Bundesministerium
des Innern
und für Heimat

G7 GERMANY
2022

- *Entwurf* -

Eckpunkte für ein

KRITIS-Dachgesetz

Von der Alarmierung von Rettungskräften über die Stromversorgung bis zum Zahlungsverkehr – Kritische Infrastrukturen (KRITIS) sind für unsere Gesellschaft unverzichtbar. Jede und jeder Einzelne 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, über Terrorismus und Sabotage bis hin zu menschlichem Versagen. Ausfälle und Störungen der Kritischen Infrastrukturen können zu Versorgungsengpässen und erheblichen Störungen der öffentlichen Sicherheit führen. Die aktuellen Krisen wie die Covid-19-Pandemie oder die Auswirkungen des Ukraine-Kriegs und Sabotageakte wie jüngst bei der Deutschen Bahn und den Gaspipelines Nord Stream haben die Bedeutung und die Verwundbarkeit der Kritischen Infrastrukturen verdeutlicht. Die Resilienz von KRITIS ist für den Schutz von Bevölkerung, Wirtschaft und Gesellschaft in Deutschland essentiell.

Im Bereich der Cybersicherheit Kritischer Infrastrukturen gibt es mit dem BSI-Gesetz sowie der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) bereits umfassende Regelungen. Jenseits der Regulierung im Bereich Cybersicherheit gibt es jedoch in Deutschland bislang kein sektor- und gefahrenübergreifendes „Gesetz zum Schutz Kritischer Infrastrukturen“. Gesetzliche Regelungen mit explizitem Bezug zum physischen Schutz spezifischer Kritischer Infrastrukturen finden sich vereinzelt und in unterschiedlicher Qualität in Fachgesetzen. Teilweise werden dabei abstrakte Zielsetzungen formuliert, Befugnisse von Behörden festgeschrieben oder konkrete Vorgaben für Betreiber gemacht. Darüber hinaus fördern eine Vielzahl weiterer gesetzlicher Regelungen, Normen und Standards mittelbar auch den physischen Schutz Kritischer Infrastrukturen, wie etwa bautechnische Vorschriften. Aufgrund vielfältiger sektorübergreifender Verflechtungen ergeben sich darüber hinaus aber Fragestellungen, die über Ressort- und Sektorengrenzen hinweg diskutiert und bearbeitet werden müssen. Die Abhängigkeiten der Sektoren stellen komplexe Herausforderungen dar.

Gibt es Ausfälle in einem Sektor, etwa Energie, IT oder Logistik, kann dies schwere Auswirkungen auch auf andere Sektoren haben.

Vor dem Hintergrund uneinheitlicher Regelungen für den physischen Schutz Kritischer Infrastrukturen und angesichts sektorübergreifender Abhängigkeiten wird mit dem KRITIS-Dachgesetz zum ersten Mal das Gesamtsystem zum physischen Schutz Kritischer Infrastrukturen in den Blick genommen und gesetzlich geregelt. Das KRITIS-Dachgesetz ergänzt damit auch die bestehenden Regelungen zum Cyberschutz von Kritischen Infrastrukturen und wird für ein kohärentes und resilientes System sorgen.

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 Rahmen 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. Das sektor- und gefahrenübergreifende KRITIS-Dachgesetz ergänzt sektorspezifische gesetzliche und nicht-gesetzliche Regelungen. Auf Grundlage des KRITIS-Dachgesetzes werden wertvolle Erkenntnisse zur Lage in den KRITIS-Sektoren gewonnen. Hierauf basierend können weitergehende sektorspezifische Regelungen getroffen werden, um etwaige Regelungslücken zu schließen.

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

Ziele des KRITIS-Dachgesetzes:

- **Die Resilienz des Gesamtsystems der Kritischen Infrastrukturen wird durch einheitliche Mindestvorgaben für Resilienzmaßnahmen in allen Sektoren gestärkt**.
- Der Schutz Kritischer Infrastrukturen ist eine **akteursübergreifende und gesamtstaatliche Aufgabe**. In erster Linie müssen die Betreiber der Kritischen Infrastrukturen – ob private Unternehmen oder öffentliche Einrichtungen – für ihre Funktionsfähigkeit sorgen. Der bislang verfolgte kooperative Ansatz wird mit dem KRITIS-Dachgesetz durch **verpflichtende Schutzstandards für die physische Sicherheit** erweitert. 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.

- **Das Gesamtsystem beim physischen Schutz Kritischer Infrastrukturen muss im Vordergrund stehen**. Sektor- 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 Zusammenwirken erfordert. Gibt es Ausfälle in einem Sektor, etwa Energie oder Verkehr, kann dies schwere Auswirkungen auch auf andere Sektoren haben.
- Den Verflechtungen und Abhängigkeiten von Kritischen Infrastrukturen wird auch auf **administrativer Ebene** Rechnung getragen. In einem neuen Ansatz wird der 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 Festlegung von Definitionen, Sektoren, kritischen Dienstleistungen sowie Schwellenwerten dient diesem Ziel. Gemäß den Vorgaben aus der CER-Richtlinie werden Kritische Infrastrukturen mindestens in 11 Sektoren (Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, Digitale Infrastruktur,

öffentliche Verwaltung, Weltraum, Produktion, Verarbeitung und Vertrieb von Lebensmitteln) identifiziert. Bei der Ermittlung der Kritischen Infrastrukturen werden 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. Diese erbringen in sechs oder mehr Mitgliedstaaten der Europäischen Union dieselben oder ähnliche kritische Dienstleistungen und unterliegen daher nach der CER-Richtlinie einer verstärkten Aufsicht auf europäischer Ebene.

2. Risiken besser erkennen

   Die Gefahren für die kritischen Dienstleistungen werden einer regelmäßigen Bewertung unterzogen. Staatliche Risikobewertungen für die kritischen Dienstleistungen werden den Betreibern eine Grundlage für ihre eigenen regelmäßig vorzunehmenden spezifischen Risikobewertungen und den 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 sektorübergreifende 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. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) hat bereits Methoden für derartige Risikobewertungen erarbeitet und erfolgreich verwendet 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 sich umfassend gegenüber 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 zählt

   - die Einrichtung eines betrieblichen Risiko- und Krisenmanagements;

- die Durchführung von Risikoanalysen und – bewertungen;
- die Erstellung von Resilienzplänen und
- die Umsetzung geeigneter und verhältnismäßiger technischer und organisatorischer Maßnahmen sowie von Sicherheitsmaßnahmen 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 die Mindestvorgaben ausrichten.

4. <u>Störungen des Gesamtsystems erkennen und beheben</u>
   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 erstattet 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 sektorübergreifende Auswertungen vornehmen können, damit mit den aus Sicherheitsvorfällen gewonnen Erfahrungen Anpassungen für den Schutz Kritischer Infrastrukturen vorgenommen werden können. Diesem Zweck dient auch die Erstellung eines alle zwei Jahre zu erstellenden Berichts über Sicherheitsvorfälle durch die Zuständige Behörde. Dieser Bericht wird auch an die Europäische Kommission übermittelt.

5. <u>Schaffung eines institutionellen Rahmens</u>
   Die Zusammenarbeit der Vielzahl der am Schutz Kritischer Infrastrukturen beteiligter Akteure auf staatlicher Seite und bei den Betreibern Kritischer Infrastrukturen wird klarer herausgearbeitet. Durch klare Verantwortlichkeiten und Ansprechpartner für alle Fragestellungen im Zusammenhang mit dem physischen Schutz Kritischer Infrastrukturen wird eine bessere Zusammenarbeit erreicht.

   Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) wird zu der übergreifenden Zuständigen Behörde für den physischen Schutz Kritischer Infrastrukturen

ausgebaut. Das BBK verfügt hier bereits über umfangreiche methodische und sektorübergreifende Expertise. Dem BBK 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 die Aufsichtsbehörden vernetzen und insoweit bestehende Strukturen ergänzen. Eine derartige übergreifende Behörde ist für das mit dem KRITIS-Dachgesetz verfolgten Ziel der Betrachtung des Gesamtsystems erforderlich. Hierdurch werden außerdem eine schnelle Informationsweitergabe sowie die Bündelung von Wissen und Kompetenzen ermöglicht. 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 Bundesministerium des Innern und für Heimat (BMI) wird seine Koordinierungsrolle in Deutschland und im europäischen System verstärken und als Verbindungsstelle zu anderen Mitgliedstaaten, Drittstaaten und der Europäischen Kommission fungieren.