

## Stellungnahme

### **Zum Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen**

**Eine angemessene Bewertung von Gesetzentwürfen erfordert eine angemessene Frist der Auseinandersetzung damit. Anzuhörende Verbände bündeln die Interessen und die Expertise der Verbandsmitglieder. Allerdings steht diese Expertise nur auf Anfrage zur Verfügung und die Expertinnen und Experten sind im operativen Alltag mit anderen Aufgaben ausgelastet. Es ist daher zwingend, die Anhörungsfristen zu verlängern.**

#### **Der Bundesverband Paket und Expresslogistik:**

Der Bundesverband Paket- und Expresslogistik (BPEX) ist die politische Interessenvertretung der Paketbranche in Deutschland. Die Branche liefert flächendeckend täglich ca. 14 Mio. Sendungen an ca. neun Mio. private, gewerbliche und institutionelle Empfängerinnen und Empfänger. Die rund 4.000 Unternehmen der Branche erzielen jährliche Umsätze in Höhe von derzeit 27,6 Mrd. Euro.

#### **I. Im Allgemeinen**

Der Schutz der IT-Sicherheit von Kritischen Infrastrukturen ist derzeit im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) geregelt. Durch die Umsetzung der NIS-2-Richtlinie mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) werden die Regelungen zum Cyberschutz von Kritischen Infrastrukturen und weiteren wichtigen Einrichtungen weiterentwickelt. Das KRITIS-DachG soll neben diese Regelungen treten und den physischen Schutz kritischer Anlagen regeln.

Es wäre wünschenswert gewesen, die beiden Referentenentwürfe aufgrund der inhaltlichen Zusammenhänge zumindest parallel zur Diskussion zu stellen. Wir hätten daher ein gemeinsames Gesetzgebungsverfahren als sinnvoller erachtet. Da dies nun bedauerlicherweise nicht der Fall ist, sollte mindestens auf eine Harmonisierung der Regelungen geachtet werden. Wir sehen vor allem Bedarf bei den verwendeten Begriffen und Definitionen, in Bezug auf die Umsetzungsprozesse und die Kompetenzen der beteiligten Behörden. Mit der parallelen Behandlung physischer und cybersicherheitsrelevanter Verpflichtungen in zwei unterschiedlichen Gesetzgebungsverfahren besteht von Natur aus die Gefahr von Doppelregulierung und Inkonsistenzen. Die parallelen Gesetzesvorschläge führen zu einer komplexen Vorgabesystematik, deren wechselseitige Abhängigkeiten und Zuständigkeiten der einzelnen Behörden eine Umsetzung für Unternehmen unnötig erschweren. Dabei sollten – im Gegenteil – der Dokumentationsaufwand und zusätzliche bürokratische Belastungen

minimiert werden, um nicht unnötig Kapazitäten zu binden, die die Unternehmen in die Verbesserung ihrer Sicherheitsvorkehrungen investieren könnten. Die Aufteilung in zwei getrennte Gesetzgebungsverfahren erschwert es den Unternehmen zusätzlich, die eigene Betroffenheit überhaupt festzustellen, die jeweils relevanten Anforderungen abzuleiten und rechtskonform umzusetzen.

Insbesondere vor dem Hintergrund, dass mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zwei unterschiedliche Aufsichtsbehörden für die Umsetzung des KRITIS-DachG und des NIS2UmsuCG verantwortlich zeichnen, die sich wiederum mit weiteren sektorspezifischen Aufsichtsbehörden vernetzen müssen, sollten die Prozesse der Zusammenarbeit zwischen den Behörden klar definiert werden. Nur so lässt sich ein Doppelaufwand für die Unternehmen, z. B. durch Mehrfachmeldungen, verhindern und effektive Warnhinweise durch die Behörden an die Unternehmen gewährleisten. Alle Maßnahmen müssen darauf hinwirken, das Schutzniveau der Unternehmen zu verbessern und deren eigene Sicherheitsbemühungen zu unterstützen. Eine angemessene personelle Ausstattung der Behörden ist dafür eine weitere Voraussetzung.

Der vorgeschlagene Regelungsrahmen insgesamt (inkl. NIS2UmsuCG) erhöht für potenziell betroffene Unternehmen die Komplexität der zukünftig beachtlichen Pflichten zur Umsetzung und Dokumentation von betrieblichen Maßnahmen. Wiederum werden wesentliche Inhalte, die über die Betroffenheit bestimmen, in nachrangige Rechtsakte mit geringeren Beteiligungsmöglichkeiten für die Wirtschaftsverbände verlagert.

Grundsätzlich weisen wir an dieser Stelle darauf hin, dass sich die Kommentierung des Gesetzentwurfs aufgrund der fehlenden Rechtsverordnung insgesamt als schwierig gestaltet, weil so für die Unternehmen ihre tatsächliche Betroffenheit schwer abschätzbar ist.

Darüber hinaus gilt, dass die Geschäftsprozesse der Unternehmen nicht ohne konkreten Anlass disruptiv verändert werden dürfen und dass die gesetzlich veranlassten Maßnahmen die Fortführung unternehmerischer Prozesse zulassen bzw. ermöglichen müssen. Dies betrifft unter anderem Aspekte wie die Cybersicherheit, Verhaltensregeln für Mitarbeitende, robuste analoge Ersatzprozesse und die Schadensminimierung im Angriffsfall bis zur Herstellung einer dauerhaften und hinreichenden Robustheit aller relevanten unternehmensinternen und -übergreifenden Prozesse.

Hier wäre ein konsistenter Ordnungsrahmen hilfreich, der den Unternehmen verlässliche Orientierung gibt und größtmögliche Transparenz über die rechtlichen Verpflichtungen herstellt.

## **II. Im Einzelnen**

### **§ 2**

Zur Vermeidung praxisferner Pflichten muss in § 2 klargestellt werden, dass mobile Betriebsmittel (Fahrzeuge, Trailer, mobile Umschlagtechnik) keine „Anlagen“ i. S. d. Gesetzes sind.

### **§ 4 Abs. 1**

Positiv ist zu bewerten, dass die Systematik zur Bestimmung von KRITIS grundsätzlich beibehalten werden soll und auch im Gesetzentwurf explizit festgehalten wurde.

### **§ 4 Abs. 2**

Behörden können nach entsprechendem Ermessen zukünftig einseitig die Identifizierung als Betreiber kritischer Anlagen vornehmen. Dies ist als problematisch zu bewerten. Hierfür maßgebliche Kriterien sind zwar im Referentenentwurf aufgeführt, jedoch erscheinen diese weder als abschließende Aufzählung noch sind sie spezifisch, da beispielsweise sowohl „Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten“ (Nummer 3) als auch der „Marktanteil des Betreibers“ (Nummer 4) nicht näher eingegrenzt werden.

Die dem Bundesinnenministerium zugebilligte Befugnis zur Festlegung weiterer Betreiber kritischer Anlagen unter Berücksichtigung der nationalen Risikoanalysen und Risikobewertungen nach § 8 erscheint ohne Kenntnis der Rechtsverordnung nach § 16 als zu weitgehend. Soweit eine Anlehnung an den bestehenden Rahmen der BSI-KritisV beabsichtigt sein sollte, sollte dies klar formuliert sein. Derzeit ist unklar, welche Erwägungen überhaupt dafür maßgeblich sein könnten, den Anwendungsbereich in Abweichung von den Regelschwellenwerten auszuweiten.

Vielmehr sehen wir die Möglichkeit, dass eine Freiheit des Bundesinnenministeriums oder anderer Behörden, Festlegungen zu treffen, zu Lasten eines konsistenten, an klaren Maßstäben ausgerichteten Regelungsrahmens ginge und zudem Raum für eher opportunistische (also tagespolitischen Erwägungen folgende) Vorschläge zur Ausdehnung der Regulierung schafft.

### **§ 4 Abs. 3**

Nach dem vorliegenden Entwurf ist nicht konkret abzusehen, ob ein Anlagenbetreiber im Geltungsbereich des Gesetzes tätig ist oder nicht. Weder liegt eine Rechtsverordnung nach § 4 Abs. 3 vor, noch sind die Kriterien und damit verbundene Ermessensspielräume nach § 5 ausreichend spezifiziert. Zudem können nach § 8 Abs. 4 weitere Betreiber zur Registrierung als Betreiber kritischer Anlagen vorgeschlagen werden, was im Zweifelsfall für die Betreiber überraschend sein kann. Das ist nicht akzeptabel, da sich eine Reihe von Rechtsfolgen damit verbindet. Mindestens müssen Rechtsfolgen der Betroffenheit für die Unternehmen schon im Gesetz auf eine vorab nachvollziehbare Grundlage gestellt werden.

Gleiches gilt für das Verhältnis neuer Verpflichtungen zu bereits aufgrund anderweitiger Vorschriften geltender Obliegenheiten und Maßnahmen, die den Zielen des KRITIS-DachG bereits dienen.

#### **§ 4 Abs. 7 und 8**

Unklar sind uns bisher die Folgen des Verhältnisses anderer Regelungen zum vorliegenden Gesetz. Offenbar bleiben die Pflichten zur gesonderten Dokumentation der getroffenen Maßnahmen weiter bestehen (es reicht nicht der einfache Verweis auf bestehende Auditierung beispielsweise nach dem LuftSiG) ebenso wie alle sonstigen Vorschriften des KRITIS-DachG.

#### **§ 8**

Die Betreiber kritischer Anlagen sollen diese über ein gemeinsames Online-Meldeportal von BBK und BSI registrieren und eine Kontaktstelle bzw. eine Ansprechperson benennen, die jederzeit erreichbar ist. Das BBK erstellt eine Liste der Betreiber kritischer Anlagen.

Für die Unternehmen ist häufig ein größerer Rechercheaufwand erforderlich, um ihre Betroffenheit festzustellen, wenn es überhaupt gelingt. Wir halten daher ein behördliches Self-Assessment-Tool zur Betroffenheitsprüfung für erforderlich. Ein gemeinsames Portal für die Registrierung ist auf jeden Fall hilfreich. Das Portal sollte auch Prüfmöglichkeiten enthalten, anhand derer die Unternehmen ihre Betroffenheit vor der Registrierung als Self-Service einfach selbst überprüfen können.

Es ist allerdings nicht erkennbar, ab wann eine Anlage als kritische Anlage gilt und wie der Betreiber genau von der entsprechenden Einstufung Kenntnis erlangt, wenn es sich nicht um ein Verfahren nach § 8 Abs. 3 in Verbindung mit Abs. 5 handelt. Vor diesem Hintergrund ist unvorhersehbar, ab wann die dreimonatige Frist zur Registrierung greifen würde.

Neben der Fristenfrage müsste für die Registrierung sichergestellt werden, dass eine Registrierung bei einer gemeinsam vom BBK und dem BSI eingerichteten Registrierungsmöglichkeit danach differenziert erfolgen kann, ob eine Anlage nach der Rechtsverordnung nach § 4 oder einer anderweitigen Verfügung als kritisch eingestuft wird. Es muss also klar sein, ob die Registrierung für beide Rechtskreise oder nur nach dem KRITIS-DachG vorgenommen wird. Schließlich wird gemäß BSiG-E § 2 Nr. 22 eine kritische Anlage ausschließlich durch Rechtsverordnung bestimmt.

#### **§ 8 Abs. 7**

Weil die Betreiber einer Anlage Verpflichtungen auf der Grundlage des § 8 nicht belastbar ausschließen bzw. erwarten können, sind die Umsetzungsfristen von neun Monaten (bzgl. § 12) bis zehn Monaten (bzgl. §§ 13, 18 und 20) zu knapp bemessen. Schon mit Blick auf die in der Folgenabschätzung genannten Personalbedarfe von mehreren Mitarbeitenden erscheint der Zeitraum unrealistisch. Solche Stellen müssten erst besetzt werden, bevor

eine operative Tätigkeit möglich ist. Verglichen mit den Regelungen im BSIG scheint deshalb eine Anpassung erforderlich: Dort gelten (§ 39 BSIG-E) Nachweispflichten für Betreiber kritischer Anlagen „frühestens drei Jahre nachdem sie erstmals oder spätestens drei Jahre nachdem sie erneut als ein Betreiber einer kritischen Anlage gelten“ sowie ggf. binnen zwölf Monaten, falls die alte Nachweisfrist für bestehende Betreiber kritischer Anlagen bei Inkrafttreten des Gesetzes innerhalb von zwölf Monaten abgelaufen wäre.

## **§ 12**

Die Pflichten nach dem Gesetz scheinen mit einem hohen bürokratischen Aufwand verbunden zu sein. Die Intervalle (vier Jahre) zwischen den planmäßig durchzuführenden staatlichen Risikoanalysen halten wir für zu lang. Eine vierjährige Aktualisierung wird den sich sehr dynamisch entwickelnden Bedrohungsszenarien sowie den technologischen Rahmenbedingungen und Entwicklungen nicht gerecht.

Die in § 12 Abs. 1 Nr. 2 verlangte Berücksichtigung der Abhängigkeiten „anderer Sektoren [...] in benachbarten Mitgliedstaaten und Drittstaaten“ durch die Betreiber lehnen wir als nicht praktikabel ab. Ohne Zugriff auf die dafür nötigen Informationen können Unternehmen solche Analysen nicht leisten. Wir fordern daher, diese Pflicht zu streichen und entsprechende sektorübergreifende Risikoanalysen als staatliche Aufgabe auszugestalten. Dies entspräche auch der Richtlinie (EU) 2022/2557, welche derartige Pflichten für Betreiber nicht vorsieht.

Vorlagen und Muster für die Risikobewertung durch Betreiber nach § 12 Abs. 3 könnten nützlich sein. Erklärungsbedürftig bleibt im vorliegenden Entwurf allerdings, welche konkreten Anforderungen der § 12 Abs. 1 Nr. 2 dafür begründet. Dies scheint auf eine umfassende Bewertung anhand von Vorketten abzielen (ob der Betreiber solche Vorleistungen bezieht oder für andere kritische Betreiber solche bereitstellt). In der Begründung ist dies nicht weiter erläutert. Die Verpflichtung zur Ermittlung möglicher Risiken durch die Betreiber sollte sich auf direkte (eigene) Risiken der Anlage sowie Inhalte aus den öffentlichen Bewertungen beschränken.

## **§ 13**

In praktischer Hinsicht sind die gesetzlich geforderten Resilienzmaßnahmen mit den bestehenden Strukturen, wenn auch mit erheblich wachsendem materiellem Aufwand, darstellbar. Umso bedauerlicher ist es, dass der Gesetzgeber keine orientierenden Informationen zu den fehlenden Rechtsverordnungen geben kann, die für die Ermittlung des Aufwandes unverzichtbar sind.

Wir regen an, in § 13 Abs. 1 einen ausdrücklichen Bestandsschutz für bereits bestehende Anlagen aufzunehmen. Die Vorgabe, den jeweiligen „Stand der Technik“ einzuhalten, sollte sich auf Neuanschaffungen oder grundlegende Umbauten beziehen. Der Hinweis darauf, dass „insgesamt ein Verhältnismäßigkeitsmaßstab anzuwenden ist“ ist für die konkrete

Beurteilung zu unklar abgegrenzt. Wir fordern einen klaren Bestandsschutz für Fahrzeuge, Trailer und Bestandsdepots. Der Aspekt „Stand der Technik“ sollte auf Neubauten oder wesentliche Umbauten begrenzt werden; flächige Nachrüstpflichten für Flotten sind abzulehnen. Für Bestandsanlagen ist stattdessen ein angemessenes Nachrüstkonzept vorzusehen, das übermäßige Härten vermeidet. Eine solche Änderung ist nötig, um unverhältnismäßige Eingriffe in laufende Betriebe zu verhindern und das gesetzliche Schutzziel dennoch bei technischen Erneuerungen zu erfüllen.

#### **§ 14**

Der Gesetzgeber sollte in § 14 klarstellen, dass Rechtsverordnungen nur im Rahmen der gesetzlich determinierten Grenzen erlassen werden dürfen. Eine Ausweitung von Pflichten über das Gesetz hinaus lehnen wir ab. Rechtsfolgen für die Unternehmen müssen schon im Gesetz auf eine vorab nachvollziehbare Grundlage gestellt werden. Zudem regen wir an, eine Verpflichtung zur Anhörung der Wirtschaftsverbände vor Erlass der Verordnung einzufügen, um Transparenz und Praxistauglichkeit sicherzustellen. Schließlich sollte geprüft werden, die geplante KRITIS-Verordnung mit der bestehenden BSI-KritisV zu harmonisieren oder zusammenzuführen, um Doppelregelungen zu vermeiden und den Ordnungsrahmen verschlankt zu gestalten.

#### **§ 18**

Für bürokratiearme Prozesse sollte nur eine Meldung über das Portal des BSI erforderlich sein, deren Umfang klar definiert werden muss. Es wäre ein klarer Beitrag zu bürokratiearmer Regulierung, wenn Meldeverpflichtungen gegenüber anderen Stellen, die nach derzeitigem Stand bestehen bleiben sollen, und gegenüber dem BKK aufgehoben werden würden. Über das Portal sollten die Meldungen an andere Behörden weitergeleitet werden. Dafür sind effektive technische und organisatorische Prozesse zu definieren und auf ein angemessenes Schutzniveau sensibler Informationen zu achten.

Der Umgang mit den Informationen muss im Sinne des Geheimschutzes erfolgen (analog zu § 5 Abs. 4 und 5 BSIG).

#### **§ 20**

Bemerkenswert ist die zuletzt (im Vergleich zu früheren Entwürfen) neu eingeführte Verpflichtung von Geschäftsleitern. Das folgt dem Beispiel bei der Neufassung der Vorschriften zur Cyberabwehr (Umsetzung von NIS2). Eine solche Regelung wird jedoch in vielen Fällen ins Leere gehen bzw. unbillige Haftungsrisiken für Leiter nationaler Unternehmensteile begründen. In internationalen Konzernunternehmen werden IT-Systeme in der Regel zentral betrieben und überwacht. Nationale Geschäftsleiter haben typischerweise keinen Einfluss auf wesentliche Aspekte des Risikomanagements. Auch bei der Abwehr physischer Gefahren bestehen in der Regel unternehmensweite Standards oder aber es kommen bereits gesetzliche Vorschriften zur Umsetzung (die nach § 4 Abs. 7 des Referentenentwurfs unberührt bleiben). Es erscheint daher sowohl unrealistisch als auch

eigenartig unflexibel, wenn Geschäftsleiter Maßnahmen billigen müssen oder zu überwachen haben, für die eine rechtliche Verpflichtung besteht. Dies ist nach unserer Auffassung die Aufgabe der Aufsichtsbehörde. Desgleichen ist eine undifferenzierte Pflicht der Geschäftsleistungen zur Schulung nach § 20 Abs.2 fragwürdig. Vielmehr beruhen effiziente Unternehmensstrukturen wesentlich auf einer arbeitsteiligen Organisation mit spezialisierten Fachabteilungen. Die Funktion von Geschäftsleitern ist es, diese Fachabteilungen zu steuern. Dieser Aufgabe können sie nicht nachkommen, wenn sie sämtliche spezialgesetzliche Obliegenheiten persönlich nachhalten müssten. Pragmatischer wäre daher allenfalls eine Unterrichtungspflicht als Instrument zur expliziten Einbindung der Unternehmensleitung.

Berlin, im September 2025