Referentenentwurf

des Bundesministeriums des Innern und für Heimat

Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen

(KRITIS-Dachgesetz – KRITIS-DachG)

A. Problem und Ziel

Am 13. Januar 2023 trat die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164; CER-Richtlinie) in Kraft. In der mit der CER-Richtlinie aufgehobenen Richtlinie 2008/114/EG des Rates (EKI-Richtlinie) war lediglich ein Verfahren für die Ausweisung europäischer kritischer Infrastrukturen im Energiesektor und im Verkehrssektor vorgesehen, deren Störung oder Zerstörung erhebliche grenzüberschreitende Auswirkungen in mindestens zwei Mitgliedstaaten hätte. Mit der CER-Richtlinie wurde ein einheitlicher europäischer Rechtsrahmen für die Stärkung der Resilienz kritischer Einrichtungen (im Folgenden wird statt „kritische Einrichtungen“ die Begrifflichkeit „kritische Anlage“ oder „Betreiber kritischer Anlagen“ verwendet) in mindestens elf Sektoren gegen Gefahren auch außerhalb des Schutzes der IT-Sicherheit im Binnenmarkt geschaffen. Ziel ist es, einheitliche Mindestverpflichtungen für Betreiber kritischer Anlagen festzulegen und deren Umsetzung durch kohärente, gezielte Unterstützungs- und Aufsichtsmaßnahmen zu garantieren. Um die Resilienz dieser Anlagen, die für das reibungslose Funktionieren des Binnenmarktes von entscheidender Bedeutung sind, zu stärken, schafft die CER-Richtlinie einen übergreifenden Rahmen („Dach“), der im Sinne des All-Gefahren-Ansatzes Naturkatastrophen oder vom Menschen verursachte, unbeabsichtigte oder vorsätzliche Gefährdungen berücksichtigt. Die CER-Richtlinie ist gemäß ihrem Artikel 26 Absatz 1 bis zum 17. Oktober 2024 in nationales Recht umzusetzen.

Der Schutz der IT-Sicherheit von Kritischen Infrastrukturen ist bereits im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) niedergelegt. Durch die Umsetzung der NIS-2-Richtlinie[1)] mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) und durch die DORA-Verordnung[2)] werden die Regelungen für Schutz der IT-Sicherheit kritischer Anlagen und weiteren Einrichtungen weiterentwickelt. Das KRITIS-DachG wird für die Resilienz kritischer Anlagen nach dem „All-Gefahrenansatz“ (Im Folgenden zur Abgrenzung von der IT-Sicherheit untechnisch „physischer Schutz“) neben diese Regelungen treten, aber gleichzeitig eine größtmögliche Kohärenz mit den Regelungen der IT-Sicherheit kritischer Anlagen sowie von wichtigen und besonders wichtigen

---

1) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27. Dezember 2022, S. 80.).

2) Verordnung (EU) 2022/2554 des Europäischen Parlamentes und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1–79).

Einrichtungen vorsehen, indem die Schnittstellen zwischen den Bereichen berücksichtigt und angeglichen, bzw. – soweit möglich und sinnvoll – übereinstimmend geregelt werden.

Ziel ist ein kohärentes System zur Stärkung der Resilienz kritischer Anlagen und wichtiger und besonders wichtiger Einrichtungen mit Blick auf physische Maßnahmen und IT-Sicherheitsmaßnahmen, welches die jeweiligen europarechtlichen Vorgaben umsetzt.

Zu beachten ist dabei, dass bei der Umsetzung der NIS-2-Richtlinie das bereits umfassend bestehende Regelungswerk erweitert wird, während im Hinblick auf die Resilienzmaßnahmen dieses Gesetzes mit der Umsetzung der CER-Richtlinie erstmals darüber hinausgehende Regelungen getroffen werden. Daher ist der Anwendungsbereich und die Regelungsintensität des KRITIS-DachG geringer als bei den Regelungen zur Umsetzung der NIS-2-Richtlinie, die bereits auf ein existierendes Regelungssystem aufsetzen und dieses weiterentwickeln. Durch gestufte Anforderungen an Betreiber kritischer Anlagen und wichtige und besonders wichtige Einrichtungen im KRITIS-DachG und dem NIS-2-Umsetzungsgesetz wird damit auch den Belangen der Wirtschaft Rechnung getragen.

Kritische Anlagen umfassen sind ein Teilbereich sog. Kritischer Infrastrukturen (KRITIS), der in bundesgesetzlicher Kompetenz geregelt wird, um einen gesamtheitlichen Überblick über die für die bundesweite Versorgungssicherheit elementaren Anlagen und diesbezügliche Störungen zu schaffen und ihnen Vorgaben zur Steigerung ihrer Resilienz zu machen.

Resilienzmaßnahmen nach dem KRITIS-DachG können auch von Betreibern Kritischer Infrastrukturen in den nach diesem Gesetz festgelegten Sektoren ergriffen werden, wenn sie die Schwellenwerte der auf der Grundlage des KRITIS-DachG zu erlassenden Rechtsverordnung nicht erreichen. So wird sichergestellt, dass auch kleinere und mittlere Unternehmen Maßnahmen zur Stärkung ihrer Resilienz ergreifen.

Um über das KRITIS-DachG hinausgehend die gesamtstaatlichen strategischen Ziele und politische Maßnahmen zur Stärkung der Resilienz Kritischer Infrastrukturen festzulegen, wird gemäß Artikel 4 der CER-Richtlinie bis 17. Januar 2026 eine nationale Strategie zur Verbesserung der Resilienz Kritischer Infrastrukturen (Nationale KRITIS-Resilienzstrategie) verabschiedet. Sie wird die derzeit gültige KRITIS-Strategie der Bundesregierung von Juni 2009 aktualisieren und erweitern.

B. Lösung

Die europarechtlichen Vorgaben der CER-Richtlinie werden mit dem vorliegenden neuen Stammgesetz umgesetzt. Es enthält Regelungen zur Identifizierung kritischer Anlagen, die in einer Verordnung weiter konkretisiert werden, sowie für deren Registrierung. Kritische Anlagen, die in mindestens sechs Mitgliedstaaten betrieben werden, werden als kritische Anlagen von besonderer Bedeutung für Europa identifiziert und unterliegen besonderen Maßnahmen. Den Betreibern der kritischen Anlagen werden Maßnahmen auferlegt, die die Resilienz der Anlage stärken sollen. Dazu gehört die Erarbeitung und Umsetzung von Resilienzplänen, in denen auf der Basis von Risikoanalyse und -bewertungen der Betreiber dargestellt wird, welche geeigneten und verhältnismäßigen technischen, sicherheitsbezogenen und organisatorischen Maßnahmen zur Stärkung der Resilienz getroffen werden. Anhang 1 zu dem Gesetz enthält zur Orientierung eine Übersicht von Maßnahmen, die die Betreiber kritischer Anlagen im Rahmen der Risikobeherrschung unter Beachtung von Eignung und Verhältnismäßigkeit insbesondere berücksichtigen können. Darüber hinaus müssen Betreiber kritischer Anlagen eine Kontaktstelle benennen und erhebliche Störungen melden. Um einen Gesamtüberblick über die Risiken für kritische Dienstleistungen zu erhalten und die Betreiber kritischer Anlagen bei ihren Maßnahmen zu unterstützen, werden regelmäßig staatliche Risikoanalysen und -bewertungen für die kritischen Dienstleistungen durchgeführt. Mittels der eingegangenen Meldungen über erhebliche Störungen sollen

weitere Betreiber kritischer Anlagen gewarnt und das Gesamtsystem zielgerichtet verbessert werden. Auch die Betreiber Kritischer Infrastrukturen, die die Schwellenwerte der auf der Grundlage des KRITIS-DachG zu erlassenden Rechtsverordnung nicht erreichen, können die Resilienzmaßnahmen nach dem KRITIS-DachG ergreifen. So wird sichergestellt, dass auch kleinere und mittlere Unternehmen Maßnahmen zur Stärkung ihrer Resilienz ergreifen. Das Gesetz enthält keine Entscheidungen über Ressourcenverteilungen.

Das KRITIS-DachG wird somit im Hinblick auf nicht-IT-bezogene Maßnahmen zur Stärkung der Resilienz kritischer Anlagen erstmals einheitliche bundesgesetzliche sektorenübergreifende Mindeststandards normieren.

Beim KRITIS-DachG 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 IT-Sicherheit und physischen Resilienzmaßnahmen von kritischen Anlagen berücksichtigt und angeglichen, bzw. – soweit möglich und sinnvoll – übereinstimmend geregelt. Die im KRITIS-DachG getroffenen Bestimmungen zu kritischen Anlagen orientieren sich an den bisherigen Regelungen zur IT-Sicherheit von Kritischen Infrastrukturen unter Berücksichtigung der geplanten Umsetzung der NIS-2-Richtlinie, um den Aufbau des Systems unter dem „All-Gefahren-Ansatz“ auch für die Wirtschaft zu erleichtern. Um ein Auseinanderfallen kritischer Anlagen im Sinne des BSIG einerseits und im Sinne des KRITIS-DachG andererseits zu vermeiden, werden kritische Anlagen künftig nur noch durch das KRITIS-DachG und die dazugehörige Rechtsverordnung bestimmt. Mit der Rechtsverordnung wird ersichtlich, welche Verpflichtungen für Betreiber kritischer Anlagen und weiterer Einrichtungen im Hinblick auf physische Resilienzmaßnahmen nach dem KRITIS-DachG und im Hinblick auf die IT-Sicherheit nach dem BSIG gelten. Darüber hinaus werden für die Registrierung der Betreiber sowie für die Meldung von erheblichen Störungen gemeinsame technische Lösungen angestrebt. Die enge Zusammenarbeit der beteiligten Behörden ist überdies im BSIG und im KRITIS-DachG geregelt. Weitere Angleichungen zwischen den Regelungen des BSIG und den Regelungen dieses Gesetzes werden nach der in § 18 vorgesehenen Evaluierung angestrebt.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Diese Angaben können derzeit noch nicht hinreichend konkretisiert werden und sollen daher im Verlaufe der weiteren Abstimmung ermittelt werden.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Es entsteht kein Erfüllungsaufwand für die Bürgerinnen und Bürger.

E.2 Erfüllungsaufwand für die Wirtschaft

Der Erfüllungsaufwand wird gegenwärtig in Zusammenarbeit mit dem Statistischen Bundesamt ermittelt. Die Darstellung soll sodann parallel zur Abstimmung des Entwurfs gemeinsam mit Ressorts und Ländern erarbeitet werden.

E.3 Erfüllungsaufwand der Verwaltung

Der Erfüllungsaufwand wird gegenwärtig in Zusammenarbeit mit dem Statistischen Bundesamt ermittelt. Die Darstellung soll sodann parallel zur Abstimmung des Entwurfs gemeinsam mit Ressorts und Ländern erarbeitet werden.

F. Weitere Kosten

Auswirkungen auf Einzelpreise, das allgemeine Preisniveau und das Verbraucherpreisniveau sind nicht zu erwarten.

Referentenentwurf des Bundesministeriums des Innern und für Heimat

Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen

(KRITIS- Dachgesetz – KRITIS-DachG)[3)]

Vom […]

Der Bundestag hat das folgende Gesetz beschlossen:

§ 1

Zweck des Gesetzes

Dieses Gesetz legt Kriterien zur Identifizierung kritischer Anlagen und Verpflichtungen für Betreiber kritischer Anlagen fest zur Gewährleistung der ungehinderten Erbringung von Dienstleistungen, die für die Aufrechterhaltung wichtiger wirtschaftlicher Tätigkeiten und Funktionen unerlässlich sind. Es legt weiterhin Vorschriften fest, die darauf abzielen, die Betreiber kritischer Anlagen bei ihren Verpflichtungen zu unterstützen, die Betreiber kritischer Anlagen zu beaufsichtigen und die Verpflichtungen durchzusetzen.

§ 2

Begriffsbestimmungen

Im Sinne dieses Gesetzes ist oder sind

1. „CER-Richtlinie“ Richtlinie des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164);

2. „Kritische Infrastrukturen“ Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der wirtschaftlichen Tätigkeit, der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden;

3. „kritische Anlage“ eine Anlage, die eine hohe Bedeutung für das Funktionieren des Gemeinwesens hat, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für wirtschaftliche Tätigkeiten, die öffentliche Sicherheit oder Ordnung eintreten würden; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach § 4;

[3)] Dieses Gesetz dient der Umsetzung der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Ra-tes (ABl. L 333 vom 27.12.2022, S. 164).

[Bei der Änderung von unterschiedlichen Vorschriften bitte den EU-Umsetzungshinweis präzise den einzelnen Artikeln zuordnen, so dass die Umsetzung bei den einschlägigen Stammvorschriften dokumentiert werden kann.]

4. „kritische Dienstleistung“ eine Dienstleistung zur Versorgung der Allgemeinheit, deren Ausfall oder Beeinträchtigung zu einer Gefährdung von wirtschaftlichen Tätigkeiten, zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde;

5. „Betreiber kritischer Anlagen“ eine natürliche oder juristische Person oder rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine kritische Anlage ausübt;

6. „Resilienz“ die Fähigkeit des Betreibers einer kritischen Anlage, einen Vorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Vorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen;

7. „Risiko“ das Potenzial für Verluste oder Beeinträchtigungen, die durch einen Vorfall verursacht werden;

8. „Risikoanalysen“ das systematische Verfahren zur Bestimmung des Risikos;

9. „Risikobewertungen“ der Prozess des Vergleichs und der Priorisierung von Risiken in Bezug auf deren Wirkung auf die kritische Dienstleistung und das Treffen von Entscheidungen hinsichtlich der Notwendigkeit von geänderten oder zusätzlichen Maßnahmen zur Risikobehandlung;

10. „Vorfall“ ein Ereignis, das die Erbringung einer kritischen Dienstleistung erheblich beeinträchtigt oder beeinträchtigen könnte.

    [Hinweis: Die nachfolgenden Begriffsbestimmungen dienen der Umsetzung der NIS-2-Richtlinie und sind dem Referentenentwurf des BMI für ein NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz entnommen. Die im Rahmen der Ressortabstimmung des vorgenannten Referentenentwurfs vorgenommenen Änderungen werden hier nachvollzogen werden. Das KRITIS-DachG muss diese Begriffsbestimmungen enthalten, damit die Festlegung von Einrichtungsarten und Schwellenwerten nach BSI-Gesetz und Schwellenwerten nach KRITIS-DachG zukünftig in einer einzigen Rechtsverordnung (nach § 15 KRITIS-DachG) erfolgen kann]

11. „Besonders wichtige Einrichtung“

    a) ein Großunternehmen, das einer der durch Rechtsverordnung nach § 15 bestimmten Einrichtungsarten der Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten (Business-to-Business) oder Weltraum zuzuordnen ist,

    b) ein qualifizierter Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter, jeweils unabhängig von der Unternehmensgröße,

    c) ein mittleres Unternehmen, das Anbieter von Telekommunikationsdiensten oder öffentlich zugänglichen Telekommunikationsnetzen ist,

    d) ein Betreiber kritischer Anlagen oder

    e) eine Einrichtung, die gemäß Rechtsverordnung nach § 15 dem Teilsektor Zentralregierung des Sektors öffentliche Verwaltung angehört,

ausgenommen Einrichtungen, die gemäß Artikel 2 Absatz 4 der Verordnung (EU) 2022/2554 von deren Anwendungsbereich ausgenommen wurden sowie solche, die als Finanzunternehmen gemäß Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 vergleichbaren Anforderungen unterliegen, wie sie dieser Teil für besonders wichtige Einrichtungen vorsieht.

12. „Wichtige Einrichtung“

a) ein mittleres Unternehmen, das einer der durch Rechtsverordnung nach § 15 bestimmten Einrichtungsarten der Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten (Business-to-Business) oder Weltraum zuzuordnen ist,

b) ein mittleres Unternehmen oder Großunternehmen, das einer der durch Rechtsverordnung nach § 15 bestimmten Einrichtungsarten der Sektoren Logistik, Siedlungsabfallentsorgung, Produktion, Chemie, Ernährung, verarbeitendes Gewerbe, Anbieter digitaler Dienste oder Forschung zuzuordnen ist,

c) wer Güter im Sinne des Teils B der Kriegswaffenliste herstellt oder entwickelt oder vom Bundesamt zugelassene Produkte mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder für die IT-Sicherheitsfunktion wesentliche Komponenten solcher Produkte herstellt,

d) wer Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung oder nach § 1 Absatz 2 der Störfall-Verordnung einem solchen gleichgestellt ist,

und keine besonders wichtige Einrichtung ist, sowie ausgenommen Einrichtungen, die gemäß Artikel 2 Absatz 4 der Verordnung (EU) 2022/2554 von deren Anwendungsbereich ausgenommen wurden sowie solche, die als Finanzunternehmen gemäß Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 vergleichbaren Anforderungen unterliegen, wie sie dieser Teil für besonders wichtige Einrichtungen vorsieht.

§ 3

Nationale zuständige Behörde für die Resilienz kritischer Anlagen

(1) Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) ist nationale zuständige Behörde nach Artikel 9 Absatz 1 Satz 1 der CER-Richtlinie und zentrale Anlaufstelle nach Artikel 9 Absatz 2 der CER-Richtlinie. Das BBK unterstützt die Betreiber kritischer Anlagen nach § 4 bei der Umsetzung ihrer nach diesem Gesetz zu erfüllenden Maßnahmen.

(2) Das Bundesamt für Informationssicherheit (BSI) und die Bundesnetzagentur (BNetzA) übermitteln dem BBK die für seine Aufgabenerfüllung erforderlichen Informationen hinsichtlich IT-Sicherheitsrisiken, -bedrohungen, -vorfällen, nicht IT-sicherheitsbezogenen Risiken, Bedrohungen und Vorfällen, die kritische Anlagen betreffen, sowie in Bezug auf entsprechende Maßnahmen, die gemäß der Richtlinie (EU) 2022/2555 ergriffen werden. Das BBK übermittelt an BSI und BNetzA Informationen hinsichtlich der in Satz 1 genannten Risiken, soweit dies für deren Aufgabenerfüllung erforderlich.

(3) Das BBK übermittelt der Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) Informationen, soweit dies erforderlich ist für deren Aufgabenerfüllung insbesondere in

Bezug auf die ergriffenen Maßnahmen gemäß der Verordnung (EU) 2022/2554. Die BaFin übermittelt an das BBK die für dessen Aufgabenerfüllung erforderlichen Informationen.

§ 4

Kritische Anlagen

(1) Eine Anlage ist ab dem durch die Rechtsverordnung nach § 15 festgelegten Stichtag eine kritische Anlage, wenn sie einer der durch Rechtsverordnung nach § 15 festgelegten Anlagenarten in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum, öffentliche Verwaltung oder Siedlungsabfallentsorgung zuzuordnen ist und die durch Rechtsverordnung festgelegten Schwellenwerte erreicht oder überschreitet.

(2) Eine Anlage ist ab dem nächsten folgenden durch die Rechtsverordnung nach § 15 als Stichtag festgelegten Tag keine kritische Anlage mehr, wenn sie die durch die Rechtsverordnung festgelegten Schwellenwerte unterschreitet.

§ 5

Verhältnis zu weiteren spezialgesetzlichen Regelungen

(1) Andere über die Mindestvorgaben nach diesem Gesetz hinausgehende Anforderungen an die Betreiber kritischer Anlagen bleiben unberührt.

(2) Unbeschadet der Regelungen dieses Gesetzes können Bund und Länder im Rahmen ihrer jeweiligen Zuständigkeiten resilienzsteigernde Maßnahmen sowie Vorgaben für ein Störungsmonitoring festlegen, insbesondere in den Sektoren und Bereichen Medien und Kultur, Bildung, Betreuung.

§ 6

Anforderungen an Betreiber Kritischer Infrastrukturen

(1) Resilienzmaßnahmen nach § 11 Absatz 1 Satz 1 und § 11 Absatz 1 Satz 3 können, soweit geeignet und verhältnismäßig, auch von Betreibern Kritischer Infrastrukturen in den nach § 4 Absatz 1 festgelegten Sektoren, die die Schwellenwerte der Rechtsverordnung nach § 155 nicht erreichen, zur Steigerung ihrer Resilienz ergriffen werden.

(2) Die Betreiber Kritischer Infrastrukturen nach Absatz 1 können zur Umsetzung der Verpflichtung nach Absatz 1 die nach § 11 Absatz 5 zu entwickelnden branchenspezifischen Resilienzstandards berücksichtigen.

§ 7

Kritische Anlagen von besonderer Bedeutung für Europa

(1) Eine Anlage gilt als kritische Anlage von besonderer Bedeutung für Europa, wenn

1. sie gemäß der Rechtsverordnung nach § 15 als kritische Anlage eingestuft wurde, und

2. sie für oder in sechs oder mehr Mitgliedstaaten der Europäischen Union die gleiche oder ähnliche Dienstleistungen gemäß der [Liste wesentlicher Dienste] der Europäischen Kommission erbringt und

3. ihr Betreiber eine Meldung durch die Europäische Kommission erhalten hat, dass sie von besonderer Bedeutung für Europa ist.

(2) Der Betreiber einer kritischen Anlage nach Absatz 1 teilt dem BBK mit, welche kritischen Dienstleistungen er für oder in diesen Mitgliedstaaten anbietet und für welche oder in welchen Mitgliedstaaten er diese anbietet. Das Bundesministerium des Innern und für Heimat teilt dies der Europäischen Kommission unverzüglich mit.

(3) Sobald die Europäische Kommission das Bundesministerium des Innern und für Heimat über ihre Entscheidung informiert, eine Anlage als kritische Anlage von besonderer Bedeutung für Europa zu betrachten, leitet das BBK diese Meldung unverzüglich an den Betreiber dieser kritischen Anlage weiter.

(4) Das BBK konsultiert im regelmäßigem Abstand die zuständigen Behörden anderer Mitgliedstaaten der Europäischen Union, sofern kritische Anlagen kritische Dienstleistungen erbringen, die zwischen zwei oder mehr Mitgliedstaaten verbunden sind, Teil von Unternehmensstrukturen sind, die mit kritischen Anlagen in anderen Mitgliedstaaten verbunden sind oder zu ihnen in Bezug stehen oder als kritische Anlage in einem Mitgliedstaat eingestuft wurden und kritische Dienstleistungen für andere oder in anderen Mitgliedstaaten erbringen.

(5) Wenn eine kritische Anlage mit besonderer Bedeutung für Europa identifiziert wurde, kann das Bundesministerium des Innern und für Heimat einen Antrag bei der Europäischen Kommission auf Einrichtung einer Beratungsmission stellen. Auf Anforderung der Europäischen Kommission, übermittelt das Bundesministerium des Innern und für Heimat der Europäischen Kommission

1. die entsprechenden Teile der Risikobewertungen gemäß § 10 der Betreiber der kritischen Anlagen,

2. eine Auflistung der Maßnahmen nach § 11 und

3. eine Auflistung der Aufsichts- und Durchsetzungsmaßnahmen, die das BBK ergriffen hat.

§ 8

Registrierung der kritischen Anlage

(1) Betreiber kritischer Anlagen sind verpflichtet, spätestens bis zum ersten Werktag, der darauffolgt, dass die Anlage erstmalig oder erneut als kritische Anlage nach § 4 gilt, die von ihnen betriebene kritische Anlage bei einer gemeinsam vom BBK und dem Bundesamt für Sicherheit in der Informationstechnik eingerichteten Registrierungsmöglichkeit zu registrieren.

(2) Wenn der Betreiber seine Pflicht zur Registrierung einer kritischen Anlage nicht erfüllt, kann das BBK die Registrierung im Einvernehmen mit der sonst zuständigen Aufsichtsbehörde des Bundes auch selbst vornehmen.

(3) Jeder Betreiber einer kritischen Anlage muss dem BBK eine Kontaktstelle oder eine Person mit vergleichbarer Aufgabenstellung als Ansprechpartner benennen.

(4) Die Betreiber haben sicherzustellen, dass sie über die benannte Kontaktstelle jederzeit erreichbar sind.

(5) Das BBK erstellt eine Liste der Betreiber kritischer Anlagen. Diese Liste wird spätestens alle vier Jahre aktualisiert.

§ 9

Nationale Risikoanalysen und Risikobewertungen

(1) Die für die Sektoren zuständigen Bundesministerien führen alle vier Jahre oder auf Veranlassung für die auf der Grundlage der Rechtsverordnung nach § 15 bestimmten kritischen Dienstleistungen Risikoanalysen und -bewertungen gemäß ihren fachlichen und sektorspezifischen Zuständigkeiten durch, die mindestens

1. die die Wirtschaftsstabilität bedrohenden naturbedingten, klimatischen und vom Menschen verursachten Risiken berücksichtigen, darunter solche sektorübergreifender oder grenzüberschreitender Art, Unfälle, Naturkatastrophen, gesundheitliche Notlagen, sowie hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten gemäß der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates2),

2. die die Wirtschaftsstabilität beeinträchtigenden Risiken berücksichtigen, die sich aus dem Ausmaß der Abhängigkeit zwischen den im Anhang genannten Sektoren, einschließlich dem Ausmaß der Abhängigkeit gegenüber in anderen Mitgliedstaaten und Drittstaaten ansässigen kritischen Anlagen, ergeben, sowie die Auswirkungen, die eine in einem Sektor auftretende erhebliche Störung auf andere Sektoren haben kann, darunter alle wesentlichen Risiken für den Binnenmarkt und die Bevölkerung,

3. die allgemeine Risikobewertung nach Artikel 6 Absatz 1 des Beschlusses Nr. 1313/2013/EU,

4. die sonstige Risikobewertungen, die im Einklang mit den Anforderungen der entsprechenden sektorspezifischen Rechtsakte der Union sind, einschließlich der Verordnungen (EU) 2017/1938 und (EU) 2019/941 des Europäischen Parlaments und des Rates sowie der Richtlinien 2007/60/EG und 2012/18/EU des Europäischen Parlaments und des Rates, sowie

5. sämtliche gemäß § 12 gemeldeten Informationen über Vorfälle berücksichtigen.

(2) Die Bundesministerien stellen dem BBK die Risikoanalysen und -bewertungen zur Verfügung. Das BBK wertet die durch die Bundesministerien durchgeführten Risikoanalysen und -bewertungen sektorenübergreifend aus und stellt die entsprechenden Elemente der Risikoanalysen und -bewertungen den Betreibern kritischer Anlagen nach § 4 zur Verfügung.

(3) Das BBK übermittelt der Europäischen Kommission innerhalb von drei Monaten nach Durchführung einer Risikoanalyse- und -bewertung entsprechende Informationen über die ermittelten Arten von Risiken und die Ergebnisse dieser Risikoanalyse- und -bewertungen, aufgeschlüsselt nach den im Anhang der CER-Richtlinie genannten Sektoren und Teilsektoren.

§ 10

Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen

(1) Betreiber kritischer Anlagen führen auf Grundlage der durchgeführten staatlichen Risikoanalysen und -bewertungen nach § 9 und anderer Informationsquellen erstmals neun Monate nach der Registrierung als kritische Anlage nach § 8, und dann spätestens alle vier Jahre Risikoanalysen und -bewertungen durch, die

1. die entsprechenden, die Wirtschafsstabilität beeinträchtigenden, naturbedingten, klimatischen und vom Menschen verursachten Risiken berücksichtigen, darunter solche sektorübergreifender oder grenzüberschreitender Art, Unfälle, Naturkatastrophen, gesundheitliche Notlagen, sowie hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten gemäß der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates und

2. die entsprechenden, die Wirtschafsstabilität beeinträchtigenden, Risiken berücksichtigen, die sich aus dem Ausmaß der Abhängigkeiten anderer Sektoren von der kritischen Dienstleistung, die von der kritischen Anlage - auch in benachbarten Mitgliedstaaten und Drittstaaten - erbracht wird, und dem Ausmaß der Abhängigkeit der kritischen Anlage von den kritischen Dienstleistungen, die von anderen Anlagen in anderen Sektoren - auch in benachbarten Mitgliedstaaten und Drittstaaten - erbracht wird, Rechnung tragen.

(2) Hat ein Betreiber einer kritischen Anlage aufgrund von Verpflichtungen aus anderen öffentlich-rechtlichen Vorschriften für einen anderen Anlass bereits gleichwertige, Risikoanalysen und -bewertungen vorgenommen, erfüllt er die nach § 10 festgelegten Anforderungen. Das BBK kann im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes eine bestehende Risikoanalyse und -bewertung, die von einem Betreiber der kritischen Anlage durchgeführt wurde und die sich mit den in Absatz 1 Nummer 1 und Nummer 2 genannten Risiken und dem Ausmaß der Abhängigkeit befasst, als vollständig oder teilweise den Verpflichtungen nach diesem Artikel entsprechend erklären, wenn sie dem BBK vom Betreiber der kritischen Anlage vorgelegt werden.

(3) Die Vorschriften der Absätze 1 und 2 gelten nicht für Betreiber kritischer Anlagen in den Sektoren Finanz- und Versicherungswesen und Informationstechnik und Telekommunikation.

§ 11

Resilienzmaßnahmen der Betreiber kritischer Anlagen

(1) Betreiber kritischer Anlagen sind verpflichtet, geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu treffen. Diese Maßnahmen sind auf der Grundlage der nach § 9 bereitgestellten Informationen über die staatlichen Risikoanalysen und -bewertungen sowie den Ergebnissen der eigenen Risikoanalyse und -bewertung nach § 10 zu treffen. Dabei soll der Stand der Technik eingehalten werden.

(2) Technische, sicherheitsbezogene und organisatorische Maßnahmen sind verhältnismäßig, wenn der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls oder einer Beeinträchtigung der kritischen Dienstleistung zu den Folgen ihres Ausfalls oder ihrer Beeinträchtigung angemessen erscheint.

(3) Zu den Maßnahmen zählen Maßnahmen, die erforderlich sind, um

1. das Auftreten von Vorfällen zu verhindern,

2. einen angemessenen physischen Schutz der Räumlichkeiten der kritischen Anlagen zu gewährleisten,

3. auf Vorfälle zu reagieren, sie abzuwehren und die Folgen solcher Vorfälle zu begrenzen,

4. nach Vorfällen die Wiederherstellung zu gewährleisten,

5. ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeiter zu gewährleisten, einschließlich des Personals externer Dienstleister und

6. das entsprechende Personal für die unter den Nummern 1 bis 5 genannten Maßnahmen durch Informationsmaterialien, Schulungen und Übungen zu sensibilisieren.

(4) Maßnahmen, die von den Betreibern der kritischen Anlage bei der Abwägung nach Absatz 2 insbesondere berücksichtigt werden können, enthält Anhang 1.

(5) Betreiber kritischer Anlagen und ihre Branchenverbände können branchenspezifische Resilienzstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das BBK stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt

1. im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik oder

2. im Einvernehmen mit einer zuständigen Aufsichtsbehörde des Bundes.

(6) Die Betreiber kritischer Anlagen müssen die Maßnahmen nach Absatz 1 in einem Resilienzplan darstellen. Der Resilienzplan ist dem BBK spätestens zu einem vom BBK bei der Registrierung im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik festgelegten Zeitpunkt und anschließend alle zwei Jahre nachzuweisen.

(7) Haben Betreiber kritischer Anlagen Dokumente zur Stärkung der Resilienz erstellt oder Maßnahmen zur Stärkung der Resilienz aufgrund von Verpflichtungen, die für die genannten Maßnahmen nach Absatz 1 relevant sind, ergriffen, so können sie diese Dokumente und Maßnahmen verwenden, um die nach § 11 festgelegten Anforderungen zu erfüllen. Diese Dokumente sind dem BBK zu dem nach Absatz 6 Satz 2 festgelegten Zeitpunkt vorzulegen. Das BBK kann im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes bestehende Maßnahmen zur Verbesserung der Resilienz einer kritischen Anlage, die die in Absatz 1 genannten technischen, sicherheitsbezogenen und organisatorischen Maßnahmen betreffen, als vollständig oder teilweise den Verpflichtungen nach § 11 entsprechend erklären. Legt der Betreiber einer kritischen Anlage Bescheide, Genehmigungen, Zertifizierungen oder ähnliche Nachweise zur Resilienzsteigerung von in anderem Zusammenhang zuständigen Behörden vor, gelten die darin beschriebenen Maßnahmen ohne weitere Überprüfung als insoweit die nach § 11 festgelegten Anforderungen erfüllend.

(8) Betreiber kritischer Anlagen haben die Erfüllung der Anforderungen nach Absatz 1 spätestens zu einem vom BBK bei der Registrierung im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik festgelegten Zeitpunkt und anschließend alle zwei Jahre dem BBK auf geeignete Weise nachzuweisen. Der Nachweis kann durch Audits erfolgen. Die Betreiber übermitteln dem BBK die Ergebnisse der durchgeführten Audits einschließlich der dabei aufgedeckten Mängel. Das BBK kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Mängeln die Vorlage eines geeigneten Mängelbeseitigungsplanes und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes die Beseitigung der Mängel verlangen. Das BBK kann die

Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen. Das BBK kann zur Ausgestaltung des Verfahrens der Audits und Erbringung des Nachweises nach Satz 2 Anforderungen an die Art und Weise der Durchführung, an die Geeignetheit der zu erbringenden Nachweise sowie fachliche und organisatorische Anforderungen an die Prüfer und die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und Einrichtungen und der betroffenen Wirtschaftsverbände festlegen. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des BBK, die abrufbar ist unter der URL http:// /[genaue URL noch einzufügen].

(9) Bei erheblichen Zweifeln an der Einhaltung der Anforderungen nach dem Absatz 1 kann das BBK im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes die Einhaltung der Anforderungen überprüfen. Bei der Durchführung der Überprüfung kann es sich eines qualifizierten unabhängigen Dritten bedienen. Der Betreiber der kritischen Anlage hat dem BBK und den zuständigen Aufsichtsbehörden des Bundes und den in deren Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung kann das BBK Gebühren und Auslagen bei dem Betreiber der kritischen Anlage nur erheben, sofern das BBK auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach Absatz 1 begründeten.

(10) Das BBK kann im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes im Anschluss an die Aufsichtsmaßnahme nach Absatz 9 bei Verstößen gegen die Anforderungen nach dem Absatz 1 den Betreiber der kritischen Anlage anweisen, erforderliche und verhältnismäßige Maßnahmen zu ergreifen, um festgestellte Verstöße innerhalb einer angemessenen Frist zu beheben und diesen Behörden Informationen über die ergriffenen Maßnahmen zu übermitteln.

(11) Die Vorschriften und die Zuständigkeit der Fachbehörden im Rahmen des Zivil- und Katastrophenschutzes im Fall einer Krisensituation bleiben unberührt.

(12) Hinsichtlich des personellen Schutzes bleiben die Vorschriften des Sicherheitsüberprüfungsgesetzes (SÜG) in Verbindung mit der Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) sowie die Fachgesetze hinsichtlich der Zuverlässigkeitsüberprüfungen unberührt.

(13) Die Verpflichtungen nach Absatz 1 bis 10 treffen die Betreiber der kritischen Anlage frühestens nach Ablauf von zehn Monaten nach Registrierung als kritische Anlage nach § 4.

(14) Die Vorschriften nach § 11 gelten nicht für kritische Anlagen in den Sektoren Finanz- und Versicherungswesen und Informationstechnik und Telekommunikation.

§ 12

Meldewesen für Störungen

(1) Betreiber kritischer Anlagen sind, unbeschadet anderer gesetzlicher Meldeverpflichtungen gegenüber zuständigen Behörden, verpflichtet, Vorfälle, die die Erbringung ihrer kritischen Dienstleistungen erheblich stören könnten, unverzüglich über ihre Kontaktstelle im Sinne von § 8 Absatz 3 an eine vom BBK im Einvernehmen mit dem BSI eingerichtete gemeinsame Meldestelle zu melden. Hierbei sind insbesondere Angaben zu Anzahl und Anteil der von der Störung betroffenen Nutzer, bisherige und voraussichtliche Dauer

der Störung sowie das betroffene geografisches Gebiet der Störung, unter Berücksichtigung des Umstandes, ob das Gebiet geografisch isoliert ist, zu berücksichtigen.

(2) Die Meldungen müssen sämtliche verfügbaren Informationen enthalten, die erforderlich sind, damit die Art, Ursache und mögliche Folgen des Vorfalls nachvollzogen und ermittelt werden können, einschließlich verfügbarer Informationen, die notwendig sind, um zu bestimmen, ob der Vorfall grenzüberschreitende Auswirkungen hat.

(3) Betreiber kritischer Anlagen übermitteln eine erste Meldung bis spätestens 24 Stunden nach Kenntnisnahme des Vorfalls, es sei denn, dies ist in operativer Hinsicht nicht möglich. Spätestens einen Monat danach wird ein ausführlicher Bericht übermittelt.

(4) Das BBK unterrichtet die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten, sofern der Vorfall erhebliche Auswirkungen auf Betreiber kritischer Anlagen und die Aufrechterhaltung der Erbringung kritischer Dienstleistungen in einem oder in mehreren anderen Mitgliedstaaten haben könnte.

(5) Hat ein Vorfall erhebliche Auswirkungen auf die Kontinuität der Erbringung kritischer Dienstleistungen für oder in sechs oder mehr Mitgliedstaaten oder könnte er solche Auswirkungen haben, so meldet das Bundesministerium des Innern und für Heimat diesen Vorfall der Europäischen Kommission.

(6) Das BBK übermittelt dem betreffenden Betreiber der kritischen Anlage im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes sachdienliche Folgeinformationen.

(7) Auswertungen zu Störungsmeldungen teilt das BBK mit den zuständigen Aufsichtsbehörden des Bundes und den sonstigen zuständigen Aufsichtsbehörden.

(8) Die Verpflichtungen nach § 12 treffen den Betreiber einer kritischen Anlage nach Ablauf von zehn Monaten nach der Registrierung als kritische Anlage nach § 8.

(9) Die Vorschriften nach § 12 gelten nicht für kritische Anlagen in den Sektoren Finanz- und Versicherungswesen und Informationstechnik und Telekommunikation.

§ 13

Einsatz kritischer Komponenten; Verordnungsermächtigung

§ 14

Berichtspflichten

Das BBK übermittelt folgende Informationen an die Europäische Kommission:

1. innerhalb von drei Monaten nach Durchführung einer Risikoanalyse- und -bewertung nach § 9 Informationen über die ermittelten Arten von Risiken und die Ergebnisse dieser Risikoanalysen und -bewertungen, aufgeschlüsselt nach den im Anhang der CER-Richtlinie genannten Sektoren und Teilsektoren,

2. nach der Ermittlung der kritischen Anlagen unverzüglich und anschließend alle vier Jahre die Liste der wesentlichen Dienste gemäß Artikel 7 Absatz 2a der CER-Richtlinie, die Zahl der ermittelten kritischen Anlagen für jeden in § 15 festgelegten Sektor für jede

aufgrund der Rechtsverordnung nach § 14 festgelegte kritische Dienstleistung sowie die Schwellenwerte, die zur Spezifizierung eines oder mehrerer der in Artikel 7 Absatz der CER-Richtlinie genannten Kriterien angewandt werden,

3. bis zum 17. Juli 2028 und danach alle zwei Jahre der Europäischen Kommission und der Gruppe für die Resilienz kritischer Einrichtungen einen zusammenfassenden Bericht über die Anzahl und die Art der eingegangenen Meldungen nach § 12 und der gemäß § 11 ergriffenen Maßnahmen, zur Unterrichtung anderer Mitgliedstaaten.

§ 15

Ermächtigung zum Erlass von Rechtsverordnungen

Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz ohne Zustimmung des Bundesrates

1. unter Festlegung der in den jeweiligen Sektoren Energie, Transport und Verkehr, Bankwesen, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, öffentliche Verwaltung, Weltraum sowie Siedlungsabfallentsorgung wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Anlagen davon als kritische Anlagen im Sinne dieses Gesetzes gelten,

2. sowie welche Einrichtungsarten in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten (Business-to-Business), öffentliche Verwaltung und Weltraum Einrichtungsarten besonders wichtiger Einrichtungen sind, und

3. welche Einrichtungsarten in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Siedlungsabfallentsorgung, Logistik, Produktion, Chemie, Ernährung, verarbeitendes Gewerbe, Anbieter digitaler Dienste oder Forschung Einrichtungsarten wichtiger Einrichtungen sind.

Der nach Satz 1 als bedeutend anzusehende Versorgungsgrad ist anhand von branchenspezifischen Schwellenwerten für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen. In der Rechtsverordnung können auch Stichtage festgelegt und Teile der Bundesverwaltung als kritische Infrastruktur bestimmt werden.

§ 16

Ausnahmebescheid

(1) Das Bundesministerium des Innern und für Heimat kann auf Vorschlag des Bundeskanzleramts, des Bundesministeriums für Verteidigung oder auf eigenes Betreiben Betreiber kritischer Anlagen nach § 4 Absatz 1 von Verpflichtungen nach diesem Gesetz nach Maßgabe des Absatzes 2 teilweise (einfacher Ausnahmebescheid) oder des Absatzes 3

insgesamt (erweiterter Ausnahmebescheid) befreien, sofern durch den Betreiber kritischer Anlagen gleichwertige Vorgaben eingehalten werden.

(2) Betreiber kritischer Anlagen, die

1. in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten (relevante Bereiche) tätig sind oder Dienste erbringen, oder

2. ausschließlich für Behörden, die Aufgaben in relevanten Bereichen nach Nummer 1 erfüllen, tätig sind oder Dienste erbringen,

können für diese Tätigkeiten oder Dienste von den Maßnahmen nach § 10 und § 11 und Meldepflichten nach § 12 befreit werden. Die Resilienz dieser Betreiber kritischer Anlagen muss in diesen Fällen anderweitig gewährleistet sein und beaufsichtigt werden.

(3) Betreiber kritischer Anlagen, die ausschließlich in den relevanten Bereichen nach Absatz 2 Nummer 1 tätig sind oder Dienste erbringen, können insgesamt von den in Absatz 2 genannten Pflichten und von der Registrierungspflicht nach § 8 befreit werden. Absatz 2 Satz 2 gilt entsprechend.

(4) Ein Ausnahmebescheid nach diesem Gesetz ist zu widerrufen, wenn nachträglich Tatsachen eintreten, die zur Ablehnung einer Erteilung einer Ausnahme hätten führen müssen. Abweichend von Satz 1 kann im Falle eines vorübergehenden Wegfalls der Voraussetzungen des Absatz 2 Nummer 1 oder 2 aus besonderen Gründen von einem Widerruf abgesehen werden.

§ 17

Verarbeitung personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch das BBK nach diesem Gesetz ist zulässig, soweit

1. dies zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben erforderlich und

2. eine Verarbeitung anonymisierter oder künstlich erzeugter Daten hierfür nicht in gleicher Weise geeignet ist.

(2) Die Verarbeitung personenbezogener Daten durch das Bundesamt zu anderen Zwecken als demjenigen, zu dem die Daten ursprünglich erhoben wurden, ist unbeschadet von § 23 des Bundesdatenschutzgesetzes zulässig, wenn die Verarbeitung erforderlich ist zur

1. Sammlung, Auswertung oder Untersuchung von Informationen über Vorfälle nach § 12 oder

2. zur Unterstützung oder Beratung in Fragen zur Gewährleistung der Resilienz durch Betreiber kritischer Anlagen

und

kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

(3) Das BBK sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes vor.

§ 18

Evaluierung

Das Bundesministerium des Innern und für Heimat wird die Regelungen dieses Gesetzes regelmäßig, spätestens nach Ablauf von fünf Jahren nach Inkrafttreten des Gesetzes auf wissenschaftlich fundierter Grundlage evaluieren.

§ 19

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich

1. entgegen § 8 Absatz 1 in Verbindung mit § 4 eine Registrierung nicht oder nicht rechtzeitig vornimmt;

2. entgegen § 8 Absatz 3 dem BBK keine Kontaktstelle oder eine Person mit vergleichbarer Aufgabenstellung als Ansprechpartner benennt;

3. entgegen § 10 Absatz 1 Risikoanalysen und -bewertungen nicht oder nicht rechtzeitig durchführt;

4. entgegen § 11 Absatz 8 6 Satz 2 dem BBK innerhalb des dort geregelten Zeitraums den Resilienzplan nach § 10 Absatz 6 Satz 1 oder Bescheide, Genehmigungen, Zertifizierungen oder ähnliche Nachweise von anderen Behörden im Sinne von § 10 Absatz 7 Satz 4 nicht vorlegt, oder

5. entgegen § 11 Absatz 9 Satz 3 das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten nicht gestattet, auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise nicht vorlegt, Auskunft nicht erteilt und die erforderliche Unterstützung nicht gewährt.

(2) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das BBK.

(3) Die Höhe der Bußgelder beträgt […]

(4) Die Verhängung von Bußgeldern durch das BBK muss verhältnismäßig sein. Stellt das BBK fest, dass ein Betreiber einer kritischen Anlage seinen Verpflichtungen aus diesem Gesetz im Sinne des Absatzes 1 nicht nachgekommen ist, muss es zunächst den Betreiber einer kritischen Anlage auffordern, innerhalb einer angemessenen Frist seinen Verpflichtungen aus diesem Gesetz nachzukommen, insbesondere die erforderlichen und verhältnismäßigen Maßnahmen zu ergreifen, um festgestellte Verstöße gegen dieses Gesetz zu beheben.

§ 20

Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich der Absätze 2 und 3 am Tag nach der Verkündung in Kraft.

(2) §§ 6 bis 8, §§ 10 bis 12 und § 16 dieses Gesetzes treten am 1. Januar 2026 in Kraft.

(3) § 19 tritt am 1. Januar 2027 in Kraft.

Anhang 1 (insbesondere zu berücksichtigende Maßnahmen nach § 11 Absatz 1)

Zu den bei einer Abwägung durch den Betreiber kritischer Anlagen zu berücksichtigenden Maßnahmen nach § 11 Absatz 1 können insbesondere folgende zählen:

a) um das Auftreten von Vorfällen zu verhindern:

- Maßnahmen der Notfallvorsorge

- Maßnahmen zur Anpassung an den Klimawandel

b) um einen angemessenen physischen Schutz ihrer Räumlichkeiten und Kritischen Infrastrukturen zu gewährleisten:

- Maßnahmen des Objektschutzes, u.a. das Aufstellen von Zäunen und Sperren

- Instrumente und Verfahren für die Überwachung der Umgebung

- Detektionsgeräte

- Zugangskontrollen

c) um auf Vorfälle zu reagieren, sie abzuwehren und die Folgen solcher Vorfälle zu begrenzen:

- Risiko- und Krisenmanagementverfahren und –protokolle

- vorgegebene Abläufe im Alarmfall

d) um nach Vorfällen die Wiederherstellung zu gewährleisten:

- Maßnahmen zur Aufrechterhaltung des Betriebs (z.B. Notstromversorgung)

- Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wiederaufzunehmen

e) um ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeiter zu gewährleisten:

- Festlegung von Kategorien von Personal, das kritische Funktionen wahrnimmt,

- Festlegung von Zugangsrechten zu Räumlichkeiten, kritischen Infrastrukturen und zu sensiblen Informationen

- Berücksichtigung von Verfahren für Zuverlässigkeitsüberprüfungen und Benennung von Kategorien von Personal, die solche Zuverlässigkeitsüberprüfungen durchlaufen müssen; dabei bleiben die Vorschriften der Fachgesetze hinsichtlich der Zuverlässigkeitsüberprüfungen unberührt

- Festlegung angemessener Schulungsanforderungen und Qualifikationen

f) um das entsprechende Personal für die unter den Buchstaben a bis e genannten Maßnahmen zu sensibilisieren:

- Schulungen

- Informationsmaterial

- Übungen

Zur Unterstützung der Betreiber kritischer Anlagen bei der Abwägung stellt das BBK Vorlagen und Muster zur Verfügung.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Das KRITIS-DachG wird im Hinblick auf physische Maßnahmen zur Stärkung der Resilienz kritischer Anlagen erstmals einheitliche bundesgesetzliche sektorenübergreifende Mindeststandards normieren.

Der Schutz der IT-Sicherheit Kritischer Infrastrukturen ist bereits im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) niedergelegt. Durch die Umsetzung der NIS-2-Richtlinie mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) und durch die DORA-Verordnung werden die Regelungen zum Cyberschutz von Kritischen Infrastrukturen weiterentwickelt. Das KRITIS-DachG wird neben diese Regelungen treten, aber gleichzeitig eine größtmögliche Kohärenz mit den künftigen Regelungen des Cyberschutzes von kritischen Anlagen und weiteren Einrichtungen vorsehen, indem die Schnittstellen zwischen den Bereichen berücksichtigt und angeglichen, bzw. – soweit möglich und sinnvoll – übereinstimmend geregelt werden.

Damit wird ein kohärentes System zur Stärkung der Resilienz kritischer Anlagen und weiterer Einrichtungen mit Blick auf physische Maßnahmen und Cyberschutzmaßnahmen geschaffen, welches die jeweiligen europarechtlichen Vorgaben umsetzt.

Zu beachten ist dabei, dass beim Cyberschutz bei der Umsetzung der NIS-2-Richtlinie das bereits umfassend bestehende Regelungswerk erweitert wird, während im Hinblick auf physische Resilienzmaßnahmen mit der Umsetzung der CER-Richtlinie erstmals umfassende Regelungen getroffen werden. Daher ist die Reichweite des KRITIS-DachG geringer als die Reichweite der Regelungen zur Umsetzung der NIS-2-Richtlinie, die bereits auf ein existierendes Regelungssystem aufsetzt und dieses weiterentwickelt.

Die im KRITIS-DachG getroffenen Bestimmungen zu kritischen Anlagen orientieren sich an den bisherigen Regelungen zum Cyberschutz von Kritischen Infrastrukturen unter Berücksichtigung der geplanten Umsetzung der NIS-2-Richtlinie, um den Aufbau des Systems unter dem All-Gefahren-Ansatz auch für die Wirtschaft zu erleichtern.

Für eine bessere Übersichtlichkeit wird es eine gemeinsame Rechtsverordnung zur Bestimmung kritischer Anlagen sowie wichtiger und besonders wichtiger Einrichtungen nach dem KRITIS-DachG und dem BSIG geben. Mit der Rechtsverordnung wird ersichtlich, welche Verpflichtungen für Betreiber von kritischen Anlagen und wichtigen und besonders wichtigen Einrichtungen im Hinblick auf physische Resilienzmaßnahmen nach dem KRITIS-DachG und im Hinblick auf den Cyberschutz nach BSIG gelten. Darüber hinaus wird für die Registrierung der Betreiber sowie für die Meldung von Störungen eine gemeinsame technische Lösung angestrebt, sodass hier möglichst geringer Verwaltungsaufwand für die Wirtschaft entsteht. Die enge Zusammenarbeit der beteiligten Behörden ist überdies im KRITIS-DachG und im BSIG geregelt. Weitere Angleichungen zwischen den Regelungen dieses Gesetzes und den Regelungen des Cyberschutzes werden nach der in § 18 vorgesehenen Evaluierung angestrebt.

Das KRITIS-DachG verfolgt in erster Linie den Ansatz, Betreibern kritischer Anlagen konkrete Vorgaben zur Aufrechterhaltung, Stärkung oder Herstellung ihrer Handlungsfähigkeit

und Resilienz zu machen, um dem Risiko einer Beeinträchtigung ihres Geschäftsbetriebs entgegenzuwirken, damit dieser auch bei Störungen oder Ausfällen aufrechterhalten oder schnell wiederhergestellt werden kann. Geregelt werden damit Vorgaben, die präventiv zur Risikovorsorge in den wirtschaftlichen Betrieb eingreifen und somit einen wirtschaftslenkenden Zweck verfolgen. Betreiber kritischer Anlagen müssen künftig die nach diesem Gesetz vorgesehenen Aufgaben und Maßnahmen in ihre wirtschaftliche Betätigung integrieren, welche einen nicht unerheblichen Effekt auf ihre wirtschaftlichen Abläufe und Organisationen haben können und damit wirtschaftslenkend in den Betrieb von kritischen Anlagen eingreifen. Insbesondere wird erstmalig gesetzlich festgelegt, welche Anlagen als kritische Anlagen gelten mit der Folge, dass die Betreiber dieser kritischen Anlagen dann den Vorgaben dieses Gesetzes folgen müssen.

Funktionierende und resiliente Infrastrukturen und Dienstleistungen wie die Stromversorgung, die Wasserversorgung oder die Lebensmittelproduktion sind die Grundlage für die moderne Wirtschaft Deutschlands und sind Voraussetzung für Wohlstand und Wachstum. Kommt es zu Störungen oder Ausfällen bei bestimmten Infrastrukturen, ist dies nicht nur für das betroffene Unternehmen nachteilig, sondern kann aufgrund gegenseitiger Abhängigkeiten und Verflechtungen in einer europaweit und global vernetzten Welt zu einer Vielzahl an weiteren Störungen und Ausfällen im gleichen Sektor oder in anderen Sektoren führen. Diese Kaskadeneffekte können Auswirkungen auf die gesamte Wertschöpfungskette haben. Diese Anlagen, Infrastrukturen, Dienstleistungen und Unternehmen, die als kritische Anlagen betrachtet werden, gilt es daher zu identifizieren und besonders resilient zu machen. Dies gilt sowohl im Hinblick auf Maßnahmen des Cyberschutzes, als auch im Hinblick auf physische Maßnahmen, die die Resilienz von kritischen Anlagen stärken. Die Abhängigkeiten innerhalb und zwischen den Sektoren müssen stärker in den Blick genommen werden.

Mit zunehmend durch den Klimawandel bedingten natursächlichen Krisen und solchen, die durch neue geo- und wirtschaftspolitische Situationen ausgelöst werden, wachsen die Herausforderungen für das Funktionieren der Wirtschaft. Betreiber kritischer Anlagen sehen sich immer mehr einer gestiegenen Bedrohungslage und Vulnerabilität ihrer Unternehmen ausgesetzt und müssen die Herausforderung sich an die neuen Bedingungen anpassen. Die künftigen Krisenszenarien sind nicht vorhersehbar und können unerwartete Ausmaße für Wirtschaft und Gesellschaft annehmen. Um Resilienz und Handlungsfähigkeit von kritischen Anlagen die entsprechende wirtschaftspolitische Priorität einzuräumen, sind neue und veränderte wirtschaftliche Rahmenbedingungen notwendig, die den Betreibern kritischer Anlagen größere Orientierung und Handlungssicherheit bieten sollen.

Wie in der Marktwirtschaft üblich und entsprechend ihres jeweiligen Eigeninteresses, sind die Betreiber von Kritischen Infrastrukturen in erster Linie selbst verantwortlich für die Sicherung ihrer Funktionsfähigkeit. Sie ergreifen auf Basis gesetzlicher Regelungen eigenverantwortlich Maßnahmen, um die Resilienz ihrer Anlagen zu erhöhen. Sektorenübergreifende Regelungen zu Kritischen Infrastrukturen bestehen bislang nur im Bereich der Cybersicherheit, nicht aber im Hinblick auf physische Maßnahmen. Hier fehlen sektorenübergreifende, einheitliche Vorgaben für Maßnahmen zur Steigerung der Resilienz. Bereits existierende Regelungen in Fachgesetzen und in untergesetzlichem Recht zum physischen Schutz auf Bundes- und Landesebene sind branchen- und sektorspezifisch, nicht aber sektorenübergreifend, geregelt und sind von unterschiedlicher Regelungstiefe und verfolgen unterschiedliche Zielsetzungen. Teilweise werden nur abstrakte Zielsetzungen formuliert, Befugnisse von Behörden festgeschrieben oder es werden nur branchentypische konkrete Vorgaben für Betreiber gemacht.

Das KRITIS-DachG trifft erstmalig bundeseinheitliche und sektorenübergreifende Vorgaben, um kritische Anlagen zu identifizieren und normiert erstmalig sektorenübergreifende Maßnahmen und Mindeststandards für physische Resilienzmaßnahmen. Damit schafft das KRITIS-DachG einen verbindlichen und systematischen Rahmen für die Stärkung der Resilienz eines wichtigen Bereichs der Kritischen Infrastrukturen. Dies bietet Betreibern

kritischer Anlagen eine Orientierung über ihre wirtschaftliche und gesellschaftliche Relevanz und die daraus für sie resultierenden Verpflichtungen mit dem Ziel, ihren Geschäftsbetrieb jederzeit aufrechterhalten und bei Störungen oder Ausfällen zügig wiederherstellen zu können. Zudem sieht das KRITIS-DachG ein Verfahren für Risikobewertungen vor und schreibt ein Störungsmonitoring für alle erfassten Sektoren vor mit dem Ziel, einen fortlaufenden Überblick über die Risiken und die erheblichen Störungen von kritischen Anlagen zu schaffen, um mögliche Lücken zielgerichtet schließen zu können aber auch, um die Zusammenarbeit aller Beteiligten sachgerecht und ergebnisorientiert zu verstärken.

Diese enge Vernetzung bei der Stärkung der Resilienz von kritischen Anlagen kann allerdings nicht nur innerhalb Deutschlands stattfinden. In einer zunehmend verflochtenen Unionswirtschaft kommt Kritischen Infrastrukturen eine unverzichtbare Rolle bei der Aufrechterhaltung wichtiger wirtschaftlicher Tätigkeiten und gesellschaftlichen Funktionen im europäischen Binnenmarkt zu. Die Richtlinie des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27. Dezember 2022, S. 164, im Folgenden CER-Richtlinie) schafft dafür einen Unionsrahmen, der darauf abzielt, die Resilienz von kritischen Einrichtungen im Binnenmarkt durch Festlegung harmonisierender Mindestverpflichtungen zu verbessern und diesen Unternehmen durch kohärente und gezielte Unterstützungs- und Aufsichtsmaßnahmen zu helfen. Dafür schlägt die CER-Richtlinie einen neuen Weg ein und konkretisiert die Aufgaben und Pflichten von allen kritischen Einrichtungen, deren Dienste für das Funktionieren des Binnenmarkts wesentlich sind und legt Unionsvorschriften fest, die darauf abzielen, die Resilienz kritischer Einrichtungen zu verbessern. Dazu gehören u.a. Begriffsbestimmungen, Mindestvorgaben für Resilienzmaßnahmen, die Einführung eines Meldewesens für Sicherheitsvorfälle sowie Berichtspflichten gegenüber der Europäischen Kommission.

Darüber hinaus erfolgt die Ermittlung von kritischen Einrichtungen im Binnenmarkt bislang uneinheitlich, denn die entsprechenden Sektoren und Kategorien von Einrichtungen werden nicht in allen Mitgliedstaaten kohärent als kritisch eingestuft. Mit der CER-Richtlinie soll daher ein solides Maß an Harmonisierung in Bezug auf die in ihren Anwendungsbereich fallenden Sektoren und Kategorien von Einrichtungen erreicht werden. Die Vorgaben der CER-Richtlinie stützen sich auf Art. 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und dienen der Harmonisierung des Binnenmarktes.

Die Vorgaben der CER-Richtlinie sowie die anfangs geschilderten Notwendigkeiten einer nationalen gesetzlichen Regelung sollen daher in dem vorliegenden Gesetz zur Umsetzung der CER-Richtlinie und für die Stärkung der Resilienz kritischer Anlagen (KRITIS-DachG) vereint werden.

Resilienzmaßnahmen nach dem KRITIS-DachG können auch von Betreibern Kritischer Infrastrukturen in den nach diesem Gesetz festgelegten Sektoren ergriffen werden, wenn sie die Schwellenwerte der auf der Grundlage des KRITIS-DachG zu erlassenden Rechtsverordnung nicht erreichen. So wird sichergestellt, dass auch kleinere und mittlere Unternehmen Maßnahmen zur Stärkung ihrer Resilienz ergreifen

Um über das KRITIS-DachG hinausgehend die gesamtstaatlichen strategischen Ziele und politische Maßnahmen zur Stärkung der Resilienz Kritischer Infrastrukturen festzulegen, wird gemäß Artikel 4 der CER-Richtlinie bis 17. Januar 2026 eine nationale Strategie zur Verbesserung der Resilienz Kritischer Infrastrukturen (Nationale KRITIS-Resilienzstrategie) verabschiedet. Sie wird die derzeit gültige KRITIS-Strategie der Bundesregierung von Juni 2009 aktualisieren und erweitern.

II. Wesentlicher Inhalt des Entwurfs

Die unionsrechtlichen Vorgaben der CER-Richtlinie werden mit dem vorliegenden Gesetz umgesetzt. Folgende Regelungen werden neu geschaffen:

- Vorgaben zur Identifizierung von kritischen Anlagen und kritischen Anlagen mit besonderer Bedeutung für Europa.

- Vorgaben zur Registrierung von kritischen Anlagen.

- Etablierung von staatlichen Risikoanalysen und -bewertungen für kritische Dienstleistungen.

- Gesetzliche Verankerung wesentlicher nationaler Anforderungen für Resilienzmaßnahmen von Betreibern kritischer Anlagen.

- Einführung eines Meldewesens für Störungen.

- Umsetzung einer Ausschlussklausel für kritische Anlagen, die einen besonderen Bezug zum Sicherheits- und Verteidigungsbereich aufweisen. Für solche kritische Anlagen gelten dann die jeweils einschlägigen Vorgaben für den Sicherheits- bzw. Verteidigungsbereich.

- Einführung von Bußgeldvorschriften.

Über die Umsetzung der CER-Richtlinie hinaus werden Betreiber Kritischer Infrastrukturen in den nach diesem Gesetz festgelegten Sektoren dazu aufgefordert, Resilienzmaßnahmen nach dem KRITIS-DachG zu ergreifen, auch wenn sie die Schwellenwerte der auf der Grundlage des KRITIS-DachG zu erlassenden Rechtsverordnung nicht erreichen. Alternativen

Keine.

III. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes für das Gesetz zur Umsetzung der CER-Richtlinie und für die Stärkung der Resilienz kritischer Anlagen (KRITIS-DachG) folgt aus Artikel 74 Abs. 1 Nr. 11 (Recht der Wirtschaft) in Verbindung mit Artikel 72 Absatz 2 Grundgesetz (GG). Das Recht der Wirtschaft umfasst grundsätzlich alle Normen, die das wirtschaftliche Leben und die wirtschaftliche Betätigung regeln und alle Vorschriften, die sich in irgendeiner Form auf die Erzeugung, Herstellung und Verteilung von Gütern des wirtschaftlichen Bedarfs beziehen (z. B. BVerfGE 8, 143, 148 f.). Die Zuständigkeit erfasst das öffentliche und das private Wirtschaftsrecht, also auch die wirtschaftliche Betätigung der öffentlichen Hand.

Eine bundesgesetzliche Regelung dieser Materie ist zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine Regelung durch den Landesgesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch im Interesse der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte (zum Beispiel unterschiedliche Anforderungen an die von den Betreibern von kritischen Anlagen zu treffenden Maßnahmen) erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten.

Für den Sektor „Staat und Verwaltung“ des Bundes ergibt sich die Gesetzgebungskompetenz des Bundes kraft Natur der Sache.

Die Gesetzgebungskompetenz des Bundes für die Regelungen der Bußgeldvorschriften und Ordnungswidrigkeiten folgt aus Artikel 74 Absatz 1 Nummer 1 GG (Strafrecht).

IV. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union vereinbar. Er dient in weiten Teilen der Umsetzung der CER-Richtlinie.

Der Gesetzentwurf ist mit völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar.

V. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Der Gesetzesentwurf trägt zur Rechts– und Verwaltungsvereinfachung bei, da er erstmalig bundeseinheitliche kritische Anlagen identifiziert und sektorenübergreifende Vorgaben für physische Resilienzmaßnahmen schaffen wird, um bestehende Lücken zu schließen. Bei Wahrung der verfassungsrechtlichen Zuständigkeiten der Aufsichtsbehörden auf Bundes – und Landesebene in den einzelnen Sektoren wird das BBK eine koordinierende Rolle erhalten, damit erstmalig ein sektorenübergreifender Überblick über das Gesamtsystem der kritischen Anlagen als einen wesentlichen Teilbereich der Kritischen Infrastrukturen geschaffen wird.

2. Nachhaltigkeitsaspekte

Der Gesetzentwurf ist konform zu dem Leitprinzip der Bundesregierung einer nachhaltigen Entwicklung hinsichtlich des Aufbaus und der Förderung einer widerstandsfähigen Infrastruktur sowie der Sicherung von Lebensqualität und sozialem Zusammenhalt. Er kommt zudem dem Leitgedanken der Bundesregierung zur Berücksichtigung der Nachhaltigkeit nach. Das Einführen bundeseinheitlicher Vorgaben für die Identifizierung kritischer Anlagen sowie Mindestvorgaben für den physischen Schutz fördert eine Stärkung von Lebensqualität durch die Schaffung eines hohen Niveaus an Sicherheit und Resilienz. So ist es im Sinne der Deutschen Nachhaltigkeitsstrategie ein hohes Maß an Versorgungssicherheit für die Bürgerinnen und Bürger zu gewährleisten und den sozialen Zusammenhalt und gleichberechtigte Teilhabe an der wirtschaftlichen Entwicklung zu gewährleisten, dem dieser Gesetzentwurf nachkommt. Eine Prüfung der Prinzipien der nachhaltigen Entwicklung im Hinblick auf die Nachhaltigkeit wurde vorgenommen: Der Gesetzentwurf entspricht in seinen Wirkungen insbesondere den SDG-Indikatoren 3, 8 und 9, deren Ziel der Aufbau und die Förderung einer widerstandsfähigen Infrastruktur ist, sowie ein dauerhaftes, breitenwirksames und nachhaltiges Wirtschaftswachstum und ein gesundes Leben für alle Menschen jeden Alters zu gewährleisten und ihr Wohlergehen zu fördern.

Behinderungen etwaiger Nachhaltigkeitsziele durch den Gesetzentwurf wurden nicht festgestellt.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Keine

4. Erfüllungsaufwand

a. Erfüllungsaufwand für die Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

b. Erfüllungsaufwand für die Wirtschaft

c. Erfüllungsaufwand für die Verwaltung

[Der EA Verwaltung im Bundesministerium des Innern und für Heimat inkl. Geschäftsbereich sowie für die übrigen Ressorts wird im Rahmen der Ressortabstimmung abgefragt.]

Der Verwaltung entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben insgesamt ein Aufwand von insgesamt [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten. Durch die gesetzliche Änderung entstehen einmalige Sachkosten in Höhe von [●] Euro.

Bundeskanzleramt (BKAmt)

Beim BKAmt entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das BKAmt [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.z

Bundesministerium für Wirtschaft und Klimaschutz (BMWK)

Beim BMWK entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium der Finanzen (BMF)

Beim BMF entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium des Innern und für Heimat (BMI)

Beim BMI entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Beim BSI entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das BSI [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesamt für Bevölkerungs- und Katastrophenschutz (BBK)

Beim BBK entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das BBK [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS)

Bei der BDBOS entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt die BDBOS [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesamt für Kartographie und Geodäsie (BKG)

Beim BKG entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das BKG [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Auswärtiges Amt (AA)

Beim AA entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium der Justiz (BMJ)

Beim BMJ entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium für Arbeit und Soziales (BMAS)

Beim BMAS entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium der Verteidigung (BMVg)

Beim BMVg entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium für Ernährung und Landwirtschaft (BMEL)

Beim BMEL entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ)

Beim BMFSFJ entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium für Gesundheit (BMG)

Beim BMG entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium für Digitales und Verkehr (BMDV)

Beim BMDV entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)

Beim BMUV entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium für Bildung und Forschung (BMBF)

Beim BMBF entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ)

Beim BMZ entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen (BMWSB)

Beim BMWSB entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Bundesbeauftragter für den Datenschutz und für die Informationsfreiheit (BfDI)

Beim BfDI entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

§ [●] . Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●] . Euro jährlich.

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig im Gesamthaushalt ausgeglichen werden.

5. Weitere Kosten

Keine.

6. Weitere Gesetzesfolgen

Durch den Gesetzesentwurf wird die Versorgungssicherheit für Verbraucherinnen und Verbraucher erhöht.

Die Regelungen des Gesetzentwurfs sind inhaltlich geschlechtsneutral aufgrund der vorrangig gegebenen unmittelbaren Betroffenheit der Zielgruppe des Regelungsvorhabens und damit ohne Gleichstellungsrelevanz. Die weitere Stärkung und Förderung im Bereich des physischen Schutzes kritischer Anlagen betrifft jedoch sowohl mittel- als auch unmittelbar Frauen und Männer. § 1 Absatz 2 des Bundesgleichstellungsgesetzes bestimmt, dass Rechts- und Verwaltungsvorschriften des Bundes die Gleichstellung von Frauen und Männern auch sprachlich zum Ausdruck bringen sollen. Dies wurde in der Entwicklung der Gesetzesformulierung unter Einbeziehung bereits gegebener Diktion berücksichtigt.

Die Regelungen entsprechen zudem den Anforderungen des „Gleichwertigkeits-Checks“. Der Gesetzentwurf dient der Versorgungssicherheit der Bevölkerung durch Stärkung der Resilienz von kritischen Anlagen. Auch wird dem Schutz einer Daseinsvorsorge mit ihren unterschiedlichen Bereichen, die eine wesentliche Voraussetzung für gleichwertige Lebensverhältnisse der Menschen und den gesellschaftlichen Zusammenhalt Rechnung getragen. Auswirkungen auf die vorhandene Siedlungs- und Raumstruktur oder demographische Belange sind nicht zu erwarten.

VI. Befristung; Evaluierung

Eine Befristung ist nicht vorgesehen, da das Gesetz der Umsetzung der CER-Richtlinie dient, die unbefristet gilt. Das Gesetz soll anhand der Konzeption zur Evaluierung neuer Regelungsvorhaben gemäß dem Beschluss des Staatssekretärausschusses Bessere Rechtsetzung und Bürokratieabbau vom 23. Januar 2013 maximal fünf Jahre nach Inkrafttreten der jeweils evaluierungsbedürftigen Regelungen evaluiert werden.

§ 18 sieht dazu eine Evaluierungsklausel vor. Auf die Begründung zu § 18 wird verwiesen.

B. Besonderer Teil

Zu § 1 (Zweck des Gesetzes)

Dieses Gesetz bestimmt Maßnahmen zur Resilienzerhöhung für kritische Anlagen zur Sicherstellung der Funktionsfähigkeit der Wirtschaft, die auch für die Versorgungssicherheit der Bevölkerung elementar sind. Insbesondere werden für Betreiber kritischer Anlagen konkrete Vorgaben zur Aufrechterhaltung, Stärkung oder Herstellung der Handlungsfähigkeit und Resilienz festgelegt, um dem Risiko einer Beeinträchtigung ihres Geschäftsbetriebs

entgegenzuwirken, damit dieser auch bei Störungen oder Ausfällen aufrechterhalten oder schnell wiederhergestellt werden kann.

Mit den Regelungsinhalten wird erstmalig ein Dach über insgesamt 11 KRITIS-Sektoren gesetzt, indem in diesen Sektoren kritischen Anlagen bestimmt werden, ein Rahmen für verpflichtende Resilienzmaßnahmen unter Berücksichtigung branchenspezifischer Erfordernisse vorgeschrieben und eine Kontrolle sowie ein Überblick über die Sektoren gewährleistet wird.

Zudem wird erstmalig ergänzend zu den bereits existierenden Regelungen zum Cyberschutz von Kritischen Infrastrukturen im BSIG sowie in der BSI-Kritisverordnung, die die Gewährleistung der IT-Sicherheit bezwecken, ein All-Gefahrenansatz zugrunde gelegt, der alle über die Gefahren von Cyberangriffen hinausgehende Gefahren, von Naturkatastrophen bis hin zu von Menschen gemachten Gefahren, mit dem Ziel der Sicherstellung der Arbeitsfähigkeit der Wirtschaft berücksichtigt.

Im Einzelnen bestimmt dieses Gesetz Kriterien und Kategorien für die Identifizierung von kritischen Anlagen. Die Definition, ob ein Betreiber einer Anlage, der in diesen Bereichen tätig ist, auch eine kritische Anlage betreibt, wird durch eine Rechtsverordnung näher bestimmt.

Die im Anwendungsbereich dieses Gesetzes erfassten kritischen Anlagen für das Funktionieren der Wirtschaft die Aufrechterhaltung der elementaren Versorgungssicherheit der Bevölkerung stellen einen Teilbereich der Kritischen Infrastrukturen dar, also derjenigen Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Produktions- und Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Zugrunde gelegt wird die Betrachtungsebene des Bundes und diejenigen Organisationen und Einrichtungen werden adressiert, von denen auch die kleinen und mittleren Unternehmen abhängen.

Auch Organisationen oder Einrichtungen, die nicht in den Anwendungsbereich dieses Gesetz fallen, können hohe gesamtwirtschaftliche und -gesellschaftliche Relevanz haben und auf einer anderen Betrachtungsebene als Kritische Infrastrukturen betrachtet werden.

Das Gesetz enthält keine Entscheidungen über Ressourcenverteilungen. Es regelt nicht, dass Anlagen und Einrichtungen in bestimmten Situationen auf Grund anderer Normen eine Bevorzugung erfahren, nur weil sie nach diesem Gesetz als kritische Anlagen identifiziert wurden. Dies gilt insbesondere für kerntechnische Anlagen, deren Schutz in Krisenzeiten aufrechterhalten werden muss auf Grund der von ihnen ausgehenden Gefahr.

Weiterhin sieht das Gesetz eine Registrierungspflicht für die Betreiber kritischer Anlagen vor.

Um die Resilienz kritischer Anlagen zu stärken, werden Mindestvorgaben festgelegt, deren Umsetzung die Betreiber kritischer Anlagen nachweisen müssen. Ebenso müssen Vorfälle gemeldet werden.

Das BBK bekommt eine koordinierende Rolle. Es soll erstmalig auf Bundesebene ein gesamtheitlicher Überblick über kritische Anlagen, über Vorfälle und die Abhängigkeiten zwischen den Sektoren geschaffen werden.

Zu § 2 (Begriffsbestimmungen)

Die Begriffsbestimmungen werden zur Steigerung der Übersichtlichkeit in Nummern anstatt von einzelnen Absätzen gestaltet.

Zu Nr. 1 (CER-RL)

Die Begriffsbestimmung dient der Vereinfachung der zahlreichen Zitate der CER-Richtlinie im KRITIS-DachG.

Zu Nr. 2 (Kritische Infrastrukturen)

Die Begriffsbestimmung entstammt der Nationalen Strategie zum Schutz Kritischer Infrastrukturen" (KRITIS-Strategie) vom 17. Juni 2009. Die mit dem vorliegenden Gesetz geregelten kritischen Anlagen stellen einen Teilbereich der Kritischen Infrastrukturen dar.

Zu Nr. 3 (kritische Anlage)

Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 1 und Nr. 4 der CER-Richtline. Statt „kritische Einrichtung“ wird der Begriff „kritische Anlage“ verwendet.

Zu Nr. 4 (Betreiber kritischer Anlagen)

Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 1 und Nr. 4 der CER-Richtline. Statt „kritische Einrichtung“ wird der Begriff „Betreiber kritischer Anlagen“ verwendet.

Zu Nr. 4 (kritische Dienstleistungen)

Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 1 und Nr. 4 der CER-Richtline.

Zu Nr. 5 (Resilienz)

Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 2 der CER-Richtline.

Zu Nr. 6 (Risiko)

Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 6 der CER-Richtline.

Zu Nr. 7 (Risikoanalysen)

Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 7 der CER-Richtline. Zwar lässt sich der Begriff „Risikoanalyse“ in der Form, wie er in diesem Gesetz verwendet wird, in der CER-Richtlinie nicht finden. Die CER-Richtlinie verwendet unter Artikel 2 Nr. 7 insgesamt den Begriff der „Risikobewertung“. Im deutschen Sprach- und Rechtsgebrauch wird der Begriff „Risikobewertung“ jedoch enger gefasst. Während der Begriff „Risikobewertung“ im deutschen Sprachgebrauch der in diesem Gesetz definierten Beschreibung entspricht („Prozess der Priorisierung und des Vergleichs von Risiken“), geht der Begriff in der CER-Richtlinie weiter und nimmt noch den Prozess zur Bestimmung der Art und des Ausmaßes eines Risikos auf, also das, was im deutschen Sprachgebrauch unter „Risikoanalyse“ verstanden wird. Diese weitergehende Begriffsbestimmung wird daher in diesem Gesetz durch den Begriff „Risikoanalyse“ ergänzt. Die Aufteilung „Risikoanalyse“ und „Risikobewertung“ in diesem Gesetz dient der Harmonisierung des Begriffs „Risikobewertung“ im Sinne der CER-Richtlinie.

Zu Nr. 8 (Risikobewertungen)

Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 7 der CER-Richtline. Hier gelten die Ausführungen zu § 2 Nr. 8 (Risikoanalyse). Der europarechtliche Begriff der

„Risikobewertung“ ist weitergehender als im deutschen Sprach- und Rechtsgebrauch und umfasst auch eine Risikoanalyse gemäß der Definition in § 2 Nr. 8 dieses Gesetzes. Die Aufteilung „Risikoanalyse“ und „Risikobewertung“ in diesem Gesetz dient der Harmonisierung des Begriffs „Risikobewertung“ im Sinne der CER-Richtlinie.

Zu Nr. 9 (Vorfall)

Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 3 der CER-Richtline. Statt „Sicherheitsvorfall“ wird er mit dem Begriff „Vorfall“ umgesetzt.

Zu Nr. 10 (besonders wichtige Einrichtungen)

Besonders wichtige Einrichtungen bilden im NIS-II Umsetzungsgesetz (§ 28 Absatz 6 BSI-G-neu) eine neue Einrichtungsart und sollen zukünftig die alte Systematik des § 2 Nr. 10 BSI-G i.V.m. BSI-Kritisverordnung ablösen, wonach bestimmte Pflichten im Bereich der IT-Sicherheit für Unternehmen anhand von Schwellenwerten bestimmt wird. Die besonders wichtigen Einrichtungen orientieren sich nunmehr insbesondere an der sog. „sizecap-rule“, die Mitarbeitergröße und Umsatz des Unternehmens berücksichtigt. Dies dient der Umsetzung von Artikel 3 Absatz 1 der NIS-2-Richtlinie. Der Zusatz am Ende der Nummer 10 dient der Umsetzung von Artikel 2 Absatz 10 der NIS-2-Richtlinie. Die Betreiber kritischer Anlagen nach § 2 Nr. 3 dieses Gesetztes stellen eine Teilmenge der besonders wichtigen Einrichtungen nach NIS II Umsetzungsgesetz dar. Regelungen für besonders wichtige Einrichtungen finden im Rahmen dieses Gesetzes zwar nicht statt, sind aber Gegenstand der nach § 15 gemeinsam zu erlassenden Rechtsverordnung von KRITIS-DachG sowie NIS-2-Umsetzungsgesetz.

Zu Nr. 11 (wichtige Einrichtungen)

Die Begriffsbestimmung dient der Umsetzung von Artikel 3 Absatz 2 der NIS-2-Richtlinie und ordnet sich in die Systematik der „sizecap-rule“ wie in Nr.10 beschrieben ein. Die Kriterien des Umsatzes und der Mitarbeiterzahl sind bei den wichtigen Einrichtungen niedrigschwelliger angelegt, und haben, die IT-Sicherheit, betreffend niedrigere Anforderungen.

Zu § 3 (Nationale zuständige Behörde für die Resilienz Kritischer Anlagen)

Zu Absatz 1:

§ 3 Abs. 1 regelt, dass das BBK nationale zuständige Behörde i.S.d. Art. 9 Abs. 1 Satz 1 der CER-Richtlinie und zentrale Anlaufstelle i.S.d. Artikel 9 Absatz 2 der CER-Richtlinie ist.

Im Einklang mit Artikel 9 Absatz 1 der CER-Richtlinie werden die Mitgliedstaaten verpflichtet, eine oder mehrere Behörden zu ernennen oder einzurichten, die für die Überwachung und gegebenenfalls die Durchsetzung von Bestimmungen dieser Richtlinie zuständig sind.

Im Einklang mit Artikel 9 Absatz 2 der CER-Richtlinie muss jeder Mitgliedstaat eine zentrale Anlaufstelle benennen oder einrichten, die als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit den zentralen Anlaufstellen anderer Mitgliedstaaten und mit der in Artikel 19 der CER-Richtlinie genannten Gruppe für die Resilienz kritischer Einrichtungen fungiert. Die Errichtung und Benennung einer solchen dient der Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation sowie Koordinierung von Fragen im Zusammenhang mit der Resilienz kritischer Anlagen.

Sowohl als nationale zuständige Behörde als auch als zentrale Anlaufstelle wird das BBK im Geschäftsbereich des Bundesministeriums des Innern und für Heimat benannt. Hierdurch wird zum einen eine effektive Umsetzung der CER-Richtlinie gewährleistet. Das BBK

verfügt hier bereits über umfangreiche methodische und sektorenübergreifende Expertise im Bereich des physischen Schutzes kritischer Anlagen. Das erforderliche sektorenspezifische Fachwissen wird durch die Einbeziehung der zuständigen Aufsichtsbehörden des Bundes und / oder den sonst zuständigen Aufsichtsbehörden erlangt.

Auch der Gesamtüberblick auf sektorübergreifende Gefahren und Abhängigkeiten ist zu berücksichtigen. Dieser ganzheitliche Ansatz - über die isolierte Betrachtung einzelner Sektoren und kritischer Anlagen hinaus - schafft eine tragfähige Grundlage um bei der Entwicklung von effektiven Schutzmaßnahmen zugunsten betroffener Betreiber unterstützend mitzuwirken sowie ggf. frühzeitig auf etwaige Gefahren hinzuweisen.

In seiner Funktion als zentrale Anlaufstelle nach Artikel 9 Absatz 2 CER-Richtlinie wird das BBK koordinierend über die nationale Ebene hinaus auf EU-Ebene mit Vertretern der zentralen Anlaufstellen anderer Mitgliedstaaten und mit der in Artikel 19 der CER-Richtlinie genannten Gruppe für die Resilienz kritischer Einrichtungen zusammenarbeiten. Dies steht im Einklang mit der CER-Richtlinie, wonach jede zentrale Anlaufstelle mit den zuständigen Behörden ihres Mitgliedstaats, mit den zentralen Anlaufstellen anderer Mitgliedstaaten und mit der Gruppe für die Resilienz kritischer Einrichtungen in Kontakt stehen und gegebenenfalls die Kommunikation mit ihnen abstimmen soll. Hierunter fällt unter anderem auch der Austausch über bewährte Verfahren (Best Practice) sowie Erfahrungen, um die Resilienz kritischer Anlagen auch mitgliedsstaatsübergreifend kontinuierlich zu verbessern und zu stärken.

Die Benennung des BBK sowohl als nationale zuständige Behörde und zentrale Anlaufstelle dient zudem auch der Vereinheitlichung und Klarheit, an wen sich im Rahmen des gesetzlichen Auftrags nach diesem Gesetz zu wenden ist.

Zu Absatz 2

Artikel 9 Absatz 5 der CER-Richtlinie sieht vor, dass die zuständige Behörde mit den nach Richtlinie (EU) 2022/2555 zuständigen Behörden in Bezug auf Cybersicherheitsrisiken, Cyberbedrohungen und Cybersicherheitsvorfälle und in Bezug auf nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle, die kritische Anlagen betreffen, sowie in Bezug auf entsprechende Maßnahmen, die von seiner zuständigen Behörde und den zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555 ergriffen wurden, zusammenarbeitet und Informationen austauscht. Die enge Zusammenarbeit insbesondere mit dem Bundesamt für Sicherheit in der Informationstechnik aber auch der Bundesnetzagentur ist wesentlich, um Kohärenz beim Cyberschutz und beim physischen Schutz von kritischen Anlagen zu erreichen.

Der Informationsaustausch zwischen den Behörden erscheint aus Gründen der Kohärenz geboten und erforderlich. Etwaige Cybersicherheitsrisiken, Cyberbedrohungen und Cybersicherheitsvorfälle können mitunter auch Auswirkungen auf die Sicherheit und den physischen Schutz kritischer Anlagen haben. Umgekehrt können nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle, die kritische Anlagen betreffen, Auswirkungen auf den Cyberschutz haben. Die frühzeitige Identifizierung möglicher Risiken sowie deren Auswirkungen auf den physischen Schutz oder umgekehrt ermöglicht das Ergreifen angemessener Gegenmaßnahmen. Ein regelmäßiger Austausch der Behörden fördert bewährte Verfahren, schafft gemeinsame Erfahrungen und etabliert fortlaufend effektive Prozessstränge. Dies soll eine gebotene und angemessene Reaktion auf bereichsübergreifende mögliche Bedrohungen und Vorfälle ermöglichen.

Zu Absatz 3

Artikel 9 Absatz 1 der CER-Richtlinie sieht vor, dass in Bezug auf die kritischen Anlagen in den Sektoren des Bankenwesens sowie der Finanzmarktinfrastrukturen die in Artikel 46 der Verordnung (EU) 2022/2554 genannten Behörden zuständig sind. Gemäß Art. 8 S. 1 der

CER-Richtlinie gelten weitergehende Maßnahmen und Verpflichtungen nach Art. 11 der CER-Richtlinie sowie der Kapitel III, IV und VI nicht für die ermittelten kritischen Anlagen der Sektoren des Bankenwesens, der Finanzmarktinfrastrukturen sowie digitalen Infrastruktur. Angesichts der engen Verflechtungen und potentieller sektorübergreifender Gefahren ist ein für die gegenseitige Aufgabenerfüllung erforderlicher Informationsaustausch zwischen dem BBK und der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) -auch aus Gründen der Kohärenz- geboten.

Zu § 4 (Kritische Anlagen)

Zu Absatz 1:

§ 4 definiert den Anwendungsbereich des KRITIS-DachG. In Umsetzung der CER- Richtlinie werden kritische Anlagen in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation und Weltraum ermittelt. Zusätzlich werden kritische Anlagen im Sektor Siedlungsabfallentsorgung ermittelt. Dieser Sektor ist bereits gem. § 2 Abs. 10 Nr. 1 BSIG als Sektor der Kritischen Infrastruktur festgelegt. Im Sinne einer weitgehenden Kohärenz der Adressaten für Vorgaben für den Cyberschutz und für physische Resilienzmaßnahmen wird dieser Sektor über die Mindestvorgaben der CER-Richtlinie in den Anwendungsbereich des vorliegenden Gesetzes aufgenommen. Während der Regelungsbereich für den Cyberschutz ausgeweitet wird, sollen die Resilienzmaßnahmen nach der CER-Richtlinie im ersten Schritt nur für einen kleineren Kreis von Betreibern kritischer Anlagen gelten. Die Ausweitung des Anwendungsbereichs wird Gegenstand der in § 18 vorgesehenen Evaluierung.

Innerhalb dieser Sektoren sind nur solche Anlagen kritische Anlagen, die einen oder mehrere kritische Dienstleistungen erbringen, die für das Funktionieren der Gesamtwirtschaft des Gemeinwesens von hoher Bedeutung sind und ein Vorfall eine erhebliche Störung bei der Erbringung eines oder mehrerer kritischen Dienstleistungen durch die Anlage, oder bei der Erbringung von anderen kritischen Dienstleistungen in den im Anhang genannten Sektoren, die von diesen kritischen Dienstleistungen abhängen, bewirken würde.

In einer konkretisierenden Rechtsverordnung nach § 15 wird festgelegt, welche Dienstleistungen überhaupt in den Sektoren als kritisch im Sinne des KRITIS-DachG gelten. Diese Rechtsverordnung orientiert sich systematisch und inhaltlich an der BSI – Kritisverordnung, die im Rahmen der Cyberschutzregeln bisher definiert, welche Anlagen als kritisch eingestuft werden. Demnach liegt aus Bundessicht Kritikalität vor, sofern eine Anlage eine kritische Dienstleistung ausführt und einen in der Rechtsverordnung festgelegten Schwellenwert überschreitet. Der Schwellenwert wird auf Grundlage des Kriteriums der zu versorgenden Bevölkerung berechnet. Dabei soll – ebenso wie in der BSI-Kritisverordnung eine zu versorgende Bevölkerung von 500.000 Personen zu Grunde gelegt werden. Sofern ein Betreiber einer kritischen Anlage eine Bevölkerungszahl von dieser Größe versorgt, wird davon ausgegangen, dass dies aus Bundessicht für die Aufrechterhaltung der Wirtschaft wesentlich ist.

Unter Berücksichtigung der dem Bund zustehenden Gesetzeskompetenz aus Art. 74 Absatz 1 Nr. 11 GG – dem Recht der Wirtschaft – wird bei der Umsetzung der CER-Richtlinie der Schwerpunkt auf das Schutzziel der Aufrechterhaltung der wichtigen wirtschaftlichen Tätigkeiten gelegt. Die im vorliegenden Gesetz enthaltenen Regelungen zur Stärkung der Resilienz bewirken daneben insbesondere auch eine Stärkung der weiteren in der CER-Richtlinie genannten Schutzziele der öffentlichen Gesundheit und Sicherheit. Im Hinblick auf den Anwendungsbereich bedeutet dies, dass die Dienstleistung aus Bundessicht für die Aufrechterhaltung wichtiger wirtschaftlicher Tätigkeiten von entscheidender Bedeutung ist.

Zu Absatz 2

Die Regelung dient dazu, dass bei Veränderung der Werte der Anlagen, die für die Berechnung der Schwellenwerte entscheidend sind, die Verpflichtungen des KRITIS-DachG nicht mehr gelten, sofern die Schwellenwerte unterschritten werden.

Zu § 5

Zu Absatz 1

Absatz 1 enthält eine Klarstellung, dass andere über die Mindestvorgaben nach diesem Gesetz hinausgehende Anforderungen an die Betreiber kritischer Anlagen unberührt bleiben.

Zu Absatz 2

Nicht alle Kritischen Infrastrukturen gemäß § 2 Nr. 2 erfüllen die Voraussetzungen nach § 4 Absatz 1 und fallen damit in den Anwendungsbereich dieses Gesetzes. Auf einer anderen Betrachtungsebene und / oder zu einem anderen Schutzzweck sind weitere Organisationen oder Einrichtungen in Deutschland für Wirtschaft und Gesellschaft wichtig und schützenswert. Absatz 2 verweist auf die Möglichkeit, dass weitere Anlagen durch fachlich zuständige Bundes- oder Landesbehörden ermittelt werden können, um ihnen in eigener Zuständigkeit Vorgaben zur Stärkung der Resilienz machen. Die Länder sind im Rahmen ihrer Zuständigkeit insbesondere dafür verantwortlich, für Personal, welches für die Aufrechterhaltung der kritischen Anlagen nach § 4 essentiell ist, Regelungen zu schaffen, die die ungestörte Ausübung ihrer Tätigkeit nicht beeinträchtigen. Damit sind z.B. Regelungen gemeint, die die Unterbringung von Kindern in Kindertagesstätten, die umfassende Pflege von pflegebedürftigen Angehörigen und die Fahrt zur Tätigkeitsstätte in geeigneter Weise gewährleisten.

§ 5 Absatz 2 stellt klar, dass die zuständigen Bundes- oder Landesbehörden weiteren Kritische Infrastrukturen sowie weitere bedeutsame Einrichtungen, die nicht unter die Sektoren dieses Gesetzes fallen, z. B. in den Sektoren und Bereichen Medien und Kultur und Bildung und Betreuung resilienzsteigernde Vorgaben oder Vorgaben zu einem Störungsmonitoring machen können.

Zu § 6 (Anforderungen an Betreiber Kritischer Infrastrukturen)

Zu Absatz 1

Resilienzmaßnahmen nach dem KRITIS-DachG können auch von Betreibern Kritischer Infrastrukturen in den nach diesem Gesetz festgelegten Sektoren ergriffen werden, wenn sie die Schwellenwerte der auf der Grundlage der nach § 15 zu erlassenden Rechtsverordnung nicht erreichen. So wird ein starker Appell dahingehend ausgesprochen, dass auch kleinere und mittlere Unternehmen Maßnahmen zur Stärkung ihrer Resilienz ergreifen. Diese Regelung erfolgt nicht in Umsetzung der CER-Richtlinie.

Zu Absatz 2

Betreiber Kritischer Infrastrukturen nach Absatz 1 können zur Umsetzung der Verpflichtung nach Absatz 1 die nach § 11 Absatz 5 zu entwickelnden branchenspezifischen Resilienzstandards berücksichtigen. Durch die branchenspezifischen Resilienzstandards wird ihnen Orientierung gegeben, welche konkreten Maßnahmen in der jeweiligen Branche geeignet und verhältnismäßig sein könnten.

Zu § 7 **(Kritische Anlagen von besonderer Bedeutung für Europa)**

Zu Absatz 1

Zwar sind kritische Einrichtungen in der Regel als Teil eines immer stärker verflochtenen Dienstleistungs- und Infrastrukturnetzes tätig und erbringen häufig wesentliche Dienste in mehr als einem Mitgliedstaat, doch sind einige dieser kritischen Einrichtungen für die Union und ihren Binnenmarkt von besonderer Bedeutung, da sie wesentliche Dienste für oder in sechs oder mehr Mitgliedstaaten erbringen und daher eine spezifischen Unterstützung auf Unionsebene erhalten könnten.

Zu Absatz 2

Der Betreiber der kritischen Anlage hat dem BBK bei Registrierung mitzuteilen, dass kritische Dienstleistungen für oder in mehr als sechs Mitgliedstaaten erbracht werden. Dies beinhaltet die Mitteilung darüber, welche Dienstleistungen sie für oder in diesen Mitgliedstaaten anbieten und für welche oder in welchen Mitgliedstaaten diese angeboten werden. Nach Meldung des Betreibers der kritischen Anlage beim BBK, dass es Dienstleistungen nach EU VO [Delegierter Rechtsakt - Liste wesentlicher Dienste] in mindestens sechs Mitgliedstaaten erbracht werden, teilt das BBK der Europäischen Kommission unverzüglich die Identität solcher kritischen Einrichtungen sowie die Informationen, die diese zur Verfügung stellen, mit.

Die Europäische Kommission konsultiert das BBK, das eine kritische Einrichtung ermittelt hat, die zuständige Behörde anderer betroffener Mitgliedstaaten sowie die betreffende kritische Einrichtung. Bei diesen Konsultationen teilen die Behörden der Mitgliedstaaten der Europäischen Kommission mit, ob es sich seiner Einschätzung nach bei den Diensten, die diesem Mitgliedstaat von der kritischen Einrichtung erbracht werden, um wesentliche Dienste handelt.

Zu Absatz 3

Stellt die Kommission auf der Grundlage der Konsultationen fest, dass die betreffende kritische Einrichtung für oder in sechs oder mehr Mitgliedstaaten wesentliche Dienste im Sinne der EU VO [Delegierter Rechtsakt - Liste wesentlicher Dienste]erbringt, so teilt die Kommission dem Betreiber dieser kritischen Anlage über das BBK mit, dass sie als kritische Anlage von besonderer Bedeutung für Europa gilt, und unterrichtet den Betreiber dieser kritische Anlage über ihre Verpflichtungen gemäß diesem Kapitel sowie über den Zeitpunkt, ab dem diese Verpflichtungen für sie gelten. Sobald die Kommission die zuständige Behörde über ihre Entscheidung informiert, eine Einrichtung als kritische Einrichtung von besonderer Bedeutung für Europa zu betrachten, leitet die zuständige Behörde diese Meldung unverzüglich an diese kritische Einrichtung weiter.

Diese Vorgaben gelten für die betreffenden Betreiber kritischer Anlagen von besonderer Bedeutung für Europa ab dem Tag des Eingangs der in Absatz 3 genannten Mitteilung.

Nach Feststellung der Europäischen Kommission, dass der Betreiber der Anlage kritische Dienstleistungen im Sinne der EU-VO [Delegierter Rechtsakt - Liste wesentlicher Dienste]für oder in mindestens sechs Mitgliedstaaten erbringt, teilt die Europäische Kommission dem Betreiber dieser kritischen Anlage über das BBK mit, dass sie als kritische Anlage von besonderer Bedeutung für Europa gilt, und unterrichtet den Betreiber der kritischen Anlage über ihre Verpflichtungen nach § 7 ff. sowie über den Zeitpunkt, ab dem diese Verpflichtungen für sie gelten. Sobald die Europäische Kommission die zuständige Behörde über ihre Entscheidung informiert, eine Anlage als kritische Anlage von besonderer Bedeutung für Europa zu betrachten, leitet das BBK diese Meldung unverzüglich an den Betreiber dieser kritischen Anlage weiter.

Zu Absatz 4

Der Absatz 4 dient der Umsetzung des Artikel 18 der CER-Richtlinie.

Kritische Anlagen mit besonderer Bedeutung für Europa sollen auf Grund ihrer Bedeutung eine spezielle Unterstützungsleistung durch die Europäische Kommission erhalten. Sofern die Feststellung erfolgt ist, dass es sich um eine kritische Anlage nach § 5 handelt, kann über das Bundesministerium des Innern und für Heimat ein entsprechender Antrag bei der Europäischen Kommission auf Einrichtung der Beratungsmission erfolgen. Die Beratungsmission ist der Europäischen Kommission unterstellt und wird von dort organisiert. Es sind entsprechende Teile der Risikoanalysen und -bewertungen der Betreiber der kritischen Anlage, die Auflistung der getroffenen Maßnahmen sowie die Aufsichts- und Durchsetzungsmaßnahmen, die das BBK ergriffen hat, der Kommission auf Anforderung zur Verfügung zu stellen. Dies kann auch erforderlich sein, um eine kritische Anlage bei der Erfüllung ihrer Verpflichtungen nach dieser Richtlinie beraten zu können oder um zu bewerten, ob eine kritische Anlage von besonderer Bedeutung für Europa diese Verpflichtungen erfüllt.

Zu § 8 (Registrierung der kritischen Anlage)

Absatz 1

Angelehnt an die Registrierungspflicht der Betreiber kritischer Anlagen nach § 8 b Abs. 3 BSIG soll eine Registrierung bei einer gemeinsam vom BBK und dem und dem Bundesamt für Sicherheit in der Informationstechnik eingerichteten Registrierungsmöglichkeit durch die Betreiber selbst erfolgen, um ein kohärentes System zwischen den hiesigen Vorschriften und den Vorschriften des BSIG zu schaffen. Auch soll ein zu hoher bürokratischer Aufwand vermieden werden. Unter anderem wird durch die Registrierung auch sichergestellt, dass die Verpflichtungen bzw. Resilienzanforderungen aus diesem Gesetz an die relevanten Betreiber nachvollzogen bzw. überprüft werden können. Die Registrierung dient auch der Umsetzung des Art. 6 Abs. 1 der CER-Richtlinie. Hiernach sind bis zum 17. Juli 2026 die kritischen Anlagen zu ermitteln.

Zu Absatz 2

Ebenfalls in Anlehnung an § 8b Abs. 3 S. 2 BSIG kann das BBK die Registrierung im Einvernehmen mit den sonst zuständigen Bundesbehörden selbst vornehmen. Im Falle betreiberseitigen Unterlassens der Registrierung trotz Vorliegens der gesetzlichen Verpflichtung hierzu ist behördenseitig - ggf. im Einvernehmen mit der zuständigen Behörde - eine Erfassung von Amts wegen zu veranlassen. Hierdurch soll ebenfalls die Einhaltung und Überprüfung der betreiberseitigen Verpflichtungen aus diesem Gesetz sichergestellt bzw. nachvollzogen werden.

Zu Absatz 3

Nach § 7 Abs. 3 muss jeder Betreiber einer kritischen Anlage dem BBK eine Kontaktstelle oder eine Person mit vergleichbarer Aufgabenstellung als Ansprechpartner benennen. Hierdurch wird unter anderem auch bei meldepflichtigen Vorfällen nach diesem Gesetz ein schneller Informationsfluss gewährleistet.

Zu Absatz 4

Die Erreichbarkeit zu jeder Zeit nach § 7 Abs. 4 dieses Gesetzes knüpft auch an mögliche sektorübergreifende Gefahren und Abhängigkeiten. Unverzügliche Informationen an und von Behörden sowie weiterer unter Umständen betroffener Betreiber kritischer Anlagen kann in Einzelfällen geboten und erforderlich erscheinen.

Zu Absatz 5

Die Erstellung der Liste dient primär der Umsetzung der Art. 6 Abs. 1, 6 Abs. 3, 6 Abs. 4 und 6 Abs. 5 der CER-Richtlinie.

Nach Art. 6 Abs. 1 der CER-Richtlinie hat jeder Mitgliedstaat seine kritischen Anlagen bis zum 17. Juli 2026 zu ermitteln.

Nach Art. 6 Abs. 3 S. 1 der CER-Richtlinie erstellt jeder Mitgliedstaat eine Liste mit ermittelten kritischen Anlagen. Hierbei ist sicherzustellen, dass diesen kritischen Anlagen innerhalb eines Monats nach der entsprechenden Ermittlung ihre Einstufung als kritische Anlage mitgeteilt wird.

Nach Art. 6 Abs. 4 der CER-Richtlinie stellen Mitgliedstaaten sicher, dass ihre nach dieser Richtlinie zuständigen Behörden den zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555 innerhalb eines Monats nach der entsprechenden Einstufung die Identität der kritischen Anlagen mitteilt.

Nach Art. 6 Abs. 5 der CER-Richtlinie überprüfen die Mitgliedstaaten die Liste der ermittelten kritischen Anlagen im Bedarfsfall, mindestens jedoch alle vier Jahre, und aktualisieren sie gegebenenfalls.

Zu § 9 (Nationale Risikoanalysen und Risikobewertungen)

Zu Absatz 1-3

Durch regelmäßige Risikoanalysen und Risikobewertungen sollen kritische Einrichtungen ermittelt und Betreiber kritischer Anlagen bei der Vornahme von Resilienzmaßnahmen nach § 11 dieses Gesetzes unterstützt werden, sowie die Bedarfe an privaten und staatlichen Schutzmaßnahmen herausgearbeitet werden. Die Maßnahmen zur Ermittlung der kritischen Anlagen und zur Gewährleistung ihrer Resilienz sollen einem risikobasierten Ansatz folgen, bei dem diejenigen Anlagen im Fokus stehen, die für die Erfüllung wichtiger wirtschaftlicher Tätigkeiten mit einem nicht unerheblichen gesellschaftlichen Einfluss am bedeutendsten sind. Für diesen risikobasierten Ansatz müssen natürliche und vom Menschen verursachte Risiken – einschließlich Risiken grenzüberschreitender oder sektorübergreifender Art – analysiert und bewertet werden, die sich auf die Erbringung kritischer Dienstleistungen auswirken könnten. Zu diesen Risiken gehören insbesondere Unfälle, Naturkatastrophen, gesundheitliche Notlagen wie etwa Pandemien und hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten, krimineller Unterwanderung und Sabotage. Bei der Risikoanalyse und der Risikobewertung sollen die Erkenntnisse anderer thematisch betroffener Fachressorts (z.B. diejenigen der Sicherheitsbehörden) in die Bewertungen mit einfließen. Bei der Durchführung von Risikobewertungen sollten andere allgemeine oder sektorspezifische Risikobewertungen berücksichtigt werden, die gemäß anderer Unionsrechtsakte durchgeführt werden, und das Ausmaß der Abhängigkeit zwischen Sektoren, auch in Bezug auf Sektoren in anderen Mitgliedstaaten und Drittstaaten, Rechnung tragen.

Die Verantwortung für die Durchführung einer Risikoanalyse und -bewertung liegt bei dem jeweils fachlichen und sektorspezifisch zuständigen Ressort. Dabei soll ein praktikabler und bürokratiearmer Austausch bzw. eine Verzahnung zwischen den Ressorts und ihren Geschäftsbereichsbehörden ermöglicht werden. Die Ergebnisse der Risikobewertungen sollten bei der Ermittlung kritischer Anlagen verwendet werden sowie Informationen darüber liefern, wie Betreiber kritischer Anlagen ihre Resilienzanforderungen erfüllen können. Vor diesem Hintergrund wertet das BBK die Risikoanalysen und -bewertungen aus.

Zu § 10 (Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen)

Zu Absatz 1

Den Betreibern kritischer Anlagen sollten die entsprechenden Risiken, denen sie ausgesetzt sind, in ihrer Gesamtheit bekannt sein und auf dieser Grundlage geeignete Resilienzmaßnahmen treffen. Dazu sieht die Vorschrift vor, Betreiber kritischer Anlagen zu verpflichten, diejenigen Risiken zu analysieren und zu bewerten, die die Aufrechterhaltung ihres Geschäftsbetriebs und damit die Erbringung ihrer kritischen Dienstleistung stören oder unterbrechen können. Als Grundlage dafür sollen die staatlichen Risikoanalyse und -bewertungen nach § 8 dieses Gesetzes dienen. Auch andere Informationsquellen können herangezogen werden. Die Risikoanalyse und -bewertung ist grundsätzlich alle vier Jahre durchzuführen, erstmalig neun Monate nach Veröffentlichung der Mitteilung nach § 10 Abs. 8 dieses Gesetzes. Darüber hinaus sollen Betreiber kritischer Anlagen eine Risikoanalyse und -bewertung dann vornehmen, wenn ihre besondere Situation oder die Entwicklung der Risiken dies erfordern.

Zu Absatz 2

Zur Vermeidung von Doppelverpflichtungen und unnötiger Bürokratie können Betreiber kritischer Anlagen mit Risikoanalysen und -bewertungen, die sie bereits auf der Grundlage anderer öffentlich-rechtlicher Vorschriften durchgeführt und dokumentiert haben, ihrer Verpflichtung aus Abs. 1 nachkommen. Dazu müssen die bereits durchgeführten anderen Risikoanalysen und -bewertungen für die Risikoanalyse und -bewertung nach § 9 dieses Gesetzes gleichwertig sein, d.h. dem Sinn und Zweck der Risikoanalyse und -bewertung gemäß § 9 dieses Gesetzes entsprechen. Sie können diese Bewertungen und entsprechende Dokumentation dazu verwenden, um die in § 9 dieses Gesetzes festgelegten Anforderungen zu erfüllen. Das BBK prüft die andere Risikoanalyse und -bewertung und kann die Gleichwertigkeit im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes ganz oder teilweise feststellen (Äquivalenzprüfung).

Zu Absatz 3

Nach Art. 8 der CER-Richtlinie sind kritische Anlagen in den Sektoren Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation von der Vorschrift ausgenommen.

Zu § 11 (Resilienzmaßnahmen der Betreiber kritischer Anlagen)

Zu Absatz 1:

Im Einklang mit Artikel 13 der CER-Richtlinie werden Betreiber kritischer Anlagen dazu verpflichtet, geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu treffen. Diese Maßnahmen sind entsprechend Artikel 13 Abs. 1 der CER-Richtlinie auf der Grundlage der nach § 8 bereitgestellten Informationen über die staatlichen Risikoanlaysen und-bewertungen sowie den Ergebnissen der eigenen Risikoanalyse- und -bewertung nach § 9 zu treffen. Mit dieser Regelung soll ein risikobasierter All-Gefahren-Ansatz beim Ergreifen von Maßnahmen zur Stärkung der Resilienz verfolgt werden.

Dabei soll der Stand der Technik eingehalten werden. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden. Die Verpflichtung zur Berücksichtigung des Stands der Technik schließt die Möglichkeit zum Ergreifen solcher Maßnahmen nicht aus, die einen ebenso effektiven Schutz wie die anerkannten Vorkehrungen nach dem Stand der Technik bieten.

Zu Absatz 2:

Bei den von den Betreibern der kritischen Anlagen zu treffenden technischen, sicherheitsbezogenen und organisatorischen Maßnahmen ist die Verhältnismäßigkeit zu wahren. Diese ist gewahrt, wenn der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls oder einer Beeinträchtigung der kritischen Dienstleistung zu den Folgen ihres Ausfalls oder ihrer Beeinträchtigung angemessen erscheint. Dabei können auch wirtschaftliche Aspekte berücksichtigt werden.

Zu Absatz 3:

Nr. 1 – 6 enthalten die Ziele, die die Maßnahmen erreichen sollen.

Zu Absatz 4:

Anhang 1 zu diesem Gesetz enthält eine beispielhafte Auflistung von konkreten Maßnahmen, die die Betreiber der kritischen Anlagen bei der Abwägung, welche Maßnahmen geeignet und verhältnismäßig sind, berücksichtigen können.

Zu Absatz 5:

Absatz 5 ermöglicht in Branchen, in denen es fachlich sinnvoll ist, die Erarbeitung branchenspezifischer Resilienzstandards und verankert damit den kooperativen Ansatz, wie er in der Nationalen Strategie zum Schutz Kritischer Infrastrukturen festgeschrieben wurde und im UP KRITIS und seinen Branchenarbeitskreisen realisiert wird. Ziel ist es, dass sich Betreiber kritischer Anlagen branchenintern zusammenfinden und branchenspezifische Resilienzstandards erarbeiten. Die Bewertung und Anerkennung der vorgetragenen Standards soll durch das BBK im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes erfolgen, um die Vereinbarkeit und Koordinierung mit anderen Belangen zu gewährleisten und die fachliche Expertise der zuständigen Aufsichtsbehörden einzubeziehen. Auch dann, wenn branchenspezifische Resilienzstandards erarbeitet wurden, steht es dem einzelnen Betreiber frei, abweichend davon auch eigene den Stand der Technik berücksichtigende Maßnahmen umzusetzen.

Zu Absatz 6:

Im Einklang mit Artikel 13 Absatz 2 der CER-Richtlinie müssen Betreiber kritischer Anlagen die von ihnen zur Steigerung der Resilienz getroffenen Maßnahmen nach den Absätzen 1 bis 3 in einem Resilienzplan darstellen. Der Resilienzplan ist dem BBK spätestens zu einem vom BBK bei der Registrierung im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik festgelegten Zeitpunkt und anschließend alle zwei Jahre nachzuweisen.

Zu Absatz 7:

Zur Vermeidung von Verwaltungsaufwand können zur Erfüllung dieser Anforderung Dokumente oder Maßnahmen verwendet werden, die aufgrund von Verpflichtungen aus anderen Rechtsakten, die für die die in Absatz 1 genannten Maßnahmen relevant sind, ergriffen werden. Das BBK kann im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes bestehende Maßnahmen zur Verbesserung der Resilienz einer kritischen Anlage, die die in Absatz 1 genannten technischen, sicherheitsbezogenen und organisatorischen Maßnahmen betreffen, als vollständig oder teilweise den Verpflichtungen nach § 11 entsprechend erklären (Äquivalenzprüfung). Damit das BBK diese Prüfung durchführen kann, sind dem BBK diese Dokumente zu dem Absatz 6 Satz 2 festgelegten Zeitpunkt vorzulegen. Legt der Betreiber einer kritischen Anlage Bescheide, Genehmigungen, Zertifizierungen oder ähnliche Nachweise von anderen Behörden, etwa zum Brandschutz oder der Notstromversorgung, vor, gelten die darin beschriebenen Maßnahmen ohne weitere Überprüfung als insoweit die nach § 10 festgelegten Anforderungen erfüllend.

Zu Absatz 8:

Die Erfüllung der Anforderungen nach Absatz 1 muss der Betreiber der kritischen Anlage auf geeignete Weise nachweisen. Der Nachweis kann durch Audits erfolgen. Der Betreiber übermittelt in diesem Fall dem BBK die Ergebnisse der durchgeführten Audits einschließlich der dabei aufgedeckten Mängel. Das BBK kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Mängeln die Vorlage eines geeigneten Mängelbeseitigungsplanes und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes die Beseitigung der Mängel verlangen. Das BBK kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen. Das BBK kann zur Ausgestaltung des Verfahrens der Audits und Erbringung des Nachweises nach Satz 2 Anforderungen an die Art und Weise der Durchführung, an die Geeignetheit der zu erbringenden Nachweise sowie fachliche und organisatorische Anforderungen an die Prüfer und die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und Einrichtungen und der betroffenen Wirtschaftsverbände festlegen. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des BBK.

Zu Absatz 9:

Bei erheblichen Zweifeln an der Einhaltung der Anforderungen nach dem Absatz 1 kann das BBK im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes die Einhaltung der Anforderungen überprüfen. Bei der Durchführung der Überprüfung kann sich eines qualifizierten unabhängigen Dritten bedient werden. Der Betreiber der kritischen Anlage hat dem BBK und den zuständigen Aufsichtsbehörden des Bundes und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung kann das BBK Gebühren und Auslagen bei dem Betreiber der kritischen Anlage nur erheben, sofern das BBK auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach Absatz 1 begründeten.

Zu Absatz 10:

Bei Verstößen gegen die Anforderungen des Absatz 1 soll entsprechend Art 23 Abs.3 der CER-Richtlinie der Betreiber der kritischen Anlage zunächst angewiesen werden, erforderliche und verhältnismäßige Maßnahmen zu ergreifen, um festgestellte Verstöße innerhalb einer angemessenen Frist zu beheben und diesen Behörden Informationen über die ergriffenen Maßnahmen zu übermitteln.

Zu Absatz 11:

Der Hinweis, dass die Vorschriften und die Zuständigkeit der Fachbehörden im Rahmen des Zivil- und Katastrophenschutzes unberührt bleiben, ist deklaratorischer Natur.

Zu Absatz 12:

Absatz 12 enthält eine Klarstellung, dass das nach § 11 Absatz 3 Nr. 5 zu gewährleistende Sicherheitsmanagement hinsichtlich der Mitarbeitenden die Vorschriften des Sicherheitsüberprüfungsgesetzes (SÜG) in Verbindung mit der Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) sowie die Fachgesetze wie das Atomgesetz, das Luftsicherheitsgesetz, [das Sicherheitsgewerbegesetz] und die Hafensicherheitsgesetze hinsichtlich der Zuverlässigkeitsüberprüfungen unberührt lässt.

Zu Absatz 13:

Mit § 11 Absatz 13 wird Art. 6 Absatz 3 Unterabsatz 2 der CER-Richtlinie umgesetzt. Die Verpflichtung zur Ergreifung und Umsetzung von Resilienzmaßnahmen nach § 10 treffen den Betreiber einer kritischen Anlage erst nach Ablauf von 10 Monaten nach der Registrierung als kritische Anlage nach § 8. Dadurch erhält der Betreiber eine angemessene Übergangsfrist, um sich auf die Verpflichtungen nach § 11 vorzubereiten.

Zu Absatz 14:

Im Einklang mit Artikel 8 der CER-Richtlinie gelten dies Vorschriften des § 11 nicht für kritische Anlagen in den Sektoren Finanz- und Versicherungswesen und Informationstechnik und Telekommunikation.

Zu § 12 (Meldewesen für Störungen)

Zu Absatz 1

Im Einklang mit der Begründung zur CER-Richtlinie soll dem BBK und den Sektorbehörden mit der Einrichtung eines zentralen Meldewesens für die Meldung bestimmter Vorfälle ermöglicht werden, sich einen umfassenden Überblick über die Auswirkungen, die Art, die Ursache und die möglichen Folgen von Störungen und die Abhängigkeiten der Sektoren zu verschaffen.

Die Meldung erfolgt an eine im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik eingerichtete gemeinsame Meldestelle. Bereits jetzt sind Betreiber Kritischer Infrastrukturen verpflichtet, dem Bundesamt für Sicherheit in der Informationstechnik über ein Online-Meldeportal gemäß § 8b Abs. 4 Nr. 1 BSIG Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben, zu melden.

Nach § 8 Abs. 4 Nr. 2 BSIG sind Betreiber Kritischer Infrastrukturen ferner verpflichtet, dem Bundesamt für Sicherheit in der Informationstechnik über ein Online-Meldeportal auch erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen könne, zu melden.

Das bereits existierende Online-Meldeportal des Bundesamtes für Sicherheit in der Informationstechnik wird für Störungen nach diesem Gesetz, die den physischen Schutz kritischer Anlagen betreffen, erweitert. Hierdurch wird der Verwaltungsaufwand sowohl für die beteiligten Behörden aber auch der Betreiber erheblich reduziert.

Die Störungsmeldung nach diesem Gesetz erfolgt unbeschadet anderer gesetzlicher Meldeverpflichtungen gegenüber weiteren zuständigen Behörden. Bereits bestehende Meldungsverpflichtungen der Betreiber gegenüber anderen Stellen, bleiben daher, sofern gegeben, bestehen.

Zu Absatz 2

Mit § 12 Absatz 2 dieses Gesetzes wird Art. 15 Abs. 2 S. 1 der CER-Richtlinie umgesetzt.

Zu Absatz 3

Betreiber kritischer Anlagen sind verpflichtet, den zuständigen Behörden unverzüglich Vorfälle zu melden, die die Erbringung kritischer Dienstleistungen erheblich stören oder erheblich stören könnten.

Betreiber sollten daher eine erste Meldung spätestens 24 Stunden, nachdem sie Kenntnis von einem Vorfall erhalten haben, melden. Der Umfang der Erstmeldung sollte lediglich diejenigen Informationen enthalten, die unbedingt erforderlich sind, um das BBK über den Vorfall zu unterrichten und es der kritischen Anlage zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. In einer solchen Meldung sollte, soweit möglich, die mutmaßliche Ursache des Vorfalls angegeben werden. Betreiber kritischer Anlagen haben sicherzustellen, dass die Ressourcen zur vorrangigen Bewältigung möglicher Vorfälle durch den Ressourceneinsatz für die Erstmeldung nicht beeinträchtigt werden.

Der Erstmeldung hat spätestens einen Monat nach dem Vorfall ein ausführlicher Bericht zu folgen.

Zu Absatz 4

Mit § 11 Absatz 4 dieses Gesetzes wird Art. 15 Abs. 3 der CER-Richtlinie umgesetzt, wonach der wechselseitige mitgliedstaatenübergreifende Informationsaustausch bei einschlägigen Störungsfällen über die zentralen Anlaufstellen im Sinne dieses Gesetzes gewährleistet wird.

Zu Absatz 5

Mit § 12 Absatz 5 dieses Gesetzes wird Art. 15 Abs. 1 S. 4 der CER-Richtlinie umgesetzt. Eine Störung, die erhebliche Auswirkungen auf die Kontinuität der Erbringung wesentlicher Dienste für oder in sechs oder mehr Mitgliedstaaten hat oder solche Auswirkungen haben könnte, ist aufgrund ihrer besonderen Tragweite der Europäischen Kommission zu melden.

Zu Absatz 6

Mit § 12 Absatz 6 dieses Gesetzes wird Art. 15 Abs. 4 S. 1 der CER-Richtlinie umgesetzt.

Sachdienliche Folgeinformationen können im Einzelfall Betreiber kritischer Anlagen neben deren originärer Verpflichtung zur Resilienzstärkung nach diesem Gesetz unterstützen, weitere hilfreiche Reaktionsverfahren und Prozesse für die Resilienzstärkung zu etablieren.

Zu Absatz 7

Die Mitteilung über Auswertungen zu Störungsmeldungen an zuständige Aufsichtsbehörden des Bundes und den sonstigen zuständigen Aufsichtsbehörden erfolgt zum Zwecke der Unterrichtung und soweit es für die Aufgabenerfüllung der Behörden erforderlich ist.

Zu Absatz 8

Die Verarbeitung möglicher personenbezogener Daten durch BBK erfolgt in zulässiger Weise in erforderlichem Umfang zum Zwecke der Aufgabenerfüllung.

Zu Absatz 9

Mit § 11 Absatz 9 wird Art. 6 Abs. 3 Unterabsatz 2 der CER-Richtlinie umgesetzt. Die Verpflichtung zur Meldung von Störungen nach § 11 treffen den Betreiber einer kritischen Anlage erst nach Ablauf von 10 Monaten nach der Registrierung als kritische Anlage nach § 7. Dadurch erhält der Betreiber eine angemessene Übergangsfrist, um sich auf die Verpflichtungen nach § 10 vorzubereiten.

Zu Absatz 10

§ 12 Absatz 10 dieses Gesetzes regelt, dass § 12 nicht für kritische Anlagen in den Sektoren Finanz- und Versicherungswesen und Informationstechnik und Telekommunikation gilt.

Gemäß Art. 8 S. 1 der CER-Richtlinie gelten Maßnahmen und Verpflichtungen des Kapitel III dieser Richtlinie nicht für die ermittelten kritischen Anlagen der Sektoren des Bankenwesens sowie der Finanzmarktinfrastrukturen und digitalen Infrastruktur. Störungsmeldungsverpflichtungen nach § 12 dieses Gesetzes beruhen auf § 15 der CER-Richtlinie, der sich in Kapitel III der Richtlinie wiederfindet.

Zu § 13 (Einsatz von Kritischen Komponenten; Verordnungsermächtigung)

Zu § 14 (Berichtspflichten)

Das Bundesministerium des Innern und für Heimat ist verpflichtet, im Rahmen der Ermittlung der kritischen Anlagen an die Europäische Kommission bestimmte Informationen zu übermitteln. Das Bundesministerium des Innern und für Heimat wird im Rahmen der Ausübung seiner Fachaufsicht durch das BBK über dessen Tätigkeit auch im Zusammenhang mit dem KRITIS-DachG unterrichtet. Die Unterrichtung dient auch der Information über den Stand der Umsetzung des KRITIS-DachG.

Zu Nr. 1 – Nr. 3

Nr. 1: Im Einklang mit Art. 5 Abs. 4 der CER-Richtlinie sollen innerhalb von drei Monaten nach Durchführung von staatlichen Risikoanalysen und -bewertungen entsprechende Informationen über die ermittelten Arten von Risiken und die Ergebnisse dieser Risikobewertungen, aufgeschlüsselt nach den im Anhang genannten Sektoren und Teilsektoren an die Europäische Kommission übermittelt werden.

Nr. 2: Im Einklang mit Art. 7 Absatz 2 a der CER-Richtlinie sollen die kritischen Dienstleistungen, die über die Liste wesentlichen Dienste [EU VO - Liste wesentliche Dienste] hinausgehen, übermittelt werden. Ebenso soll die Zahl der ermittelten kritischen Anlagen für jeden in der Rechtsverordnung nach § 15 festgelegten Sektor sowie die Schwellenwerte, die zur Identifizierung der kritischen Anlagen in der Rechtsverordnung nach § 15 festgelegt werden, an die Europäische Kommission übermittelt werden und mindestens alle vier Jahre aktualisiert werden.

Nr. 3: Im Einklang mit Artikel 9 der CER-Richtlinie sollen bis zum 17. Juli 2028 und danach alle zwei Jahre legt das Bundesministerium des Innern und für Heimat der Europäischen Kommission und der gemäß Artikel 19 der CER-Richtlinie genannten Gruppe für die Resilienz kritischer Einrichtungen einen zusammenfassenden Bericht über die bei ihnen eingegangenen Meldungen nach § 12, einschließlich der Zahl der Meldungen, der Art der gemeldeten Vorfälle und der gemäß § 14 ergriffenen Maßnahmen, vor.

Zu § 15 (Ermächtigung zum Erlass von Rechtsverordnungen)

Die genannten Regelungen des Gesetzes bedürfen zwingend der näheren Ausgestaltung. Das Bundesministerium des Innern und für Heimat erhält daher die Ermächtigungsgrundlage zum diesbezüglichen Erlass von Verordnungen, die die Grundlage für den sachgerechten Vollzug der Regelungen beinhalten.

Zu § 16 (Ausnahmebescheid)

§ 16 dient der Umsetzung von Artikel 1 Absatz 6 -bis 8 der CER-Richtlinie. Damit wird von der Möglichkeit der Schaffung einer Ausnahme für die Anwendung des KRITIS-DachG Gebrauch gemacht. Der Grund einer teilweisen oder vollständigen Ausnahme von den in Artikel 12, 13 und 15 der CER-Richtlinie – umgesetzt in den §§ 8 ff. – genannten Pflichten ist die Wahrung des nationalen Sicherheitsinteresses. So ist es in den Erwägungsgründen 11 der CER-Richtlinie angelegt, dass es zur Wahrung wesentlicher Interessen der nationalen Sicherheit, dem Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit der Mitgliedstaaten erforderlich sein muss, Einrichtungen von obigen Pflichten auszunehmen,

wenn derartige Auskünfte oder eine Preisgabe dem nationalen Sicherheitsinteresse zuwiderliefe. Als relevante Bereiche führt Artikel 1 Absatz 6 und 7 der CER-Richtlinie die Bereiche der nationalen Sicherheit, öffentlichen Sicherheit, der Verteidigung oder Strafverfolgung, einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten an. Um dem Sinne einer Ausnahmeregelung, die nicht zu weit greift, gerecht zu werden, ist ein Ausgleich zwischen einem „hohen Resilienzniveau“ (siehe Erwägungsgrund 8 der CER-Richtlinie) und dem Mitgliedsstaatsinteresse der Wahrung nationaler Sicherheitsinteressen zu erbringen.

Bei dem hiesigen Ausnahmebescheid ist von einem nichtbegünstigenden Verwaltungsakt auszugehen. Gemäß § 48 Absatz 1 Satz 2 VwVfG bestimmt die Legaldefinition die Begünstigung wie folgt: Ein Verwaltungsakt ist begünstigend, wenn er ein Recht oder einen rechtlich erheblichen Vorteil begründet oder bestätigt. Ein Recht könnte in der Art begründet sein, als dass die der Befreiung unterliegende Einrichtung entweder ganz oder teilweise den Pflichten der §§ 8 ff. nicht nachkommen muss. Andererseits entfallen diese Pflichten nicht einfach. Eine Begünstigung ist nach dem objektiven Regelungsgehalt des Verwaltungsakts unter Berücksichtigung des Zwecks der ihm zugrunde liegenden Norm zu beurteilen, nämlich derart, dass eine Befreiung von obigen Pflichten nicht der Einrichtung, die den Ausnahmebescheid erhält, sondern dem nationalen Sicherheitsinteresse zugutekommen. Der Ausnahmebescheid soll gerade kein Recht verleihen, sondern nur die Pflichten des Adressaten des Ausnahmebescheids anderweitig ausgestalten, zumal gleichwertige Maßnahmen, die denen der Befreiung gleichkommen nach Sinn und Zweck getroffen werden müssen.

Zu Absatz 1

Zunächst wird obig genanntem Ziel durch ein begrenztes Vorschlagsrecht, durch Bundeskanzleramt, Bundesverteidigungsministerium und Bundesinnenministerium entsprochen. Dabei ist ein Antragsrecht der betreffenden Einrichtung bewusst nicht vorgesehen. Weiterhin einschränkend sind umfasste Bereiche der Einrichtungen. Hierbei wird insbesondere auf die auch in der CER-Richtlinie explizit genannten, rechtlich anerkannten Kategorien, der öffentlichen Sicherheit und Ordnung verwiesen. Als Begrenzung der Ausnahmeregelung einzubeziehender Erwägungsgrund sollte auf die Wesentlichkeit der Interessen der nationalen Sicherheit abzustellen sein.

Nicht zuletzt muss andererseits jedoch bei Ausnehmen von den genannten Pflichten das hohe gemeinsame Niveau des physischen Schutzes durch Umsetzung gleichwertiger Maßnahmen gewährleistet werden. Hierbei wird auf Artikel 1 Absatz 1 e) und Erwägungsgrund 8 der CER-Richtlinie verwiesen, die vorsieht, dass ein hohes Resilienzniveau zu erreichen ist und besondere Anforderungen sowie die Sicherstellung einer spezifischen Aufsicht für kritische Anlagen zu gewährleisten sind. Dem soll dadurch Rechnung getragen werden, dass Absatz 1 bestimmt, dass bei einer Ausnahme der Betreiber der kritischen Anlage gleichwertige Vorgaben zu erfüllen hat. Die Kontrolle über die Einhaltung obläge dem vorschlagenden Ressort.

Zu Absatz 2

Absatz 2 dient der Umsetzung von Artikel 1 Absatz 1 e) der CER-Richtlinie. Absatz 2 Satz 1 setzt die Möglichkeit der Schaffung einer Ausnahme, wie von der Richtlinie vorgesehen, um. Dabei bestimmt Absatz 2 einen einfachen Ausnahmebescheid, die Befreiung von Maßnahmen von Risikobewertungen, Meldepflichten und Resilienzmaßnahmen. Satz 2 verweist hierbei, wie obig bereits angemerkt, auf die Schaffung gleichwertiger Standards zur Wahrung der Resilienz.

Zu Absatz 3

Absatz 3 dient der Umsetzung von Artikel 1 Absatz 7 der CER-Richtlinie.

Mit Absatz 3 wurde die Möglichkeit einer vollständigen Befreiung von sowohl Risikoanalysen und -bewertungen, Meldepflichten als auch Registrierungspflichten im Rahmen eines sogenannten erweiterten Ausnahmebescheids geschaffen. Betroffene Betreiber kritischer Anlagen müssen hierfür ausschließlich in den obig genannten Bereichen tätig sein oder Dienste erbringen. Satz 2 stellt die Wahrung von gleichwertigen Maßnahmen sicher.

Zu Absatz 4

Absatz 4 sieht eine Regelung des Widerrufs einer rechtmäßigen Befreiung vor. Für den Widerruf einer rechtmäßigen Befreiung sollte von § 49 VwVfG abgewichen werden, um der spezifischen Interessenlage der Vorschrift Genüge zu tun. Absatz 4 Satz 1 regelt den Fall des späteren Wegfalls der Voraussetzungen zur Erteilung eines Ausnahmebescheids. Satz 2 sieht hiervon eine Rückausnahme vor, wenn die Voraussetzungen nur vorübergehend entfallen und ein besonderer Grund vorliegt.

Zu § 17 (Verarbeitung personenbezogener Daten)

Zu Absatz 1

Mit § 17 wird auf der Grundlage von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e der Verordnung (EU) 2016/679 eine bereichsspezifische Rechtgrundlage für das Bundesamt zur Verarbeitung personenbezogener Daten geschaffen

Zu Absatz 2

Absatz 2 ermöglicht die Weiterverarbeitung personenbezogener Daten. Die Regelung trägt dem Erfordernis Rechnung, dass das Bundesamt für die Erfüllung seiner gesetzlichen Aufgaben eine datenschutzrechtliche Rechtsgrundlage benötigt, um personenbezogene Daten zum Zwecke der Sammlung, Auswertung und Untersuchung von Vorfällen nach § 12 dieses Gesetzes und zur Unterstützung, Beratung und Warnung in Fragen zur Gewährleistung der Resilienz durch Betreiber kritischer Anlagen zu verarbeiten. Das Bundesamt muss in der Lage sein, zur Erfüllung seiner Aufgaben aus § 3 alle ihm aus öffentlichen, privaten, staatlichen, bekannten oder anonymen Quellen erlangten und zur Verfügung gestellten Daten auszuwerten, um Betreiber kritischer Anlagen dabei zu unterstützen, angemessene Resilienzmaßnahmen über die bereits bestehenden hinaus zu entwerfen oder zu etablieren. Hierzu ist allerdings auch eine Interessenabwägung erforderlich.

Zu Absatz 3

Absatz 3 verweist auf § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes. Dem BBK steht es frei, zur Wahrung der Interessen der betroffenen Person darüber hinaus weitere geeignetere technische oder organisatorische Maßnahmen zu ergreifen.

Zu § 18 (Evaluierung)

Gemäß dem Beschluss des Staatssekretärausschusses Bessere Rechtsetzung und Bürokratieabbau vom 23. Januar 2013 sind wesentliche Regelungsvorhaben zu evaluieren. Das KRITIS-DachG ist als ein solches wesentliches Regelungsvorhaben anzusehen. Mit dem Ziel, erstmalig sektorenübergreifende physische Resilienzmaßnahmen für Betreiber von kritischen Anlagen vorzusehen und damit die Aufrechterhaltung der Wirtschaftsstabilität angesichts der wechselseitigen Abhängigkeiten zu regeln, werden Regelungsinhalte getroffen, deren Auswirkungen sowohl für die Wirtschaft als auch für den Verwaltungsvollzug noch nicht vollständig bekannt sind und zum aktuellen Zeitpunkt auch noch nicht vollständig abgeschätzt werden können. Durch erste Abschätzungen der Erfüllungsaufwände besteht

eine große Wahrscheinlichkeit, dass die jährlichen Erfüllungsaufwände für Wirtschaft und Verwaltung jeweils 1 Mio. EURO überschreiten.

Mit der Evaluierungsklausel soll ein kontinuierlich wirkendes qualitatives Überprüfungs-instrument etabliert werden, ob die Zielsetzung des KRITIS-DachG, der Aufrechterhaltung der Wirtschaftsstabilität angesichts der wechselseitigen Abhängigkeiten, erreicht wird. Evaluiert werden soll insbesondere, ob

· kritische Anlagen nach den Bestimmungen dieses Gesetzes angemessen, bürokratiearm und zielorientiert identifiziert werden können,

· die Identifizierung von kritischen Anlagen erweitert werden sollte,

· das BBK seinen Aufgaben aus diesem Gesetz hinreichend nachkommen kann, insbesondere in fachlich sachkundiger und personeller Hinsicht, aber auch hinsichtlich der erforderlichen Ausstattung,

· die Zusammenarbeit und der Informationsaustausch zwischen dem BBK und den fachlich zuständigen Aufsichtsbehörden im Sinne des Gesetzes funktioniert.

Die Bundesregierung legt frühestens nach Ablauf von 5 Jahren, spätestens nach Ablauf von 7 Jahren nach Inkrafttreten des Gesetzes einen Evaluierungsbericht vor. Aus diesem sollte insbesondere hervorgehen,

· ob das Ziel des Gesetzes erreicht wurde,

· welche Kosten und Nutzen bei der Umsetzung dieses Gesetzes entstanden sind,

· ob eine Weiterentwicklung der Vorschriften dieses Gesetzes erforderlich ist und

· welche weiteren Schlussfolgerungen oder Handlungsoptionen oder Vorgehensweisen empfohlen werden (Handlungsempfehlungen)

Gemäß Art. 25 der CER-Richtlinie nimmt die EU-Kommission eine eigene Evaluierung der Richtlinie vor. Sie legt den ersten Bericht bis zum 17.Juni 2029 vor. Die Bundesregierung ist gehalten, zu überprüfen, inwiefern Ergebnisse dieser Evaluierung auf die Evaluierung des KRITIS-DachG Berücksichtigung finden können, ebenso auch Evaluierungsergebnisse anderer Mitgliedsstaaten.

Zu § 19 (Bußgeldvorschriften)

Nach Art. 22 der CER-Richtlinie müssen die Mitgliedstaaten bei Verstößen gegen die in diesem Gesetz umgesetzten Vorgaben aus der CER-Richtlinie Sanktionen erlassen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

In dem Zusammenhang soll jedoch der Tatsache Rechnung getragen werden, dass die Verpflichtungen aus diesem Gesetz für die Betreiber kritischer Anlagen neu sind und bislang nur aus vereinzelten spezifischen Branchen Erfahrungswerte zur Umsetzbarkeit vorliegen. Dies gilt insbesondere für die Identifizierung von kritischen Anlagen nach § 4 und für die Aufstellung, Dokumentation und den Nachweis von Resilienzmaßnahmen. Daher sieht § 19 eine gestufte Sanktionsvorschrift vor: Den Betreibern kritischer Anlagen wird zunächst eine sanktionsfreie Zeit zugestanden, indem die Vorschrift erst am 01. Januar 2027 in Kraft tritt. Damit wird den Betreibern kritischer Anlagen eine ausreichende Vorlaufzeit eingeräumt, sich mit den Vorgaben des Gesetzes vertraut zu machen und die Vorgaben schrittweise zu erfüllen. In Anlehnung an Art. 21 Abs. 3 der CER-Richtline und dem Grundsatz der Verhältnismäßigkeit geschuldet, muss das BBK bei festgestellten Verstößen

zunächst darauf hinwirken, dass Betreiber einer kritischen Anlage die Möglichkeit bekommen, den Verstoß zu beheben, ohne sofort mit einem Bußgeld belangt zu werden.

Das BBK wird nur bei originären Verstößen gegen die Vorgaben dieses Gesetzes tätig. § 17 Absatz 2 Satz 2 soll insofern Doppelsanktionierungen verhindern und Vorgaben aus anderen fachlichen Verfahren berücksichtigen, insbesondere im Sinne des § 10 Absatz 7 Satz 4. Werden Verstöße gegen solche Vorgaben (z.B. Auflagen, Bedingungen oder Nebenbestimmungen) aus fachlich anderen Bescheiden, Genehmigungen, Zertifizierungen oder ähnlichen Nachweisen bereits durch die zuständige Fach- bzw. Aufsichtsbehörde sanktioniert, können Betreiber kritischer Anlagen nicht noch einmal nach diesem Gesetz für denselben Verstoß sanktioniert werden.

Zu § 20 (Inkrafttreten)

§ 20 regelt das Inkrafttreten des Gesetzes.

Zu Absatz 1

Das Gesetz tritt mit Ausnahme der Absätze 2 und 3 am Tag nach der Verkündung in Kraft.

Zu Absatz 2

§§ 6 bis 8, §§ 10 bis 12 und § 16 treten abweichend von Absatz 1 am 01. Januar 2026 in Kraft. Damit wird eine ausreichende Übergangszeit zwischen dem Inkrafttreten der gesetzlichen Bestimmungen und der Anwendung der den Betreibern auferlegten Verpflichtungen vorgesehen, damit sie sich auf die Verpflichtungen nach diesem Gesetz einstellen und die erforderlichen Vorbereitungen treffen können. Die Frist ermöglicht gleichzeitig die Einhaltung der Anforderung des Art. 6 Abs. 1 CER-Richtlinie, nach der die kritischen Anlagen bis zum 17. Juli 2026 ermittelt werden müssen. Da die Ermittlung der kritischen Anlagen über die Registrierung der kritischen Anlagen nach § 8 erfolgt, dient die Festlegung des Zeitpunkts des Inkrafttretens dieser Regelung am 01. Januar 2026 diesem Ziel.

Zu Absatz 3

Die in § 19 vorgesehenen Bußgeldvorschriften treten abweichend von Absatz 1 erst am 01. Januar 2027 in Kraft. Damit wird den Betreibern der kritischen Anlagen eine ausreichende Übergangszeit zwischen dem Inkrafttreten der gesetzlichen Bestimmungen, der Umsetzung von Maßnahmen und einer Sanktionierung der neuen Vorschriften vorgesehen.