STELLUNGNAHME

Berlin, 4. September 2025

Deutsche Industrie- und Handelskammer

Referentenentwurf des Bundesministeriums des Innern eines Gesetzes zur Umsetzung der CER-Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz und weitere)

Wir bedanken uns für die kurzfristige Gelegenheit zur Stellungnahme zu dem o. g. Entwurf.

Staat und Wirtschaft sind gemeinsam gefordert, die Sicherheit der Netze und kritischer Anlagen zu gewährleisten. Einheitliche Maßstäbe zur Verbesserung der Sicherheit, insbesondere kritischer Infrastrukturen, sind von besonderer Bedeutung für das Funktionieren der gesamten deutschen Wirtschaft. Das Gesetz adressiert dieses Anliegen, indem es die physische Sicherheit und Resilienz von Betreibern kritischer Infrastrukturen stärken soll. Es setzt die EU CER-Richtlinie (EU 2022/2557) um und reguliert Betreiber kritischer Anlagen mit zusätzlichen Maßnahmen und Pflichten insbesondere in den Bereichen Business Continuity Management, physische Sicherheit, Risiko- und Krisenmanagement.

Das Wichtigste in Kürze

Die Sicherheit der kritischen Infrastrukturen gewinnt immer mehr an Bedeutung. Insbesondere der russische Angriffskrieg gegen die Ukraine, aber auch zunehmende geopolitische Spannungen haben sicherheitsrelevante Auswirkungen auf Infrastrukturen und Lieferketten. Sind diese ganz oder teilweise nicht verfügbar, drohen Schäden für die gesamte Wirtschaft. Wir stimmen ausdrücklich dem Ziel des Gesetzes zu, die physische Resilienz kritischer Anlagen zu verbessern. Bei der Erhöhung der Resilienz lassen sich physische Sicherheit und die Sicherheit von Daten und Informationen nicht mehr trennen. Sie sollten im Zusammenhang betrachtet werden.

Unternehmen benötigen klare rechtliche Vorgaben, um rechtssicher handeln zu können. Wir verweisen dahingehend auf unserer bisherigen Stellungnahmen aus 2023 und 2024. Unternehmen befürchten weiterhin Doppelregulierungen und Inkonsistenzen, die einer effektiven

und effizienten Umsetzung entgegenstehen. Wünschenswert wäre gewesen, zumindest die beiden oben genannten Referentenentwürfe aufgrund der inhaltlichen Zusammenhänge parallel zur Diskussion zu stellen.

Die Regelungen des KRITIS-Dachgesetzes müssen praktikabel umsetzbar sein und sollten dem Ziel der eigenen Unternehmenssicherheit dienen. Zusätzliche Registrierungs- und Meldepflichten, Fristen und Dokumentationen sollten mit angemessenem Aufwand umsetzbar sein. Die Umsetzung sollte durch unterstützende Maßnahmen und effektive Zusammenarbeitsprozesse zwischen Staat und Wirtschaft flankiert werden. Generell erreichen uns immer wieder Hinweise von Unternehmen, dass die hohe Komplexität der Vorgaben einer wirksamen Umsetzung in der Praxis entgegensteht. Unternehmen wünschen sich verständliche, logisch aufgebaute Regelungen ohne Redundanzen und komplizierte Verflechtungen mit anderen Fachgesetzen.

Insbesondere vor dem Hintergrund, dass zusätzlich zum Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) weitere Aufsichtsbehörden von Bund und Ländern für die Umsetzung verantwortlich zeichnen, die sich untereinander vernetzen müssen, sollten die Prozesse der Zusammenarbeit zwischen den Behörden klar definiert werden. Nur so lassen sich Doppelaufwand für die Unternehmen, z. B. durch Mehrfachmeldungen, verhindern und umgekehrt effektive Warnhinweise an die Unternehmen gewährleisten. Alle Maßnahmen müssen darauf hinwirken, das Schutzniveau der Unternehmen zu verbessern und deren eigene Sicherheitsbemühungen zu unterstützen. Die öffentliche Hand sollte den Unternehmen insbesondere passgenaue Informationen zur aktuellen Sicherheitslage (Cyber- und analoge Bedrohungen) mit konkreten Handlungsempfehlungen zur Verfügung stellen.

Erforderlich wäre ein übergreifendes Gesamtkonzept, das analoge und digitale Sicherheit von Staat, Wirtschaft und Gesellschaft umfassend und gleichermaßen adressiert und in Bezug auf die Belastungen der betroffenen Unternehmen dem Angemessenheitsprinzip Rechnung trägt. Der Grundgedanke muss eine Partnerschaft auf Augenhöhe zwischen allen Akteuren sein. Eine aus einem solchen Gesamtkonzept abgeleitete KRITIS-Resilienzstrategie – die eigentlich Grundlage dieses Gesetztes sein müsste – soll jedoch erst bis zum 17. Januar 2026 durch die Bundesregierung verabschiedet werden. Die im Entwurf skizzierte Chronologie der Umsetzungserfordernisse ist eine Herausforderung, die leicht aus dem Takt kommen kann – insbesondere durch die nötigen Abstimmungen zwischen BBK, BSI sowie weiteren Behörden auf Bundesebene und auf Ebene der Bundesländer.

Unterschiedliche Auslegungen durch Landesbehörden müssen vermieden werden. Die überwiegende Zahl der Unternehmen spricht sich deutlich für eine bundesweit einheitliche Zuständigkeit aus. Insbesondere in Krisensituationen ist eine einheitliche Anlauf- und Meldestelle

eine wesentliche Entlastung für betroffene Betreiber, um Kommunikations- und Abstimmungsaufwand zu minimieren.

Im Einzelnen

Behördenzuständigkeit und Zusammenarbeit der Behörden (§ 3)

Das BBK ist zuständige Behörde im Hinblick auf Aufgaben des Bundes. Vorgesehen ist, dass neben weiteren Sektorbehörden des Bundes auch Behörden der Länder für bestimmte Betreiber, Dienstleistungen und Sektoren zuständig sind.

Die Einbeziehung der Länder in die Umsetzung stößt bei den Unternehmen auf geteiltes Echo. So steht einer weniger häufig vermuteten größeren Nähe zu den Unternehmen, und damit einfacheren Austausch- und Kooperationsprozessen, die vielfach geäußerte Befürchtung gegenüber, dass die Zuständigkeit unterschiedlicher Landesbehörden auch zu unterschiedlicher Behördenpraxis führen wird. Sofern die beabsichtigte Teilung der Zuständigkeiten zwischen Bundes- und Länderbehörden beibehalten wird, ist sie so auszugestalten, dass klare Zuständigkeiten definiert werden und vor allem eine bundesweit einheitliche Handhabung gewährleistet ist.

Betroffenheit von Unternehmen (§§ 4, 5)

Betreiber müssen ihre kritischen Anlagen selbst identifizieren. Eine Anlage gilt grundsätzlich dann als kritisch, wenn sie den Sektoren Energie, Transport und Verkehr, Finanzwesen, Sozialversicherung, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung zuzuordnen ist und bestimmte Schwellenwerte erreicht oder überschreitet. Dabei gilt grundsätzlich der Regelschwellenwert von 500.000 zu versorgenden Einwohnern. Hier sind Flexibilisierungen vorgesehen. Auch kleinere Einrichtungen unterhalb des Regelschwellenschwertes sollen nach Ansicht des Gesetzgebers unter bestimmten Bedingungen unter das KRITIS-Dachgesetz fallen können. Die Anlagenarten, Schwellenwerte etc. sollen durch eine Verordnung konkretisiert werden, die noch nicht vorliegt. Bei der Festlegung der Anlagenkategorien will man sich an der etablierten Praxis der derzeitigen BSI-Kritisverordnung anlehnen.

Die Unternehmen benötigen frühzeitig Rechtssicherheit. Es muss einfach zu beurteilen sein, ob sie vom KRITIS-Dachgesetz und/oder NIS2UmsuCG betroffen sind, und welche Pflichten sich für sie ergeben. Wesentliche Inhalte, die über die Betroffenheit bestimmen, werden in nachrangige Rechtsakte mit geringeren Beteiligungsmöglichkeiten für die Wirtschaft verlagert. Die konkretisierenden Rechtsverordnungen sollten zeitnah verabschiedet werden. 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.

Positiv ist, dass die Systematik zur Bestimmung kritischer Anlagen grundsätzlich beibehalten werden soll (§ 4 Abs 1). Zwar wurde im KRITIS-Dachgesetz der Schwellwert von 500.000 zu versorgenden Einwohnern gesetzt. Diese Systematik wird jedoch „aufgebrochen", wenn Behörden nach entsprechendem Ermessen zukünftig einseitig die Identifizierung als Betreiber kritischer Anlagen vornehmen können (§ 4 Abs 2). Hierfür maßgebliche Kriterien sind zwar im Entwurf aufgeführt, werden jedoch teilweise nicht näher eingegrenzt, zum Beispiel „Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten" (Nummer 3) oder der „Marktanteil des Betreibers" (Nummer 4). Hier bräuchte es nachvollziehbare und angemessene Kriterien.

Registrierung kritischer Anlagen (§ 8)

Die Betreiber kritischer Anlagen sollen diese spätestens drei Monate nach Erfüllung der Betroffenheitskriterien über ein gemeinsames Online-Meldeportal von BBK und BSI registrieren und eine Kontaktstelle bzw. Ansprechperson benennen, die jederzeit erreichbar ist.

Das Portal sollte auch Prüfmöglichkeiten enthalten, anhand derer die Unternehmen ihre Betroffenheit vor der Registrierung als Self-Service einfach selber überprüfen können. Bestehende Registrierungen nach BSIG sollten im Sinne des Once-only Prinzps für die Registrierungen nach KRITIS-Dachgesetz ohne erneute Registrierung anerkannt und übernommen werden. Insbesondere die Angabe sensibler Informationen, etwa zum Standort kritischer Anlagen, erhöht das Risiko für die unberechtigte Einsicht in solche Informationen. Die Datenübermittlung und -speicherung sollte nach Stand der Technik sicher und vollautomatisiert erfolgen.

Nationale Risikoanalysen und Risikobewertungen der Unternehmen (§§ 11, 12)

Die jeweils zuständigen Bundes- und Landesministerien müssen im Bedarfsfall, mindestens jedoch alle vier Jahre Risikoanalysen und -bewertungen durchführen. Das BMI legt dafür methodische und inhaltliche Vorgaben durch Rechtsverordnung fest, wertet die Risikoanalysen und -bewertungen sektorenübergreifend aus und das BBK stellt relevante Teile den Betreibern, Länder- und Bundesbehörden zur Verfügung. Die Betreiber wiederum müssen auf dieser Grundlage und weiterer Informationen erstmals zum 17. Juli 2026 und dann mindestens alle vier Jahre eigene Risikoanalysen durchführen. Auch dafür erlässt das BMI eine Rechtsverordnung. Es kann die Ermächtigung zum Erlass der Rechtsverordnung auf das BBK übertragen.

Der Ansatz einer doppelten Risikoanalyse und Risikobewertung aus staatlicher und darauf aufbauend aus unternehmerischer Perspektive ist grundsätzlich unterstützenswert.Unternehmen sind darauf angewiesen, dass der Staat seine Informationen dazu mit der Wirtschaft teilt, auch um den Bedarf angemessener staatlicher und privater Schutzmaßnahmen zu erkennen. Eine

vierjährige Aktualisierung wird den sich sehr dynamisch entwickelnden Bedrohungsszenarien sowie den technologischen Rahmenbedingungen und Entwicklungen nicht gerecht. Insofern ist eine Initiierung „im Bedarfsfall“ richtig. Es stellt sich allerdings weiterhin die Frage, was genau damit gemeint ist.

Resilienzpflichten und Resilienzplan der Betreiber kritischer Anlagen (§ 13)

Die Betreiber kritischer Anlagen müssen auf Basis der Risikoanalysen und -bewertungen Resilienzmaßnahmen nach dem Stand der Technik umsetzen. Dabei ist ein „Verhältnismäßigkeitsmaßstab“ anzuwenden. Die Umsetzungsfrist dafür beträgt 10 Monate nach ihrer Registrierung. Im Entwurf sind entsprechende Maßnahmen aufgelistet. Die Betreiber müssen die Maßnahmen in einem Resilienzplan darstellen, in dem die Erwägungen bei der Auswahl der Maßnahmen und Risikoanalysen dargelegt werden. Das BBK stellt bis zum 17. Januar 2026 Vorlagen und Muster für Resilienzpläne auf seiner Internetseite bereit.

Positiv ist, dass das BBK zur Unterstützung der Betreiber Vorlagen und Muster zur Verfügung stellen wird. Ergänzende Hinweise beispielsweise zu der Frage, wie die Redundanz in den Lieferketten sinnvollerweise aussehen soll, sind sicherlich hilfreich. So ist beispielsweise die Einführung komplexer Scada-Systeme zur Steuerung von Energienetzen aufwändig und langwierig. Es sollte nicht gemeint sein, dass die Unternehmen auch in solchen Fällen schnell den Lieferanten insgesamt wechseln können müssen. Für andere Sektoren wie die Medizintechnik gilt dies gleichermaßen. Eine praxisgerechte Forderung nach Redundanz sollte bedeuten, dass ein ersatzbedürftiges Teilsystem entweder offen ist für Reparaturen/Anpassungen, oder aber, dass es an den kritischen Punkten durch eine andere Teil- oder Zwischenlösung überbrückt werden können muss.

Unternehmen schätzen die 10-Monatsfrist zum Treffen geeigneter Resilienzmaßnahmen als zu kurz ein. Bereits Beschaffungsprozesse für eventuelle Komponenten und Systeme können hier länger dauern. Eine 2-Jahresfrist entspricht den praktischen Bedingungen eher.

Mindestanforderungen; branchenspezifische Resilienzstandards (§ 14)

Sektorübergreifende Mindeststandards kann das BMI erlassen, sektorspezifische Mindestvorgaben die jeweils zuständigen Behörden. Betreiber kritischer Anlagen oder ihre Branchenverbände können branchenspezifische Resilienzstandards zur Konkretisierung der Verpflichtungen vorschlagen. Das BBK stellt in Abstimmung mit den zuständigen Behörden fest, ob die branchenspezifischen Resilienzstandards geeignet sind, und veröffentlicht diese auf seiner Internetseite. Vorgesehen ist außerdem, dass Bundesländer branchenspezifische Resilienzstandards erlassen können, wenn bis zum 01.01.2030 noch keine Resilienzstandards für einzelne Sektoren durch das BBK anerkannt wurden.

Unternehmen kritisieren einhellig den Ansatz , dass Landesbehörden nach Verstreichung der Frist branchenspezifische Anforderungen an die Betreiber definieren. Sie befürchten, dass aufgrund von Uneinigkeiten zwischen Bund und Bundesländern rechtsunsicherheiten entstehen oder sich ein Flickenteppich regional unterschiedlicher Regelungen bildet. Dies würde z. B. auch die Zulieferer von IT-Dienstleistungen für KRITIS-Betreiber betreffen, weil daraus unterschiedliche Anforderungen an Softwarelösungen je nach Bundesland resultieren können, was den Komplexitätsgrad dieser Lösungen – und damit die Kosten – enorm erhöhen würde. Die Regelung zu länderspezifischen Branchenstandards sollte daher gestrichen werden.Die Veröffentlichung „branchenspezifischer Resilienzstandards“ durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe „auf Antrag“ erleichtert betroffenen Unternehmen die Umsetzung der geforderten Maßnahmen. Der Begriff „auf Antrag“ ist hier offen gehalten: Um dem Ziel der Transparenz zu dienen, sollte dieser „Antrag“ durch die in Absatz 2 genannten „Betreiber kritischer Anlagen oder ihre Branchenverbände“ formlos gestellt werden können.

Nachweise (§ 16)

Betreiber müssen die Umsetzung der Resilienzmaßnahmen auf Nachfrage gegenüber der jeweils zuständigen Behörde nachweisen. Dabei sollen auch bereits aufgrund anderer gesetzlicher Vorgaben (z. B. BSIG, EnWG) erbrachte Nachweise anerkannt werden.

Diese Praxisorientierung unterstützen wir. Entscheidend ist hier grundsätzliche die Zusammenarbeit zwischen Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Zwar kann das BBK das BSI z. B. um Übersendung bereits für NIS2 eingereichter Nachweise ersuchen, aber die beiden Behörden können gegebenenfalls zu unterschiedlichen Bewertungen kommen. Dann müsste das betroffene Unternehmen sowohl mit BSI als auch BBK nach Lösungen suchen.

Meldungen von Vorfällen (§ 18)

Betreiber kritischer Anlagen müssen Vorfälle unverzüglich an eine vom BBK und BSI eingerichtete gemeinsame Meldestelle melden. Eine Erstmeldung soll bis spätestens 24 Stunden nach Kenntnis des Vorfalls erfolgen und spätestens einen Monat danach ein ausführlicher Bericht abgeben werden. Das BBK veröffentlicht Details zum Meldeverfahren und den Inhalten der Meldungen auf seiner Internetseite. Es übermittelt den zuständigen Aufsichtsbehörden von Bund und Ländern Auswertungen zu Meldungen von Vorfällen. Sofern ein „öffentliches Interesse“ besteht, kann das BBK nach Anhörung des Betreibers die Öffentlichkeit informieren oder den Betreiber verpflichten, dies zu tun.

Bereits bestehende Meldeverpflichtungen der Betreiber gegenüber anderen Stellen sollen nach dem Willen des Gesetzgebers bestehen bleiben. Für bürokratiearme Prozesse sollte nach Ansicht der DIHK nur eine Meldung über die gemeinsame Meldestelle erforderlich sein. Zu prüfen wäre deshalb, inwiefern auch bereits bestehende Meldeverpflichtungen gegenüber

anderen Stellen über dieses Meldeportal abgewickelt werden können. Für die Weiterverteilung der Informationen an andere Behörden sind effektive technische und organisatorische Prozesse zu definieren und auf ein angemessenes Schutzniveau sensibler Informationen zu achten. Unternehmen regen an, hier zu definieren, dass der Umgang mit den Informationen im Sinne des Geheimschutz erforderlich ist.

Die Meldungen von Sicherheitsvorfällen müssen so aufbereitet werden, dass nicht nur an den von einem Vorfall betroffenen Betreiber „sachdienliche Folgeinformationen“, z. B. Leitlinien, übermittelt werden (§ 18 Abs 6), sondern weitere potenziell gefährdete Betreiber kritischer Dienstleistungen gezielte Warn- und Umsetzungshinweise erhalten. Wir verweisen an dieser Stelle auf unsere Ausführungen zum Entwurf vom Sommer 2023: Die meldenden Unternehmen erwarten, dass sie auch einen konkreten Mehrwert im Sinne eines „Rückkanals“ haben, indem sie zielgerichtet aktuelle Informationen zur Gefährdungslage und Handreichungen erhalten.

Unterstützung der Betreiber kritischer Anlagen (§ 19)

Positiv ist, dass das BBK Betreibern kritischer Anlagen Vorlagen, Muster und Leitlinien für die Umsetzung zur Verfügung stellt und dass es auch Beratungen, Schulungen und Übungen anbieten kann.

Geschäftsleiterverantwortung (§ 20)

Geschäftsleitungen werden verpflichtet, die Resilienzmaßnahmen umzusetzen und die Umsetzung durch geeigente Organisationsmaßnahmen sicherzustellen.

Die Pflicht zur ordnungsgemäßen Unternehmensleitung umfasst grundsätzlich auch physische Maßnahmen zur Sicherheit. Insofern ist die Verankerung der Verantwortung für die Resilienzmaßnahmen in der Unternehmensführung im Gesetzentwurf grundsätzlich richtig – aber nicht erforderlich. Eine Orientierung an allgemeinen Grundsätzen wird als ausreichend erachtet.

Ausnahmebescheid (§ 17)

Vor allem für Sicherheitsbehörden gibt es Abweichungen und Ausnahmebescheide zu den Maßnahmen.

Die Herausnahme der o. g. Stellen aus dem Geltungsbereich des Gesetzes ist nachvollziehbar, wenn bereits vergleichbare Vorgaben bestehen. Allerdings sollten Störungen entweder auch durch diese Stellen an das zentrale Portal gemeldet werden, oder sichergestellt werden, dass die relevanten Informationen dazu ebenfalls dem BBK zur Verfügung gestellt werden, um ein umfassendes Lagebild für die Betreiber kritischer Infrastrukturen zu generieren.

Ansprechpartnerin

Dr. Katrin Sobania, sobania.katrin@dihk.de, Tel. 030/20308-2109

Wer wir sind:

Unter dem Dach der Deutschen Industrie- und Handelskammer (DIHK) sind die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich die DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein.

Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zu gemeinsamen Positionen der Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Grundlage dieser Stellungnahme sind die der DIHK bis zur Abgabe der Stellungnahme zugegangenen Äußerungen der IHKs sowie die wirtschaftspolitischen/europapolitischen Positionen sowie insbesondere die Beschlüsse des DIHK Vorstandes vom 27. Juni 2018 „Daten- und Informationssicherheit – Vertrauen nachhaltig gewährleisten“ und des DIHK-Präsidiums vom 22. Juni 2023 „Netze – Lebensadern der Wirtschaft: Netzausbau in Deutschland bedarfsgerecht, sicher und nachhaltig gestalten“. Sollten der DIHK noch weitere in dieser Stellungnahme noch nicht berücksichtigte relevante Äußerungen zugehen, wird die DIHK diese Stellungnahme entsprechend ergänzen.