Stellungnahme

zum Referentenentwurf des BMI: Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie (EU 2022/2557) und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz)

24.08.2023

Das Deutsche Verkehrsforum begrüßt grundsätzlich den Referentenentwurf zum KRITIS-Dachgesetz, den das Bundesinnenministerium am 27. Juli 2023 vorlegte. Das Gesetz verfolgt den „All-Gefahrenansatz“ und adressiert damit sowohl Naturkatastrophen als auch vom Menschen verursachte, unbeabsichtigte oder vorsätzliche Gefährdungen. Es nimmt vor allem den Schutz kritischer Infrastrukturen im physischen Bereich in den Blick und soll als Ergänzung des bereits vorliegenden IT-Sicherheitsgesetzes (BSIG) dienen. Die Beurteilung des Gesetzentwurfes ist zum aktuellen Zeitpunkt nur eingeschränkt möglich, weil die angekündigte Rechtsverordnung zur Bestimmung Kritischer Anlagen noch nicht vorliegt.

Detaillierte Bewertung:

Trotz vieler positiver Ansätze bittet das Deutsche Verkehrsforum, den Entwurf des KRITIS-Dachgesetzes in einigen Punkten präziser zu formulieren.

§ 2 Begriffsbestimmungen

Die Definitionen und Vorgaben der verschiedenen gesetzlichen Regelungen müssen harmonisiert werden. Beim Vergleich des Entwurfs zum KRITIS-Dachgesetz mit dem IT-Sicherheitsgesetz und der CER-Richtlinie sind die Begriffe nicht einheitlich und teilweise widersprüchlich. So heißt es im KRITIS-Dachgesetz, dass Kritische Infrastrukturen „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen“ umfassen. Laut BSIG sind kritische Infrastrukturen „Einrichtungen, Anlagen oder Teile davon. Diese müssen bestimmten Sektoren zugeordnet sein und eine hohe Bedeutung für das Funktionieren des Gemeinwesens haben“. Die CER-Richtlinie definiert hingegen kritische Infrastrukturen als „Objekte, Anlagen, Ausrüstung, Netze oder Systeme oder Teile eines Objekts, einer Anlage, Ausrüstung, eines Netzes oder eines Systems, die für die Erbringung eines wesentlichen Dienstes erforderlich sind“.

Unter den Begriffsbestimmungen wird zwischen „Risikoanalysen“ und „Risikobewertungen“ unterschieden. Dies deckt sich nicht mit dem englischen Text der CER-Richtlinie, in der lediglich von „Risk Assessment“, also der „Risikobeurteilung“ gesprochen wird, so wie es auch in Normen, darunter ISO 31000, ISO 27001 und BSI-200, der Fall ist. So sollte auch im KRITIS-Dachgesetz allein der Begriff „Risikobeurteilung“ verwendet werden. Er deckt unserer Ansicht nach den Prozess von Identifikation, Analyse und Bewertung ab. Bei der Umsetzung von Maßnahmen sollte der Begriff „Risikobehandlung“ verwendet werden.

Wenig nachvollziehbar ist, dass unter Nr. 11 „Besonders wichtige Einrichtungen“ die Logistik genannt wird, die aus europäischer Sicht nicht als eigenständige kritische Kategorie erachtet wird. So sollte die Logistik in Deutschland nicht als eigenständiger Sektor, sondern, wie in der BSI-Kritisverordnung

für bestimmte KRITIS-Bereiche bereits geschehen, innerhalb der weiteren Sektoren eingestuft werden.

§ 3 Nationale zuständige Behörde für die Resilienz kritischer Anlagen

Der Referentenentwurf zum KRITIS-Dachgesetz nennt das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) als zuständige Behörde und zentrale Anlaufstelle. Andere Behörden unterstützen Betreiber kritischer Infrastrukturen oder übermitteln dem BBK erforderliche Informationen über Sicherheitsrisiken.

Wenig verständlich erscheint, dass neben dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine zweite Aufsichtsbehörde geschaffen werden soll. Es besteht die Gefahr konkurrierender Auslegungen gesetzlicher Grundlagen, vor allem in Bereichen, in denen sich die Zuständigkeiten überschneiden. Ein Beispiel:

> Ein physischer Zaun ist mit Sensoren ausgestattet, die sowohl ein Durchschneiden (1) als auch ein Überklettern (2) detektieren. Als Reaktion auf 1 oder 2 werden Kameras in dem Bereich und zusätzlich ein AI-Drohnenschwarm aktiviert. Diese beobachten die Verdächtigen, bis die Wasserschutzpolizei eintrifft. Frage: Welche Aufsichtsbehörde ist für welchen Teil des Szenarios verantwortlich, welche auditiert welche Systeme?

Um zusätzliche bürokratische Abläufe und Unklarheit bei den Zuständigkeiten in Sicherheits- und Regulierungsfragen zu vermeiden, sollte es eine enge Abstimmung und Zusammenarbeit zwischen den Behörden wie Bundesministerium für Digitales und Verkehr und, Bundesinnenministerium sowie allen relevanten Oberen Bundesbehörden (BBK, BSI oder Bundesnetzagentur) geben. Zuständigkeiten müssen klar definiert sein. Im besten Fall entscheidet sich der Gesetzgeber für eine zentrale Aufsichtsbehörde.

§ 4 Kritische Anlagen

Der Gesetzentwurf ist hinsichtlich der Benennung von Kriterien zur Identifizierung kritischer Anlagen unvollständig. Statt Rahmenbedingungen klar aufzuführen, beispielsweise bei der Versorgungssicherheit die Betroffenheit von 500.000 Mitbürgerinnen und Mitbürgern oder die Wiederanlaufmöglichkeiten in der Energieversorgung zu nennen, verweist der Entwurf auf eine Rechtsverordnung, die erst später vorliegen wird. Wichtig an dieser Stelle ist, nicht nur Unternehmen, sondern auch die öffentliche Bundesverwaltung einzubeziehen. Auch hier sollte ein Schwellenwert von 500.000 Betroffenen gelten. Das gilt vor allem für das BBK selbst, das im Falle einer Krise das weitere Vorgehen koordinieren muss.

Nach Auffassung des Deutschen Verkehrsforums sollte sich der Gesetzgeber an den Vorgaben der CER-Richtlinie orientieren, welche kritischen Anlagen in den Anwendungsbereich des KRITIS-Dachgesetzes fallen. Der vorliegende Entwurf gibt mit Blick auf die konkretisierende Rechtsverordnung nach § 15 nur den Hinweis, dass sich diese „systematisch und inhaltlich“ an der BSI-Kritisverordnung orientieren soll. Unklar ist, welche Kriterien künftig gelten sollen.

§ 7 Kritische Anlagen von besonderer Bedeutung für Europa

In Abs. 1 Nr.2 heißt es, dass „eine Anlage als kritische Anlage von besonderer Bedeutung für Europa gilt, wenn sie „für oder in sechs oder mehr Mitgliedstaaten der Europäischen Union die gleiche oder

ähnliche Dienstleistung gemäß der „Liste wesentlicher Dienste“ (Delegierte Verordnung vom 25.07.2023 Ergänzung der Richtlinie (EU)2022/2557) des Europäischen Parlaments und des Rates durch eine Liste wesentlicher Dienste) der Europäischen Kommission erbringt“. Hier gilt es, genauer zu formulieren. Nicht die erbrachte Dienstleistung in mindestens sechs Mitgliedstaaten darf Kriterium sein, sondern die Überschreitung von Schwellenwerten. In Deutschland gilt als Richtwert eine Betroffenheit von 500.000 Personen.

§ 9 Nationale Risikoanalysen und Risikobewertungen und § 10 Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen

Beim Thema Risikobetrachtung sollte nur die Versorgungssicherheit als Kriterium herangezogen werden. Sektorspezifische nationalen Risikoanalysen sind zu begrüßen, um die Besonderheiten des jeweiligen Sektors berücksichtigen zu können. Hier wünschen wir uns eine starke Einbindung der Wirtschaftsverbände, um die Unternehmenssicht darstellen zu können.

Sollten durch nationale Analysen und Bewertungen bestimmte Risiken identifiziert sein, ist es für Betreiber kritischer Anlagen schwierig, diese in ihre Resilienzpläne aufzunehmen. Beispiele sind Sabotage oder Bedrohungen von terroristischen Vereinigungen. In diesen Fällen sollten Bund und Länder Maßnahmen entwickeln, um Betreiber kritischer Anlagen und/oder kritischen Anlagen zu schützen.

Nach Ansicht des Deutschen Verkehrsforums ist es wichtig, eine zeitliche Abfolge für Risikoanalysen festzulegen. Danach sollten zunächst die nationalen Analysen vorliegen, bevor Betreiber kritischer Anlagen ihre Betrachtungen erstellen. Erst danach können Maßnahmen identifiziert werden, um den Risiken entgegenzuwirken. In einem weiteren Schritt müssen sie implementiert und ihre Implementierung nachgewiesen werden. Nachweispflichten sollten gemäß internationalen Standards alle drei Jahre erbracht werden.

§ 11 Resilienzmaßnahmen der Betreiber kritischer Anlagen

Das Deutsche Verkehrsforum weist darauf hin, dass in dem Entwurf des § 11 KRITIS-Dachgesetz ein Bestandsschutz berücksichtigt werden muss. Die Formulierung in Absatz 1 „Dabei soll der Stand der Technik eingehalten werden.“, kann zu umfangreichen Nachrüstpflichten mit förderrechtlichen Problemen führen. Es können für Betreiber kritischer Anlagen somit ein unverhältnismäßig zusätzlicher Aufwand und zusätzliche Investitionen entstehen. In diesem Zusammenhang ist es wichtig zu erwähnen, dass der Finanzierungsbedarf, der durch das KRITIS-Dachgesetz entsteht, näher zu beziffern ist. Daraus ergibt sich ein besonderer Förderbedarf für Unternehmen, die in den Schutz ihrer Anlagen investieren müssen. Ein Beispiel:

> Der Hamburger Hafen liegt in der Mitte der nördlichen und südlichen Stadtteile der Freien und Hansestadt Hamburg, das Hafengebiet umfasst 7.145 Hektar. Sowohl auf der A1 als auch auf der A7 findet Güterverkehr in und aus dem Hafengebiet heraus statt. Würde man zu Kontrollzwecken den physischen Zugang zu dem gesamten Hafengebiet abriegeln, wäre ein erheblicher Investitionsaufwand in die Verkehrsinfrastruktur notwendig, um einen Verkehrskollaps zu verhindern. Selbst wenn man nur mit Sensoren und Transpondern in den Lkw arbeiten würde, wäre eine zumindest stichprobenartige Kontrolle der Lkw notwendig. Dies würde zu erheblichen Rückstauungen führen, die von der vorhandenen Verkehrsinfrastruktur nicht abgefangen werden könnten.

Beim Thema Zuverlässigkeitsüberprüfungen sind Unternehmen unter anderem aufgrund des Datenschutzes die Hände gebunden. So ist eine Überprüfung von Personal externer Dienstleister nicht möglich. § 11 sollte so angepasst werden, dass sich Zuverlässigkeitsüberprüfungen auf künftiges Personal, nicht jedoch auf die bestehende Belegschaft erstrecken sollte.

In § 11 Absatz 6 sollte auch der Zeitraum genauer definiert werden, in dem ein Resilienzplan erstellt werden muss. Der Begriff Resilienzplan ist zudem noch genauer zu definieren und gegebenenfalls in § 2 Begriffsbestimmungen aufzunehmen. Wichtig ist dabei festzulegen, ob es sich in dem Plan um Maßnahmen handeln muss, die bereits implementiert sind oder künftig implementiert werden sollen oder ob beides gemeint ist. Bei der erstmaligen Registrierung einer kritischen Anlage ist zu beachten, dass realistische Fristen festgelegt werden und auch die Reihenfolge wie bereits weiter oben erwähnt, eingehalten wird, d. h. erst eine nationale, dann eine betriebliche Risikoanalyse, die Erstellung des Resilienzplans und die Umsetzung. Internationaler Standard sind Nachweisezyklen alle drei Jahre.

§12 Meldewesen für Störungen

Bei Meldungen von Störungen sollte der Grundsatz „Ein Vorfall – eine Meldung“ gelten. Darüber hinaus ist zwar eine gemeinsame Meldestelle von BBK und BSI geplant, der Informationsfluss geht aber nur in eine Richtung von Betreibern kritischer Infrastrukturen zu Behörden. Doch dies darf keine Einbahnstraße sein, auch umgekehrt müssen Informationen über nationale und europäische physikalische Störungen, Bedrohungen und Risiken vom BBK an die Betreiber fließen, damit sie ihre Aufgabe erfüllen können. Hier sollte sich das KRITS-Dachgesetz am BSIG und dem NIS2UMsuCG orientieren, wo dieser Sachverhalt geregelt ist.

§ 15 Ermächtigung zum Erlass von Rechtsverordnungen

Bei der Erarbeitung der Rechtsverordnung sollten Wirtschaftsverbände aller Sektoren frühzeitig einbezogen werden, zumal es dabei um die Festlegungen als kritische Anlagen geht. Das Deutsche Verkehrsforum bietet seine Mitarbeit unter Einbindung seiner rund 170 Mitgliedsunternehmen an.

Wir wären Ihnen sehr dankbar, wenn Sie unsere Anmerkungen im weiteren Gesetzgebungsverfahren und in der Ressortabstimmung berücksichtigen könnten.

***