VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

Zum Diskussionspapier des Bundesministeriums des Innern und für Heimat für „Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland“

Berlin, 20.10.2023

Mit der Veröffentlichung der NIS-2-Richtlinie im europäischen Gesetzblatt im Dezember 2022 wurde der Grundstein für die nationale Umsetzung gelegt. Mit 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 dem aktuell vorgelegten Diskussionspapiers für „wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland“ nimmt die Debatte weiter Gestalt an.

Für die Internetwirtschaft sind die Veränderungen im Bereich der IT-Sicherheitsregulierung gravierend. Werden mit den vorgenommenen Vorgaben doch der Anwendungsbereich von IT-Sicherheitsregulierung 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 ausgearbeitet. 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 NIS2-Richtlinie, die seit Dezember 2022 in Kraft ist, noch einmal grundlegend überarbeitet. Der Ansatz der bisher definierten KRITIS-Sektorenwurde 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.

Der im Juli bekannt gewordene Entwurf eines NIS2 Umsetzungs- und Anwendungsgesetzes (NIS2UmsuCG) sowie das nunmehr vorliegende

Diskussionspapier und das derzeit in Beratung befindliche KRITIS-DachG greifen diese Systematik auf, entwickeln sie jedoch weiter und schaffen darüber hinaus auch eigene Definitionen. 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.

Das vorliegende Diskussionspapier enthält derzeit noch zahlreiche Lücken zu Regelungen wie bspw. dem Umgang mit kritischen Komponenten. Dementsprechend ist auf dieser Basis eine abschließende Bewertung nicht möglich. Aus Sicht der Internetwirtschaft ist diese Frage zentral und sollte in jedem Fall weiter auch im Dialog den betroffenen Unternehmen und Institutionen weiter erörtert 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 jenseits des von der EU vorgezeichneten Rahmens ist dabei nicht hilfreich.

I. Zu den Punkten des Diskussionspapiers im Einzelnen:

I.1. Zu Teil I: Allgemeine Vorschriften

Die Definitionen des Diskussionspapiers sind aus Sicht der Internetwirtschaft mit denen aus dem im Juli bekannt gewordenen Entwurf zum NIS2UmsuCG weitgehend deckungsgleich. Diese wiederum sind zum großen Teil der NIS2-Richtlinie entnommen. Grundsätzlich ist dies positiv zu bewerten. Allerdings sollte bei der Definition von Rechenzentrumsdiensten geprüft werden, ob und in welchem Umfang und abweichend von der europäischen Regulierung eine weitere Konkretisierung der Definition sinnvoll ist, um zu klären, inwieweit hier der reine Rechenzentrumsbetrieb gemeint ist, oder in welchem Umfang sich diese Definition mit Fragen zu Cloud Computing überschneidet. Zumindest wären hier eine Klarstellung und eine Erläuterung in der Begründung hilfreich. Auffällig ist, dass die Definition von „kritischen Komponenten“ aus dem vorliegenden Diskussionspapier entfernt worden ist, so dass hier keine Bewertung vorgenommen werden kann. Aus Sicht der Internetwirtschaft sind die Vorgaben zum Einsatz kritischer Komponenten zentral für die Regulierung der IT-Sicherheit und sind für die Digitalisierung und den Netzausbau in Deutschland von großer Bedeutung. Die Möglichkeit, bestimmte Hersteller oder Produkte auszuschließen sollte daher zügig und möglichst transparent dargestellt werden, da im Fall von Rechtsunsicherheiten auf betroffene Unternehmen eine enorme finanzielle Belastung zukommen könnte und ihr Ruf als verlässliche Partner untergraben werden könnte, weil bei einer Untersagung für die Verwendung von Komponenten auch Verträge von betroffenen Unternehmen mit externen Zulieferern betroffen sind. Eine zeitnahe Klarstellung darüber, wie die das

BMI hier weiter vorgehen möchte, ist daher aus Sicht der Internetwirtschaft wichtig.

Darüber hinaus wird in den Begriffsbestimmungen auch der Begriff der „kritischen Anlage“ definiert. Dieser Begriff ist so in der NIS2-Richtlinie nicht enthalten und es ist nicht ersichtlich, wie sich dieser Begriff aus der NIS2-Richtlinie ableitet oder in welchem Verhältnis er zu den grundlegenden Einrichtungen der NIS2-Richtlinie steht. Aus Sicht der Internetwirtschaft ist der Begriff problematisch, da er sich an den alten Definitionen der kritischen Infrastrukturen aus der NIS-Richtlinie orientiert. Er sollte – wie auch das Konzept der kritischen Infrastrukturen – aus dem Gesetz gestrichen werden, um ein europaweit harmonisiertes Regulierungsgefüge nicht durch nationale Sonderregelungen zu untergraben. Auch im Sinne einer besseren Nachvollziehbarkeit für Unternehmen ist diese Sonderregelung nicht hilfreich.

I.2. Zu Teil III: Sicherheit der Informationstechnik von Einrichtungen

In Kapitel 1 § 28 werden unter den besonders wichtigen Einrichtungen auch die Betreiber kritischer Anlagen aufgeführt. Aus Sicht der Internetwirtschaft ist dies problematisch, da auch ein entsprechender Verweis auf das KRITIS-DachG an dieser Stelle nicht erfolgt. Dieses führt kritische Infrastrukturen und kritische Anlagen auf. eco plädiert dafür, den Begriff der kritischen Anlage aus dem Gesetz zu streichen. Dies betrifft auch deren besondere Verpflichtungen in Kapitel 2 § 31.

Die Ausnahmeregelung für Betreiber von Telekommunikationsnetzen könnte unter Umständen zu kurz greifen. Hier sollte darauf geachtet werden, dass Rechenzentren, die zum Betrieb eines Telekommunikationsnetzes dienen, nicht unter eine Doppelregulierung fallen.

In Kapitel 2 § 30 werden sowohl die Betreiber von besonders wichtigen Einrichtungen als auch die Betreiber von wichtigen Einrichtungen denselben Auflagen und Berichtspflichten unterworfen. Aus Sicht der Internetwirtschaft läuft dies dem Gedanken der NIS2-Richtlinie zuwider. Diese sieht eben nicht identische Auflagen für Betreiber von wesentlichen und wichtigen Einrichtungen vor. Eine Unterscheidung der Kategorien würde in diesem Licht keinen Sinn ergeben. eco plädiert dafür, das Regulierungsgefüge der NIS2-Richtlinie zu übernehmen und die Anforderungen an die verschiedenen Kategorien von Einrichtungen an diese anzupassen.

Unklar ist auch die in Kapitel 2 § 30 (3ff.) geschaffene Regelung zu den Auflagen, die die Betreiber besonders wichtiger und wichtiger Einrichtungen zu erfüllen haben. Hier besteht ein Problem, wenn nationale Regelungen aus dem zukünftigen NIS2UmsuCG keiner europäischen Regelung der NIS2-Richtlinie entsprechend zugeordnet werden und diese quasi als Sonderregulierung neben den bestehenden Systematiken der NIS2-Richtlinie bestehen. Es besteht zu befürchten, dass in diesem Fall das Regulierungsgefüge der NIS2-Richtlinie auseinanderfällt. Positiv festzuhalten ist, dass die nationalen Regelungen nicht den europäischen Vorgaben vorgestellt werden. Allerdings ist der gewählte Ansatz des Diskussionspapiers aus der Sicht von eco dennoch kritikwürdig, da die Vorgabe, nationale Regelungen

greifen nur dort, wo es auf europäischer Ebene keine Regelung gibt, die Anerkennung einer Regulierungslücke durch die Durchführungsrechtsakte der Europäischen Kommission im Unbestimmten lässt, so dass Unternehmen dazu gehalten sind, die nationale Regulierung weiter daraufhin zu überprüfen, ob es mögliche Regulierungslücken in der europäischen Regulierung gemäß NIS2-Richtlinie gibt, und diese dann um die Erfüllung zusätzlicher nationaler Regelungen zu ergänzen. Zudem ist nicht ersichtlich, unter welchen Voraussetzungen welche Instanz eine solche Regulierungslücke und damit die Gültigkeit eines nationalen Regelwerkes festlegen darf. Auch ist unklar, ob sich eine solche Regelungslücke immer ex ante identifizieren lässt. Analog gilt dies auch für die etablierten Meldefristen in § 32 und die in § 39 eröffnete Nachweispflicht gegenüber dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Die Internetwirtschaft sieht hier den Bedarf zur weiteren Klarstellung – auch um die Planungssicherheit der betroffenen Unternehmen zu gewährleisten.

Grundsätzlich ist die Einführung von Branchenstandards sinnvoll und zu begrüßen. Bei der Festlegung von Branchenstandards sieht eco allerdings Herausforderungen daraus resultieren, dass diese im Benehmen mit dem BBK und zusätzlich mit der zuständigen Bundesaufsichtsbehörde zu klären seien. Dies könnte im Fall der Internetwirtschaft dazu führen, dass drei Behörden, die Bundesnetzagentur (BNetzA), das BSI und das BBK involviert sind. Dies sollte umgekehrt nicht dazu führen, dass Unternehmen unverhältnismäßigem Aufwand bei der Erarbeitung von Branchenstandards ausgesetzt sind und diese durch langwierige Abstimmungsprozesse durch Behörden untergraben werden.

Die Verpflichtung zur Registrierung von wichtigen, besonders wichtigen Einrichtungen und kritischen Anlagen gemäß NIS2-Richtlinie ist zwar grundsätzlich nachvollziehbar. ES sollte dabei jedoch nicht außer Acht gelassen werden, dass die Anforderungen, so wie sie derzeit im Text dargelegt sind, problematisch sind, da sie unverhältnismäßige Berichtspflichten umfassen könnten und auch Informationen, die den jeweiligen Betreibern der Einrichtungen nicht bekannt sind.

In Kapitel 2 § 34 wird auf Einrichtungen gem. § 63 Abs. 1 Satz 1 verwiesen. Dieser § 63 taucht im Diskussionspapier nicht auf, so dass nicht geklärt werden kann, welche Einrichtungen oder Unternehmen hier tatsächlich erfasst sind. Die Begründung zu § 34 führt an, dass damit der Artikel 27 der NIS2-Richtlinie umgesetzt werden soll. Die Auflagen entsprechen denen der NIS2-Richtlinie. Es kann nicht abschließend bewertet werden, ob der Adressatenkreis dieser Regelung auch im Sinne der NIS2-Richtlinie korrekt umschrieben ist. eco behält sich hier eine weitere Kommentierung nach Klärung des Sachverhalts vor. Allerdings wird durch den Paragrafen eine Ordnungswidrigkeit eröffnet, wenn eine verpflichtete Einrichtung nicht korrekt oder gar nicht meldet. Hier ist fraglich, inwieweit hier der Regulierungsrahmen der NIS2-Richtlinie überschritten werden, die hier keine entsprechende Regelung vorsieht. Aus Sicht der Internetwirtschaft sollte dieser Bußgeldtatbestand aus dem Gesetz gestrichen werden, da durch das Bußgeld kein ordnungsrechtlicher Mehrwert zu erhoffen ist. In der praktischen Umsetzung des

Entwurfs stellen sich zudem weitere Fragen wie Nachweispflichten und Haftungsfragen in den jeweiligen Mitgliedsstaaten.

Die in Kapitel II § 38 eröffneten Verpflichtungen für Geschäftsführer sieht eco – wie auch schon in der NIS2-Richtlinie problematisch. Sie ermöglichen keine Delegierung an spezialisierte Fachkräfte für IT-Sicherheit. Aus Sicht der Internetwirtschaft ist dies nicht hilfreich, da es diese von ihrer Verpflichtung entbindet. Die Regelung begründet eine direkte persönliche Haftung für die Geschäftsführer von wichtigen Einrichtungen und bietet diesen keine Möglichkeit zur Exkulpation. Dies dürfte bei entsprechender Kritikalität und den zu erwartenden Schäden eine prohibitiv hohe Abschreckungswirkung haben, entsprechende Stellen zu besetzen. Auch lässt der Entwurf offen, welche Maßnahmen als geeignete Schulung aus Sicht des Gesetzgebers angesehen werden, so dass für die betroffenen Personen das Risiko nicht absehbar ist.

I.3. Zu Teil 4: Datenbanken der Domain-Name-Registrierungsdaten

Die NIS2-Richtlinie verpflichtet Betreiber von Top-Level Domains (TLD) und die Einrichtungen, die Domänennamenregistrierungsdienste erbringen, eine Datenbank zu erstellen, in denen verschiedene Datensätze über die Domäneninhaber hinterlegt sind. eco bekräftigt noch einmal, dass er den gewählten Ansatz für nicht sinnvoll hält und darin keinen Mehrwert für die Steigerung der IT-Sicherheit sieht. eco weist in diesem Zusammenhang auch darauf hin, dass nach wie vor diskutiert wird, welche Daten einer Domain bzw. eines Domaininhabers unter welchen Rahmenbedingungen als personenbezogen eingestuft werden. In einem Multi-Stakeholder Ansatz sollten hier gemeinsam Leitlinien erarbeitet werden, die ein möglichst breites Anwendungsfeld eröffnen und die Registrierst und Registraren eine rechtssichere Ausübung ihrer Geschäftstätigkeit ermöglicht.

Die in § 52 eröffnete Verpflichtung zur Zugangsgewährung ist aus Sicht der Internetwirtschaft nicht konkret genug gefasst. Hier wird die Formulierung der Richtlinie zwar weitgehend übernommen. Eingefügt wird jedoch zusätzlich der Begriff der der berechtigten Zugangsnachfrager. Hier wird nicht klargestellt, wer diese in den Augen des Gesetzgebers sind. Aus Sicht der Internetwirtschaft kommen lediglich zuständige Aufsichtsbehörden bzw. Stellen, die zur Beseitigung von Störungen beauftragt sind, infrage. eco appelliert an den Gesetzgeber, die Domain-Name-Registrierungsdatenbank nicht für andere Zwecke als die der Gewährleistung der Sicherstellung des Domain-Name-Systems (DNS) zu verwenden.

I.4. Zu Teil 6: Verordnungsermächtigungen, Grundrechtseinschränkungen, Berichtspflichten

Die im Diskussionspapier vorgesehen Verordnungsermächtigungen bedürfen einer kritischen Prüfung und Überarbeitung. Aus Sicht der Internetwirtschaft sind sie nicht dazu geeignet, ein einheitliches und harmonisiertes Regulierungsgefüge zu schaffen und so zu einer stringenten, nachvollziehbaren und verhältnismäßigen Regulierung von IT-Sicherheit beizutragen. Es sollte im Rahmen der Erarbeitung der Verordnungen auch darauf geachtet werden, dass etwaig bestehende Standards,

Normen und Zertifikate wie das IT-Gütesiegel des BSI weiter Bestand haben können, sofern die NIS2-Richtlinie keine gegenteiligen Vorgaben macht.

Die Verordnungsermächtigung für das BMI zur Erteilung von Sicherheitszertifikaten in § 57 (1) verweist auf einen § 54, der nicht im Diskussionspapier enthalten ist. eco behält sich eine Kommentierung im weiteren Verlauf des Gesetzgebungsverfahrens vor.

Die Verordnungsermächtigung für das IT-Sicherheitskennzeichen gem. § 57 (2) verweist auf den § 52 des vorliegenden Diskussionspapiers. Dies kann nicht zutreffen, da dort keine sinnvoll hierzu passende Regelung zu finden ist.

Die in § 57 (3) geschaffene Verordnungsermächtigung, für Unternehmen oder Dienste Auflagen zu schaffen, die zwar selbst nicht wichtige oder besonders wichtige Einrichtungen oder kritische Anlagen sind, diesen aber möglicherweise ihre Produkte zur Verfügung stellen, ist aus Sicht der Internetwirtschaft mit dem Ansatz der NIS2-Richtlinie nicht vereinbar, da sie den Anwendungsbereich den Einschätzungen von Ministerien überlässt. Für die Betroffenen Unternehmen ist dies weder vorhersehbar noch nachvollziehbar. Der Anwendungsbereich sollte durch den Gesetzgeber und nicht im Wege einer Verordnungsermächtigung definiert und festgelegt werden. Es ist auch zu bezweifeln, dass eine solch zentrale Regelung, die unter Umständen massiv in die Geschäftstätigkeit von solchen Zulieferbetrieben eingreift, auf dem Verordnungsweg geschaffen werden soll.

Die in § 57 (4) geschaffene Regelung zur Definition von Versorgungsgraden läuft aus Sicht der Internetwirtschaft der Systematik von NIS2 zuwider. Sie sollte gestrichen werden, da die Kritikalität einer Dienstleistung durch die NIS2-Richtlinie nach anderen Maßstäben ermittelt wird und Doppelregulierung aus Sicht der Internetwirtschaft problematisch ist.

I.5. Zu Anlage I und Anlage II

Positiv hervorzuheben ist, dass im Diskussionspapier alle Elemente der NIS2-Richtlinie aus der dortigen Anlage I übernommen wurden, wenn auch die Zuordnung in zwei Fällen nicht eindeutig ist. Problematisch hingegen ist die Zuordnung der Dienste, die in der NIS2-Richtlinie als wichtige Einrichtungen deklariert sind, im vorliegenden Diskussionspapier hingegen als „sonstige kritische Sektoren“ bezeichnet werden. Aus Sicht der Internetwirtschaft ist diese Unschärfe in Verbindung mit der oben dargelegten Problematik kritischer Einrichtungen dazu geeignet, Dienste und Einrichtungen, die der NIS2-Richtlinie entsprechend „wichtige“ Einrichtungen sind, in der deutschen Regulierung als „besonders wichtige“ (nach deutscher Lesart) Einrichtungen behandelt werden. eco drängt darauf, hier Klarheit herzustellen und auf die europäischen Vorgaben bei der Klärung der Zuordnung von Sektoren zu beachten.

II. Fazit:

Der vorliegende Diskussionsentwurf für die Umsetzung der NIS2-Richtlinie bedarf an mehreren Stellen einer gründlichen Überprüfung und Überarbeitung. Sowohl

das eröffnete Regulierungsgefüge zwischen den wichtigen Einrichtungen, den besonders wichtigen Einrichtungen und den kritischen Anlagen ist nicht nur mit den europäischen Vorgaben nicht vereinbar, sie ist auch in sich unschlüssig. Dass dieses unbestimmte Regulierungsgefüge, durch eine allgemeine Verordnungsermächtigung erweitert werden kann, trägt nicht zur Rechtssicherheit für die möglicherweise betroffene Unternehmen bei. Aus Sicht der Internetwirtschaft sollten klare Regelungen geschaffen werden, die die europäischen Vorgaben möglichst stringent umsetzen. Das Diskussionspapier macht derzeit keine Aussage zum Umgang mit dem Einsatz kritischer Komponenten und lässt damit einen für die betroffenen Unternehmen zentralen Aspekt und Fragestellungen unbeantwortet. eco plädiert hier für einen transparenten, verhältnismäßigen und nachvollziehbaren Ansatz, der nicht den Eindruck erweckt, Unternehmen seien der Willkür staatlicher oder behördlicher Entscheidungen ausgeliefert. In diesem Kontext bedarf der vorliegende Entwurf dringend weiterer Klarstellungen. Eine bessere Harmonisierung der deutschen Pläne zur IT-Sicherheitsregulierung mit den europäischen Vorgaben unter Wahrung eines hohen Sicherheits- und Schutzniveaus ist machbar.

Zuletzt wäre eine Klarstellung begrüßenswert, dass bereits erarbeitete und geltende Standards möglichst als Ansatzpunkt für die Ausgestaltung der Regulierung dienen sollten und nicht alle Vorgaben komplett neu erarbeitet werden. Aus Sicht der Internetwirtschaft ist dies nicht produktiv, da die geltenden Standards ein hohes Schutzniveau sicherstellen und bereits bei entsprechenden Einrichtungen etabliert sind.