

KRITIS-Dachgesetz und Katastrophenschutz

Berlin (BE). Das „neue“ KRITIS Dachgesetz soll die klaren Ansprüche von Schützen, Sichern, und Stärken festschreiben und die Möglichkeit zum entschiedenen Handeln geben. Bundesinnenminister Alexander Dobrindt will durch dieses Dachgesetz kritische Infrastrukture vor Bedrohungen sichern, ihre Funktionsfähigkeit härten und unsere Resilienz für den Krisenfall schützen. Die Bundesregierung legte das Gesetz zur Stärkung kritischer Anlagen am 29.01.26 vor.

Der Bundestag hatte am 29.01.26, nach einer einstündigen Aussprache den Gesetzentwurf der Bundesregierung „zur Umsetzung der Richtlinie (EU) 2022 / 2557 und zur Stärkung der Resilienz kritischer Anlagen“ (Kritis-Dachgesetz, 21/2510, 21/3855) in der vom Innenausschuss geänderten Fassung (21/3906) angenommen. Dafür stimmten CDU/CSU, AfD und SPD, dagegen Bündnis 90/Die Grünen und Die Linke.

Zum Gesetz beschloss der Bundestag darüber hinaus eine Entschließung, der die Unionsfraktion, die AfD- und die SPD-Fraktion zustimmten. Die Linke votierte dagegen, die Grünen enthielten sich.

Das Gesetz soll Deutschland resilient machen und für einen ganzheitlichen Schutz der kritischen Infrastruktur“ (21/2725) sorgen. Dazu lag eine Beschlussempfehlung des Innenausschusses vor (21/3761).

Das Gesetz sei der Ausdruck der innenpolitischen Zeitenwende, so Vertreter der CDU im Bundestag. Mit dem Gesetz würden mehr Sicherheit, Klarheit und auch mehr Handlungsfähigkeit geschaffen. Bei dem Gesetz konzentrierte man sich auf die wichtigsten Anlagen und ziehe die Evaluierung „deutlich vor“, um schnelles Handeln und auch ein Nachsteuern zu ermöglichen.

Der Gesetzentwurf allein löse die Probleme jedoch nicht. Mit Blick auf Konflikte mit Transparenzvorgaben verwies man auf einen Entschließungsantrag der Koalitionsfraktionen. In diesem werde die Bundesregierung aufgefordert, alle Transparenzpflichten zu überprüfen, sie gegebenenfalls neu zu bewerten und Daten zu löschen. „Wir dürfen unsere kritische Infrastruktur nicht weiter auf dem Silbertablett präsentieren“, sagte der Abgeordnete Schmidt in der Debatte und appellierte an die Länder, das Gesetz zügig auf den Weg zu bringen.

In den Beratungen mit den Ländern wurde eine Öffnungsklausel mit den Ländern für eigene Entscheidungen vereinbart.

Was ist und wer gehört zur Kritischen Infrastruktur?

Die KRITIS sind lebenserhaltende Einrichtungen und Systeme, deren Ausfall oder Beeinträchtigung zu Versorgungsengpässen, zu gestörter öffentlicher Sicherheit oder drastischen Folgen für die Gesellschaft führt. Siebzehn Sektoren (Bereiche), darunter Energie, Wasser, Gesundheit, Transport, Energie, Wasser, Ernährung, Gesundheit, Transport, IT und Finanzen, Verkehr, Finanz- & Versicherungswesen, Staat & Verwaltung, Medien & Kultur gehören zu den lebenswichtigen Sektoren.

Der Schutzbedarf von hoher Verletzlichkeit wie bei Cyberangriffen, Naturkatastrophen oder Terroranschlägen ist durch strenge Sicherheitsvorkehrungen (IT-Sicherheitsgesetz, Gesetz für Sicherheit und Ordnung u.s.w.) geregelt und für die Betreiber von Einrichtungen und die Behörden verpflichtend geregelt. So haben die Betreiber von Stromnetzen, Wasserwerken, Krankenhäuser, Lebensmittelversorger, Finanzämter und Flughäfen die Aufrechterhaltung der Betriebe zu erhalten als verpflichtende Auflagen. Dieses gilt auch für die Behörden, die die öffentliche Sicherheit und Ordnung durch Resilienz und den Katastrophenschutz zu gewährleisten haben.

In der Debatte forderte die AfD angesichts der tiefen Eingriffe in Wirtschaft, Verwaltung und unternehmerische Freiheit müsse der Entwurf seine Schlagkraft beweisen. Kritisiert wurde von der AfD, dass entscheidende Fragen im Gesetz in Ministerien, Ämtern und nachgeordneten Behörden ausgelagert wurden. Sie vertritt auch die Auffassung, dass der Bund Kompetenzen an sich ziehe, die regional verankert gewesen seien. Dadurch würden Akteure vor Ort sozusagen un Ausführungsorganen degradiert. Das Gesetz könne den Erfüllungsaufwand nicht klar beziffern. Gerade kommunale Unternehmen gingen ins Risiko, ohne zu wissen, was morgen per Verordnung verlangt werde, kritisierte Abgeordneter Raue. Seine Fraktion werde dem Entwurf dennoch zustimmen, um Verantwortung zu übernehmen, betonte er. Seine Fraktion erwarte auch eine umgehende und angemessene Ausgestaltung der Rechtsverordnung.

Der Abgeordnete Rasha Nasr (SPD) sagte, der Gesetzentwurf sei „kein spektakuläres Gesetz, aber ein fundamental wichtiges.“ Es Sorge dafür, dass man das, was man im Alltag für selbstverständlich halte, zuverlässig funktioniere. Die Risiken seien in den vergangenen Jahren vielfältiger geworden: Die

Frage sei nicht mehr, ob Störungen auftreten, sondern wann und wie gut wir auf sie vorbereitet seien. Die Koalition wolle im Entwurf sicher stellen, dass sich die Pflichten auf diejenigen konzentrierten, bei denen es um systemische Relevanz gehe. Die Öffnungsklausel ermögliche es den Ländern, unter dem bundeseinheitlichen Schwellenwert weitere Anlagen als kritisch zu identifizieren, wenn diese für die regionale Versorgung von besonderer Bedeutung seien.

In punkto Transparenzpflichten sagte Nasr, Transparenz habe dort ihre Grenzen, wo sie unsere Sicherheit gefährde. Die Bundesregierung und die Länder müssten bestehende Transparenz- und Veröffentlichungspflichten überprüfen und anpassen.

Kritisch und auf Mängel des Gesetzes verweisen die Grünen: So fehle eine Strategie gegen hybride Bedrohungen. Dr. Konstantin von Notz (Bündnis 90/Die Grünen) betonte, dass die Bundesrepublik täglich angegriffen werde. Dabei nehme die Dreistigkeit, mit der autoritäre Kräfte vorgehen, massiv zu. Die Folge seien Schäden in der Wirtschaft, bei der Versorgungssicherheit und nicht zuletzt beim Vertrauen der Menschen in die Wirkmächtigkeit des Staates.

Es fehle eine Gesamtstrategie gegen hybride Bedrohungen. Nötig seien weiter die Stärkung des Bundesamts für Sicherheit in der Informationstechnik (BSI), eine Grundgesetzänderung zur besseren Abwehr von Cyberangriffen wie auch Maßnahmen gegen das Treiben der russischen Schattenflotte oder klare Verantwortlichkeiten bei der Drohnenabwehr. Die Grünen stellen aber auch fest, dass mit Blick auf das Kritis-Dachgesetz auf die Kritik aus der Anhörung reagiert wurde. Moniert wurde eine Auslagerung von Details in Rechtsverordnungen.

Die Linke kritisierte, dass der Bundestag und die Ministerien wie das Verteidigungsministerium oder das Auswärtige Amt vom Gesetzentwurf ausgenommen würden. Aus Sicht der Grünen müsse bei der kritischen Infrastruktur die physische und digitale Sicherheit zusammengedacht werden. Der Gesetzentwurf hingegen setze auf neue Meldepflichten, neue Verordnungen und neue Bürokratie, so die Linke.

Die Bundesregierung, die auf Abbau von Bürokratie setzen wolle, sieht die Sicherheit durch Meldewege und Formulare, also mehr Bürokratie. Die derzeitigen Bedrohungen und Sicherheitsslücken (Anmerkung Red.: Katastrophe Ahrtal, Angriffe auf E-Mailkonten usw) haben gezeigt, dass Sicherheitsslücken, Hintertüren in Software sowie Schwachstellen nicht die Gewähr für eine sichere Krisenbewältigung gegeben sind. Mit Blick auf den jüngsten Anschlag auf das Stromnetz in Berlin sagte er, dieser habe gezeigt, wie schnell der Katastrophenschutz an seine Grenzen

gebracht werde. Für echten Schutz kritischer Infrastrukturen brauche es mehr als Zäune, Warnschilder und Meldepflichten. Neben einer „schonungslosen Gefährdungsanalyse für alle Ballungsgebiete brauche es beispielsweise Redundanzen. An zu vielen Orten fehlten doppelte Leitungen oder getrennte Leitungswege.

Gesetzentwurf der Bundesregierung

Mit dem Gesetz wird die EU-Richtlinie 2022/2557 über die Resilienz kritischer Einrichtungen, die sogenannte CER-Richtlinie, in deutsches Recht umgesetzt. Durch bundeseinheitliche Regelungen für den physischen Schutz kritischer Infrastrukturen will die Bundesregierung die Resilienz der Wirtschaft und dadurch auch die Versorgungssicherheit der Bevölkerung stärken. (Red.: Erst Wirtschaft dann Bevölkerung sichern?)

Das Kritis-Dachgesetz macht Vorgaben zur Identifizierung von Betreibern kritischer Anlagen und kritischen Einrichtungen mit besonderer Bedeutung für Europa sowie Vorgaben zur Registrierung von Betreibern kritischer Anlagen. Es zielt zudem auf die Etablierung von nationalen Risikoanalysen und Risikobewertungen für kritische Dienstleistungen und die gesetzliche Verankerung wesentlicher nationaler Anforderungen für Resilienzmaßnahmen von Betreibern kritischer Anlagen ab. Außerdem wird ein Meldewesen für Vorfälle eingeführt.

Änderungen im Innenausschuss und EntschlieÙung

Der Innenausschuss hatte am 28.01.26 Änderungen am Regierungsentwurf vorgenommen. Den Ländern wird die Möglichkeit gegeben, weitere kritische Anlagen für kritische Dienstleistungen, die alleine in ihrer Zuständigkeit liegen, zu identifizieren. Für die Festlegung der zugrunde zu legenden Kriterien und Verfahren wird das Bundesinnenministerium ermächtigt, eine Rechtsverordnung zu erlassen, der der Bundesrat zustimmen muss.

In der vom Bundestag beschlossenen EntschlieÙung wird die Bundesregierung aufgefordert, Informations-, Transparenz- und Veröffentlichungspflichten für Kritis-Betreiber zu überprüfen und anzupassen. Auch soll die Bundesregierung unter anderem auf die „konsequente Anwendung bereits bestehender Ausnahmen“ von diesen Pflichten hinwirken und bereits veröffentlichte, öffentlich zugängliche Infrastrukturinformationen „überprüfen und, wo möglich, konsequent aus den öffentlich zugänglichen Bereichen“ entfernen.

Stellungnahme des Bundesrates

Der Bundesrat stellt fest, dass beim Schutz der kritischen Infrastruktur (KRITIS) Handlungsbedarf be-

steht und ein einheitliches Regelwerk für Resilienzmaßnahmen gefahren- und sektorübergreifend dringend ist. Kritische Infrastrukturen sind zugleich Rückgrat und Schwachstelle unserer modernen Gesellschaft. Angesichts hybrider Bedrohungen und einer verschärften geopolitischen Sicherheitslage muss dem Schutz der Kritischen Infrastruktur besondere Aufmerksamkeit zukommen. Der Bundesrat hatte am 28.01.26 eine Stellungnahme (21/3855) abgegeben. Darin begrüßt die Länderkammer, dass die Bundesregierung mit dem Gesetzentwurf den Handlungsbedarf zur Steigerung der Resilienz der Kritischen Infrastruktur aufgreift. In der Sache wird der Gesetzentwurf seiner intendierten und durch die gewählte Gesetzesbezeichnung ausdrücklich betonten Zielsetzung allerdings nicht gerecht. Die gebotene Steigerung des Schutz- und Resilienz-Niveaus der KRITIS bleibt deutlich hinter den Erwartungen der Länder zurück und läuft Gefahr, nicht bundesweit einheitlich erreicht zu werden. Zwischen Bund und Ländern besteht Einigkeit, dass es eines besseren Schutzes Kritischer Infrastruktur bedarf und hierfür ein verlässlicher Rechtsrahmen zu schaffen ist.

Gesamtgesellschaftliche Resilienz und flächendeckende Versorgungssicherheit können nur durch eine Härtung des Gesamtsystems KRITIS bewirkt werden. Dies verlangt eine verbindliche Festlegung aller KRITIS-Sektoren, eine höhere Regulationsintensität im Sinne konkreter Vorgaben für KRITIS-Betreiber zur Krisenvorsorge sowie flankierend eine fachgesetzliche Regulierung in allen Bereichen Kritischer Infrastruktur. Insbesondere mit Blick hierauf erfüllt der Gesetzentwurf nicht die in der Nationalen Sicherheitsstrategie und der Deutschen Resilienzstrategie durch den Bund gesetzten Ziele zur Verbesserung des Schutzes der Kritischen Infrastruktur und löst auch die Zusagen im Eckpunktepapier für das KRITIS DachG-E (vgl. BT-Druck-sache 20/5491) nicht ein.

Der Gesetzentwurf bedarf aus Sicht des Bundesrates insbesondere folgende Schärfungen:

a) Was zur Kritischen Infrastruktur in Deutschland gehört, muss umfassend, abschließend und bundesweit definiert werden, um in der Praxis einen einheitlichen Vollzug der Maßnahmen in Bund, Ländern und Kommunen sowie auf Betreiberseite rund um den Schutz und die Resilienz der Kritischen Infrastruktur sicherzustellen. Dabei muss das Gesetz orientiert an der zwischen Bund und Ländern vereinbarten und etablierten KRITIS-Bereichseinteilung unabhängig von der Gesetzgebungskompetenz alle KRITIS-Sektoren zumindest benennen, auch wenn sodann im Anwendungsbereich einzelne KRITIS (wie vorgesehen) ausgenommen sind (bspw., weil die Gesetzgebungskompetenz bei den Ländern liegt). Die im Gesetzentwurf vorgesehene Sektoraufschlüsselung

entspricht nicht den gängigen Sektorenbezeichnungen und ist unvollständig (u.a. die Sektoren „Staat und Verwaltung“ sowie „Medien und Kultur“ fehlen). Daneben werden Teile der kritischen Dienstleistungen im Gesetz genannt, während die restliche KRITIS-Definition in einer Verordnung erfolgen soll, zu der jedoch noch kein Entwurf vorliegt.

b) Die durch den Gesetzentwurf von KRITIS-Betreibern geforderten Resilienzmaßnahmen müssen alle Teile des Risiko- und Krisenmanagements für KRITIS systematisch adressieren, also die Vermeidung von Störungen/Ausfällen, die Vorbereitung auf (unvermeidbare) Störungen/Ausfälle, die Bewältigung von eingetretenen Störungen/Ausfällen und die Nachsorge im Sinne des Lernens aus Ereignissen. Die im Gesetzentwurf genannten Maßnahmen (§ 13 Absatz 3 KRITISDachG-E) sind diesen einzelnen Teilbereichen des KRITIS-Schutzes falsch zugeordnet, was zu beheben ist.

Die Resilienzplichten der Betreiber stehen insgesamt unter einem Abwägungsgebot, bei dem explizit genannt wird, dass wirtschaftliche Aspekte der Betreiber zu berücksichtigen sind. Anstatt (wie im Entwurf) den Fokus auf das Risiko eines Vorfalls zu legen, sollte die Versorgungssicherheit der genannten Wirtschaftlichkeit gegenübergestellt werden, was jedoch im Abwägungszusammenhang nicht angeführt wird.

c) Der im Gesetzentwurf festgelegte Regelschwellenwert von 500.000 versorgten Personen, der die Grundlage für die Berechnung von spezifischen Kennzahlen für kritische Dienstleistungen sein wird, um damit den Anwendungsbereich des Gesetzes abzustecken, muss die Kritische Infrastruktur flächendeckend im Sinne der Versorgungssicherheit im gesamten Bundesgebiet erfassen. Dies kann nur durch eine Absenkung des Regelschwellenwerts erreicht werden.

d) Für die im Gesetz vorgesehenen konkretisierenden Rechtsverordnungen muss eine Zustimmungsbedürftigkeit des Bundesrates etabliert werden, da sich erst hieraus die eigentlichen Wirkungen zur Resilienzsteigerung der KRITIS, aber auch die Vollzugsaufwände in den Ländern ergeben. Somit sind die Länder hiervon direkt in ihren Finanzen, Behörden und Verwaltungsabläufen betroffen.

e) Für einen umfassenden KRITIS-Schutz in Deutschland ist das KRITISDachG-E nur ein Baustein, den es mit weiteren notwendigen fachgesetzlichen Neuregelungen durch den Bundesgesetzgeber zu ergänzen gilt. Gesetzliche Regelungen zum Schutz Kritischer Infrastruktur finden sich derzeit in unterschiedlicher Regelungstiefe in Fachgesetzen, wobei in den Gesetzesvorbemerkungen ausgeführt wird: „[Es] fehlt

eine Übersicht über die bereits auf Grund anderer Fachgesetze ergriffenen Maßnahmen, die zur Resilienzsteigerung der Betreiber kritischer Anlagen getätigt wurden.“ So hat der Bund bislang auch nicht dargelegt, wie die Regelungen eines „Dachgesetzes“ mit den weiteren nötigen fachgesetzlichen Regelungsinhalten in Einklang gebracht werden und ineinandergreifen. Es sollten analog den dezidierten Änderungen im Energierecht in den Artikeln 2 und 3 auch für die restlichen KRITIS-Bereiche die fachgesetzlichen Anpassungen vollzogen werden.

f) Das KRITISDachG-E sollte auch Regelungen zum Schutz sicherheitsrelevanter Informationen treffen, die sich unter anderem an Betreiber kritischer Anlagen richten und die Veröffentlichung sensibler Informationen wirksam verhindern.

Weitere Anmerkungen zeigen vorgeschlagene Sektorenbezeichnungen vor, die für die Umsetzung eine wesentliche Voraussetzung sind. Sie knüpfen überwiegend an die Festlegungen der BSI-KritisV an. Der vorgeschlagene Sektor „Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende“ entspricht, wie § 3 Absatz 2 Nummer 11 KRITIS-DachG-E zeigt, eher einer kritischen Dienstleistung. Die Aufnahme dieses Bereichs sollte daher unter der passenderen Sektorenbezeichnung „Sozialwesen“ erfolgen.

Die bisher unvollständige Sektoreinteilung ist um die Sektoren „Staat und Verwaltung“ (Nummer 11) so-wie „Medien und Kultur“ (Nummer 12) zu ergänzen. Vom Bund in diesem Punkt angeführte kompetenz-rechtliche Bedenken dringen bei Lichte besehen nicht durch. Denn der Bund hat im gesamtstaatlichen Gefüge die Verantwortung angemessene Rahmenbedingungen für das Funktionieren gesellschaftlicher Abläufe zu schaffen. Dies gilt nicht nur unter dem Blickwinkel der Wirtschaft, wobei der Kompetenztitel in Artikel 74 Absatz 1 Nummer 11 des Grundgesetzes auch eine gefahrenabwehrrechtliche Annexkompetenz einschließt. In Anbetracht der aktuellen Herausforderungen durch die in Deutschland und Europa grundlegend veränderte Sicherheitslage besteht ein unabweisbarer Bedarf zur normativen Ausgestaltung der Rahmenbedingungen für eine funktionierende und resiliente Kritische Infrastruktur. Diese Rahmenbedingungen muss und kann der Bund nach Artikel 73 Absatz 1 Nummer 1 des Grundgesetzes (Verteidigung einschließlich des Schutzes der Zivilbevölkerung) setzen, was etwa Vorgaben zur Handlungsfähigkeit des Staates auf allen Ebenen im äußeren Notstand und die Normierung des Sektors „Staat und Verwaltung“ deckt. Der Sektor „Medien und Kultur“ wird als KRITIS-Sektor bereits in der Entwurfsbegründung angeführt (vgl. u. a. BR-Drucksache 558/25, S. 39 und

50, teilweise als Sektor „Kultur und Medien“ [sic] bezeichnet). Er hat in diesem Kontext ebenfalls essenzielle Bedeutung und bedarf einer bundesrechtlichen Normierung. In Zeiten von Fake News und gezielten Desinformationskampagnen bedarf es der Sicherung verlässlicher öffentlicher und unabhängiger Informationsquellen in einer pluralistischen Gesellschaft. Die Medien sind auch für die Warnung und Information der Bevölkerung sowohl im Vorfeld als auch ad hoc in einer Krisenlage gleich welcher Art (Katastrophe oder äußerer Notstand) unentbehrlich. Die nationale Bedeutung der Kultur wird etwa an der Notwendigkeit eines wirksamen Kulturgüterschutzes deutlich (vgl. § 25 ZSKG), sodass jedenfalls kraft Sachzusammenhangs eine Normierung auch des Sektors „Medien und Kultur“ im Interesse einer gesamtstaatlich einheitlichen und verlässlichen KRITIS-Definition erfolgen kann.

Weiterhin ist zu prüfen, welche Auswirkung auf den Realfall die zu schaffende Meldestruktur für das reale Handeln haben wird.

Für das Meldewesen ist vorgesehen, dass BSI und BBK eine gemeinsame Meldestelle einrichten, an die die Betreiber kritischer Anlagen im Sinne des Gesetzes Vorfälle zu melden haben. Während im Bereich der IT-Sicherheit durch das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vorgesehen ist, dass das BSI wenigstens den zuständigen Aufsichtsbehörden des Bundes die bei ihm eingegangenen Meldungen unverzüglich zur Verfügung stellt, sieht das KRITISDachG-E lediglich eine Übermittlung von „Auswertungen zu Meldungen von Vorfällen“ an die zuständigen Behörden vor – und dies ohne einen konkreten Zeitraum zu nennen. In dieser Form dient das vorgesehene Meldewesen rein statistischen Zwecken und ist nicht für die Bewältigung von Vorfällen tauglich.

Die Länder sind in akuten Störsituationen vom Informationsfluss abgeschnitten, obwohl hier wesentliche Aufgaben des Krisenmanagements und der Bewältigung von Vorfällen wahrgenommen werden. Die in den Ländern zuständigen Behörden können nur dann frühzeitig Folgen von Ereignissen abschätzen und zielgerichtet Bewältigungsmaßnahmen ergreifen, wenn sie zeitnah über eingetretene Ereignisse informiert werden. Es ist völlig unverständlich, warum die beim Bund vorliegenden Erkenntnisse über Vorfälle nicht sofort im Sinne des behördenübergreifenden Austauschs an die zuständigen Behörden in den Ländern weitergegeben werden sollen, zumal ein „Vorfall“ im Sinne des Gesetzes per Definition ohnehin bereits eine bestimmte Eskalationsstufe erreicht haben muss („ein Ereignis, das die Erbringung ei-

ner kritischen Dienstleistung erheblich beeinträchtigt oder beeinträchtigen könnte“). Dies entspricht nicht der in der Nationalen Sicherheitsstrategie festgelegten Zielsetzung, mit dem Dachgesetz einen gesetzlichen Rahmen zu schaffen, der „die Zusammenarbeit zwischen Bundes- und Landesebene [...] verbessert“ (vgl. BR-Drucksache 558/25, S. 36).

Insbesondere in der aktuellen Sicherheitslage ist es entscheidend, ein Monitoring der Funktionsfähigkeit der KRITIS und eingetretener Störungen engmaschig und stets aktuell durchzuführen. Hierbei hilft die Übermittlung generischer Auswertungen von Vorfallmeldungen (wie sie im Gesetzentwurf lediglich vorgesehen ist) nicht weiter. Die Erfahrungen mit den Regelungen im Bereich der IT-Sicherheit (IT-SiG seit 2015) haben gezeigt, dass für die außergesetzliche Organisation eines Informationsaustauschs über Meldungen zwischen Bund und Ländern u. a. eine Rechtsgrundlage fehlt. Dieser Fehler darf sich nicht wiederholen; das KRITIS-DachG-E muss die Meldungsweitergabe von Anfang an verbindlich vorsehen und damit legalisieren. Zudem sollte ein Zeitraum für die Auswertungen zu Meldungen von Vorfällen festgelegt werden – halbjährliche Berichte (gemäß dem Änderungsvorschlag) scheinen hier ein gutes Mittelmaß zwischen einem engen Monitoring, das auch das rechtzeitige Erkennen von Trendentwicklungen ermöglicht, und dem hierfür entstehenden administrativen Aufwand beim Bund zu bilden. Die unzureichende Berücksichtigung der Länder setzt bereits bei der Ausgestaltung des Meldeverfahrens an, welches keine verbindliche Mitwirkungsmöglichkeit für diese vorsieht. § 18 Absatz 3 KRITIS-DachG-E ermächtigt das BKK zur Ausgestaltung der Einzelheiten des Meldewesens, verlangt jedoch ausschließlich das Einvernehmen des BSI. Dieser Absatz soll dahingehend geändert werden, dass für die Ausgestaltung des Meldeverfahrens auch das Einvernehmen der Landesbehörde für sektorübergreifende Angelegenheiten erforderlich ist, um eine übergreifende Zusammenarbeit des Bundes und der Länder zur effektiven Umsetzung des KRITISDachG-E zu gewährleisten.

Obwohl die Länder insbesondere im Krisenmanagement und der Gefahrenabwehr die maßgeblichen Aufgaben beim KRITIS-Schutz wahrnehmen, sieht der Gesetzentwurf lediglich vor, dass das BKK nur die zuständigen Behörden über erfolgte Registrierungen informiert (Artikel 1 § 8 Absatz 5 KRITISDachG-E), was im Falle der Zuständigkeit einer Bundesbehörde die Länder außen vorlässt. Es ist jedoch unverzichtbar, dass die Länder eine Gesamtübersicht über die in ihrem Land befindlichen KRITIS-Anlagen haben – unabhängig davon, ob die Vollzugsbehörde nach KRITISDachG-E eine Bundes- oder Landesbehörde ist. Daher ist es elementar, dass diese anhand der

bereits bestehenden Systematik des Risiko- und Krisenmanagements zum Schutz der KRITIS präzise die einzelnen Handlungsverpflichtungen benennen und trennscharf voneinander abgrenzen.

Darüber hinaus ist zu prüfen, die Fristen im Gesetzestext an dessen Inkrafttreten zu koppeln. Der vorliegende Gesetzentwurf sieht an mehreren Stellen fixe Fristen und Stichtage vor (bspw. für die Erstellung der Nationalen KRITIS-Resilienzstrategie, der Risikoanalysen und der Betreiberpflichten). Erste Fristen liegen bereits so zukunftsnahe, dass angesichts des noch laufenden Gesetzgebungsverfahrens erwogen werden sollte, die starren Datumsangaben durch einen bestimmten Zeitraum nach Inkrafttreten des Gesetzes zu ersetzen.

Der Bundesrat sieht gemäß seiner Stellungnahme einen erheblichen Nachbesserungsbedarf und eine Anpassung an die Lebenswirklichkeit in der Bundesrepublik des Gesetzentwurfes.

Beispiel:

So spricht er sich unter anderem für eine Absenkung des im Gesetzentwurf vorgesehenen Regelschwellenwerts von 500.000 versorgten Einwohnern aus, den eine Kritis-Anlage überschreiten müsse, bevor der entsprechende Betreiber den Anforderungen des Gesetzes unterliege. Die Mehrheit der Bevölkerung in Deutschland werde indes von Kritis-Betreibern versorgt, die unterhalb des Schwellenwerts liegen, argumentiert der Bundesrat und plädiert für einen Schwellenwert von 150.000 zu versorgenden Personen.

Dazu schreibt die Bundesregierung in ihrer Gegenäußerung, dass sich der Regelschwellenwert von 500.000 zu versorgenden Einwohnern je Anlage im Gesetzentwurf „an den Prinzipien der Versorgungssicherheit und der Wirtschaftlichkeit“ orientiere. Sie könne sich jedoch „an dieser Stelle Regelungen zur Eröffnung von Spielräumen der Länder für die Identifizierung von Kritis auch jenseits des Regelschwellenwertes vorstellen“.

Einheitliche Meldestelle für Betreiber kritischer Anlagen

Dabei sollte die Bundesregierung dem Antrag zufolge sicherstellen, dass in dieser Gesetzesvorlage eine einheitliche Meldestelle für die Betreiber kritischer Anlagen geschaffen sowie das nationale IT-Sicherheitsrecht systematisiert wird und einheitliche IT-Sicherheitsstandards für Bund und Länder gelten. Auch sollten mit dem Entwurf nach dem Willen der Fraktion die öffentliche Verwaltung in den Schutzbereich aufgenommen und Bereichsausnahmen für die Bundesverwaltung gestrichen werden.

Des Weiteren plädierte die Fraktion dafür, mit dem Gesetzentwurf unter anderem das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seiner Unabhängigkeit zu stärken und den Bundestag „in den Definitionsrahmen einer Kritischen Infrastruktur“ aufzunehmen. Ferner drang die Fraktion darauf, dass „die zahlreichen kleinen und mittleren Unternehmen, die durch die Absenkung von Schwellenwerten neu unter den Kritis-Schutz fallen und die gesetzgeberischen Vorgaben umzusetzen haben, bestmöglich beraten werden“. Die Bundesregierung sollte zugleich aufgefordert werden, ein „One-Stop-Shop“-Verfahren zu implementieren, bei dem sich der Betreiber nur an eine Aufsichtsbehörde wenden muss. (lbr/sto/hau/29.01.2026).

Antrag der Grünen

Die Bundesregierung wird im abgelehnten Antrag der Grünen (21/2725) aufgefordert, den Entwurf für ein Kritis-Dachgesetz vorzulegen, das „einen effektiven und einheitlichen Kritis-Schutz schafft, der die EU-Vorgaben für die physische und digitale Sicherheit vereinheitlicht, Betreiber kritischer Anlagen künftig nur noch durch das Dachgesetz und die dazugehörige Rechtsverordnung bestimmt und Deutschland insbesondere durch das Schaffen von einheitlichen Mindeststandards, Risikoanalysen und ein Störungsmonitoring insgesamt widerstandsfähiger gegen Krisen und Angriffe macht“.

Texinfo: Drucksache 21/3855 28.01.2026
des Bundestages

Behördliche und private Vorsorge

Die staatliche Lebensmittelnotreserve des Bundes, oft als Zivile Notfallreserve bezeichnet, dient der Sicherstellung der Grundversorgung der Bevölkerung in Krisen- oder Katastrophenfällen. Angesichts der aktuellen Sicherheitslage plant das Bundeslandwirtschaftsministerium (Stand Mai 2026) eine deutliche Aufstockung und Modernisierung dieser Reserven.

Spätestens seit dem mehrtägigen Stromausfall in Berlin will auch die Bundesregierung besser gerüstet sein. So ist geplant, die staatliche Notreserve um Fertiggerichte in Konserven zu erweitern. Bisher werden an rund 150 Standorten vor allem Getreide, Erbsen, Linsen und Dosenmilch für Notfälle gelagert.

Neben der Lebensmittelnotreserve, bekannt bereits seit den 1960er Jahren (kalte Krieg), im Rahmen des Kriegfalles und des Bevölkerungsschutzes hat das Bundesinnenministerium im Mai 2026 zur Anlegung der privaten Vorsorge für ca. 10 Tage aufgerufen.

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) hat im November seinen Ratgeber „Vorsorgen für Krisen und Katastrophen“ überarbeitet. Empfohlen wird, sich so zu bevorraten, dass man etwa zehn Tage allein durchhalten kann. Der Ratgeber enthält detaillierte Informationen zum Aufbau von Reserven und Checklisten.

Aber nicht nur Lebensmittel gehören zur Notfallvorsorge. Geräte wie Gaskocher, Dosenöffner, Besteck, Becher und Teller, persönliche Medikamente, Wolldecken, Kopfkissen, Taschenlampe, Radio (evtl. ohne Fremdstrom), Batterien für die Geräte, die man eingelagert hat sowie Wasch- und Zahnputzsachen und etwas Bargeld (Münzen und Scheine).

Wenn dann der Notfall eintritt, kommt es schnell zu Situationen, wie im SWR beschrieben:

Im Heilbronner Outdoor-Fachgeschäft Adventure Company steigt bei neuen Krisen die Nachfrage nach Camping-Gaskochern. Vor allem ältere Kundinnen und Kunden äußern beim Kauf Sorgen, sagt Mitarbeiter Julius Gaub dem SWR. Gekauft werde meist ein „Klassiker für um die 45 Euro“.

Wichtig ist jedoch, egal ob kompetente Notfallpackungen gekauft oder selbst zusammen gestellte Pakete, auf den Packungen sollte das Einlagerungsdatum stehen. Ein regelmäßiges Überprüfen ist erforderlich bzw. ein Austausch ist wichtig. Überlagerte oder schlechte Lebensmittel helfen im Notfall nicht weiter.

Ein wichtiges Detail ist auch die Notfallmappe, hier sollten, zumindest in Kopie (auf Papier) die wichtigsten Dokumente zur Ausweisung, zur Eigentumbestätigung und zur Gesundheitsvorsorge enthalten sein.

Texinfo: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
<https://www.bbk.bund.de>, Bearbeitet: Horst-Dieter Scholz

Auf dieser Homepage ein Beitrag vom 05.05.26

Feuerwehr und Sankt Florian - Sankt Florian und Mitverantwortung