

# Betriebs Berater

BB

23 | 2026

Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ... 1.6.2026 | 81. Jg.  
Seiten 1281–1344

## DIE ERSTE SEITE

**Prof. Dr. iur. Michael Stahlschmidt**, M.R.F., LL.M., MBA, LL.M., RA/FAStR/  
FAInsSanR/FAMedR/StB

Die „Regulatory Technical Standards“ – ein Beitrag zum Bürokratieabbau?

## WIRTSCHAFTSRECHT

**Stephan Schmidt**, RA/FAIT-Recht, CIPP/E

Das KRITIS-Dachgesetz: Neuer bundeseinheitlicher Rechtsrahmen für die Resilienz kritischer Anlagen | 1283

**Simon Wegmann**, RA, und **Hanna Kröhnert**, RAin

Die Ampel steht auf grün für den Digital Omnibus – aber was bringt er mit? | 1290

## STEUERRECHT

**Miriam Schubert**, LL.M., RORin

Eine kritische Auseinandersetzung mit dem Beschluss des BVerfG vom 27.11.2024 – 1 BvR 1726/23 und der Rechtsprechungsänderung des BVerfG zu kommunalen Verpackungssteuern sowie daraus resultierender Chancen und Risiken für Kommunen – Teil I | 1303

## BILANZRECHT UND BETRIEBSWIRTSCHAFT

**Dr. Norbert Lüdenbach**, WP/StB, und **Prof. Dr. Robert Braun**

Inkonsistenzen bei der Bilanzierung von Erwerbsgewinnen oder -verlusten nach IFRS sowie HGB/EStG | 1321

## ARBEITSRECHT

**Jessica Bucher**, RAin, und **Benedikt Bögle**, RA

Verfahrensrechtlicher Schutz von Geschäftsgeheimnissen im Prozess vor den Arbeitsgerichten | 1330



Stephan Schmidt, RA/FAIT-Recht, CIPP/E

# Das KRITIS-Dachgesetz: Neuer bundeseinheitlicher Rechtsrahmen für die Resilienz kritischer Anlagen

Das KRITIS-Dachgesetz (KRITIS-DachG) setzt die CER-Richtlinie (EU) 2022/2557 in deutsches Recht um und schafft erstmals bundeseinheitliche und sektorübergreifende Mindeststandards für den physischen Schutz kritischer Anlagen. Es ergänzt für die betroffenen Sektoren das bestehende Regime der IT-Sicherheit nach dem BSI-G und den auf seiner Grundlage erlassenen Regelungen um einen All-Gefahren-Ansatz. Der vorliegende Beitrag analysiert das neue Gesetz in seinen wesentlichen Regelungsstrukturen und erläutert die Pflichten für betroffene Betreiber.

## I. Einleitung und rechtspolitischer Hintergrund

Am 16.3.2026 wurde das Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (nachfolgend: KRITIS-DachGEG) im Bundesgesetzblatt verkündet.<sup>1</sup> Dieses enthält als Art. 1 das „Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen“ (nachfolgend KRITIS-DachG) und in den weiteren Artikeln entsprechende Anpassungen von sektoralen Regelungen. Es ist am 17.3.2026 in Kraft getreten und schließt damit eine Regulierungslücke, die das deutsche Recht seit Jahrzehnten prägte: Erstmals existieren sektorübergreifende Mindeststandards für den physischen Schutz kritischer Anlagen. Damit vollzieht der Gesetzgeber einen Paradigmenwechsel: Weg von einer primär auf IT-Sicherheit ausgerichteten KRITIS-Regulierung, hin zu einem umfassenden Resilienz-Konzept, das sämtliche Gefahrendimensionen – von Naturkatastrophen über Sabotage bis hin zu hybriden Angriffen – in den Blick nimmt. Resilienz bezeichnet dabei die Fähigkeit, Ereignissen zu widerstehen oder sich daran anzupassen und dabei seine Funktionsfähigkeit zu erhalten oder schnell wiederzuerlangen.<sup>2</sup>

Der rechtspolitische Druck zur Schaffung eines solchen Instruments hatte sich in den vergangenen Jahren erheblich verstärkt. Anschläge auf die Nord-Stream-Pipelines, Sabotagevorfälle an der Deutschen Bahn sowie ein Brandanschlag auf die Energieinfrastruktur im Süden Berlins Anfang 2026 verdeutlichten die Verwundbarkeit zentraler Versorgungsstrukturen und machten den Handlungsbedarf auch für ein breiteres Publikum sichtbar. Auf europäischer Ebene hatte die EU bereits mit der CER-Richtlinie (Richtlinie über die Resilienz kritischer Einrichtungen)<sup>3</sup> ein verbindliches Resilienz-Regime geschaffen, welches die Mitgliedstaaten bis zum 17.10.2024 umzusetzen hatten. Deutschland geriet dabei in Verzug, was zu einem Vertragsverletzungsverfahren führte.<sup>4</sup>

Für die Unternehmenspraxis hat das KRITIS-DachG erhebliche Bedeutung: Es verpflichtet nicht nur zu einer Registrierung der betroffenen Unternehmen, sondern schreibt auch eigene Risikoanalysen, die Aufstellung von Resilienzplänen, physische Schutzmaßnahmen, ein

gestuftes Meldewesen und – für die Geschäftsleitung – eine eigene Verantwortlichkeit bei der Umsetzung und Überwachung vor.

## II. Europarechtlicher Hintergrund: Die CER-Richtlinie

### 1. Von der ECI-Richtlinie zur CER-Richtlinie

Die europäische Regulierung kritischer Infrastrukturen hat eine längere Geschichte. Vorgänger der CER-Richtlinie war die EU-Infrastrukturschutz-Richtlinie 2008/114/EG<sup>5</sup> über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen (ECI-Richtlinie), welche sich allerdings in ihrer praktischen Wirkung als wenig effektiv erwiesen hatte, beschränkte sie sich doch im Wesentlichen auf ein Meldeverfahren und die Pflicht zur Erstellung von Sicherheitsplänen für die Sektoren Energie und Verkehr.

Die CER-Richtlinie trat am 16.1.2023 in Kraft und verfolgt ein grundlegend anderes Regelungskonzept. Während sich die ECI-Richtlinie allein auf den Schutz europäisch bedeutsamer Infrastrukturen konzentrierte, richtet die CER-Richtlinie ihren Fokus auf sämtliche Einrichtungen, deren Ausfall erhebliche Auswirkungen auf die Erbringung wesentlicher Dienstleistungen haben kann und zielt mit einem umfassenden All-Gefahren-Ansatz auf die Stärkung der physischen Resilienz kritischer Einrichtungen ab.<sup>6</sup>

### 2. Wesentliche Regelungsgehalte der CER-Richtlinie

Die CER-Richtlinie verpflichtet die Mitgliedstaaten zu einem mehrstufigen Regulierungsrahmen. Auf nationaler Ebene sind zunächst eine nationale Resilienzstrategie sowie sektorale Risikoanalysen zu erstellen (Art. 4, Art. 5 CER-RL). Sodann müssen die Mitgliedstaaten kritische Einrichtungen identifizieren und sie über ihren Status informieren (Art. 6 CER-RL). Den als kritisch identifizierten Einrichtungen obliegen umfassende Pflichten: Risikobewertungen (Art. 12 CER-RL), Resilienzmaßnahmen (Art. 13 CER-RL) sowie Meldepflichten bei erheblichen Vorfällen (Art. 15 CER-RL).

1 BGBl. 2026 I Nr. 66 vom 16.3.2026.

2 Ausführlich zum Resilienzbegriff *Hornung/Pfeiffer/Zurawski*, ZfDR 2026, 37 f.

3 RL (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14.12.2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der RL 2008/114/EG des Rates, ABl. L 333 vom 27.12.2022.

4 PM der Europäischen Kommission vom 17.7.25, unter [https://germany.representation.ec.europa.eu/news/vertragsverletzungsverfahren-im-juli-entscheidungen-zu-deutschland-2025-07-17\\_de](https://germany.representation.ec.europa.eu/news/vertragsverletzungsverfahren-im-juli-entscheidungen-zu-deutschland-2025-07-17_de) (Abruf: 15.5.2026).

5 RL 2008/114/EG des Rates vom 8.12.2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl. L 345 vom 23.12.2008.

6 *Schmidt*, MMR 2026, 269, 270.

Die CER-Richtlinie steht in enger Wechselwirkung mit der NIS-2-RL,<sup>7</sup> welche die Cybersicherheit wesentlicher und wichtiger Einrichtungen regelt. Art. 3 Abs. 1 lit. f NIS-2-RL bestimmt, dass kritische Einrichtungen im Sinne der CER-RL zugleich als wesentliche Einrichtungen im Sinne der NIS-2-RL gelten, sofern sie in deren Anwendungsbereich fallen. Damit entsteht ein duales Regulierungsregime, das physischen Schutz und Cybersicherheit miteinander verzahnt.

### III. Gesetzgebungsverfahren und politischer Kontext

Bereits im Juli 2023 legte die damalige Bundesregierung einen Referentenentwurf vor.<sup>8</sup> Mit der vorzeitigen Beendigung der Legislaturperiode Anfang 2025 verfiel der Entwurf jedoch dem verfassungsrechtlichen Diskontinuitätsprinzip.

Die neue Bundesregierung nahm das Vorhaben in nahezu unveränderter Form wieder auf. Am 6.11.2025 erfolgte die erste Lesung des entsprechenden Entwurfs im Bundestag. Der Bundestag verabschiedete das Gesetz am 29.1.2026 in der durch den Innenausschuss geänderten Fassung.<sup>9</sup>

Das anschließende Bundesratsverfahren offenbarte erhebliche Bundesländer-Konflikte. Der Innenausschuss des Bundesrates empfahl am 20.2.2026 die Anrufung des Vermittlungsausschusses.<sup>10</sup> Die Länder kritisierten insbesondere den Schwellenwert von 500 000 versorgten Einwohnern als zu hoch – eine Absenkung auf 150 000 Personen wurde gefordert – und bemängelten, die Länderöffnungsklausel des § 5 Abs. 7 KRITIS-DachG führe zu einer Rechtszersplitterung. Zudem monierten die Länder das Fehlen konkreter Betreiberpflichtungen, insbesondere mit Blick auf die Vorbereitung auf Ausfälle sowie deren Nachsorge, und dass eine nachgelagerte Verordnung nicht geeignet sei, ein einheitliches und verbindliches Schutzniveau zu gewährleisten. Letztlich stimmte der Bundesrat dem Gesetz am 6.3.2026 dennoch zu und adressierte lediglich die Aufspaltung der Aufsichtsbefugnisse im Eisenbahnsektor in einer Entschließung.<sup>11</sup>

### IV. Verhältnis zum bisherigen Recht

#### 1. Bisherige Rechtslage: BSIG und BSI-KritisV

Das Recht der kritischen Infrastrukturen war in Deutschland bislang primär durch das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und die auf seiner Grundlage erlassene Verordnung zur Bestimmung kritischer Anlagen nach dem BSI-Gesetz (BSI-KritisV) geprägt. Das Regelungssystem beruhte auf einem zweigliedrigen Ansatz: Das BSIG normierte die grundlegenden Pflichten, insbesondere in § 8a (IT-Sicherheitsmaßnahmen), § 8b (Meldepflichten) und § 8d (Nachweis- und Prüfpflichten). Die BSI-KritisV konkretisierte anschließend – und inhaltlich maßgeblich –, welche Anlagen überhaupt als kritisch gelten, indem sie für neun Sektoren spezifische Anlagenkategorien und Schwellenwerte festlegte. Seit der ersten KRITIS-Verordnung 2016 gab es vier separate Änderungsverordnungen, die Schwellenwerte und Anlagen an die aktuellen Umstände anpassten. Das Regelungsmodell wies jedoch erhebliche Defizite auf. Erstens war der Regelungsgegenstand auf IT-Sicherheit beschränkt;<sup>12</sup> physische Bedrohungen blieben ohne bundesgesetzliche Mindestanforderungen.<sup>13</sup> Zweitens wurde die entscheidende Frage, welche Anlagen überhaupt kritisch sind, nicht durch das Parlamentsgesetz, sondern allein durch die BSI-KritisV bestimmt – ein Defizit,

das im Schrifttum im Lichte der verfassungsrechtlichen Wesentlichkeitstheorie kritisch beurteilt wurde.<sup>14</sup> Drittens blieben Sektoren wie die „Öffentliche Verwaltung“ bis zuletzt aus dem Anwendungsbereich ausgespart, obwohl dieser für die Versorgungssicherheit erhebliche Bedeutung hat.<sup>15</sup>

Das BSIG wurde durch das IT-Sicherheitsgesetz 2.0 vom 18.5.2021 reformiert. Dieses brachte zwar erhebliche Erweiterungen – insbesondere die Einführung der Kategorie der „Unternehmen in besonderem öffentlichen Interesse“<sup>16</sup> sowie die Aufnahme des Sektors Siedlungsabfallentsorgung<sup>17</sup> –, ließ das Grundproblem der fehlenden physischen Resilienzpfllichten aber unberührt.

#### 2. Die NIS2-Richtlinien-Umsetzung als komplementärer Rechtsrahmen

Mit dem Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 2.12.2025 wurde zunächst der digitale Teil des Resilienzrahmens novelliert. Das neue BSIG erfasst nun in erheblich erweitertem Umfang besonders wichtige und wichtige Einrichtungen und verschärft die Anforderungen an Cybersicherheitsmaßnahmen, Meldewesen und Lieferkettensicherheit. Betreiber kritischer Anlagen im Sinne des KRITIS-DachG gelten zugleich als besonders wichtige Einrichtungen nach dem BSIG.

Das KRITIS-DachG ergänzt diesen digitalen Rechtsrahmen nun um den physischen Schutz. Die Trennlinie zwischen beiden Gesetzen folgt – vereinfacht – dem Schutzgegenstand: Das BSIG schützt IT-Systeme und informationstechnische Prozesse; das KRITIS-DachG schützt die physisch-materielle Substanz der Anlagen. Freilich ist die Grenzziehung nicht immer trennscharf – ein Hochwasser, das einen Serverraum überflutet, betrifft gleichzeitig physische und digitale Sicherheitsebenen.

Zudem liegen BSIG und KRITIS-DachG unabgestimmt nebeneinander, was aber in erster Linie daran liegt, dass bereits die europäischen Richtlinien uneinheitlich und nicht in einem Regelungsvorhaben erlassen wurden.<sup>18</sup> KRITIS-DachG und BSIG bilden ein komplementäres Doppelregime, das beide Schutzrichtungen – physisch und digital – abdeckt. Da Betreiber kritischer Anlagen im Sinne des KRITIS-DachG nach § 28 Abs. 1 Nr. 1 BSI als besonders wichtige Einrichtungen nach dem BSIG gelten, unterliegen sie kumulativ beiden Regel-

7 RL (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der VO (EU) Nr. 910/2014 und der RL (EU) 2018/1972 sowie zur Aufhebung der RL (EU) 2016/1148 (NIS-2-Richtlinie), Abl. L 333/80 v. 27.12.2022.

8 Ausführlich zum 1. Entwurf Kipker/Dittrich, ZRP 2023, 230 f.; Historie der Referenten- und Regierungsentwürfe unter <https://www.openkritis.de/it-sicherheitsgesetz/kritis-dachgesetz-sicherheitsgesetz-3-0.html> (Abruf: 15.5.2026).

9 Vgl. Plenarprotokoll 21/56, S. 6704.

10 Ausschussempfehlung BR-Dr 81/1/26, unter <https://www.bundesrat.de/SharedDocs/drucksachen/2026/0001-0100/81-1-26.pdf> (Abruf: 15.5.2026).

11 Beschlussdrucksache BR-Dr. 81/26, unter [https://www.bundesrat.de/SharedDocs/drucksachen/2026/0001-0100/81-26\(B\).pdf?\\_\\_blob=publicationFile&v=2](https://www.bundesrat.de/SharedDocs/drucksachen/2026/0001-0100/81-26(B).pdf?__blob=publicationFile&v=2) (Abruf: 15.5.2026).

12 Vgl. Kipker/Dittrich, ZRP 2023, 230.

13 Vgl. Kment, NVwZ 2025, 1369, 1373.

14 Heckmann, MMR 2015, 289; Ritter, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, BSIG § 2, Rn. 31.

15 Hornung, NJW 2015, 3334, 3335; Fischer, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl. 2024, § 13, Rn. 30; vgl. hierzu insgesamt auch Schreiber, BB 2026, 323 ff.

16 Fischer, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl. 2024, § 13, Rn. 1; Ritter, in: Kipker Cybersecurity, 2. Aufl. 2023, Kap. 15.2, Rn. 25.

17 Beucher/Ehlen/Utzerath, in: Kipker Cybersecurity, 2. Aufl. 2023, Kap. 14, Rn. 44.

18 So auch Kipker/Dittrich, NIS-2-Umsetzung: Der große Wurf gelingt noch nicht, 18.6.2025, unter <https://www.security-insider.de/deutschland-nis-2-richtlinie-it-sicherheit-a-7d14f9df6d80a83faebca326b14227/> (Abruf: 15.5.2026); vgl. auch Schreiber, Die Erste Seite, BB Heft 39/2025.

werken. In der Praxis empfiehlt sich daher ein integriertes Compliance-Management, das beide Pflichtenebenen zusammenführt.

### 3. Ablösung der BSI-KritisV

Von besonderer praktischer Bedeutung ist, dass die BSI-KritisV nach Art. 9 KRITISDachGEG außer Kraft tritt – und zwar zu dem Zeitpunkt, zu dem die Rechtsverordnung nach § 4 Abs. 3 und § 5 Abs. 1 KRITIS-DachG in Kraft tritt. Diese neue Verordnung des Bundesministeriums des Innern (BMI) wird die BSI-KritisV vollständig ersetzen und für beide Gesetze – BSIG und KRITIS-DachG – den sektorspezifischen Anwendungsbereich festlegen. Bis zum Erlass dieser Verordnung gilt die BSI-KritisV fort, sodass der Übergangszeitraum für die Praxis beherrschbar bleibt.

## V. Anwendungsbereich des KRITIS-DachG

### 1. Sektoren

Der sachliche Anwendungsbereich des KRITIS-DachG richtet sich nach einem Sektorenmodell. § 4 Abs. 1 KRITIS-DachG benennt abschließend zehn Sektoren: Energie, Transport und Verkehr, Finanzwesen, Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum und Siedlungsabfallentsorgung. Im Vergleich zur bisherigen BSI-KritisV kommt nur der Sektor Weltraum neu hinzu; alle anderen Sektoren entsprechen dem bekannten KRITIS-Kanon.

Ausweislich der Gesetzesbegründung gelten Einrichtungen der Langzeitpflege nicht als Gesundheitsdienstleister und sind von § 4 Abs. 1 Nr. 5 KRITIS-DachG nicht erfasst.<sup>19</sup>

### 2. Kritische Anlage und kritische Dienstleistung

Das KRITIS-DachG definiert in § 2 Nr. 3 die kritische Anlage als eine Anlage, die innerhalb eines der genannten Sektoren eine kritische Dienstleistung erbringt. Unter einer kritischen Dienstleistung versteht das Gesetz eine Dienstleistung zur Versorgung der Allgemeinheit in den genannten Sektoren, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde. Welche Anlagenkategorien und Dienstleistungen konkret in den Anwendungsbereich fallen, bestimmt das BMI durch Rechtsverordnung nach § 4 Abs. 3 und § 5 Abs. 1 KRITIS-DachG. Nach § 4 Abs. 3 KRITIS-DachG wird zunächst festgelegt, welche kritischen Dienstleistungen zu den Sektoren gehören. In § 5 Abs. 1 KRITIS-DachG wird festgelegt, welche Anlagen für die Aufrechterhaltung kritischer Dienstleistungen in den Sektoren als erheblich und damit als kritisch im Sinne des KRITIS-DachG gelten. Die Entwurfsbegründung geht von etwa 1 700 kritischen Anlagen aus.<sup>20</sup>

Diese Verordnungsermächtigung knüpft strukturell an das bekannte Modell der BSI-KritisV an. Nach Angaben der Gesetzesbegründung soll sich die neue Verordnung inhaltlich eng an der bisherigen BSI-KritisV orientieren, damit Betreiber, die bislang als KRITIS-Betreiber galten, auch künftig als solche erfasst werden. Gleichwohl besteht bis zur Verkündung der neuen Rechtsverordnung Rechtsunsicherheit: Die genaue Anlagendefinition fehlt noch, sodass Betreiber gut beraten sind, schon jetzt eine eigene Betroffenheitsanalyse auf Basis der bisherigen BSI-KritisV vorzunehmen.

Das BMI ist nach § 5 Abs. 3 KRITIS-DachG befugt, im Einzelfall abweichende Entscheidungen zu treffen – also Anlagen trotz Über-

schreitens des Schwellenwertes vom Anwendungsbereich auszunehmen oder Anlagen unterhalb des Schwellenwertes einzubeziehen, wenn qualitative Faktoren wie sektor- und branchenübergreifende Interdependenzen, Marktanteil oder geographische Reichweite dies rechtfertigen. Betreiber, die von einer solchen Feststellung betroffen sind, werden durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) gem. § 5 Abs. 5 KRITIS-DachG schriftlich oder elektronisch informiert und gegebenenfalls zur Registrierung aufgefordert. Diese Einzelfallklausel eröffnet einerseits Flexibilität, birgt andererseits aber erhebliche Rechtsunsicherheit für die betroffenen Unternehmen.

§ 7 Abs. 2 KRITIS-DachG regelt für Einrichtungen der Bundesverwaltung, dass das BMI mit Einvernehmen der betroffenen Einrichtung festlegt, welche kritischen Dienstleistungen von der jeweiligen Einrichtung der Bundesverwaltung erbracht werden und für die dann das KRITIS-DachG nach den Maßgaben in § 7 Abs. 1 KRITIS-DachG entsprechend anwendbar ist. Lediglich im Geschäftsbereich des Auswärtigen Amtes und des Bundesministeriums der Verteidigung (BMVg) sind die Ziele des Gesetzes durch „ergebnisäquivalente Maßnahmen“ umzusetzen.

### 3. Betreiberbegriff

Als Betreiber einer kritischen Anlage gilt gemäß § 2 Nr. 1 KRITIS-DachG grundsätzlich jede natürliche oder juristische Person oder eine rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine oder mehrere kritische Anlagen ausübt. Dieser Betreiberbegriff knüpft an einen wirtschaftlich-faktischen Beherrschungsbegriff an, ohne auf eine bestimmte Rechtsform oder formale Eigentümerstellung abzustellen.

Wichtige und besonders wichtige Einrichtungen im Sinne des BSIG, die keine KRITIS-Anbieter sind und andere Unternehmen, fallen nicht in den Anwendungsbereich des KRITIS-DachG. Zudem erlaubt § 22 KRITIS-DachG mit einem einfachen oder erweiterten Ausnahmebescheid Betreiber kritischer Anlagen ganz oder teilweise von ihren Sicherheitspflichten zu befreien, wenn sie in Bereichen der öffentlichen Sicherheit tätig sind. Der Ausnahmetatbestand entspricht der Regelung in § 37 BSIG.<sup>21</sup>

### 4. Schwellenwerte

Der zentrale quantitative Maßstab ist der Regelschwellenwert von 500 000 versorgten Einwohner je Anlage (§ 5 Abs. 2 S. 2 KRITIS-DachG). Dieser entspricht dem Schwellenwert, der bereits der bisherigen BSI-KritisV zugrunde liegt, und stellt damit Kontinuität zur bisherigen Rechtslage sicher. Zugleich werden die Schwellenwerte durch die noch zu erlassende Rechtsverordnung sektorspezifisch konkretisiert – ähnlich wie die BSI-KritisV für jeden Sektor anlagenspezifische Kapazitäts- oder Leistungsgrößen definiert.

Dieser Schwellenwert erscheint mit Blick darauf, dass wohl ein Großteil der Bevölkerung von Unternehmen versorgt wird, die unterhalb der Schwelle von 500 000 liegen, zu hoch und es findet sich auch keinerlei Begründung dafür, warum dieser Wert seit seiner Einführung im Jahr 2016, als das erste IT-Sicherheitsgesetz erlassen wurde, nicht

<sup>19</sup> BT-Drs. 21/2510, 45.

<sup>20</sup> BT-Drs. 21/2510, 37.

<sup>21</sup> Voigt, in: Voigt, IT-Sicherheitsrecht, 3. Aufl. 2026, Rn. 421.

angepasst wurde.<sup>22</sup> Der Bundesrat hatte in seiner Stellungnahme eine Absenkung des Schwellenwertes auf 150 000 versorgte Personen empfohlen und verwies darauf, dass die Mehrheit der Bevölkerung in Deutschland von KRITIS-Betreibern versorgt wird, die unterhalb des Schwellenwertes liegen, sodass das KRITIS-DachG im Tatsächlichen nur eine punktuelle, jedoch keine flächendeckende Verbesserung des Schutz- und Versorgungsniveaus mit sich bringen wird.<sup>23</sup> Die Bundesregierung hielt demgegenüber am Wert von 500 000 fest und verwies auf die Möglichkeit der Länder, nach § 5 Abs. 7 KRITIS-DachG im Rahmen ihrer Zuständigkeiten niedrigere Schwellenwerte für Anlagen festzulegen, die ausschließlich in ihrem Zuständigkeitsbereich liegende kritische Dienstleistungen erbringen. Diese Lösung ist rechtspolitisch nachvollziehbar, da sie einerseits das bewährte System des Bundes nicht aufbricht, andererseits den Ländern Gestaltungsspielraum lässt. Kritisch anzumerken ist allerdings, dass die Länderöffnungsklausel zu einer Fragmentierung der Regulierung führen kann, die dem Ziel bundeseinheitlicher Mindeststandards widerspricht. Zudem fehlt es an einer tragfähigen, wissenschaftlichen Begründung, warum 500 000 versorgte Einwohner ein sinnvoller Schwellenwert ist.

In einer Protokollerklärung der Bundesregierung zur Abstimmung und Annahme des Gesetzes sichert diese im Übrigen zu, im weiteren Verfahren (spätestens bei der Evaluierung nach zwei Jahren) die Herabsetzung des Regelschwellenwerts in Höhe von 500 000 zu versorgenden Einwohnern im KRITIS-DachG geprüft wird, um einen flächendeckenden und einheitlichen KRITIS-Schutz zu gewährleisten und dem Anspruch eines Dachgesetzes gerecht zu werden.<sup>24</sup>

## VI. Pflichten der Betreiber kritischer Anlagen

### 1. Registrierungspflicht (§ 8 KRITIS-DachG)

Erste und grundlegende Pflicht jedes Betreibers einer kritischen Anlage ist die Registrierung auf der gemeinsamen Online-Plattform des BBK und des Bundesamts für Sicherheit in der Informationstechnik (BSI, § 8 Abs. 1 KRITIS-DachG). Die Registrierung hat spätestens drei Monate nach der Identifikation der Anlage als kritisch zu erfolgen, frühestens jedoch bis einschließlich zum 17.7.2026. Unklar ist, ob bestehende Registrierungen nach dem BSIG im Sinne eines Once-only-Prinzips automatisiert übernommen werden und betroffenen Einrichtungen so eine erneute vollständige Registrierung erspart bleibt.

Im Rahmen der Registrierung sind betreiber- und anlagenbezogene Angaben zu machen (§ 8 Abs. 2 KRITIS-DachG): Name und Rechtsform des Betreibers, Kontaktdaten, Sektor, Kategorie und Standort sowie Art der Anlage, die erbrachte kritische Dienstleistung sowie das Versorgungsgebiet. Zudem muss eine jederzeit erreichbare Kontaktstelle benannt werden. Jederzeit erreichbar bedeutet in der Praxis, dass Betreiber über die registrierte Kontaktstelle rund um die Uhr (24/7) in der Lage sind, BSI-Produkte zur Warnung und Information von KRITIS-Betreibern entgegenzunehmen, unverzüglich zu sichten und zu bewerten.

Praktisch bedeutsam ist, dass die Plattform noch im Aufbau begriffen war, als das Gesetz verkündet wurde. Das BSI-Meldeportal<sup>25</sup> ist zwar seit dem 6.1.2026 verfügbar; die vollständige Integration der BBK-Registrierung ist jedoch noch nicht erfolgt. Betreiber sollten die Entwicklung dieser Plattform aktiv verfolgen und rechtzeitig die erforderlichen Daten vorbereiten. Betreibern wird nach Registrierung die federführende Aufsichtsbehörde mitgeteilt und das BSI informiert (§ 8 Abs. 5 KRITIS-DachG).

derlichen Daten vorbereiten. Betreibern wird nach Registrierung die federführende Aufsichtsbehörde mitgeteilt und das BSI informiert (§ 8 Abs. 5 KRITIS-DachG).

### 2. Risikoanalyse und -bewertung durch den Betreiber (§ 12 KRITIS-DachG)

Herzstück der operativen Betreiberpflichten ist die eigene Risikoanalyse und -bewertung (§ 12 Abs. 1 KRITIS-DachG). Betreiber müssen erstmalig neun Monate nach ihrer Registrierung (§ 8 Abs. 7 KRITIS-DachG) eine solche durchführen; danach ist die Analyse im Regelturmus von vier Jahren zu wiederholen oder im Bedarfsfall anlassbezogen zu aktualisieren.

Vor den Betreiberpflichten ordnet das Gesetz staatliche Maßnahmen an, die als Grundlage der Betreiberaktivitäten dienen. Bundesministerien und Landesministerien sind verpflichtet als Grundlage für nationale Risikoanalysen eigene Risikoanalysen und Risikobewertungen durchzuführen (§ 11 Abs. 1 KRITIS-DachG). Diese Risikoanalysen und Risikobewertungen berücksichtigen mindestens naturbedingte, technische oder menschlich verursachte Risiken, alle wesentlichen Risiken für wirtschaftliche Tätigkeiten im Binnenmarkt und die Bevölkerung, die sich aus dem Ausmaß der Abhängigkeit zwischen den Sektoren ergeben und die Handlungsfähigkeit der Wirtschaft bedrohen, alle für die personelle Arbeitsfähigkeit wesentlichen Risiken in den Sektoren, die für die wirtschaftlichen Tätigkeiten im Binnenmarkt und die Bevölkerung von erheblichem Einfluss sind sowie einschlägige, gemäß § 18 KRITIS-DachG gemeldete Informationen über Vorfälle. Das BMI kann durch Rechtsverordnung inhaltliche und methodische Vorgaben für diese Risikoanalysen festlegen (§ 11 Abs. 8 KRITIS-DachG). Ergänzend sind in § 12 Abs. 3 KRITIS-DachG Unterstützungs- und Informationspflichten des Staates gegenüber den Betreibern vorgesehen – etwa die Bereitstellung von Mustern für die Risikoanalysen und Risikobewertungen.

Die Risikoanalyse muss nach § 12 Abs. 2 KRITIS-DachG die in die in § 11 Abs. 2 Nr. 1 genannten Risiken berücksichtigen. Zu diesen gehören naturbedingte, technische oder menschlich verursachte Risiken, die geeignet sein können, die Verfügbarkeit der kritischen Dienstleistungen entscheidend zu beeinträchtigen, einschließlich sektor- und länderübergreifender Risiken, Extremereignisse durch Unfälle, Naturgefahren und gesundheitliche Notlagen sowie hybride Bedrohungen, sicherheitsgefährdende oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten. Der Rückgriff auf einen All-Gefahren-Ansatz stellt dabei sicher, dass die Analyse nicht auf einzelne Bedrohungsszenarien beschränkt bleibt, sondern das gesamte Gefahrenspektrum abbildet.

Die Ergebnisse der Risikoanalyse bilden die Grundlage für die Resilienzplanung und die konkreten Resilienzmaßnahmen. Insoweit schafft das Gesetz eine logische Kausalkette: staatliche Risikoanalyse – betreibereigene Risikoanalyse – Maßnahmenplanung – Umsetzung – Nachweispflicht.

<sup>22</sup> Schmidt, MMR 2026, 269, 271.

<sup>23</sup> BT-Drs. 21/3855, 9.

<sup>24</sup> Protokollerklärung der Bundesregierung, Anlage 4 zum Plenarprotokoll 1062, S. 105, Punkt 5, unter <https://www.bundesrat.de/SharedDocs/downloads/DE/plenarprotokolle/2026/Plenarprotokoll-1062.pdf> (Abruf: 15.5.2026).

<sup>25</sup> <https://portal.bsi.bund.de/> (Abruf: 15.5.2026).

### 3. Resilienzmaßnahmen und Resilienzplan (§§ 13, 14 KRITIS-DachG)

Auf Basis der Risikoanalyse sind nach § 13 Abs. 2 KRITIS-DachG dem Stand der Technik entsprechende, verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Erhöhung der Resilienz der kritischen Anlage zu treffen. Das Gesetz enthält in § 13 Abs. 3 eine nicht abschließende Aufzählung möglicher Maßnahmen, welche jeweils den Zielen in § 8 Abs. 1 KRITIS-DachG zugeordnet sind. Dazu gehören Maßnahmen der Notfallvorsorge, Maßnahmen der baulichen und technischen Sicherung und des organisatorischen Schutzes (Objektschutz), Instrumente und Verfahren für die Überwachung der Umgebung, der Einsatz von Detektionsgeräten und Zugangskontrollen, Risiko- und Krisenmanagementverfahren und -protokolle und vorgegebene Abläufe im Alarmfall, Maßnahmen zur Aufrechterhaltung des Betriebs, die Ermittlung alternativer Lieferketten, ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeitenden sowie Schulungsmaßnahmen.

Die Maßnahmen und die diesen zugrunde liegenden Erwägungen müssen vom Betreiber in einem Resilienzplan dargestellt und der Resilienzplan muss angewendet werden. Bei der Darstellung soll auf die Risikoanalyse und Risikobewertung des Betreibers Bezug genommen werden (§ 13 Abs. 4 KRITIS-DachG).

Entscheidend ist die Einschränkung durch den Verhältnismäßigkeitsgrundsatz: Nach § 13 Abs. 2 S. 4 KRITIS-DachG sind bei der Auswahl der Maßnahmen insbesondere der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls sowie die Leistungsfähigkeit des Betreibers zu berücksichtigen. Dies eröffnet Spielraum für eine betreiberspezifische, risikoproportionale Maßnahmenauswahl. Die bloße Befolgung branchenüblicher Standards reicht allerdings nicht ohne Weiteres aus; vielmehr ist eine eigenständige Verhältnismäßigkeitsprüfung durchzuführen.

Der Resilienzplan kann von der zuständigen Aufsichtsbehörde nach § 16 Abs. 2 S. 2 KRITIS-DachG angefordert werden, wenn diese die von einem Betreiber vorgelegten Nachweise als nicht ausreichend erachtet.

Die Konkretisierung der Resilienzmaßnahmen kann nach § 14 Abs. 1 KRITIS-DachG durch Rechtsverordnung des BMI oder nach § 14 Abs. 2 durch branchenspezifische Standards erfolgen, die von den Betreibern oder ihren Verbänden erarbeitet werden. Letztere Option bietet der Wirtschaft die Möglichkeit, aktiv an der Normgebung mitzuwirken und damit praxistaugliche Standards zu entwickeln. Die Einreichung von Branchenstandards ist gegenüber ministerialverordnungsrechtlichen Vorgaben regelmäßig vorzuziehen.

Zudem kann die Europäische Kommission nach Art. 13 Abs. 6 CER-Richtlinie technische und methodische Spezifikationen der zu ergreifenden Maßnahmen in einem EU-weiten Durchführungsakt festlegen. Wenn ein solcher Rechtsakt existiert, ist er gegenüber anderen Konkretisierungen vorrangig (§ 15 KRITIS-DachG).

### 4. Meldepflichten (§ 18 KRITIS-DachG)

Das KRITIS-DachG führt ein zweistufiges System von Meldepflichten ein, übernimmt also nicht die dreistufigen Meldepflichten des BSI. Treten Vorfälle auf, die die Erbringung kritischer Dienstleistungen erheblich stören oder stören könnten, hat der Betreiber nach § 18 Abs. 1 KRITIS-DachG unverzüglich, spätestens aber 24 Stunden nach Kenntnisnahme, eine Erstmeldung bei der von

BSI und BBK eingerichteten gemeinsamen Meldestelle vorzunehmen. Diese Meldung entspricht nach ihrer Frist der „frühen Erstmeldung“ des § 32 Abs. 1 Nr. 1 BSI, schafft also eine parallele Meldesystematik. Allerdings endet diese an dieser Stelle dann auch, denn eine Meldestufe nach 72 Stunden ist – anders als in § 32 Abs. 1 Nr. 2 BSI – nicht vorgesehen. Die Abschlussmeldung nach § 18 Abs. 1 S. 3 KRITIS-DachG hat einen Monat nach der Erstmeldung zu erfolgen. Die Monatsfrist beginnt aber, im Unterschied zum BSI, nach dem 24-Stunden-Zeitraum nach Kenntnisnahme zu laufen und nicht erst nach einem 72-Stunden-Zeitraum. Die Abschlussmeldung nach dem KRITIS-DachG ist also 48 Stunden vor der Abschlussmeldung nach dem BSI fällig.

Nach § 18 Abs. 2 KRITIS-DachG müssen Meldungen die zu ihrem Zeitpunkt verfügbaren Informationen enthalten, die erforderlich sind, damit Art, Ursache und mögliche, auch grenzüberschreitende, Auswirkungen und Folgen des Vorfalls ermittelt und nachvollzogen werden können. Insbesondere sind die Anzahl und der Anteil der von dem Vorfall Betroffenen, die bisherige und voraussichtliche Dauer des Vorfalls sowie das betroffene geografische Gebiet des Vorfalls anzugeben.

Die Meldungen erfolgen über das gemeinsame Online-Portal von BBK und BSI. Dieser Kanal dient zugleich der NIS2-konformen Meldung von Cybervorfällen nach dem BSI, sodass für Betreiber, die beiden Regimen unterliegen, eine integrierte Meldemöglichkeit besteht. Dennoch ist eine organisatorische Vorkehrung zu treffen: Je nachdem, ob ein Vorfall primär die physische Anlage oder IT-Systeme betrifft, ist zu prüfen, welches Gesetz (KRITIS-DachG oder BSI) und damit welche Behörde zuständig ist.

Das BBK kann in Fällen, bei denen ein öffentliches Interesse an der Offenlegung eines Vorfalls besteht, nach Anhörung des betroffenen KRITIS-Betreibers und im Benehmen mit der zuständigen Behörde entweder selbst die Öffentlichkeit informieren oder den Betreiber zu einer entsprechenden Information verpflichten (§ 18 Abs. 9 KRITIS-DachG).

### 5. Weitere Informations- und Unterrichtungspflichten (§§ 16, 17 KRITIS-DachG)

§ 13 Abs. 6 KRITIS-DachG verpflichtet Betreiber, ihr für die Sicherheit der Anlage relevantes Personal über die Sicherheitsanforderungen, Resilienzmaßnahmen und den Umgang mit Vorfällen zu unterrichten. Diese Pflicht entspricht Art. 13 Abs. 1 lit. f CER-RL und soll sicherstellen, dass Sicherheitsbewusstsein nicht nur auf Führungsebene, sondern im gesamten Unternehmen verankert ist.

Nach § 8 Abs. 6 KRITIS-DachG sind Betreiber verpflichtet, die zuständige Aufsichtsbehörde unverzüglich zu informieren, wenn Änderungen eintreten, welche die Einordnung der Anlage als kritisch beeinflussen können – etwa durch wesentliche Kapazitätsveränderungen, Umstrukturierungen oder den Verlust eines entscheidenden Betriebsmittels. Diese Pflicht zur proaktiven Kommunikation mit der Behörde ist in der Praxis häufig unterschätzt und kann im Unternehmensalltag leicht aus dem Blick geraten.

### 6. Umsetzungs- und Überwachungspflicht für Geschäftsleitungen (§ 20 KRITIS-DachG)

Obwohl es in der CER-Richtlinie keine entsprechenden Regelungen gibt, verpflichtet § 20 Abs. 1 KRITIS-DachG, vergleichbar der Rege-

lung in § 38 Abs. 1 BStG, Geschäftsleitungen von Betreibern kritischer Anlagen, die von den Betreibern kritischer Anlagen nach § 13 Abs. 1 KRITIS-DachG zu ergreifenden Resilienzmaßnahmen umzusetzen und ihre Umsetzung durch geeignete Organisationsmaßnahmen sicherzustellen. Im Kern geht es bei der Regelung darum, dass die Geschäftsleitungen die Maßnahmen als geeignet billigen und deren Umsetzung kontinuierlich überwachen müssen. Unternimmt sie dies nicht, droht eine unmittelbare Haftung, wenn keine ausreichenden Maßnahmen ergriffen werden und dem KRITIS-Betreiber infolgedessen Schäden entstehen.<sup>26</sup> § 20 Abs. 1 KRITIS-DachG schränkt die Delegation der Maßnahmenumsetzung in der Praxis jedoch ebenso wenig wie § 38 Abs. 1 BStG ein.

§ 20 Abs. 2 KRITIS-DachG sieht als Auffangtatbestand für die Haftung vor, dass Geschäftsleitungen, die ihre Pflicht nach Abs. 1 verletzen, ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts haften, sofern keine spezialgesetzliche gesellschaftsrechtliche Regelung vorgeht. Primär gilt also gesellschaftsrechtliche Innenhaftung und das KRITIS-DachG tritt subsidiär ein, soweit, wie etwa bei öffentlich-rechtlich organisierten Trägern, gesellschaftsrechtliche Haftungsnormen fehlen. Die Regelung entspricht § 38 Abs. 2 BStG.

Anders als im § 38 Abs. 3 BStG ist im KRITIS-DachG aber keine ausdrückliche Schulungspflicht für die Geschäftsleitung verankert. Dieser Unterschied kann gerade die Leitungen der betroffenen Unternehmen, die nach den Compliance-Grundsätzen eine Vorbildfunktion für die Umsetzung einnehmen, dazu verleiten, die beiden Regelungen als nicht gleichrangig anzusehen.

## 7. Nachweispflichten

Auch die Nachweispflichten des KRITIS-DachG folgen einem abgestuften Konzept. So kann die zuständige Behörde über das BBK das BSI um die Übersendung der nach § 39 BStG vorgelegten Nachweise ersuchen (§ 16 Abs. 1 KRITIS-DachG). Wenn die so erlangten Informationen nicht ausreichen, um die Einhaltung der Resilienzpflicht aus § 13 Abs. 1 KRITIS-DachG nachzuweisen, können einzelne Betreiber von der zuständigen Behörde nach einem risikobasierten Ansatz zur Vorlage weiterer, geeigneter Nachweise aufgefordert werden (§ 16 Abs. 2 KRITIS-DachG). Die zuständige Behörde darf bei den nach § 16 Abs. 2 S. 3 KRITIS-DachG ausgewählten Betreibern auch selbst oder durch einen qualifizierten unabhängigen Dritten im Rahmen eines Audits die Einhaltung des § 13 Abs. 1 KRITIS-DachG überprüfen (§ 16 Abs. 4 KRITIS-DachG). Für diese Überprüfung muss der Betreiber der kritischen Anlage das Betreten der Geschäfts- und Betriebsräume sowie Zugang zu Informationen, Systemen und Anlagen im Zusammenhang mit der Erbringung ihrer kritischen Dienstleistung während der üblichen Betriebszeiten gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen vorlegen. Er muss zudem Auskunft erteilen und die erforderliche Unterstützung gewähren. Stellt die Behörde Mängel fest, kann sie die Vorlage eines Mängelbeseitigungsplans und Maßnahmen zur Mängelbeseitigung innerhalb einer angemessenen Frist verlangen (§ 16 Abs. 5 KRITIS-DachG). Das BBK kann im Einvernehmen mit dem fachlich zuständigen Bundesministerium sowie dem BSI das Verfahren der Erbringung von Nachweisen und der Audits konkretisieren (§ 16 Abs. 8 KRITIS-DachG).

## VII. Kritische Einrichtungen von besonderer Bedeutung für Europa

§ 9 KRITIS-DachG sieht für Betreiber kritischer Anlagen eine Einstufung als kritische Einrichtung von besonderer Bedeutung für Europa vor, wenn der Betreiber für oder in mindestens sechs EU-Mitgliedstaaten wesentliche Dienste i. S. v. Art. 2 Nr. 5 CER-Richtlinie oder Art. 2 Del. VO (EU) 2023/2450 erbringt und über diese Einstufung von der Europäischen Kommission über das Bundesamt für Bevölkerungsschutz und Katastrophenschutz informiert wurde. Die Einstufung löst zwar besondere behördliche Verfahren nach §§ 9f. KRITIS-DachG aus, hat für den Betreiber aber keine strengeren materiellrechtlichen Resilienzplichten zur Folge.

Auf Anfrage der Europäischen Kommission oder eines anderen EU-Mitgliedstaates, in dem der KRITIS-Betreiber wesentliche Dienste erbringt, muss das BMI nach § 9 Abs. 4 KRITIS-DachG, Teile der Risikoanalysen und -bewertungen und eine Auflistung der Resilienzmaßnahmen des KRITIS-Betreibers sowie eine Auflistung bisher ergriffener Aufsichts- und Durchsetzungsmaßnahmen übermitteln. Nach § 10 KRITIS-DachG kann das BMI außerdem bei der Europäischen Kommission beantragen, dass eine Beratungsmission für einen solchen KRITIS-Betreiber von besonderer Bedeutung für Europa eingerichtet wird. Im Rahmen dieser Beratungsmission kann dann bewertet werden, wie der betroffene KRITIS-Betreiber seine Pflichten zur Risikoanalyse und -bewertung, zum Ergreifen von Resilienzmaßnahmen und zum Melden von Vorfällen erfüllt hat.

Die kritische Einrichtung mit besonderer Bedeutung für Europa trifft in diesem Fall weitere, sich aus § 10 Abs. 2 KRITIS-DachG ergebende, Mitwirkungspflichten. Sie muss das BMI unterstützen, indem sie Informationen für die Beratungsmission zur Verfügung stellt. Nach § 10 Abs. 3 KRITIS-DachG muss sie der Beratungsmission zudem Zugang zu Informationen, Geschäftsräumen und Betriebsstätten, Systemen und Anlagen im Zusammenhang mit der Erbringung seiner kritischen Dienstleistungen gewähren, soweit dies für die Durchführung der Beratungsmission erforderlich ist. Die Europäische Kommission kann gem. Art. 18 Abs. 6 CER-Richtlinie die Verfahren der Beratungsmission durch einen oder mehrere vorrangig anwendbare Durchführungsrechtsakte festlegen.

## VIII. Behördliche Zuständigkeiten und Sanktionen

### 1. Aufteilung der Zuständigkeiten

Das KRITIS-DachG schafft eine mehrstufige Behördenstruktur. Das BBK ist nach § 3 Abs. 1 KRITIS-DachG die zentrale Anlauf- und Verbindungsstelle im Sinne der CER-Richtlinie für die grenzüberschreitende Zusammenarbeit. Es koordiniert die nationale Umsetzung, erstellt die nationalen Risikoanalysen und betreibt (gemeinsam mit dem BSI) die zentrale Melde- und Registrierungsplattform.

Die sektorspezifische Fachaufsicht liegt nach § 3 Abs. 2 KRITIS-DachG bei den jeweils fachlich zuständigen Bundesbehörden. So ist z. B. die Bundesnetzagentur für den Energie- und Telekommunikationssektor zuständig; das Eisenbahnbundesamt für den Sektor Transport und Verkehr (soweit Bundesbahnen betroffen sind); das Fernstraßen-Bundesamt für die kritische Dienstleistung des Straßenver-

<sup>26</sup> So auch Voigt, in: Voigt, IT-Sicherheitsrecht, 3. Aufl. 2026, Rn. 432.

kehr. Für kritische Dienstleistungen, die keiner dieser Bundesbehörden zugewiesen sind, kann das BMI, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, zuständige Bundesbehörden festlegen (§ 3 Abs. 3 KRITIS-DachG).

Diese Aufgliederung spiegelt die sektorale Aufsichtslogik des deutschen Verwaltungsrechts wider, birgt aber die Gefahr fragmentierter Vollzugspraxis.<sup>27</sup> Betreiber, die in mehreren Sektoren tätig sind, könnten mit unterschiedlichen Aufsichtsbehörden konfrontiert sein, die divergierende Anforderungen stellen. Eine stärkere Koordination der Aufsichtsbehörden wäre an dieser Stelle wünschenswert.<sup>28</sup>

## 2. Sanktionen und Bußgeldrahmen

Verstöße gegen die Pflichten des KRITIS-DachG werden als Ordnungswidrigkeiten geahndet. § 24 Abs. 2 KRITIS-DachG sieht für Pflichtverletzungen einen abgestuften Bußgeldrahmen von bis zu 1 000 000 Euro vor. Dieser Rahmen wurde im Gesetzgebungsverfahren auf Empfehlung des Innenausschusses gegenüber dem Regierungsentwurf (der noch 500 000 Euro vorsah) verdoppelt.

Im Vergleich zum BSIG fällt der Bußgeldrahmen des KRITIS-DachG deutlich niedriger aus: Das BSIG sieht für besonders wichtige Einrichtungen Bußgelder bis zu 10 000 000 Euro oder 2 % des weltweiten Jahresumsatzes vor. Diese Diskrepanz ist rechtspolitisch bemerkenswert. Cybervorfälle unterliegen damit schärferen Sanktionen als physische Resilienzpflichtverstöße, obwohl der physische Schutz in jüngster Zeit als mindestens ebenso kritisch eingestuft wird. Es ist zu bezweifeln, dass der uneinheitliche Bußgeldrahmen und insbesondere die geringeren Bußgelddrohungen aus dem KRITIS-DachG die erhoffte Steuerungswirkung erzielen können.

Eine Verletzung der Meldepflichten oder der Geschäftsleitungspflichten stellt keine Ordnungswidrigkeit nach dem KRITIS-DachG dar und führt daher auch nicht zur Verhängung von Bußgeldern.

## IX. Fazit

Das KRITIS-DachG ist ein wichtiger, lange überfälliger Schritt hin zu einem kohärenten physischen Schutzregime für kritische Infrastrukturen in Deutschland. Es schließt eine regulatorische Lücke, die angesichts der Häufung von Sabotageakten und Naturkatastrophen in den vergangenen Jahren nicht länger vertretbar war.

Gleichwohl sind Kritikpunkte anzumelden:

- Erstens fehlt bislang die konkretisierende Rechtsverordnung, die Anlagendefinitionen und Sektorzuweisungen festlegt. Ohne diese Verordnung bleibt der Anwendungsbereich des Gesetzes in wesentlichen Teilen unbestimmt. Betreiber befinden sich bis zum Erlass der Verordnung in einer schwierigen Lage der Rechtsunsicherheit.
- Zweitens ist das duale Behördenmodell – BBK für physischen Schutz, BSI für IT-Sicherheit – zwar rechtslogisch nachvollziehbar, birgt aber das Risiko von Reibungsverlusten und uneinheitlichem

Vollzug. In einem Zeitalter, in dem physische und digitale Angriffe oft kombiniert eingesetzt werden (hybride Bedrohungen),<sup>29</sup> erscheint eine stärkere institutionelle Integration wünschenswert.

- Drittens ist die asymmetrische Sanktionierung zu kritisieren: Cybersicherheitsverstöße nach dem BSIG werden mit bis zu 10 000 000 Euro oder 2 % des Jahresumsatzes belegt; Verstöße gegen physische Resilienzpflichten nach dem KRITIS-DachG nur mit bis zu 1 000 000 Euro. Diese Diskrepanz sendet das falsche Signal, dass physische Resilienz weniger ernst genommen wird als digitale.
- Viertens ist das Verhältnis von Bundesrecht und Landesrecht durch die Länderöffnungsklausel des § 5 Abs. 7 KRITIS-DachG erneut ungelöst. Zwar erhalten die Länder Gestaltungsspielraum, dies aber um den Preis einer möglichen Zersplitterung der Standards. Für bundesweit tätige Betreiber kann dies zu einem komplexen Flickenteppich verschiedener landesrechtlicher Anforderungen führen.

Der Gesetzgeber hat sich durch die Evaluierungsklausel des § 25 KRITIS-DachG – Evaluierung bereits nach zwei Jahren auf Betreiben des Bundesrates – die Möglichkeit offengehalten, zeitnah nachjustieren. Diese Flexibilitätsreserve ist angesichts des dynamischen Bedrohungsumfelds und der noch offenen Regulierungsfragen sinnvoll. Erste Erkenntnisse aus der Vollzugspraxis werden zeigen, ob die Schwellenwertsystematik sachgerecht ist, ob die Behördenkoordination zwischen BBK und BSI reibungslos funktioniert und ob die Bußgeldniveaus eine hinreichende Abschreckungswirkung entfalten.

Auf europäischer Ebene ist zu beobachten, wie die anderen Mitgliedstaaten die CER-Richtlinie umsetzen. Sollten Unterschiede in den Schutzstandards entstehen, drohen Wettbewerbsverzerrungen zu Lasten strenger regulierter Betreiber. Die Europäische Kommission ist aufgerufen, die Konvergenz der nationalen Umsetzungen zu überwachen und ggf. mit Leitlinien nachzusteuern.

Für die Unternehmenspraxis ist das KRITIS-DachG eine erhebliche Herausforderung, aber auch eine Chance: Wer jetzt investiert und eine robuste Resilienzarchitektur aufbaut, ist nicht nur rechtlich compliant, sondern auch besser gerüstet gegen die wachsenden hybriden Bedrohungen der Gegenwart.

**Stephan Schmidt**, RA/FAIT-Recht, ist Gründungspartner bei TCI Rechtsanwälte in Mainz. Er ist Mitglied im Geschäftsführenden Ausschuss der Arbeitsgemeinschaft IT-Recht im deutschen Anwaltverein (davit).



<sup>27</sup> So bereits *Eisenmenger*, NVwZ 2023, 1203, 1204.

<sup>28</sup> So auch *Skierka-Canton*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl. 2024, § 8, Rn. 63.

<sup>29</sup> Ausführlich dazu *Schmidt*, MMR 2026, 269.