VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

zum Referentenentwurf für ein Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)

Berlin, 24. August 2023

Mit dem KRITIS-Dachgesetz (KRITIS-DachG) werden in Deutschland erstmals bundesweit einheitliche Vorgaben zum physischen Schutz kritischer Anlagen geschaffen. Gleichzeitig soll mit dem Gesetz auch die europäische „Richtlinie über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates“ (CER-Richtlinie) in deutsches Recht überführt werden. Das KRITIS-DachG ist aus Sicht der Internetwirtschaft komplementär mit dem parallel in Ressortabstimmung befindlichen „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG)“ zu sehen. Hier sind die Regeln und Vorgaben für digitale Unternehmen zentral geregelt. Aus Sicht der Internetwirtschaft und im Sinne einer stringenten und nachvollziehbaren Gesetzgebung wäre es daher sinnvoll gewesen, die Vorgaben für IT-Unternehmen im NIS2UmsuCG zu bündeln. Die Vorgaben aus dem KRITIS-DachG sollten dementsprechend für die Internetwirtschaft nicht in größerem Umfang relevant sein. Auch sollte bei der Gesetzgebung darauf geachtet werden, dass durch die beiden Gesetze keine Unklarheiten oder Doppelregulierung geschaffen wird.

eco – Verband der Internetwirtschaft e.V. nimmt zu dem vorliegenden Entwurf des KRITIS-Dachgesetzes (KRITIS-DachG-E) wie folgt Stellung.

- **Zu Paragraph 2: Begriffsbestimmungen**

Die in Paragraph 2 (11) angelegte Definition von „besonders wichtigen Einrichtungen“ bezieht sich auf augenscheinlich auf die in der NIS-2 Richtlinie beschriebenen wichtigen bzw. wesentlichen Einrichtungen. Auffällig hierbei ist, dass die Abgrenzung zu den in der NIS-2 Richtlinie angelegten Definitionen nicht passend ist. Die dadurch geschaffene Unschärfe – auch im Verhältnis zu den kritischen Einrichtungen der CER-Richtlinie – ist aus Sicht der Internetwirtschaft problematisch, da die vorhandenen Definitionen in einem europäischen Kontext das Regulierungsgefüge auseinanderfallen lassen. Darüber hinaus ist nicht klar, wie sich die hier niedergelegten besonders wichtigen Einrichtungen zu den ebenfalls im Gesetzentwurf aufgeführten kritischen Anlagen verhalten, die über die CER-Richtlinie definiert sind. eco würde vor diesem Hintergrund begrüßen, wenn die Definitionen der europäischen Rechtsakte in den jeweiligen deutschen Umsetzungs- und Anwendungsgesetzen möglichst genau übernommen werden, um

ein Auseinanderfallen des Adressatenkreises der europäischen Rechtssetzung zu vermeiden und stattdessen dafür zu sorgen, dass die europäischen Vorgaben möglichst einheitlich angewendet werden können. Dies ist für die Rechtssicherheit und Rechtsklarheit wichtig.

- **Zu Paragraph 3: Nationale zuständige Behörde für die Resilienz kritischer Anlagen**

Der KRITIS-DachG-E sieht das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) als national zuständige Behörde für die Steuerung der Aktivitäten, die zum Schutz der kritischen Infrastrukturen und der (besonders) wichtigen Einrichtungen gedacht sind. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Bundesnetzagentur (BNetzA) sind in diesem Kontext dem BBK unterstellt und haben ihm Informationen zur Erfüllung ihrer Aufgaben zu übermitteln.

Aus Sicht der Internetwirtschaft bleibt hier im Unbestimmten, wie zukünftig Weisungen von BNetzA und BSI behandelt werden müssen, insbesondere, wenn sie in einem Spannungsverhältnis zu denen des BBK stehen. Auch sollte vor diesem Hintergrund klarer herausgestellt werden, in welchem Verhältnis das BBK hier zu den jeweils zuständigen Landesbehörden agiert. eco plädiert dafür, die Vorgaben für Meldestrukturen und die Federführung für die Aufsicht klar zu regeln – auch um möglichen Kompetenzstreitigkeiten entgegenzuwirken. Darüber hinaus sollte berücksichtigt werden, dass die Last durch eventuell zu erfüllende Meldepflichten für die Betreiber (besonders) wichtiger Einrichtungen und kritischer Infrastrukturen nicht grundlos komplex gestaltet werden müssen. Insgesamt sollte darauf geachtet werden, dass die jeweils zuständigen Behörden für die Erfüllung ihrer Aufgaben ausreichend personell ausgestattet sind und hierfür über das nötige Wissen verfügen.

- **Zu Paragraph 4: Kritische Anlagen**

Aus Sicht der Internetwirtschaft ist die Regelung der kritischen Anlagen problematisch. Die Definition dessen, was eine kritische Anlage ist, wird durch eine Verordnungsermächtigung für das BMI geregelt. Lediglich die betroffenen Sektoren, sowie das Erreichen bestimmter Schwellenwerte werden als Kriterien für die Zuordnung zum Bereich der kritischen Anlagen genannt. Hier bleibt unklar, in welchem Wechselverhältnis die hier dargelegten kritischen Anlagen zu den im NIS2UmsuCG angelegten und definierten kritischen Anlagen stehen. Aus Sicht der Internetwirtschaft wäre ein einheitlicher, gesetzesübergreifender und aufeinander abgestimmter „harmonischer“ Umgang mit Definitionen wünschenswert.

- **Zu Paragraph 6: Anforderungen an Betreiber Kritischer Infrastrukturen**

Paragraph 6 (1) eröffnet Betreibern kritischer Infrastrukturen, die nicht die erforderlichen Schwellenwerte erfüllen, die Möglichkeit, ebenfalls entsprechende Maßnahmen umzusetzen. Die in Paragraph 6 (2) dargelegte Verpflichtung zur Umsetzung der in Paragraph 6 (1) als freiwillig deklarierten Maßnahmen werfen erneut die Frage auf, wie genau Einrichtungen, Anlagen oder Infrastrukturen voneinander abgegrenzt sind. Die Formulierung aus dem Gesetzestext:

„(2) Die Betreiber Kritischer Infrastrukturen nach Absatz 1 können zur Umsetzung der Verpflichtung nach Absatz 1 die nach § 11 Absatz 5 zu entwickelnden branchenspezifischen Resilienzstandards berücksichtigen." lässt an dieser Stelle einen zu breiten Interpretationsspielraum. Die Begründung lässt keine weiteren Rückschlüsse zu.

Aus Sicht der Internetwirtschaft ist der hier beschrittene Weg problematisch, da sich die hier definierten Ausnahmen zu den allgemein gültigen Schwellenwerten negativ auf die Rechtssicherheit von Unternehmen auswirken werden.

- **Zu Paragraph 8: Registrierung der kritischen Anlage**

Die Schaffung einer gemeinsamen Registrierungsmöglichkeit durch das BSI und das BBK für Betreiber kritischer Anlagen gemäß Paragraph 8 ist aus Sicht der Internetwirtschaft ein positiver Schritt, um die bürokratische Belastung für Unternehmen im akzeptablen Rahmen zu halten. Unklar bleibt indes, in welchem Umfang die hier dargelegten Registrierungsmöglichkeiten auch die Registrierung kritischer Anlagen gemäß NIS2UmsuCG umfasst, die beim BSI stattfinden soll. Hier wäre mehr Klarheit in der Gesetzgebung zwingend erforderlich, um etwaig bestehende Rechtsunsicherheit insbesondere für Unternehmen, die dem NIS2UmsuCG unterworfen sind, zu vermeiden.

- **Zu Paragraph 9: Nationale Risikoanalysen und Risikobewertungen**

Die von den zuständigen Ministerien zu erstellenden Bewertungen und Analysen fokussieren sich auf den Begriff der Wirtschaftsstabilität, der im NIS2UmsuCG nicht erwähnt wird und darüber hinaus auch in seiner Bedeutung aus Sicht der Internetwirtschaft über die sonst geltenden Maßgaben zur „Gewährleistung der Daseinsvorsorge" oder der „hohen Bedeutung für das Funktionieren des Gemeinwesens". Es wäre im Sinne einer stringenten Regulierung und einer nachvollziehbaren und verständlichen Verpflichtung von Unternehmen, darauf zu achten, dass hier keine Unschärfen entstehen oder neue Berichtspflichten geschaffen werden, oder der Adressatenkreis unbeabsichtigt erweitert wird.

- **Zu Paragraph 10: Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen**

Analog zur Betrachtung von Paragraph 9 wird auch in den Vorgaben zu Risikoanalysen und Risikobewertungen für die Betreiber kritischer Anlagen auf die Wirtschaftsstabilität abgehoben. Aus Sicht der Internetwirtschaft ist auch hier auf ein kohärentes und nachvollziehbares Regulierungsgefüge zu achten. Dies gilt umso mehr, als dass durch die Regelungen von Paragraph 10 für einzelne Sektoren unter Umständen doppelte Berichtspflichten ausgelöst werden. Grundsätzlich sollten diese Regelungen nur greifen, sofern Betreiber kritischer Anlagen nicht bereits durch spezialgesetzliche Regelungen dazu verpflichtet sind, entsprechende Berichte zu erstellen. Aus Sicht der Internetwirtschaft ist die im Gesetzentwurf vorgesehene Frist zur Erstellung entsprechender Risikobewertungen von neun Monaten zwar durch europäische Gesetzgebung vorgegeben, sollte jedoch kritisch geprüft werden.

- **Zu Paragraph 11: Resilienzmaßnahmen der Betreiber kritischer Anlagen**

Aus Sicht der Internetwirtschaft ist positiv zu bewerten, dass Betreiber kritischer Anlagen aus dem Sektor der Informationstechnik und Telekommunikation wie auch in Paragraph 10 von den Regelungen ausgenommen sind, so dass zumindest für diese Rechtssicherheit besteht und sie ausschließlich an die Vorgaben aus dem NIS2UmsuCG gebunden sind. Entsprechend der Regelung in Paragraph 10 wäre auch hier zu bedenken, dass die Regelung dahingehend geändert wird, dass die hier vorgegebenen Maßnahmen greifen, sofern keine spezialgesetzlichen Regelungen vorliegen.

- **Zu Paragraph 12: Meldewesen für Störungen**

Das vorgesehene neue Meldewesen im Bereich der physischen Sicherheit sollte sich am Meldewesen im Bereich der Cybersicherheit orientieren. Erforderlich ist zudem Rechtsklarheit, welche Meldewege Unternehmen im Falle von Sicherheitsvorfällen bei Tochtergesellschaften mit Sitz im EU-Ausland einhalten müssen. Nicht praktikable Fristenregelungen, wie sie auch die EU-Richtlinie vorsieht, sollten kritisch geprüft werden, so dass eine sinnvolle Anwendung möglich ist. Die konkrete Ausgestaltung sollte sich harmonisch in den europäischen Regulierungsrahmen einfügen.

- **Zu Paragraph 13: Einsatz kritischer Komponenten; Verordnungsermächtigung**

Die genauere Ausgestaltung von Paragraph 13 wird im weiteren Verlauf des Gesetzgebungsverfahren festgelegt werden. eco behält sich vor, zu einem späteren Zeitpunkt Stellung hierzu zu nehmen. Grundsätzlich sollte beachtet werden, dass die Regelungen im KRITIS-DachG-E nicht im Widerspruch zum NIS2UmsuCG stehen oder zu einer Doppelregulierung führen. Kohärenz zwischen diesen Gesetzen ist aus Sicht der Internetwirtschaft zentral. Darüber hinaus sollte auch berücksichtigt werden, dass die hier gemachten Vorgaben verhältnismäßig und nachvollziehbar sein sollten. Einseitige, politisch geschaffene Vorgaben könnten problematisch sein. Orientierung an internationalen Standards oder an international anschlussfähigen Vorgaben wäre auch in diesem Kontext wünschenswert. Auch sollten die Regeln für den Einsatz kritischer Komponenten transparent und nachvollziehbar sein und für Unternehmen, die davon betroffen sind. Die hier noch festzulegenden Vorgaben dürfen nicht dazu führen, dass zentrale Projekte von hoher Bedeutung für Gesellschaft und Wirtschaft wie bspw. der Umbau der Stromnetze und der Ausbau erneuerbarer Energien durch undurchschaubare oder widersprüchliche Vorgaben gebremst werden. Sie sollten unbedingt auf objektiven, nachvollziehbaren Sachverhalten basieren und nicht durch Annahmen oder Vermutungen begründet werden. Sie sollten auch idealerweise an internationalen Standards orientiert sein. Entscheidend für die Verordnungsermächtigung ist auch der Bezug – also die Frage, ob Wirtschaftsstabilität oder Daseinsvorsorge im Vordergrund stehen.

- **Zu Paragraph 15: Ermächtigung zum Erlass von Rechtsverordnungen**

Der Anwendungsbereich für den Erlass von Rechtsverordnungen sieht auch vor, dass sowohl Unternehmen aus den Sektoren „Informationstechnik und Telekommunikation“ als auch Einrichtungen aus den Bereichen „Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten (Business-to-Business)[…] und Weltraum“ als besonders wichtig, als auch Einrichtungen aus den Sektoren „Informationstechnik und Telekommunikation, […] Anbieter digitaler Dienste“ als wichtige Einrichtungen eingestuft werden können. Die hier vorgenommene Generalermächtigung zum Erlass von Rechtsverordnungen wirft die Frage auf, in welchem Umfang Unternehmen aus diesen Bereichen nicht doch durch das KRITIS-DachG erfasst werden. Auch sollte geklärt werden, in welchem Umfang Unternehmen, die durch das Telekommunikationsgesetz (TKG) reguliert sind, in den Sektor Telekommunikation bzw. Informationstechnik erfasst sind. Insgesamt stellt sich die Frage, inwieweit hier entsprechende Vorgaben deutlicher gefasst werden sollten und aufgrund der Wichtigkeit der hier geschaffenen Verordnungsermächtigung auch entsprechende Sektoren und Bereiche bereits in den Gesetzestext mit aufgenommen werden sollten und welche Anlagenkategorien jeweils in einer Verordnung erfasst werden sollten. Dies trägt aus Sicht der Internetwirtschaft zur Klarheit der angestrebten Regelung bei.

Zusammenfassung und Fazit:

Mit dem KRITIS-DachG-E schafft das BMI einen zwar grundsätzlich nachvollziehbaren Rahmen für die Stärkung der Resilienz kritischer Infrastrukturen. Problematisch an dem vorliegenden Gesetzentwurf ist jedoch aus Sicht der Internetwirtschaft, dass der KRITIS-DachG-E in einem unklaren Verhältnis zu anderen relevanten Gesetzen wie dem NIS2UmsuCG steht. Der Anwendungsbereiche, sowie die für die unterschiedlichen Kategorien von Anlagen und Sektoren sollten klar voneinander abgegrenzt sein, um das Risiko einer Doppelregulierung auszuräumen. Eine abschließende Beurteilung hierzu wird erst möglich sein, wenn die in Paragraph 13 vorgesehene Verordnung vorliegt. eco plädiert dafür, den Gesetzentwurf in den weiteren Beratungen noch einmal gründlich auf konsistente, aufeinander abgestimmte und vereinheitlichte Terminologien hin zu überprüfen und darauf zu achten, dass das Regulierungsgefüge – insbesondere für Unternehmen der Internetwirtschaft – nachvollziehbar und verhältnismäßig zu gestalten. Die derzeitige Gestaltung des KRITIS-DachG-E birgt neben dem Risiko von Doppelregulierung auch einen erhöhten Prüfaufwand bei Unternehmen, inwieweit sie unter welchen Gesichtspunkten meldepflichtig sind bzw. in welche Kategorie von Anlagen sie fallen. Aus Sicht der Internetwirtschaft ist das im KRITIS-DachG-E in Verbindung mit dem NIS2UmsuCG angelegte Regulierungsschema zu komplex. Der Einsatz kritischer Komponenten ist für digitale Unternehmen, die auf importierte Güter und Bauteile angewiesen sind, eine zentrale Frage. Vor diesem Hintergrund sieht eco noch Verbesserungsbedarf im vorliegenden Gesetzentwurf. Die Verlagerung dieser zentralen Frage in eine Verordnungsermächtigung sieht eco als problematisch an.

Insgesamt wäre es im Sinne einer kohärenten und nachvollziehbaren Regulierung von kritischen Infrastrukturen im Einklang mit den entsprechenden europäischen Gesetzen begrüßenswert, wenn alle relevanten Gesetze parallel betrachtet werden könnten, so dass auch Rückschlüsse auf das gesamte Regulierungsgefüge besser möglich wären. Dem vorliegenden Gesetzentwurf fehlt es durch die singuläre Betrachtung an verschiedenen Stellen an Klarheit.