Deutscher Bundestag **Drucksache 20/5491**

20. Wahlperiode 09.12.2022

Unterrichtung

durch die Bundesregierung

Eckpunkte für das KRITIS-Dachgesetz

Von der Alarmierung von Rettungskräften über die Stromversorgung bis zum Zahlungsverkehr – Kritische Infrastrukturen (KRITIS) sind für unser Gemeinwesen unverzichtbar. Jede und jeder Ein zelne ist im Alltag auf sie angewiesen. Ihre Verfügbarkeit sichert die Handlungsfähigkeit staatlicher Institutionen und ist Voraussetzung für wirtschaftliche und gesellschaftliche Aktivitäten. Die Bandbreite der Kritischen Infrastrukturen ist groß, die Gefahren sind vielfältig und reichen von Naturkatastrophen und Pandemien, über Angriffe im Kontext hybrider Bedrohungen, menschlichem Versagen, Terrorismus und Sabotage bis hin zu einer unzureichenden Versorgung mit erforderlichen Betriebsmitteln, z.B. durch den Zusammenbruch von Lieferketten. Ausfälle und Störungen der Kritischen Infrastrukturen können zu Versorgungsengpässen und erheblichen Störungen der öffentlichen Sicherheit und Ordnung führen. Die aktuellen Krisen wie die COVID-19-Pandemie oder die Auswirkungen des Ukraine-Krieges und Sabotageakte wie jüngst bei der Deutschen Bahn und den Gaspipelines Nord Stream haben die Bedeutung und die Verwundbarkeit der Kritischen Infrastrukturen sowie die damit einhergehenden gesamtgesellschaftlichen Auswirkungen verdeutlicht. Die Resilienz von KRITIS ist für den Schutz und die Handlungsfähigkeit von Bevölkerung, Wirtschaft und Staat in Deutschland essentiell.

Im Bereich der Cybersicherheit Kritischer Infrastrukturen gibt es mit dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) sowie der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) bereits umfassende Regelungen. Jenseits dieser Regulierung im Bereich Cybersicherheit gibt es jedoch in Deutschland bislang kein sektoren- und gefahrenübergreifendes „Gesetz zum Schutz Kritischer Infrastrukturen“. Gesetzliche Regelungen mit explizitem Bezug zum physischen Schutz spezifischer Kritischer Infrastrukturen finden sich vereinzelt und in unterschiedlicher Regelungstiefe in Fachgesetzen. Teilweise werden dabei abstrakte Zielsetzungen formuliert, Befugnisse von Behörden festgeschrieben oder konkrete Vorgaben für Betreiber gemacht. Darüber hinaus fördert eine Vielzahl weiterer gesetzlicher Regelungen, Normen und Standards mittelbar auch den physischen Schutz Kritischer Infrastrukturen, wie etwa bautechnische Vorschriften. Aufgrund vielfältiger Verflechtungen ergeben sich aber Fragestellungen, die über Ressort- und Sektorengrenzen hinweg diskutiert und bearbeitet werden müssen. Die Abhängigkeiten der Sektoren untereinander stellen komplexe Herausforderungen dar. Gibt es Ausfälle in einem Sektor, etwa Energie, IT oder Logistik, kann dies schwere Auswirkungen auch auf andere Sektoren und damit auf die gesamte Wertschöpfungskette haben.

Vor dem Hintergrund uneinheitlicher bzw. fehlender Regelungen für den physischen Schutz Kritischer Infrastrukturen und angesichts sektoren- sowie länderübergreifender Abhängigkeiten wird mit dem KRITIS-Dachgesetz zum ersten Mal das Gesamtsystem zum physischen Schutz Kritischer Infrastrukturen in Deutschland in den Blick genommen und im Rahmen der dem Bund zustehenden Zuständigkeiten gesetzlich geregelt. Das KRITIS-Dachgesetz ergänzt damit auch die bestehenden Regelungen zum Cyberschutz von Kritischen Infrastrukturen und trägt zu einem kohärenten und resilienten System bei.

Zugeleitet mit Schreiben des Bundesministeriums des Innern und für Heimat vom 7. Dezember 2022.

Dazu gehört auch der Schutz vor möglichen Gefahren, die von Herstellern von kritischen Komponenten in KRITIS ausgehen. Das BSI-Gesetz enthält bereits entsprechende Regelungen in Bezug auf IT-Komponenten. Für einen umfassenden Schutz wird geprüft, ob das KRITIS-Dachgesetz entsprechende Regelungen in Bezug auf Komponenten, die keine informationstechnischen Systeme, Komponenten oder Prozesse im Sinne des BSI-Gesetzes sind, aufnehmen wird, um KRITIS insgesamt vor Einflüssen und Abhängigkeiten von bedenklichen Herstellern aus dem Ausland schützen zu können.

Das sektoren- und gefahrenübergreifende KRITIS-Dachgesetz ordnet ein und ergänzt sektorenspezifische gesetzliche und nicht-gesetzliche Regelungen. Auf Grundlage des KRITIS-Dachgesetzes sollen wertvolle Erkenntnisse zur Lage in den einzelnen KRITIS-Sektoren als Teil eines umfassenden Lagebildes gewonnen werden. Hierauf basierend können im Rahmen der jeweiligen Zuständigkeit von Bund und Ländern weitergehende sektorenspezifische Regelungen oder – sofern keine Ermächtigungsgrundlage im Grundgesetz vorhanden – Empfehlungen getroffen werden, um etwaige Regelungslücken zu schließen.

Zudem soll mit dem KRITIS-Dachgesetz die Zusammenarbeit der am Schutz Kritischer Infrastrukturen beteiligten Akteure auf staatlicher Seite und bei den Betreibern verbessert und klarer strukturiert werden.

Mit dem KRITIS-Dachgesetz wird ein Vorhaben aus dem Koalitionsvertrag realisiert. Außerdem soll das Gesetz die EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience / CER-Richtlinie) umsetzen, die voraussichtlich Ende 2022 verabschiedet wird. Der deutsche Rechtsrahmen für den Schutz Kritischer Infrastrukturen wird somit in ein europäisches Gesamtsystem eingebettet. Durch europaweit einheitliche Mindestvorgaben und verstärkte grenzüberschreitende Kooperation wird die Versorgungssicherheit in Deutschland und in Europa gestärkt. Die Stärkung der Resilienz Kritischer Infrastrukturen wird darüber hinaus auch auf Ebene der NATO als Ziel verfolgt.

Bei der Erarbeitung des KRITIS-Dachgesetzes und der damit verbundenen Umsetzung der CER-Richtlinie sowie bei der Umsetzung der NIS-2-Richtlinie durch das entsprechende Umsetzungsgesetz werden die Schnittstellen zwischen den Bereichen Cyberschutz und physischem Schutz von KRITIS berücksichtigt und angeglichen, bzw. – soweit möglich und sinnvoll – übereinstimmend geregelt.

Es gilt ein genereller Finanzierungsvorbehalt. Soweit konkrete Maßnahmen oder daran anknüpfende zukünftige Maßnahmen zu Ausgaben im Bundeshaushalt führen, stehen sie unter dem Vorbehalt verfügbarer Haushaltsmittel bzw. Planstellen/Stellen und präjudizieren keine laufenden oder künftigen Haushaltsverhandlungen. Der von der Verfassung vorgegebenen Zuständigkeitsverteilung zwischen Bund und Ländern wird Rechnung getragen.

Ziele des KRITIS-Dachgesetzes:

- Kritische Infrastrukturen werden klar identifiziert.
- Die Resilienz des Gesamtsystems der Kritischen Infrastrukturen wird durch einheitliche Mindestvorgaben für Resilienzmaßnahmen in allen Sektoren gestärkt.
- Der Schutz Kritischer Infrastrukturen ist eine ressort- und akteursübergreifende und gesamtstaatliche Aufgabe. Die Betreiber der Kritischen Infrastrukturen – ob private Unternehmen oder öffentliche Einrichtungen – müssen ihre Funktionsfähigkeit gewährleisten. Der kooperative Ansatz wird mit dem KRITIS-Dachgesetz durch verpflichtende Schutzstandards für die physische Sicherheit ergänzt. Damit wird den Betreibern mehr Orientierung und Handlungssicherheit gegeben.
- Auch durch die Schaffung eines staatlichen Rahmens mit dem einzuführenden Meldewesen für Sicherheitsvorfälle und Kontrollen übernimmt der Staat eine größere Verantwortung beim Schutz Kritischer Infrastrukturen. Das neu einzuführende Meldewesen im Bereich der physischen Sicherheit ergänzt hierbei das bereits bestehende Meldewesen im Bereich der Cybersicherheit Kritischer Infrastrukturen. Der Staat wird die Betreiber zudem weiterhin durch Analysen sowie Leitfäden, Beratung, Übungen und Schulungen unterstützen.
- Die Auswirkungen auf das Gesamtsystem aller Kritischen Infrastrukturen müssen beim physischen Schutz Kritischer Infrastrukturen im Vordergrund stehen. Sektoren- und grenzübergreifende Verflechtungen und die Abhängigkeiten der Sektoren untereinander werden stärker berücksichtigt. Der Schutz von Kritischen Infrastrukturen ist neben der fachspezifischen auch eine Querschnittsaufgabe, die alle Ressorts in die Verantwortung nimmt und deren zielgerichtetes Mitund Zusammenwirken erfordert. Gibt es Ausfälle in einem Sektor, etwa Energie, Informationstechnik/Telekommunikation oder Transport/Verkehr, kann dies schwere Auswirkungen auch auf andere Sektoren haben.
- Die Resilienz der Kritischen Infrastrukturen insgesamt und nicht nur der Schutz einzelner Kritischer Infrastrukturen muss gestärkt werden. Die Kritischen Infrastrukturen müssen in der Lage sein, Sicherheitsvorfälle, die zu schwerwiegenden und potenziell sektoren- und grenzübergreifenden Störungen führen können, zu

verhindern, sich davor zu schützen, darauf zu reagieren, und abzuwehren. Zudem müssen die Folgen eines solchen Vorfalls begrenzt, aufgefangen, bewältigt und die Wiederherstellung gewährleistet werden.

– Den Verflechtungen und Abhängigkeiten von Kritischen Infrastrukturen wird auch auf administrativer Ebene Rechnung getragen. In einem neuen Ansatz wird der physische Schutz Kritischer Infrastrukturen mit dem KRITIS-Dachgesetz als eigenständiges Thema in den Blick genommen und durch eine übergreifende zuständige Behörde koordiniert. Auch grenzüberschreitende Auswirkungen werden durch eine noch engere Kooperation in einem europäischen Rahmen berücksichtigt.

Regelungsinhalte:

1. KRITIS klar identifizieren

Mit der BSI-Kritisverordnung besteht bereits eine etablierte Bestimmung Kritischer Infrastrukturen im Sinne des BSI-Gesetzes mit dem Fokus auf mögliche Beeinträchtigungen der Versorgungssicherheit durch Bedrohungen aus dem Cyberraum. Mit dem KRITIS-Dachgesetz soll diese bestehende Bestimmung ergänzt werden durch eine systematische und umfassende Identifizierung aller besonders schützenswerten Kritischen Infrastrukturen. Die verbindliche Festlegung von Definitionen für vom Regelungsinhalt betroffenen Sektoren, kritischen Dienstleistungen und deren zugrundeliegenden Infrastrukturen sowie etwaigen Schwellenwerten kann diesem Ziel dienen. Gemäß den Vorgaben aus der CER-Richtlinie werden Kritische Infrastrukturen mindestens in elf Sektoren (Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, Digitale Infrastruktur, öffentliche Verwaltung, Weltraum, Lebensmittel (Produktion, Verarbeitung und Vertrieb)) identifiziert. Zudem wird auch der KRITIS-Sektor „Kultur und Medien“ angemessen einbezogen. Auch der Bereich der Bildung und Betreuung ist in den Blick zu nehmen, dessen Funktionsfähigkeit auch eine zentrale Voraussetzung für die Aufrechterhaltung der Kritischen Infrastrukturen ist. Bei der Ermittlung der Kritischen Infrastrukturen werden sowohl quantitative als auch qualitative Kriterien wie die Zahl der Nutzer aber auch die Bedeutung der Kritischen Infrastruktur für die Aufrechterhaltung der kritischen Dienstleistung berücksichtigt. Darüber hinaus werden Kritische Infrastrukturen identifiziert, die von besonderer Bedeutung für Europa sind. Das sind nach den Bestimmungen der CER-Richtlinie solche Infrastrukturen, die in sechs oder mehr Mitgliedstaaten der Europäischen Union dieselben oder ähnliche kritische Dienstleistungen erbringen. Sie unterliegen daher nach der CER-Richtlinie einer verstärkten Aufsicht auf EU-Ebene.

2. Bedrohungslage und Risiken besser erkennen

Die Gefahren für die Kritischen Infrastrukturen werden einer regelmäßigen Bewertung unterzogen. Staatliche Risikobewertungen für die kritischen Dienstleistungen werden den Betreibern eine Grundlage für ihre eigenen regelmäßig vorzunehmenden spezifischen Risikobewertungen und die darauf basierenden Maßnahmen geben. Mit diesen Risikobewertungen werden die Gefahren systematisch bewusstgemacht. Dabei werden alle relevanten natürlichen und vom Menschen verursachten Risiken (All-Gefahren-Ansatz) sowie sektorenübergreifende und grenzüberschreitende Risiken berücksichtigt. Die Risikobewertungen werden regelmäßig mindestens alle vier Jahre durchgeführt und ermöglichen so einen dynamischen Lernprozess, der zu angepassten Maßnahmen und somit einer stetigen Erhöhung der Resilienz führt. Um Doppelarbeiten zu vermeiden, wird die Anerkennung bereits bestehender Arbeiten aufgrund anderweitiger Vorschriften ermöglicht. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) hat bereits Methoden veröffentlicht, die für derartige Risikobewertungen erarbeitet sowie erfolgreich verwendet wurden und kann die Ressorts und Betreiber hiermit unterstützen.

3. Schutzniveau verbindlich erhöhen

Den Betreibern der Kritischen Infrastrukturen in allen Sektoren werden die gleichen Mindestvorgaben im Bereich der physischen Sicherheit auferlegt, um die Kritischen Infrastrukturen umfassend gegen Gefahren zu schützen und als Teil des Gesamtsystems resilienter zu werden. Damit wird den Betreibern Orientierung für ihr Handeln und den Aufsichtsbehörden der Auftrag gegeben, Maßnahmen zum Schutz Kritischer Infrastrukturen explizit in den Blick zu nehmen. Diese Regelungen sollen die bereits bestehenden Vorgaben im Bereich der Cybersicherheit Kritischer Infrastrukturen somit ergänzen.

Dazu zählen

– die Einrichtung eines betrieblichen Risiko- und Krisenmanagements;
– die Durchführung von Risikoanalysen und -bewertungen;
– die Erstellung von Resilienzplänen und

– die Umsetzung geeigneter und verhältnismäßiger technischer, personeller und organisatorischer Maßnahmen für die jeweilige Einrichtung. Derartige Maßnahmen können beispielsweise die Errichtung von Zäunen und Sperren, der Einsatz von Detektionsgeräten, Zugangskontrollen, Sicherheitsüberprüfungen, aber auch das Vorhalten von Redundanzen und die Diversifizierung von Lieferketten sein.

  Die KRITIS-Betreiber müssen ihre spezifischen Schutzmaßnahmen an den Risikobewertungen und den Mindestvorgaben ausrichten. Bei der Sicherung von Kritischen Infrastrukturen durch die Betreiber hat eine Abwägung stattzufinden zwischen Wirtschaftlichkeit und Risikoeintrittswahrscheinlichkeit.

Eine Unterstützung der Betreiber wird geprüft.

4. Störungen des Gesamtsystems erkennen und beheben

Mit der Einführung eines zentralen Störungs-Monitorings als Ergänzung zum bestehenden Meldewesen im Bereich der Cybersicherheit wird ein Gesamtüberblick über mögliche Schwachstellen beim physischen Schutz Kritischer Infrastrukturen ermöglicht. Durch die Meldung von Sicherheitsvorfällen können andere von dem Sicherheitsvorfall betroffene Kritische Infrastrukturen, auch in anderen Mitgliedstaaten, gewarnt werden. Eine erste Meldung muss der zuständigen Behörde zeitnah übermittelt werden. Mit der Meldung soll die zuständige Behörde Art und mutmaßliche Ursache sowie mögliche Folgen des Sicherheitsvorfalls nachvollziehen und ermitteln können. Die zuständige Behörde soll sektorenübergreifende Auswertungen vornehmen können, damit mit den aus Sicherheitsvorfällen gewonnenen Erfahrungen erforderliche Anpassungen für den Schutz Kritischer Infrastrukturen vorgenommen werden können. Diesem Zweck dient ebenso die Erstellung eines regelmäßig zu erstellenden Berichts über Sicherheitsvorfälle durch die zuständige Behörde. Dieser Bericht wird auch der Europäischen Kommission übermittelt.

5. Einen institutionellen Rahmen schaffen

Die Zusammenarbeit der vielen am Schutz Kritischer Infrastrukturen beteiligten Akteure auf staatlicher Seite und bei den Betreibern Kritischer Infrastrukturen wird klarer herausgearbeitet. Durch klare Verantwortlichkeiten, Ansprechpartner und Rangfolgen für Fragestellungen im Zusammenhang mit der Resilienz Kritischer Infrastrukturen wird eine bessere Zusammenarbeit erreicht.

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) im Geschäftsbereich des Bundesministeriums des Innern und für Heimat (BMI) wird im Rahmen der Bundeszuständigkeit zu der übergreifenden zuständigen Behörde für den physischen Schutz Kritischer Infrastrukturen im Rahmen verfügbarer Haushaltsmittel ausgebaut. Eine derartige übergreifende zuständige und verantwortliche Behörde ist für das mit dem KRITIS-Dachgesetz verfolgtem Ziel der Betrachtung des Gesamtsystems erforderlich. Das BBK verfügt hier bereits über umfangreiche methodische und sektorenübergreifende Expertise. Zentrale Aufsichtsbehörden zur Regulierung von Infrastrukturen, wie insbesondere die Bundesnetzagentur, können die Einhaltung der nach dem KRITIS-Dachgesetz vorgesehenen Mindestvorgaben für Resilienzmaßnahmen in ihrem Zuständigkeitsbereich beaufsichtigen und durchsetzen. Dem BBK sowie gegebenenfalls den anderen fachlichen Aufsichtsbehörden werden die entsprechenden Ansprechpartner sowie die Sicherheitsvorfälle gemeldet. Zudem wird das BBK, gegebenenfalls gemeinsam mit weiteren fachlichen Aufsichtsbehörden, die Einhaltung der nach dem KRITIS-Dachgesetz vorgesehenen Mindestvorgaben für Resilienzmaßnahmen beaufsichtigen und durchsetzen. Das BBK wird hierfür u. a. die bereits aufgrund von sektorenspezifischen Regelungen existierenden Aufsichtsbehörden vernetzen und insoweit bestehende Strukturen ergänzen. Hierdurch ist es möglich, Prozesse zu etablieren, die eine schnelle Informationsweitergabe und deren übergreifende Aufarbeitung (beim BBK) ermöglichen. Zudem gibt es eine zentrale Stelle für die Bündelung von Wissen und Kompetenzen auf dem Gebiet des sektoren- und gefahrenübergreifenden Schutzes von Kritischen Infrastrukturen. Das BBK wird insbesondere mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eng zusammenarbeiten, um Kohärenz beim Cyberschutz und beim physischen Schutz von Kritischen Infrastrukturen zu erreichen.

Das BMI wird seine Koordinierungsrolle in Deutschland und im europäischen System verstärken und als Verbindungsstelle zu anderen Mitgliedstaaten, Drittstaaten und der Europäischen Kommission fungieren.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333