



Bundesverband

ASW-Positionspapier

Zusammenarbeit stärkt Resilienz

Referentenentwurf KRITIS-Dachgesetz

Vorbemerkung

Kritische Infrastrukturen sind für unsere Gesellschaft unverzichtbar. Ihre Verfügbarkeit ist elementar für die Handlungsfähigkeit staatlicher Institutionen und gleichermaßen Grundlage für Wirtschaftsleistung und gesellschaftliches Agieren. Der ASW Bundesverband begrüßt deshalb den Entwurf zur Umsetzung der EU-CER-Richtlinie und damit die Bemühung, einen verbindlichen Rahmen zur Stärkung der Resilienz Kritischer Infrastrukturen zu setzen.

Im März 2023 veröffentlichte der ASW Bundesverband bereits ein Positionspapier zu den vom Bundeskabinett verabschiedeten Eckpunkten zum KRITIS-Dachgesetz (KRITIS-DachG). Gerne verweisen wir auf unsere dort vortragene Positionierung.

Im Folgenden nehmen wir Stellung zum zweiten vorgelegten Referentenentwurf vom 21.12.2023, in dem wir inhaltliche Anpassungen als notwendig erachten. Hierzu haben wir konkrete Vorschläge und Kommentare in den Referentenentwurf eingearbeitet, diese sind dem Positionspapier beigelegt. Darüber hinaus lassen sich folgende zentrale Handlungsempfehlungen herausstellen:

1. Stärkere Einbindung der Wirtschaft und Einrichtung einer Sicherheitskommission

Der ASW Bundesverband empfiehlt, den Entwurf zum KRITIS-DachG, unter Einbeziehung der Fachexpertise der Wirtschaft, zumindest in Teilen, zu ändern. Eine enge Abstimmung und Verzahnung mit der Wirtschaft sowie den Partnerverbänden der Initiative Wirtschaftsschutz zu allen sicherheitspolitischen Fragestellungen und des Wirtschaftsschutzes ist aus Sicht des ASW Bundesverbandes unabdingbar.

Vernetzte Sicherheit ist nicht nur Schlüsselfaktor bei der Schaffung einer Sicherheitsarchitektur, die den Herausforderungen des 21. Jahrhunderts gerecht wird. Vielmehr ist sie wesentlicher Meilenstein für ein kohärentes System zum Schutz Kritischer Infrastrukturen. Eine intensivierte Zusammenarbeit von Staat und Wirtschaft fördert Effektivität und Effizienz von Maßnahmen zur Resilienz Steigerung sowie die Reduktion von Komplexität. Zudem trägt sie zur Vermeidung von Redundanzen bei der Aufgabenverteilung und Entscheidungsfindung bei. Das gilt beispielsweise auch in Bezug auf die geplanten „Mindestschutzstandards“ bzw. bei der Etablierung von „branchenspezifischen Resilienz Standards“.

In diesem Zusammenhang erkennt der ASW Bundesverband das Primat der Politik zur Gesetzgebung uneingeschränkt an. Dennoch ist es essenziell, auch in regulatorischen Vorhaben auf die Expertise der Wirtschaft und seiner Unternehmen zurückzugreifen. Wirtschaftsschutz ist eine interdisziplinäre Gemeinschaftsaufgabe. Diesem Anspruch folgend, spielen Staat und Wirtschaft gleichermaßen eine elementare Rolle in dem komplexen Spannungsfeld von physischen und digitalen Bedrohungen oder Risikofeldern. Eine robuste Sicherheitspartnerschaft von Staat und Wirtschaft in Form kontinuierlicher Zusammenarbeit und eines transparenten Austausches ist Grundvoraussetzung für die erfolgreiche und zukunftsorientierte Umsetzung von Resilienz Strategien. In diesem Zusammenhang verweisen wir auf den Vorschlag aus dem ASW-Positionspapier vom 28. März 2023 – Einrichtung einer Sicherheitskommission als beratendes Organ für alle regulatorischen Vorhaben.

Explizit erbittet der ASW Bundesverband zudem eine Einbeziehung in die einheitliche und eindeutige Festlegung/Klassifizierung der zu schützenden Kritischen Infrastrukturen, die für alle Behörden und Zuständigkeitsbereiche (Bund, Länder, Kommunen sowie Sektoren) gilt. Eine Festlegung/Klassifizierung der kritischen Anlagen wird beispielsweise in § 4 KRITIS-DachG-RefE aufgenommen. Nach Auffassung des ASW Bundesverbandes sind

diese jedoch nicht konkret genug, sprich die Fragestellung, welche kritischen Anlagen hierunter fallen, bestimmt sich laut des Entwurfes nach einer zukünftig zu erlassenden Rechtsverordnung (§ 15 KRITIS-DachG-RefE). Um Handlungssicherheit für alle Betreiber Kritischer Infrastrukturen zu gewährleisten, wird eine schnellstmögliche und mit der Wirtschaft abgestimmte Umsetzung der zu erlassenden Rechtsverordnung sowie die Bezugnahme auf den Anhang der EU-Rechtsverordnung mit der Benennung der Sektoren, Teilsektoren und Arten von Einrichtungen vorgeschlagen.

2. Ressourcenaufwand der zentralen Anlaufstelle

Gemäß §3 wird das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) als national zuständige Behörde gemäß Artikel 9 Abs. 1 Satz 1 der CER-Richtlinie und als zentrale Anlaufstelle nach Artikel 9 Abs. 2 benannt. Der ASW Bundesverband begrüßt ausdrücklich die Etablierung einer zentralen Anlaufstelle im BBK. Es ist zu unterstellen, dass das BBK sowie alle involvierten staatlichen Stellen (Ressorts), eine entsprechende Ressourcenplanung vornehmen.

Der ASW Bundesverband spricht sich in diesem Kontext dafür aus, neue Kooperationsmodelle (Staat, Wirtschaft und Forschung) zu diskutieren und bereits bestehende zu stärken. Dies ergeht bereits aus dem Vorschlag des ASW-Positionspapiers vom 28. März 2023 (Einrichtung einer Sicherheitskommission als Berater für alle regulatorischen Vorhaben). Der enge Schulterschluss zwischen Staat, Wirtschaft und auch Forschung sowie ein damit verbundenes Schnittstellenmanagement sind elementar. Das gilt insbesondere vor dem Hintergrund weitreichender Veränderungen der nationalen und globalen Sicherheitslage durch hybride Bedrohungsszenarien, die sowohl Staat und Wirtschaft zunehmend vor besondere Herausforderungen stellen. Die Hebung von Synergien durch Konsolidierung von Expertise und Ressourcen (Public-Private Partnerships) spielt hier eine entscheidende Rolle. Durch eine solche Vorgehensweise könnten Erfüllungsaufwände sowie Bürokratiekosten erheblich gesenkt, die Akzeptanz von Regulierungen erhöht sowie Umsetzungszeiten verkürzt werden.

3. Verbindliche Festlegungen zum Schutz sensibler Daten

Aus Sicht des ASW Bundesverbandes handelt es sich bei der folgenden Information im KRITIS-DachG um sensible, die innere Sicherheit betreffende, und daher schützenswerte Informationen:

- §9 – Nationale Risikoanalyse und Risikobewertung
- §10 – Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen
- §11 – Maßnahmen zur Resilienz und Dokumentation dazu insbesondere Sicherheits- und Resilienz-Konzepte
- §12 – Meldungen zu Störungen
- §14 – Meldungen des BBK an die Europäische Kommission

Im Gesetzestext sollten deshalb entsprechende Regelungen zum Geheimschutz verankert werden. Der ASW Bundesverband schlägt vor, diese Informationen – entsprechend den Bestimmungen des Geheimschutzes – wenigstens als VS-vertraulich zu klassifizieren.

4. Notwendigkeit der Sicherheitsüberprüfung von Mitarbeitern in sensiblen Bereichen

Die CER-Richtlinie fordert in Artikel 14, dass für sensible Informationen die Möglichkeit bestehen muss (z.B. Schutzkonzepte der Unternehmen), diese als Verschlusssache zu klassifizieren. Der ASW Bundesverband unter-

stützt ausdrücklich diese Anforderung der CER-Richtlinie. Die Ausführungen des ASW Bundesverbands sind unter Punkt 3 bereits beschrieben. Um der Anforderung Rechnung zu tragen, ist es notwendig, alle involvierten Stellen bzw. Mitarbeiter*innen der KRITIS Betreiber einer Sicherheitsüberprüfung (mindestens Ü2) zu unterziehen. Der ASW Bundesverband spricht sich dafür aus, die jeweiligen Kontakt- und Meldestellen (nach §8 und §12) der Geheimschutzbetreuung und mindestens einer Ü2 Sicherheitsüberprüfung zu unterziehen.

Darüber hinaus ist es für die Einhaltung eines durchgängigen Sicherheitsniveaus aus Sicht des ASW Bundesverbandes notwendig, nicht nur materielle Sicherheitsstandards zu definieren, sondern auch die „Vertrauenswürdigkeit“ von Personal mit Aufgaben in sicherheitsrelevanten Bereichen prüfen zu können. Diese Prüfung der „Vertrauenswürdigkeit“ kann niedrigschwelliger angesetzt und muss somit nicht dem Grad der zuvor genannten klassischen Sicherheitsüberprüfung entsprechen. Eine derartige Vertrauenswürdigkeitsüberprüfung könnte von Wirtschaftsunternehmen in eigener Verantwortung, unter Berücksichtigung datenschutzrechtlicher Anforderungen, durchgeführt werden. Eine entsprechende gesetzliche Grundlage ist in diesem Kontext wünschenswert. Prüfungspunkte könnten z.B. sein (hier Vorschläge): Abforderung beglaubigter Zeugniskopien, Benennung von Referenzpersonen, Vorlage eines polizeilichen Führungszeugnisses, Offenlegung von ggf. weiteren vorhandenen Staatsangehörigkeiten (eigene und Lebenspartner, Eltern), Offenlegung von Auslandsreisen in besondere Länder (Liste aus Bericht des BfV).

Der ASW Bundesverband spricht sich daher für die Schaffung dieser gesetzlichen Grundlage aus und schlägt folgende Rahmenparameter vor:

- Wirtschaftsunternehmen richten einen geeigneten und angemessenen Prozess ein, um die Vertrauenswürdigkeit von Personal mit herausgehobener Bedeutung für die Resilienz und Sicherheit zu gewährleisten.
- Kriterien für Personal mit herausgehobener Bedeutung für die Resilienz und Sicherheit werden in den jeweiligen Rechtsvorschriften nach §15 festgelegt.
- Der jeweilige Prozess zur Prüfung der Vertrauenswürdigkeit wird in den Branchenstandards nach §11(5) definiert.

Die unklare Regelung bezüglich des Schutzes vertraulicher Daten und Informationen wirft ernsthafte Fragen auf. Der immense Aufwand, den Behörden für die Wirtschaft bei vermeintlich geringfügigen Sachverhalten betreiben, steht in krassem Kontrast zu den vorgesehenen Maßnahmen. Unternehmen würden, wenn sie als Behörden agieren würden, Risk Assessments und Konzepte als mindestens "VS-Vertraulich" oder "VS-Geheim" klassifizieren.

5. Realistische Darstellung des Erfüllungsaufwandes

Dem Referentenentwurf lässt in weiten Teilen die Darstellung des Erfüllungsaufwandes vermissen. Somit kann der ASW Bundesverband hierzu valide keine Bewertung abgeben.

Zum aktuellen Zeitpunkt muss jedoch seitens des ASW Bundesverbandes die Aussage, dass Auswirkungen auf das allgemeine Preisniveau und Verbraucherpreise nicht zu erwarten sind, deutlich in Frage gestellt werden. Aufwände für die vorgeschriebenen Regulierungen werden die Kostensituation von Wirtschaftsunternehmen negativ beeinflussen. Diese Annahme lässt sich insbesondere durch den Bürokratieaufwand begründen. Zu erwartende Mehrkosten müssen umlagefähig auf die Produkte und Leistungen der jeweiligen Unternehmen sein. Folglich ist mit Auswirkungen auf das allgemeine Preisniveau und den Verbraucherpreis zu rechnen.

6. Wichtige Weichenstellungen und Sicherheitsorganisation

Die aktuellen Vorschläge des Gesetzesentwurfs verpassen es, entscheidende Grundlagen zu legen. Ein essenzieller Paragraph sollte vorschreiben, dass KRITIS-Betreiber eine qualifizierte Sicherheitsorganisation und -verantwortliche etablieren müssen. Dieser sollte direkt an die Unternehmensleitung berichten und als Single Point of Contact (SPOC) für Aufsichts- und Sicherheitsbehörden fungieren.

7. Verantwortlichkeiten und Bürokratie

Statt eine klare Linie bei den Verantwortlichkeiten zu ziehen, verschärft der aktuelle Entwurf die Situation. Für lokal ansässige Organisationen mag dies akzeptabel sein, doch für Unternehmen und Konzerne mit überregionalen Tätigkeiten könnte dies zu einer erheblichen bürokratischen Belastung führen. Eine zentrale Regulierung und Koordination sind hier unabdingbar, um eine Zersplitterung von Zuständigkeiten zu vermeiden.

8. Zuverlässigkeitsüberprüfungen (§10 Abs. 5b und Abs. 3)

Die Möglichkeit und Notwendigkeit von Zuverlässigkeitsüberprüfungen gemäß dem KRITIS-Dachgesetz könnte eine solide Grundlage bieten, nicht nur für die Überprüfung von Netzleitstellen-Personal, sondern auch für andere kritische Bereiche wie Sicherheitsabteilungen, Krisenteams und spezialisierte Fachkräfte.

In § 10 Absatz 3 sollten folgende Aspekte bzw. Anforderungen als „Muss“ integriert werden:

Idealerweise sollte es in jedem Unternehmen der KRITIS-Sektoren im Vorstand und/oder in der Geschäftsführung einen Gesamtverantwortlichen für Sicherheit im Sinne des Allgefahrenansatzes geben

Die Leiter der verschiedenen etablierten Funktionen, die sich mit Gefahrenabwehr im Unternehmen befassen (z.B. Arbeitssicherheit, IT-Sicherheit, Informationssicherheit, Brandschutz, Umweltschutz) sollten regelmäßig (fachlich) an diesen Gesamtverantwortlichen berichten. Ebenso wie der Leiter einer betrieblichen Security Organisation, der das Mandat hat für die Abwehr von Gefahren aufgrund vorsätzlichen menschlichen Fehlverhaltens („doloser Handlungen“) insbesondere in der physischen Welt.

Die fachliche Verantwortung für die Umsetzung der Bestimmungen des KRITIS-DG im Unternehmen trägt der Leiter der betrieblichen Security Organisation. Sofern das KRITIS-Unternehmen noch nicht über eine geeignete Security Organisation verfügt, ist diese zeitnah einzurichten, zu mandatieren und mit zur Auftragserfüllung angemessenen personellen und finanziellen Ressourcen auszustatten.

Die Gesamtverantwortung für die Umsetzung der Bestimmungen des KRITIS-DG im Unternehmen trägt der Gesamtverantwortliche für Sicherheit im Unternehmen (Vorstand und/oder Geschäftsführer), bei dem aufgrund der regelmäßigen Meldungen der an ihn berichtenden Funktionen der betrieblichen Gefahrenabwehr ein im Sinne des Allgefahrenansatzes ein ganzheitliches Sicherheitslagebild entsteht und gepflegt wird.

Der Gesamtverantwortliche für Sicherheit, der Leiter der Security Organisation und die übrigen mit der Umsetzung der Bestimmungen des KRITIS-DG im Unternehmen betrauten Beschäftigten sind für die Wahrnehmung dieser Aufgabe regelmäßig weiterzuqualifizieren.

9. Resilienzmaßnahmen der Betreiber kritischer Anlagen; Resilienzplan (§10 Abs. 1)

Die Betreiber kritischer Anlage können weder terroristischen noch militärischen Bedrohungen begegnen bzw. Vorfälle wie z.B. Sabotage verhindern. Allein die Gefahrenabwehrbehörden auf Bundes- oder Landesebene können und dürfen die letzte Meile der Gefahrenabwehr gehen. Deshalb muss der Anwendungsbereich des KRITIS-DachG so erweitert werden, dass neben Betreibern kritischer Anlagen genauso auch Bund und Länder beim Schutz kritischer Infrastrukturen in die Pflicht genommen werden.

Die Allianz für Sicherheit in der Wirtschaft e.V. (ASW Bundesverband) vertritt die Sicherheitsinteressen der deutschen Wirtschaft auf Bundes- und EU-Ebene gegenüber der Politik, den Medien und den zentralen Sicherheitsbehörden. Der ASW Bundesverband arbeitet mit Unternehmen der freien Wirtschaft, Entscheidungsträgern der Sicherheitspolitik und -Behörden sowie unterschiedlichen Universitäten und Forschungseinrichtungen dauerhaft zusammen. Er wird getragen von den deutschen regionalen Sicherheitsverbänden sowie diversen fachspezifischen Bundesverbänden und Fördermitgliedern. Mehr zum ASW Bundesverband finden Sie unter: <https://asw-bundesverband.de>