtsrahmen ergeben. Hinzu kommt, dass der Anwendungsbereich zukünftig zahlreiche neue Unternehmen in die Regulierung einbezieht und diese verpflichtet sind, erstmalig Risikomanagementmaßnahmen im Cybersicherheitsbereich vorzuweisen und bei Cybervorfällen Meldepflichten erfüllen zu müssen. Aufgrund der knapp bemessenen Umsetzungsfrist ist bereits jetzt absehbar, dass viele Unternehmen die auf sie zukommenden Verpflichtungen nicht fristgerecht erfüllen können.

Insgesamt wäre es wünschenswert, wenn sich das BMI, das sowohl für das KRITIS-DachG als auch für das NIS2UmsuCG verantwortlich zeichnet, mehr um eine möglichst harmonische und europäisch integrationsfähige IT-Sicherheitsregulierung mit einem hohen Schutzniveau bemühen würde, als sich in formalistischen Vorgaben zu erschöpfen und diese einseitig der Wirtschaft aufzuerlegen und gleichzeitig große Teile der öffentlichen Hand, unter Umständen gar ländereigene Betriebe, aus der Regulierung herauszunehmen.