N&R

Netzwirtschaften & Recht

Energie, Telekommunikation, Verkehr und andere Netzwirtschaften

1/2026 S. 1 – 64 23. Jahrgang

dfv Mediengruppe · Frankfurt am Main

Das Gericht der EU wies diese Rügen zurück und stellte keine offensichtlichen Beurteilungsfehler der Kommission fest. Des Weiteren bestätigte das Gericht die Auffassung der Kommission, dass auf dem tschechischen Postmarkt ein Marktversagen vorliege, das die Bereitstellung einer Dienstleistung von allgemeinem wirtschaftlichem Interesse rechtfertige. Zudem wies es auch die Einwände gegen die Kostenberechnung als nach tschechischem Recht gerechtfertigt zurück und erklärte die Einreden bezüglich angeblicher Quersubventionierung in der Vergangenheit für unzulässig.

3. Beihilfekontrolle

Mit Beschluss vom 3. Februar 2025 genehmigte die Kommission eine tschechische Maßnahme zur Entschädigung des Postbetreibers Česká pošta s. p. für die Erfüllung einer Universaldienstverpflichtung im Zeitraum 2023 bis 2024.[86] Im Rahmen der Maßnahme erhält Česká pošta eine jährliche Entschädigung von bis zu 59 Millionen Euro zur Deckung der Kosten, die ihr durch die Erfüllung der öffentlichen Dienstleistungsverpflichtung entstehen. Die Kommission prüfte die tschechische Maßnahme nach den EU-Beihilfevorschriften, insbesondere nach Art. 106 Abs. 2 AEUV, der Postdienstrichtlinie 97/67/EG und den Vorschriften zur Entschädigung für öffentliche Dienstleistungen unter den Regeln für Dienstleistungen von allgemeinem wirtschaftlichem Interesse. Die Kommission kam zu dem Schluss, dass der Umfang der Universaldienstverpflichtung der Definition in der Postdienstrichtlinie 97/67/EG entspricht. Auch stellten die Postanweisungen eine Dienstleistung von allgemeinem wirtschaftlichem Interesse dar und erfüllten die Kriterien für die Übertragung von Dienstleistungen im Rahmen des DAWI-Rahmens. Die Kommission stellte außerdem fest, dass die Entschädigung die Nettokosten der öffentlichen Dienstleistung nicht übersteigen werde, wodurch eine Überkompensation der tschechischen Post ausgeschlossen sei.

4. Fusionskontrolle

Am 13. Januar 2025 genehmigte die Kommission gemäß der EU-Fusionskontrollverordnung (EG) Nr. 139/2004 die Übernahme der alleinigen Kontrolle über die International Distribution Services Plc (IDS) durch die EP Corporate Group, a. s. (EPCG).[87] EPCG ist eine tschechische Investmentgesellschaft und gehört zur Unternehmensgruppe DK Group, die letztlich von Herrn *Daniel Křetínský*, einem tschechischen Staatsbürger, kontrolliert wird. Die DK Group verfügt über ein umfangreiches Portfolio bedeutender Vermögenswerte in ganz Europa und hält über VESA Equity Investment S. à. r. l. eine Beteiligung von 27,73 % an PostNL N. V. (PostNL), dem niederländischen Universaldienstleister für Postdienstleistungen. IDS ist ein führender Anbieter von Post- und Zustelldiensten in Großbritannien mit bedeutenden Niederlassungen in Kontinentaleuropa. Die Holdinggesellschaft umfasst zwei eigenständige Unternehmen: (i) die Royal Mail Group Limited, die Briefe und Pakete hauptsächlich in Großbritannien sammelt, sortiert und zustellt, und (ii) General Logistics Systems B. V. (GLS), die international Paketdienste anbietet. Die Transaktion betrifft hauptsächlich Post- und Paketdienstleistungen.

Die Kommission kam zu dem Schluss, dass die angemeldete Transaktion aufgrund ihrer begrenzten Auswirkungen auf den Wettbewerb in den Märkten, in denen die Unternehmen tätig sind, keine wettbewerbsrechtlichen Bedenken aufwirft. Insbesondere prüfte die Kommission die Auswirkungen der Transaktion auf die Märkte für Paketdienstleistungen in den Niederlanden, wo IDS über ihre Tochtergesellschaft GLS und die DK Group über die von ihr kontrollierte PostNL tätig ist. Die Kommission stellte fest, dass die Transaktion in den Niederlanden keine Bedenken hervorruft, da

1. die beteiligten Unternehmen keine besonders engen Wettbewerber sind,
2. nach der Transaktion ausreichend Alternativen zu den Dienstleistungen der beteiligten Unternehmen bestehen bleiben, zu denen die Kunden wechseln können, und
3. der Markteintritt neuer Wettbewerber und die Expansion bestehender Wettbewerber weiterhin möglich sein werden.

5. Ausblick

Im Jahr 2026 dürfen mit Spannung die weiteren Entwicklungen im Hinblick auf ein neues EU-Zustellgesetz für Post- und Paketdienste erwartet werden, das voraussichtlich Ende 2026 verabschiedet werden und die bestehende Postdienstrichtlinie 97/67/EG ersetzen soll. Bei der Durchsetzung des Wettbewerbsrechts kann mit weiteren Beschlüssen bei der Beihilfekontrolle gerechnet werden.

86 Kommission, Beschl. v. 3.2.2025 – Az. C (2025) 668 final – Sache SA.104103 – *Czechia;* Pressemitteilung MEX/25/399 v. 3.2.2025.

87 Kommission, Beschl. v. 13.1.2025 – Az. C (2025) 253 final – Sache M.11625 – *EPCG/IDS.*

Prof. Dr. *Alexander Koch*

Der Schutz (besonders) wichtiger und kritischer Netzinfrastrukturen

Anforderungen an die Betreiber nach der Umsetzung der NIS-2- und der CER-Richtlinie

Aus Anlass der Umsetzung der Netz-und-Informations-Sicherheits-Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) und der bevorstehenden Umsetzung der Richtlinie (EU) 2022/2557 über die Resilienz kritischer Infrastrukturen („Critical Entities Resilience"- bzw. CER-Richtlinie) beleuchtet der Aufsatz den Schutz kritischer Infrastrukturen in den Netzwirtschaften. Es wird insbesondere die Differenzierung nach verschiedenen Stufen der Kritikalität – (im Kern, aber nicht abschließend:) wichtige, besonders wichtige und kritische Einrichtung – erläutert und dargestellt, welche unterschiedlichen Pflichten für die Unternehmen etwa in den Sektoren Energie, Telekommunikation, Verkehr, Post und Wasser hieran jeweils anknüpfen.

I. Einführung

Die Versorgungsnetze sind kritische Infrastrukturen. Ihr Ausfall oder auch nur ihre Beeinträchtigung kann zu erheblichen Versorgungsengpässen und zu einer Gefährdung der öffentlichen Sicherheit führen, insbesondere weil die Sektoren voneinander abhängen.[1] Besonders herausgehoben sind dabei die Sektoren Energie und Telekommunikation: Fällt einer dieser beiden Sektoren aus, hat dies unmittelbare Auswirkungen auf alle anderen Sektoren und damit die gesamte Gesellschaft. Ohne Strom funktionieren Telekommunikationsnetze nicht mehr und ohne Telekommunikation lassen sich keine Stromnetze steuern. Ohne Strom (und Telekommunikation) funktionieren keine Eisenbahnen und die Zapfsäulen an Tankstellen fallen aus. Ohne Strom und Kraftstoffversorgung brechen der übrige Verkehr und damit auch der Ernährungssektor zusammen.[2] Der Schutz kritischer Infrastrukturen ist deshalb – auch in einem grundsätzlich marktwirtschaftlich organisierten Umfeld – eine zentrale staatliche Aufgabe.[3] Da die kritischen Infrastrukturen inzwischen unionsweit (und darüber hinaus) vernetzt sind, nimmt sich (auch) der unionale Gesetzgeber dieser Aufgabe an. Eine zentrale Rolle spielen dabei die NIS-2-Richtlinie (EU) 2022/2555 und die CER-Richtlinie (EU) 2022/2557. Beide Richtlinien hätten bis Oktober 2024 in nationales Recht umgesetzt werden müssen.[4] Dem ist der deutsche Gesetzgeber – u. a. aufgrund der vorgezogenen Neuwahlen in der 20. Legislaturperiode – nicht nachgekommen.[5] Inzwischen ist allerdings das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ in Kraft getreten.[6] Hierdurch ist namentlich das BSIG neu gefasst worden. Die CER-Richtlinie (EU) 2022/2557 soll – überwiegend – in einem KRITISDachG umgesetzt werden. Hierfür liegt ein Gesetzentwurf der Bundesregierung (KRITISDachG-RegE) vor.[7]

Mit der Umsetzung der beiden Richtlinien gehen wesentliche Änderungen im Recht der kritischen Infrastrukturen einher. Diese betreffen zunächst die Terminologie: Bislang hat das BSIG im Wesentlichen zwischen kritischen Infrastrukturen (und deren Betreibern) sowie (sonstigen) Unternehmen im besonderen öffentlichen Interesse unterschieden.[8] Zukünftig sind die Betreiber kritischer Infrastrukturen (bzw. genauer: Anlagen) nur noch ein Unterfall einer besonders wichtigen Einrichtung, neben welche die wichtigen Einrichtungen treten. Damit verbunden ist eine erhebliche Ausdehnung des Kreises der nunmehr erfassten Unternehmen.

Weiter verkompliziert wird das Recht des Schutzes kritischer Infrastrukturen durch Verordnungsermächtigungen für diverse Ministerien. Die Kommission kann außerdem Durchführungsverordnungen erlassen. Anders als Richtlinien bedürfen diese Verordnungen nach Art. 288 UAbs. 2 AEUV keines nationalen Umsetzungsakts, sondern haben allgemeine Geltung. Die Kommission hat inzwischen eine erste solche Durchführungsverordnung erlassen.[9] Der Anwendungsbereich der CER-Richtlinie (EU) 2022/2557 wird durch eine delegierte Verordnung ([EU] 2023/2450) weiter ausdifferenziert.

II. Systematik

Das neue BSIG erfasst als Hauptgruppen besonders wichtige und wichtige Einrichtungen,[10] wobei die Betreiber kritischer Anlagen zunächst nur als Unterfall der Betreiber einer besonders wichtigen Einrichtung genannt werden. Allerdings kennt das neue BSIG auch Pflichten, die *nur* die Betreiber kritischer Anlagen treffen. Betreiber kritischer Anlagen sind außerdem die Adressaten des KRITISDachG-RegE. Es ist deshalb sinnvoll, diese als eigene Gruppe besonders zu betrachten (hierzu sogleich, unter 1.). An eher versteckter Stelle im BSIG gibt es zudem Sonderregelungen für bestimmte Anbieter digitaler Dienste und digitaler Infrastrukturen (hierzu unten, unter 4.). Auf diese Gruppe bezieht sich auch die NIS-2-Durchführungsverordnung (EU) 2024/2690.

Die Unternehmen einer Branche können je nach Größe in unterschiedliche Gruppen fallen: Betreiber von Inhaltszustellnetzen („Content Delivery Networks“) fallen etwa unabhängig von ihrer Größe in die Gruppe der Anbieter digitaler Dienste und digitaler Infrastruktur (§ 60 Abs. 1 BSIG und Art. 1 der NIS-2-Durchführungsverordnung [EU] 2024/2690). Erreicht ein solcher Anbieter den Schwellenwert von 75 000 Terabyte (TByte) ausgeliefertes Datenvolumen im Jahr, ist er zudem Betreiber einer kritischen Anlage (§ 28 Abs. 1 Nr. 1 BSIG i. V. m. Anhang 4 Teil 3 Nr. 2.2.2 BSI-KritisV) und damit auch eine besonders wichtige Einrichtung i. S. d. BSIG. Betreiber von (öffentlichen) Telekommunikationsnetzen fallen unabhängig von ihrer Größe in die Gruppe der wichtigen Einrichtungen (§ 28 Abs. 2 Nr. 2 BSIG). Haben sie mindestens 50 Mitarbeiter, sind sie eine besonders wichtige Einrichtung (§ 28 Abs. 1 Nr. 3 BSIG) und ab einem Schwellenwert von 100 000 Teilnehmeranschlüssen Betreiber einer kritischen Anlage (§ 28 Abs. 1 und 2 BSIG i. V. m. Anhang 4 Teil 3 Nr. 1.1.1 BSI-KritisV).[11] Von der jeweiligen Einordnung hängt ab, welche Pflichten Unternehmen zu erfüllen haben.

1. Betreiber kritischer Anlagen

Betreiber kritischer Anlagen sind Betreiber, deren Anlagen „für die Erbringung einer kritischen Dienstleistung erheblich“ sind.[12] „Kritische Dienstleistung“ ist eine „Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende,

1 Vgl. die Legaldefinition in § 2 Nr. 24 BSIG und § 2 Nr. 4 KRITISDachG-RegE (BT-Drs. 21/2510). Siehe auch Erwägungsgrund 37 der NIS-2-Richtlinie (EU) 2022/2555.

2 Siehe auch die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 33.

3 Siehe auch die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 33.

4 Art. 41 der NIS-2-Richtlinie (EU) 2022/2555 und Art. 26 der CER-Richtlinie (EU) 2022/2557. Die materiellen Regelungen für die Wirtschaft nach der CER-Richtlinie (EU) 2022/2557 greifen aber erst 2026. Die Kommission hat wegen der fehlenden Umsetzung der beiden Richtlinien im November 2024 ein Vertragsverletzungsverfahren gegen Deutschland und 22 (bzw. 23) weitere Mitgliedstaaten eingeleitet, vgl. Kommission, Pressemitteilung INF/24/5988 v. 28.11.2024.

5 Siehe zu den Gesetzentwürfen aus der 20. Legislaturperiode *Voigt/Schmalenberger*, CR 2023, 717. Mit dem Fokus auf Cloud-Dienste *Scheibenpflug/Monschke/Hildebrandt*, CR 2024, 712. Mit dem Fokus auf Sicherheitsforschung *Vettermann*, MMR 2023, 827. Siehe zur NIS-2-Richtlinie (EU) 2022/2555 *Kipker/Dittrich*, MMR 2023, 481; *Ritter*, CR 2025, 154; *Schmidt*, K&R 2025, 705; *Grosmann/Michel*, ZD 2025, 250; *Schreiber*, CR 2025, 655 (mit einem Schwerpunkt zum Verhältnis zur Datenschutz-Grundverordnung 2016/679 [DSGVO]). Siehe zum Stand der Umsetzung in der EU *Karniyevich/Emmerich*, K&R 2025, 366; 446; *Werry/Éles*, MMR 2024, 829. Siehe zur CER-Richtlinie (EU) 2022/2557 *Hornung/Muttach/Schaller*, CR 2024, 229.

6 BGBl. 2025 I, 301. Vgl. zu den Gesetzesmaterialien den Gesetzentwurf der Bundesregierung, BR-Drs. 369/25 = BT-Drs. 21/1501; Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung, BT-Drs. 21/2072; Beschlussempfehlung und Bericht des Innenausschusses, BT-Drs. 21/2782.

7 Bis Redaktionsschluss lagen der Gesetzentwurf der Bundesregierung, BR-Drs. 558/25 = BT-Drs. 21/2510, sowie die Stellungnahme des Bundesrates, BR-Drs. 558/25 (Beschluss), vor und es waren erste Beratungen im Bundestag erfolgt.

8 Etwa §§ 8a, 8b sowie § 8f BSIG 2021.

9 NIS-2-Durchführungsverordnung (EU) 2024/2690.

10 Siehe zu den Sektoren nach der NIS-2-Richtlinie (EU) 2022/2555 auch *Schmidt*, K&R 2023, 705, 706; *Voigt/Schmalenberger*, CR 2023, 717, 717 f. Siehe zum BSIG auch *Döveling/Hempel*, CR 2025, 661, 661 f.

11 Siehe allgemein zu den Schwellenwerten nach dem BSIG *Leßner*, MMR 2024, 226.

12 Vgl. die Legaldefinition in § 2 Nr. 22 BSIG. Siehe *Kipker/Dittrich*, MMR 2023, 481, 481 f.

Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde" (§ 2 Nr. 24 BSIG sowie § 2 Nr. 4 KRITISDachG-RegE). Es handelt sich hierbei – mit geringen Änderungen in der Terminologie – weitgehend um die herkömmlichen Sektoren der kritischen Infrastrukturen (KRITIS). Neu hinzugekommen ist der Weltraumsektor.[13]

Erfasst werden aber nicht alle Unternehmen der genannten Sektoren, sondern nur jene, deren Anlagen tatsächlich kritisch (für das Allgemeinwohl) sind. Diese Anlagen werden im Anwendungsbereich des BSIG durch eine Rechtsverordnung – die BSI-KritisV – weiter ausdifferenziert (§ 2 Nr. 22 i. V. m. § 56 Abs. 4 BSIG). Der KRITISDachG-RegE sieht ebenfalls eine weitere Ausdifferenzierung durch eine Rechtsverordnung vor – diese soll mit der BSI-KritisV gleichlaufen.[14]

a) BSI-KritisV

Grundsätzlich stellt die BSI-KritisV auf die von einer Anlage versorgten Personen ab. Kritisch im Sinne der Verordnung sind nur solche Anlagen, die einen Schwellenwert von 500 000 versorgten Personen erreichen. Die Systematik ist in allen Sektoren die gleiche und wird im Folgenden beispielhaft anhand des Sektors Wasser dargestellt:

Zunächst werden in einem Paragraphen die kritischen Dienstleistungen aufgeführt – im Sektor Wasser sind dies etwa die Trinkwasserversorgung und die Abwasserbeseitigung (§ 3 Abs. 1 BSI-KritisV). Es findet sodann eine weitere Unterteilung in Bereiche – etwa „Gewinnung, Aufbereitung, Verteilung sowie Steuerung und Überwachung von Trinkwasser" – statt (§ 3 Abs. 2 BSI-KritisV). Für jeden Sektor gibt es schließlich einen Anhang. Hier finden sich zunächst jeweils umfangreiche Legaldefinitionen – etwa „Gewinnungsanlage [ist] ein Brunnen oder eine Brunnenreihe, eine Sickerleitung, ein Sickerstollen, eine Zisterne, ein Entnahmebauwerk oder eine Stauanlage zur Gewinnung, Bevorratung oder Bewirtschaftung von Oberflächenwasser oder andere Wasserfassung zur Gewinnung von Rohwasser" (Anhang 2 Teil 1 Ziff. 1.1. BSI-KritisV). Es folgen (im Teil 2) Erläuterungen zur Ermittlung der Schwellenwerte. Diese werden in einer Tabelle (Teil 3) für jede Anlagenkategorie festgelegt. So werden etwa Wasserwerke (Spalte B) erfasst, die jährlich einen Schwellenwert von 22 (Spalte D) Millionen Kubikmetern aufbereiteten Wassers (Spalte C) erreichen (Anhang 2 Teil 3 Ziff. 1.2.1 BSI-KritisV).

b) Kritische Anlagen in den Netzwirtschaften

In den anderen Netzwirtschaften werden hiernach (beispielhaft) erfasst:

1. Im Sektor *Energie:*
   a) Stromerzeugungsanlagen mit einer installierten Nettoleistung von 104 Megawatt (MW),
   b) Stromübertragungs- und Stromverteilungsnetze mit 3700 Gigawattstunden (GWh) entnommener Jahresarbeit sowie
   c) Gasfernleitungen, -speicher und -verteilnetze mit 5190 GWh entnommener Jahresarbeit,
   d) Raffinerien mit 420 000 Tonnen erzeugtem Kraftstoff im Jahr,
   e) Mineralölfernleitungen und Erdöllager mit 420 000 Tonnen transportierter bzw. umgeschlagener Rohölmenge im Jahr,
   f) Tankstellennetze mit 420 000 Tonnen verteiltem Kraftstoff im Jahr,
   g) Heizwerke und Heizkraftwerke mit 2300 GWh ausgeleiteter Wärmeenergie im Jahr sowie
   h) Fernwärmenetze mit 250 000 angeschlossenen Haushalten.[15]
2. Im Sektor *Telekommunikation:*
   a) Zugangsnetze ab 100 000 Teilnehmernetzanschlüssen und
   b) Übertragungsnetze mit 100 000 Vertragspartnern.[16]
3. Im Sektor *Transport und Verkehr* (und damit auch *Eisenbahn und Post*):
   a) Anlagen oder Systeme zur Passagierabfertigung an Flugplätzen ab 20 000 000 Passagieren pro Jahr,
   b) Frachtabfertigungsanlagen ab 750 000 Tonnen pro Jahr,
   c) Personenbahnhöfe der höchsten Kategorie,
   d) Güterbahnhöfe ab 23 000 ausgehenden Zügen pro Jahr,
   e) der deutsche Teil des Schienenkernnetzes,
   f) Umschlaganlagen in See- und Binnenhäfen ab 3 270 000 Tonnen abgefertigter Fracht pro Jahr,
   g) die Bundesautobahnen sowie
   h) Logistikzentren mit 17 550 000 Tonnen Transportmenge oder 53 200 000 Sendungen im Jahr.[17]

2. Besonders wichtige Einrichtungen

Besonders wichtige Einrichtungen im Sinne des BSIG sind zunächst die gerade beschriebenen Betreiber kritischer Anlagen (§ 28 Abs. 1 Nr. 1 BSIG). Erfasst werden außerdem alle qualifizierten Vertrauensdiensteanbieter, Register der Domänennamen höchster Stufe („Top-Level-Domain-Name-Registries" bzw. TLD-Namenregister) oder Anbieter von Diensten des Domänenennamensystems („Domain Name System", DNS) (§ 28 Abs. 1 Nr. 2 BSIG).[18]

Weiter erfasst werden (mittel)große Anbieter öffentlich zugänglicher Telekommunikationsdienste und Betreiber öffentlicher Telekommunikationsnetze. Anders als im Bereich der kritischen Infrastrukturen wird hier aber nicht auf die versorgten Einwohner abgestellt, sondern auf die Unternehmensgröße. Der Schwellenwert liegt bei 50 Mitarbeitenden oder einem Jahresumsatz und einer Jahresbilanzsumme von jeweils über 10 Millionen Euro (§ 28 Abs. 1 Nr. 3 BSIG).

Die letzte Gruppe erfasst bestimmte Großunternehmen. Diese müssen zunächst einen Schwellenwert von 250 Mitarbeitenden oder einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro erreichen. Allerdings werden nur solche Unternehmen erfasst, die in der Anlage 1 zum BSIG aufgezählt sind. Das sind insbesondere Unternehmen aus den Netzwirtschaften Energie, Transport und Verkehr, Wasser und digitaler Infrastruktur (soweit nicht dem Telekommunikationssektor im engeren Sinne zugeordnet) – aber auch aus dem Finanz- und Gesundheitswesen sowie dem Weltraumsektor.

Konkret sind dies (beispielhaft)

1. im Sektor *Energie* Stromlieferanten, Netzbetreiber, Betreiber von Energiespeicheranlagen, Betreiber von Fernwärmeanlagen,[19]
2. im Sektor *Transport und Verkehr* Betreiber von Eisenbahninfrastruktur und Eisenbahnverkehrsunternehmen,[20]

13 Erwägungsgrund 37 der NIS-2-Richtlinie (EU) 2022/2555 nimmt hier Bezug auf das Weltraumprogramm der Union; ebenso Erwägungsgrund 5 der CER-Richtlinie (EU) 2022/2557.
14 Siehe unten, unter III. 4. b) aa).
15 Anhang 1 Teil 3 Ziff. 1.1.1, 1.2.1, 1.3.1, 2.2.1, 2.2.3, 2.3, 3.1.2, 3.2.1, 3.2.2, 3.3.2, 4.1.1, 4.1.2 und 4.2.1 BSI-KritisV.
16 Anhang 4 Teil 3 Ziff. 1.1.1, 1.2.1 BSI-KritisV.
17 Anhang 7 Teil 3 Ziff. 1.1.1, 1.1.2, 1.2.1, 1.2.2, 1.2.4, 1.3.5, 1.4.1, 1.6.1 BSI-KritisV.
18 Vgl. zum Anwendungsbereich auch *Kipker/Dittrich*, MMR 2023, 481, 482.
19 Anlage 1 Ziff. 1.1.1, 1.1.2, 1.1.3, 1.1.7, 1.2.1 BSIG.
20 Anlage 1 Ziff. 2.2.1, 2.2.2 BSIG.

während Post- und Logistikunternehmen hier nicht gesondert erfasst werden,

3. im Sektor *Wasser* Betreiber von Wasserversorgungsanlagen und Abwasserbeseitigung,[21]
4. im Sektor *digitale Infrastruktur* DNS-Diensteanbieter, Anbieter von Rechenzentrumsdiensten, Betreiber öffentlicher Telekommunikationsnetze und -dienste.[22]

3. Wichtige Einrichtungen

Die zweite große Gruppe bilden wichtige Einrichtungen.[23] Hierzu zählen sonstige Vertrauensdienste (§ 28 Abs. 2 Nr. 1 BSIG) sowie kleine und mittlere Telekommunikationsunternehmen, die nicht die Schwellenwerte für besonders wichtige Einrichtungen erreichen (§ 28 Abs. 2 Nr. 2 BSIG). Außerdem werden mittlere Unternehmen erfasst, die mindestens 50 Personen beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen. Der Adressatenkreis (der mittleren Unternehmen) wird ebenfalls weiter eingegrenzt, und zwar auf die gerade beschriebenen Einrichtungen der Anlage 1 zum BSIG. Allerdings wird der Kreis dann um weitere Unternehmen einer Anlage 2 zum BSIG erweitert (§ 28 Abs. 2 Nr. 3 BSIG). Diese Anlage erfasst aus den Netzwirtschaften insbesondere die gewerbliche Beförderung von Briefsendungen, Paketen und Warensendungen einschließlich der Anbieter von Kurierdiensten (Anlage 2 Ziff. 1.1.1 BSIG i. V. m. § 3 Nr. 15 PostG). Darüber hinaus werden bestimmte Unternehmen aus den Bereichen Produktion, Herstellung und Handel mit chemischen Stoffen, Lebensmitteln und Waren erfasst (Anlage 2 Ziff. 4 und 5 BSIG). Außerdem sind Anbieter von Online-Marktplätzen, Online-Suchmaschinen und sozialer Medien sowie auch Forschungseinrichtungen einbezogen (Anlage 2 Ziff. 6 und 7 BSIG).

4. Bestimmte Einrichtungsarten für digitale Dienste und digitale Infrastruktur

Eine besondere Gruppe bilden schließlich DNS-Diensteanbieter, TLD-Namenregister, „Domain-Name-Registry"-Dienstleister, Anbieter von Cloud-Computing-Diensten[24], Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste („Managed Service Provider"), Anbieter verwalteter Sicherheitsdienste („Managed Security Service Provider") sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke.[25] Diese Gruppe wird unabhängig von Schwellenwerten erfasst. Soweit die Unternehmen nicht gleichzeitig (besonders) wichtige Einrichtungen sind, gilt für sie aber nur eine (besondere) Registrierungspflicht nach dem BSIG (§ 34 BSIG).[26]

III. Verpflichtungen

Das BSIG erfasst grundsätzlich alle Betreiber wichtiger und besonders wichtiger Einrichtungen (sowie bestimmte Einrichtungsarten für digitale Dienste und digitale Infrastrukturen). Es differenziert dabei nach Verpflichtungen, die *alle* Betreiber treffen, und solchen, die nur von besonders wichtigen oder kritischen Einrichtungen erfüllt werden müssen. Verkompliziert wird die Systematik durch umfangreiche Ausnahmen für die Netzwirtschaften Telekommunikation und Energie (§ 28 Abs. 5 BSIG) (sowie u. a. den Finanzsektor [§ 28 Abs. 6 BSIG[27]]) (hierzu unten, unter 5. und 6.). Diese Netzwirtschaften unterfallen – soweit hier von Interesse – nur den Registrierpflichten (hierzu sogleich, unter 1.) sowie der Untersagungsmöglichkeit für kritische Komponenten (hierzu unten, unter 4. a) bb)). Die Betreiber kritischer Anlagen werden außerdem vom KRITISDachG-RegE erfasst (hierzu unten, unter 4. b)).

1. Allgemeine Verpflichtungen nach dem BSIG (Registrierpflicht)

Betreiber wichtiger und besonders wichtiger Einrichtungen (sowie „Domain-Name-Registry"-Diensteanbieter) müssen sich zunächst beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren und insbesondere Kontaktdaten sowie die öffentlichen Internet-Protokoll-Adressbereiche hinterlegen (§ 33 Abs. 1 BSIG). Das BSI betreibt hierfür zusammen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) ein Registerportal.[28] Registrieren sich Unternehmen nicht selbst, kann dies auch von Amts wegen erfolgen (§ 33 Abs. 3 BSIG). Außerdem kann das BSI Unterlagen anfordern, um im Verdachtsfall zu prüfen, ob Unternehmen ihrer Registrierpflicht genügt haben (§ 33 Abs. 4 BSIG).

Unabhängig von ihrer Qualifikation als wichtige oder besonders wichtige Einrichtung müssen sich auch bestimmte Einrichtungsarten für digitale Dienste und digitale Infrastrukturen registrieren (§ 34 Abs. 1 BSIG). Die entsprechenden Informationen werden vom BSI an die Agentur der Europäischen Union für Cybersicherheit[29] weitergeleitet (§ 34 Abs. 3 BSIG). Diese pflegt ein europäisches Register der entsprechenden Einrichtungen (Art. 27 der NIS-2-Richtlinie [EU] 2022/2555).

2. Verpflichtungen für wichtige (sowie besonders wichtige) Einrichtungen

a) Risikomanagement

Die zentrale Vorschrift für die IT-Sicherheit ist § 30 BSIG. Hiernach sind wichtige und besonders wichtige Einrichtungen verpflichtet, „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen … zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme,[30] Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten" (§ 30 Abs. 1 S. 1 BSIG).[31] Dabei ist eine umfassende Abwägung zwischen Risikoexposition, Größe, Umsetzungskosten und Eintrittswahrscheinlichkeit sowie der Schwere von Sicherheitsfolgen einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen vorzunehmen (§ 30 Abs. 1 S. 2 BSIG).[32]

---

21 Anlage 1 Ziff. 5.1.1, 5.2.1 BSIG.
22 Anlage 1 Ziff. 6.1.2, 6.1.5, 6.1.8, 6.1.9 BSIG.
23 *Kipker/Dittrich*, MMR 2023, 481, 482.
24 Siehe hierzu *Scheibenpflug/Monschke/Hildebrandt*, CR 2024, 712.
25 § 30 Abs. 3, § 60 Abs. 1 BSIG verwenden hier die englischsprachigen Begriffe, anders als etwa Art. 1 der NIS-2-Durchführungsverordnung (EU) 2024/2690.
26 Hierzu unten, unter III. 1.
27 Die Vorschrift erfasst außerdem die Gesellschaft für Telematik und Betreiber von Diensten der Telematikinfrastruktur i. S. d. SGB V.
28 Das Portal ist abrufbar unter https://portal.bsi.bund.de/ (zuletzt abgerufen am 7.1.2026). Das Portal basiert „auf einer Cloud-Infrastruktur von Amazon Web Services" (vgl. BSI, Pressemitteilung „Zweiter Schritt zur NIS-2-Registrierung: BSI-Portal ab sofort freigeschaltet" v. 6.1.2026), was mit Blick auf die digitale Souveränität durchaus kritisch zu bewerten ist.
29 Diese wird in Anknüpfung an ihre vorherige englischsprachige Bezeichnung als European Network and Information Security Agency (Europäische Agentur für Netz- und Informationssicherheit) nach wie vor ENISA abgekürzt.
30 Siehe zum „Begriff des Netz- und Informationssystems i. S. d. NIS-2-RL" *Krysa*, CR 2025, 578.
31 Siehe zum „Risikomanagement" nach der NIS-2-Richtlinie (EU) 2022/2555 auch *Schmidt*, K&R 2023, 705, 707. Siehe zum Entwurf aus der 20. Legislaturperiode *Kipker/Dittrich*, MMR 2023, 481, 483, und *Voigt/Schmalenberger*, CR 2023, 717, 720.
32 Siehe hierzu auch *Döveling/Hempel*, CR 2025, 661, 662.

Die hierfür *mindestens* zu ergreifenden Maßnahmen werden konkretisiert. Hierzu zählen etwa allgemeine Vorgaben, wie die Verpflichtung, ein Konzept zur Risikoanalyse zu erstellen (§ 30 Abs. 2 S. 2 Nr. 1 BSIG), aber auch konkrete Vorgaben zur Verwendung von Multi-Faktor-Authentifizierungen (§ 30 Abs. 2 S. 2 Nr. 10 BSIG). Die Aufzählung ist nicht abschließend. Die einzelnen Maßnahmen sollen den Stand der Technik[33] einhalten (§ 30 Abs. 2 S. 1 BSIG). Das BSIG greift insoweit – wie zahlreiche andere Gesetze – auf einen unbestimmten Rechtsbegriff zurück, der es ermöglicht, aktuelle Entwicklungen zu berücksichtigen. Außerdem müssen die Maßnahmen auf einem „gefahrübergreifenden Ansatz" beruhen.

Die Mindestmaßnahmen, die zwingend erfüllt werden müssen, können durch Durchführungsrechtsakte der Kommission weiter ergänzt werden[34] – bislang (Stand: Dezember 2025) liegt nur die NIS-2-Durchführungsverordnung (EU) 2024/2690 für bestimmte Einrichtungsarten für digitale Dienste und digitale Infrastruktur vor. Die Maßnahmen zum Risikomanagement werden hierin durch einen 20-seitigen Anhang – mitunter sehr detailliert[35] – weiter ausdifferenziert.[36] Ergänzend (bzw. parallel) hierzu wird außerdem das Bundesministerium des Inneren ermächtigt, weitere Konkretisierungen durch eine Verordnung vorzunehmen. Eine solche Verordnung ist bislang (Stand: Dezember 2025) noch nicht erlassen worden.

Durch eine Rechtsverordnung können (besonders) wichtige Einrichtungen zudem verpflichtet werden, „bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur [zu] verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen" (§ 30 Abs. 6 BSIG). Auch eine solche Verordnung ist bislang (Stand: Dezember 2025) nicht erlassen worden.

Wie bereits unter Geltung des alten BSIG (§ 8a Abs. 2 BSIG 2021) können für die Erfüllung der entsprechenden Verpflichtungen branchenspezifische Sicherheitsstandards (B3S) herangezogen werden (§ 30 Abs. 8 und 9 BSIG). Hierfür können – wie bisher – Branchenverbände (allerdings nur von besonders wichtigen Einrichtungen) Vorschläge machen, die dann im Einvernehmen mit den verschiedenen Aufsichtsbehörden vom BSI festgelegt werden.[37]

b) Meldepflichten

Kommt es zu einem erheblichen Sicherheitsvorfall, muss dieser gemeldet werden (§ 32 BSIG).[38] Das BSI und das BBK richten hierzu eine gemeinsame Meldestelle ein (§ 32 Abs. 1 S. 1 BSIG).[39] Meldepflichten nach anderen Vorschriften – etwa nach Art. 33 der Datenschutz-Grundverordnung 2016/679 (DSGVO) – bleiben hiervon unberührt.[40]

Der Begriff des erheblichen Sicherheitsvorfalls ist legaldefiniert als „ein Sicherheitsvorfall, der

a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder
b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann" (§ 2 Nr. 11 BSIG).

Wichtig ist insoweit zunächst, dass ein erheblicher Sicherheitsvorfall nicht erst dann vorliegt, wenn es zu einem Schadereignis gekommen ist. Vielmehr reicht es aus, dass es hierzu hätte kommen *können*.[41] Eine weitere Ausdifferenzierung kann durch Rechtsverordnung (§ 2 Nr. 11 a. E. i. V. m. § 56 Abs. 5 BSIG) oder Durchführungsrechtsakt der Kommission erfolgen. Für bestimmte Einrichtungsarten für digitale Dienste und digitale Infrastruktur liegt bereits die NIS-2-Durchführungsverordnung (EU) 2024/2690 vor. Hiernach ist etwa ein erheblicher Sicherheitsvorfall bei einem DNS-Diensteanbieter gegeben, wenn der Dienst mehr als 30 Minuten lang nicht verfügbar ist (Art. 5 lit. a der NIS-2-Durchführungsverordnung [EU] 2024/2690). In der Durchführungsverordnung wird außerdem – für ihren Anwendungsbereich – konkretisiert, wann ein (potentieller) finanzieller Verlust als erheblich anzusehen ist, nämlich ab 500.000 Euro oder 5 % des jährlichen Gesamtumsatzes (Art. 3 Abs. 1 lit. a der NIS-2-Durchführungsverordnung [EU] 2024/2690). Das dürfte auch als Richtgröße für andere Sektoren ein sinnvoller Wert sein.

Das BSIG sieht mehrere abgestufte Meldungen vor: Eine Erstmeldung hat „unverzüglich", spätestens jedoch binnen 24 Stunden zu erfolgen (§ 32 Abs. 1 Nr. 1 BSIG). Diese Frist ist deutlich kürzer als die Meldepflicht nach (Art. 33 Abs. 1) der DSGVO (72 Stunden), aber länger als die Meldefrist im Finanzsektor (vier Stunden[42]). Die Erstmeldung muss noch keine detaillierten Analysen enthalten. Mitzuteilen ist aber in jedem Fall, ob der Verdacht auf einen Angriff besteht und ob grenzüberschreitende Auswirkungen wahrscheinlich sind (§ 32 Abs. 1 Nr. 1 BSIG).[43]

Nach spätestens 72 Stunden muss die Meldung bestätigt oder aktualisiert werden und es muss eine erste Bewertung durch das Unternehmen erfolgen (§ 32 Abs. 1 Nr. 2 BSIG). Schließlich ist nach spätestens einem Monat eine ausführliche Meldung nebst umfassender Analyse vorgeschrieben (§ 32 Abs. 1 Nr. 4 BSIG). Auf Ersuchen des BSI sind außerdem Zwischenmeldungen abzugeben (§ 32 Abs. 1 Nr. 3 BSIG). Das BSI regelt die weiteren Einzelheiten des Meldeverfahrens (§ 32 Abs. 4 BSIG).

Wenn ein erheblicher Sicherheitsvorfall Auswirkungen auf die Empfänger von Diensten haben kann, kann das BSI anordnen, dass die Empfänger informiert werden müssen (§ 35 Abs. 1 BSIG).[44] Einrichtungen aus den Sektoren Finanz- und Versicherungswesen, digitale Infrastruktur, Verwaltung von Informations- und Kommunikationstechnologie (IKT)-Diensten und digitale Dienste müssen die Empfänger grundsätzlich über Abhilfemaßnahmen informieren (§ 35 Abs. 2 BSIG).

Das BSI kann einem meldenden Unternehmen technische Unterstützung leisten (§ 36 Abs. 1 BSIG). Das BSI kann zudem

33 Vgl. Bundesministerium der Justiz (BMJ), Handbuch der Rechtsförmlichkeit, BAnz 2008 Nr. 160a, Rn. 256, sowie BVerfGE 49, 89, 135 f. (Beschl. v. 8.8.1978 – Az. 2 BvL 8/77).

34 § 30 Abs. 5 BSIG stellt insoweit klar, dass entsprechende unionale Vorgaben ggf. dem BSIG vorgehen.

35 Rein exemplarisch sei hier Ziff. 11.6.2. lit. d im Anhang zur NIS-2-Durchführungsverordnung (EU) 2024/2690 genannt: Hiernach müssen Einrichtungen bei Authentifizierungsverfahren „das Zurücksetzen der Authentifizierungsdaten und die Sperrung von Nutzern nach einer vorab festgelegten Anzahl erfolgloser Anmeldeversuche verlangen".

36 Kritisch hierzu *Döveling/Hempel*, CR 2025, 661, 664 f.: „liest sich die Liste nahezu wie ein IT-sicherheitstechnisches Lehrbuch".

37 Vgl. auch die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/1501, 95, 149.

38 Siehe zu Melde- und Informationspflichten nach der NIS-2-Richtlinie (EU) 2022/2555 auch *Schmidt*, K&R 2023, 705, 707 f. Siehe zum Entwurf aus der 20. Legislaturperiode *Kipker/Dittrich*, MMR 2023, 481, 483 f., und *Voigt/Schmalenberger*, CR 2023, 717, 720.

39 Siehe Fn. 28.

40 Siehe auch für die Parallelfrage nach § 18 KRITISDachG-RegE die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 64. Siehe außerdem *Hardt/Stummer*, DuD 2025, 720, 724.

41 Siehe auch *Hardt/Stummer*, DuD 2025, 720, 721.

42 Art. 6 des Joint Technical Standards on major incident reporting, abrufbar unter https://www.eba.europa.eu/sites/default/files/2024-07/6d341d14-0c54-44ff-a849-21561baee157/JC%202024-33%20-%20Final%20report%20on%20the%20draft%20RTS%20and%20ITS%20on%20incident%20reporting.pdf (zuletzt abgerufen am 7.1.2026).

43 Siehe auch Erwägungsgrund 102 der NIS-2-Richtlinie (EU) 2022/2555 sowie *Hardt/Stummer*, DuD 2025, 720, 722.

44 Hierzu auch die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/1501, 95, 152.

Unternehmen verpflichten, die Öffentlichkeit zu informieren, oder eine Information selbst vornehmen (§ 36 Abs. 2 BSIG).

c) Besondere Verpflichtungen für die Geschäftsleitung
Verantwortlich für die Umsetzung der Risikomanagementmaßnahmen sind die Geschäftsleitungen[45] der (besonders) wichtigen Einrichtungen (§ 38 Abs. 1 BSIG). Verletzen die Geschäftsleitungen ihre Pflichten schuldhaft, so haften sie gegenüber ihren Einrichtungen (§ 38 Abs. 2 BSIG).[46] Damit die Geschäftsleitungen auch tatsächlich in der Lage sind, beurteilen zu können, welche Maßnahmen erforderlich sind, und um kontrollieren zu können, ob diese umgesetzt wurden, müssen sie regelmäßig[47] an entsprechenden Schulungen teilnehmen (§ 38 Abs. 3 BSIG).[48]

3. Sonderregelungen für besonders wichtige Einrichtungen

Besonders wichtige Einrichtungen müssen über die beschriebenen Maßnahmen hinaus weitere Anforderungen erfüllen. So kann das BSI gegenüber besonders wichtigen Einrichtungen anordnen, dass die Pflichten zum Risikomanagement[49] durch Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen nachgewiesen werden müssen (§ 61 Abs. 1 BSIG). Die entsprechenden Unternehmen können zudem verpflichtet werden, gegenüber dem BSI Nachweise zur Erfüllung dieser Pflichten – einschließlich aufgedeckter Sicherheitsmängel – zu erbringen (§ 61 Abs. 3 BSIG). Das BSI kann zudem selbst die Einhaltung der Verpflichtungen überprüfen (§ 61 Abs. 5 BSIG). Außerdem kann es ggf. Maßnahmen gegenüber den Unternehmen anordnen (§ 61 Abs. 6 ff. BSIG). Gegenüber (nur) wichtigen Einrichtungen sind Aufsichts- oder Durchsetzungsmaßnahmen lediglich im begründeten Einzelfall zulässig (§ 62 BSIG).[50]

4. Sonderregelungen für kritische Einrichtungen

Für kritische Einrichtungen – als Untergruppe der besonders wichtigen Einrichtungen – enthält das BSIG weitere Sonderregelungen (hierzu sogleich, unter a)). Die entsprechenden Unternehmen fallen zudem in den Anwendungsbereich des KRITISDachG-RegE (hierzu unten, unter b)).

a) Sonderregelungen nach dem BSIG

aa) Erweiterte Verpflichtungen
Das BSIG verschärft zahlreiche Regelungen in Bezug auf kritische Einrichtungen. Diese müssen mit Blick auf Risikomanagementmaßnahmen für kritische Anlagen erweiterte Anstrengungen unternehmen. Das Gesetz modifiziert hierzu den Verhältnismäßigkeitsmaßstab. Maßnahmen sind hiernach solange verhältnismäßig, wie sie nicht außer Verhältnis zu den „Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steh[en]“ (§ 31 Abs. 1 BSIG). Die Unternehmen müssen zudem Systeme zur Angriffserkennung einsetzen (§ 31 Abs. 2 BSIG).[51] Die Unternehmen treffen außerdem erweiterte Registrierungspflichten (§ 33 Abs. 2 BSIG) und erweiterte Meldepflichten bei einem erheblichen Sicherheitsvorfall (§ 30 Abs. 3 BSIG). Die Erfüllung der Risikomanagementmaßnahmen muss alle drei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen gegenüber dem BSI nachgewiesen werden (§ 39 Abs. 1 BSIG). Das BSI kann hierfür weitere Vorgaben machen (§ 39 Abs. 2 BSIG).

bb) Untersagung des Einsatzes kritischer Komponenten
Bislang mussten Betreiber kritischer Einrichtungen den Einsatz kritischer Komponenten vorab dem Bundesministerium des Inneren melden (§ 9b BSIG 2021). Diese Anzeigepflicht ist nun entfallen.[52] Ebenfalls entfallen ist die Verpflichtung, für kritische Komponenten eine Garantieerklärung einzuholen (bislang § 9b Abs. 3 BSIG 2021).[53] Allerdings kann das Ministerium weiterhin den Einsatz kritischer Komponenten untersagen, wenn deren Einsatz die öffentliche Ordnung oder Sicherheit voraussichtlich beeinträchtigt (§ 41 Abs. 1 BSIG). Das Ministerium orientiert sich bei der Prüfung (beispielhaft) daran, ob der Hersteller von der Regierung eines Drittstaats kontrolliert wird (§ 41 Abs. 4 Nr. 1 BSIG). Die Unternehmen sind bei der Prüfung zur Mitwirkung verpflichtet (§ 41 Abs. 5 BSIG).

b) KRITISDachG-RegE
Während die NIS-2-Richtlinie (EU) 2022/2555 sowie das BSIG Risiken mit Blick auf die Netz- und IT-Infrastruktur adressieren, verfolgen die CER-Richtlinie (EU) 2022/2557 und das diese Richtlinie umsetzende (künftige) KRITISDachG einen Allgefahrenansatz.

aa) Geltungsbereich
Adressaten des KRITISDachG-RegE sind nur die Betreiber kritischer Anlagen (§ 4 Abs. 1 KRITISDachG-RegE).[54] Die Sektoren sind insoweit identisch mit denen des BSIG.[55] Die Kommission hat inzwischen durch die delegierte Verordnung (EU) 2023/2450 die einzelnen Teilsektoren spezifiziert – etwa Elektrizitätsunternehmen, Eisenbahnunternehmen, Betreiber von Internetknoten und Anbieter elektronischer Kommunikationsdienste (Art. 2 Nr. 1 lit. a i), Nr. 2 lit. b i), Nr. 8 i) und viii) der delegierten Verordnung). Eine weitere Eingrenzung erfolgt über eine Rechtsverordnung des Bundesministeriums des Inneren (§ 4 Abs. 3[56] und § 5 Abs. 1 KRITISDachG-RegE). Diese Rechtsverordnung regelt Schwellenwerte, die – wie die BSI-KritisV – grundsätzlich auf 500 000 versorgte Einwohner bezogen sind (§ 5 Abs. 2 a. E. KRITISDachG-RegE).[57] Die Begründung zum Regierungsentwurf stellt diesbezüglich eine gemeinsame – oder jedenfalls vergleichbare – Verordnung nach dem BSIG und dem KRITISDachG-RegE in Aussicht.[58]

---

45 „Geschäftsleitung“ ist nach § 2 Nr. 13 BSIG „eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist; Leiterinnen und Leiter von Einrichtungen der Bundesverwaltung nach § 29 gelten nicht als Geschäftsleitung“. Siehe auch *Teichmann*, CR 2025, 718, 720.

46 Siehe hierzu auch *Grosmann/Gerecke/Aschenbrenner*, CR 2024, 665; *Kipker/Dittrich*, MMR 2023, 481, 485.

47 Die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/1501, 95, 154, hält Schulungen, die „alle 3 Jahre angeboten werden“, für „regelmäßig“. Dabei ist (a. a. O., S. 113) von einer vierstündigen Dauer auszugehen. Siehe auch *Teichmann*, CR 2025, 718, 720 ff.

48 Das BSI hat eine „Vorläufige Handreichung für die Empfehlung zur Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen nach dem NIS-2-Umsetzungsgesetzentwurf“ veröffentlicht, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-geschaeftsleitungsschulung.pdf?__blob=publicationFilev=3 (zuletzt abgerufen am 7.1.2026).

49 Nach § 30 BSIG, siehe hierzu oben unter 2. a).

50 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/1501, 95, 172.

51 Siehe zu § 8a Abs. 1a BSIG 2021 *Kohpeiß/Schaller*, CR 2023, 589.

52 Bericht des Innenausschusses, BT-Drs. 21/2782, 18, 22 f.

53 Bericht des Innenausschusses, BT-Drs. 21/2782, 18, 22.

54 Siehe zum Anwendungsbereich der CER-Richtlinie (EU) 2022/2557 *Hornung/Muttach/Schaller*, CR 2024, 229, 231 f.

55 Vgl. oben, unter II. 1. b). § 6 Abs. 1 KRITISDachG-RegE stellt allerdings klar, dass auch sonstige Einrichtungen – genannt werden ausdrücklich „Betreuungsangebote“ für Kinder – kritisch sein können und Regelungen für diese nicht durch das KRITISDachG-RegE gesperrt sind. Siehe auch die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 49 f. Die besondere Bedeutung der Kindestagesbetreuung für „die Funktionsfähigkeit der Wirtschaft“, aber auch „das Wohl der betreuten Kinder und ihrer Familien“ betont die Bundesregierung im Weiteren, etwa a. a. O., S. 56. Hier sieht der Bund die Länder in der Pflicht, für entsprechende§ Betreuungsangebote zu sorgen.

56 Im Einvernehmen mit elf weiteren Ministerien.

57 Der Schwellenwert ist im Bundesrat auf Kritik gestoßen, der eine Herabsetzung auf 150 000 fordert, siehe die Stellungnahme des Bundesrates, BR-Drs. 558/25 (Beschluss), 1, 15.

58 Die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, ist hier nicht ganz klar: In der Einleitung (a. a. O., S. 32) ist von einer „gemeinsame[n] Rechtsverordnung“ die Rede; an

Zudem können Anlagen abweichend hiervon als kritisch oder unkritisch qualifiziert werden (§ 5 Abs. 5 KRITISDachG-RegE).

Ähnlich der Regelungstechnik des BSIG wird der Telekommunikationssektor zunächst vom Gesetz erfasst. Es werden sodann aber wesentliche Teile wieder aus dem Geltungsbereich ausgenommen.[59] Anders als nach dem BSIG gibt es jedoch keine vergleichbare Ausnahme für den Energiesektor (wohl aber für den Finanz-, Abfall- und Sozialversicherungssektor, siehe § 4 Abs. 2 Nr. 1, 3 und 4 KRITISDachG-RegE).[60]

Der KRITISDachG-RegE differenziert grundsätzlich zwischen „normalen" kritischen Einrichtungen und „kritischen Einrichtungen von besonderer Bedeutung für Europa". Letzteres sind Betreiber, die – weiter eingegrenzte – kritische Dienstleistungen in mindestens sechs EU-Mitgliedstaaten erbringen (§ 9 Abs. 1 KRITISDachG-RegE). Die betroffenen Unternehmen können dann eine spezielle Unterstützung durch Sachverständige und Vertreter der Kommission im Rahmen einer „Beratungsmission" erhalten.[61] Allerdings erfolgt eine solche Beratungsmission nur auf Antrag des Bundesministeriums des Inneren, nicht etwa des betroffenen Unternehmens (§ 10 Abs. 1 KRITISDachG-RegE). Das betroffene Unternehmen ist aber umfassend zur Kooperation verpflichtet (§ 10 Abs. 2, 3, 5 KRITISDachG-RegE).

bb) Verpflichtungen nach dem KRITISDachG-RegE

Die Verpflichtungen nach dem KRITISDachG-RegE entsprechen in ihrer Struktur denen des BSIG.[62]

Die Unternehmen müssen ihre kritischen Anlagen zunächst registrieren (§ 8 KRITISDachGReg-E[63]).[64] Sie müssen außerdem Maßnahmen zum Risikomanagement ergreifen. Der KRITISDachG-RegE sieht hierfür ein zweistufiges Verfahren vor. In einem ersten Schritt erfolgt (in einem vierjährigen Intervall) eine umfassende Risikoanalyse und Risikobewertung durch die Betreiber (§ 12 KRITISDachG-RegE). Grundlage hierfür ist eine (vom Bundesministerium des Inneren koordinierte) nationale Risikoanalyse und Risikobewertung auf Ministerialebene (§ 11 KRITISDachG-RegE).

Auf der Grundlage der Risikoanalyse und Risikobewertung müssen „Resilienzpflichten" erfüllt werden (§ 13 KRITISDachG-RegE). Diese Pflichten sind deutlich breiter ausgelegt als die nach dem BSIG. So müssen – beispielhaft – Extremereignisse durch Unfälle, Naturgefahren oder gesundheitliche Notlagen, feindliche Bedrohungen, einschließlich terroristischer Straftaten, sowie Risiken, die sich durch Abhängigkeiten von anderen Betreibern kritischer Anlagen auch in Drittstaaten ergeben können, berücksichtigt werden (§ 12 Abs. 1 Nr. 1 [i. V. m. § 11 Abs. 2 Nr. 1], Nr. 2 KRITISDachG-RegE). Die hierfür zu treffenden Maßnahmen werden lediglich beispielhaft im Gesetz angerissen – etwa Zugangskontrollen oder ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeitenden[65] (§ 13 Abs. 3 Nr. 2 lit. d und Nr. 5 KRITISDachG-RegE). Eine weitere Ausgestaltung kann durch Rechtsverordnungen verschiedener (Bundes- und Landes-) Ministerien erfolgen (§ 14 Abs. 1, 3, 4 KRITISDachG-RegE). Außerdem können – in offensichtlicher Anlehnung an die B3S nach dem BSIG – branchenspezifische Resilienzstandards herangezogen werden (§ 14 Abs. 2 KRITISDachG-RegE).[66] Weiter verkompliziert wird das Ganze durch Durchführungsrechtsakte der Kommission, die ebenfalls technische und methodische Spezifikationen erlassen kann, denen dann Vorrang zukommt.[67]

Die Maßnahmen müssen in einem „Resilienzplan" dargestellt werden (§ 13 Abs. 4 KRITISDachG-RegE). Hierfür werden den Betreibern Vorlagen und Muster zur Verfügung gestellt (§ 13 Abs. 5 KRITISDachG-RegE).

Die ergriffenen Resilienzmaßnahmen müssen auf Ersuchen des BBK nachgewiesen werden (§ 16 KRITISDachG-RegE[68]). Werden bei der Überprüfung Mängel festgestellt, können Maßnahmen zur Beseitigung und Fristen hierfür angeordnet werden (§ 16 Abs. 6 KRITISDachG-RegE).

Schließlich besteht auch nach dem KRITISDachG-RegE eine Meldepflicht für Vorfälle (§ 18 KRITISDachG-RegE). Das Gesetz versteht dabei unter einem „Vorfall" (im Wesentlichen) „ein Ereignis, das die Erbringung einer kritischen Dienstleistung erheblich beeinträchtigt oder beeinträchtigen könnte" (§ 2 Nr. 9 KRITISDachG-RegE).[69] Für die Bestimmung der Erheblichkeit ist u. a. auf die Zahl der betroffenen Nutzer, die Dauer der Störung und das betroffene geographische Gebiet abzustellen.[70] Das BBK gestaltet das Verfahren weiter aus.

Verantwortlich für die Umsetzung und Überwachung sind – wie im Geltungsbereich des BSIG – die Geschäftsleitungen, die ggf. auch persönlich für schuldhaft verursachte Schäden haften (§ 20 KRITISDachG-RegE). Allerdings sieht der KRITISDachG-RegE keine speziellen Schulungspflichten für die Geschäftsleitungen vor.

5. Sonderregelungen für den Telekommunikationssektor

a) KRITISDachG-RegE und BSIG

Wie oben (unter 4. b) aa)) erwähnt, gilt das KRITISDachG-RegE in weiten Bereichen nicht für den Telekommunikationssektor.

Das BSIG enthält zunächst zahlreiche Sonderregelungen für Telekommunikationsunternehmen und differenziert hier detailliert zwischen wichtigen, besonders wichtigen und kritischen Einrichtungen. Im Anschluss werden dann aber weite

---

späterer Stelle (a. a. O., S. 45) heißt es, die Verordnung nach dem KRITISDachG solle sich „systematisch" an der BSI-KritisV „orientiere[n]" bzw. (a. a. O., S. 48) ein „ähnliches Verfahren" vorsehen.

59 Nach § 4 Abs. 2 Nr. 2 KRITISDachG-RegE gelten der „§ 3 Absatz 8, die §§ 9, 10, 12 bis 16, 18, 19 Absatz 2 sowie die §§ 20, 21 Absatz 6" nicht für „Betreiber kritischer Anlagen im Sektor Informationstechnik und Telekommunikation". Eine entsprechende Ausnahme ist bereits in Art. 8 i. V. m. Nr. 8 der Tabelle im Anhang der CER-Richtlinie (EU) 2022/2557 vorgesehen. Die Erwägungsgründe 9, 20 der CER-Richtlinie (EU) 2022/2557 gehen davon aus, dass insoweit die Regelungen nach der NIS-2-Richtlinie (EU) 2022/2555 ausreichend sind. Das ist durchaus zweifelhaft, wenn man in Rechnung stellt, dass die NIS-2-Richtlinie (EU) 2022/2555 klar auf die Netzwerk- und Informationssicherheit fokussiert ist, während der Ansatz der CER-Richtlinie (EU) 2022/2557 deutlich umfassender ist (und beispielsweise ausdrücklich den Klimawandel adressiert).

60 Siehe hierzu auch die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 45.

61 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 54 f.

62 Siehe zum Entwurf aus der 20. Legislaturperiode *Voigt/Schmalenberger*, CR 2023, 717, 722. Siehe zur CER-Richtlinie (EU) 2022/2557 *Hornung/Muttach/Schaller*, CR 2024, 229, 232 f.

63 Art. 6 Abs. 4 der CER-Richtlinie (EU) 2022/2557 sieht vor, dass die Mitgliedstaaten die kritischen Einrichtungen ermitteln und diesen ihre Einstufung als kritische Einrichtung mitteilen. Allerdings schließt die Richtlinie auch nicht aus, dass die Mitgliedstaaten zur Ermittlung der kritischen Anlagen deren Betreiber verpflichten, eine Eigenmeldung vorzunehmen. In § 8 Abs. 5 KRITISDachG-RegE ist eine Mitteilung an die Betreiber nach erfolgter Registrierung vorgesehen.

64 Die Registrierung kann zusammen mit der Registrierung nach § 33 BSIG erfolgen, vgl. die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 52.

65 Der KRITISDachG-RegE verwendet die geschlechterneutrale Form „Mitarbeitende", während das BSIG nur „Mitarbeiter" kennt.

66 Siehe auch die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 60.

67 Das wird – deklaratorisch – durch § 15 KRITISDachG-RegE noch einmal ausdrücklich klargestellt.

68 Die Vorschrift sieht eine Kooperation zwischen BSI und BBK vor. Das BSI legt auf Ersuchen des BBK die Informationen vor, die es nach § 39 BSIG erhalten hat. Siehe auch die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 61.

69 Ausgenommen sind Sicherheitsvorfälle nach § 2 Nr. 40 BSIG.

70 Vgl. Art. 15 Abs. 1 der CER-Richtlinie (EU) 2022/2557; hierauf weist auch die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 42, hin.

Teile des BSIG für wichtige und besonders wichtige Telekommunikationsunternehmen ausgenommen.[71] Grundsätzlich anwendbar bleiben – soweit hier relevant – nur die Registrierungspflicht (§§ 33, 34 BSIG) sowie die Untersagungsmöglichkeit für den Einsatz kritischer Komponenten (§ 41 BSIG). Grund hierfür ist, dass die übrigen Verpflichtungen spezialgesetzlich im TKG geregelt sind.[72]

Allerdings gibt es im BSIG – und zwar nicht im dritten Teil über die „Sicherheit in der Informationstechnik der Einrichtungen", sondern in Teil 2 Kapitel 1 über „Aufgaben und Befugnisse" des BSI – eine Sonderregelung für „Anbieter von Telekommunikationsdiensten" (§ 16 BSIG).[73] Hiernach kann das BSI gegenüber solchen Unternehmen zur „Abwehr erheblicher Gefahren" u. a. anordnen, Telekommunikationsdienste einzuschränken, umzuleiten oder „Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme [zu] verteil[en]" (§ 16 Abs. 1 BSIG[74]). Eine vergleichbare Ermächtigung besteht im Übrigen gegenüber den Anbietern von digitalen Diensten (§ 17 BSIG[75]).

b) TKG

Das TKG erfasst – soweit hier relevant – zunächst alle Telekommunikationsunternehmen unabhängig von ihrer Größe oder der Erreichung von Schwellenwerten. Allerdings differenziert das TKG hinsichtlich einzelner Verpflichtungen zwischen Telekommunikationsanbietern mit erhöhtem Gefährdungspotential und sonstigen Unternehmen. Die Zuordnung erfolgt durch die Bundesnetzagentur (§ 167 Abs. 1 Nr. 3 TKG).[76] Telekommunikationsanbieter mit erhöhtem Gefährdungspotential müssen etwa Systeme zur Angriffserkennung betreiben (§ 165 Abs. 3 TKG). Kritische Komponenten dürfen solche Unternehmen nur einsetzen, wenn sie von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden (§ 165 Abs. 4 TKG).

Meldungen über erhebliche Sicherheitsvorfälle müssen an das BSI und die Bundesnetzagentur erfolgen (§ 168 TKG). Anders als nach dem BSIG müssen Telekommunikationsunternehmen grundsätzlich die von einer „Gefahr potenziell betroffenen Nutzer über alle möglichen Schutz- oder Abhilfemaßnahmen" informieren (§ 168 Abs. 7 TKG).

Eine weitere Besonderheit des Telekommunikationsrechts ist, dass Telekommunikationsunternehmen einen Sicherheitsbeauftragten bestellen müssen (§ 166 TKG). Zudem wird die Bundesnetzagentur ermächtigt, einen Katalog von Sicherheitsanforderungen zu erlassen (§ 167 TKG). Anders als die branchenspezifischen Sicherheitsstandards nach dem BSIG ist dieser Katalog von Sicherheitsanforderungen verpflichtend umzusetzen. Die Bundesnetzagentur kann in diesem Katalog u. a. festlegen, welche Funktionen als kritisch anzusehen sind (§ 167 Abs. 1 S. 2 TKG). Diese Befugnis geht zukünftig (zusammen mit einer allgemeinen entsprechenden Ermächtigung) auf das Bundesministerium des Inneren über (§ 167 Abs. 2 TKG i. V. m. § 56 Abs. 7 BSIG). Im Übrigen verbleibt die Befugnis zum Erlass eines Katalogs von Sicherheitsanforderungen bei der Bundesnetzagentur.

c) Katalog von Sicherheitsanforderungen

Die Bundesnetzagentur hat dementsprechend kürzlich eine Konsultation für einen überarbeiteten Katalog – die letzte Version stammt aus dem Jahr 2020 – eingeleitet.[77]

Der dabei im Entwurf vorgelegte Katalog[78] unterscheidet drei Gruppen von Telekommunikationsunternehmen:

- Telekommunikationsunternehmen mit hoher Bedeutung für das Gemeinwohl,
- Telekommunikationsunternehmen mit Bedeutung für das Gemeinwohl und
- sonstige Telekommunikationsunternehmen.

Er knüpft dabei – wie § 28 Abs. 1 und 2 BSIG – an die Unternehmensgröße an. In die Gruppe mit den höchsten Anforderungen fallen Unternehmen mit mindestens 50 Mitarbeitern oder mehr als 10 Millionen Euro Jahresumsatz oder -bilanzsumme. In der mittleren Gruppe sind es weniger als 50 Mitarbeiter und maximal 10 Millionen Euro und in der niedrigsten Gruppe weniger als 10 Mitarbeiter und maximal 2 Millionen Euro. Betreiber von Mobilfunknetzen der 5. Generation werden pauschal der höchsten Gruppe zugeordnet.

Der Katalogsentwurf erfasst zunächst verschiedene Aspekte der Unternehmensführung – etwa in Ziff. 4.1 den Schutz des Fernmeldegeheimnisses und personenbezogener Daten oder in Ziff. 4.10 das Bewusstsein für Bedrohungen („Threat Awareness"). Ein weiteres Kapitel enthält zusätzliche Anforderungen für 5G-Netze – etwa hinsichtlich der Bestimmung von kritischen Komponenten (Ziff. 5.1) oder (technischer) Diversität (Ziff. 5.4). Innerhalb der einzelnen Abschnitte werden zunächst die Maßnahmen aufgeführt, die alle Unternehmen zu ergreifen haben, es folgen dann solche, die außerdem von Telekommunikationsunternehmen mit einfacher und hoher Bedeutung für das Gemeinwohl umgesetzt werden müssen, und schließlich werden Anforderungen aufgelistet, die nur von Unternehmen mit hoher Bedeutung für das Gemeinwohl erfüllt werden müssen. Beispielsweise müssen alle Telekommunikationsunternehmen Schutzmaßnahmen treffen, indem sie Server gegen Missbrauch absichern.[79] Unternehmen mit einfacher und hoher Bedeutung für das Gemeinwohl müssen zusätzlich regelmäßige Kontrollen der Softwareintegrität durchführen.[80] Unternehmen mit hoher Bedeutung für das Gemeinwohl müssen außerdem Software-Patching-Verfahren anwenden, um sicherzustellen, dass Softwareprodukte oder -komponenten nicht verändert wurden.[81]

---

71 § 28 Abs. 5 S. 1 BSIG erklärt die §§ 30, 31, 32, 35, 36, 38, 39, 61 und 62 BSIG für unanwendbar. Hiervon macht dann § 28 Abs. 5 S. 2 BSIG eine Rückausnahme, vgl. hierzu die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/1501, 95, 145.

72 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/1501, 95, 145. § 165 Abs. 2, 2a TKG entsprechen etwa § 30 BSIG, § 165 Abs. 2c TKG entspricht § 38 Abs. 2 BSIG und § 165 Abs. 2d TKG entspricht § 38 Abs. 3 BSIG.

73 Im Gesetzentwurf der Bundesregierung war noch eine Beschränkung auf Anbieter mit mehr als 100 000 Kunden vorgesehen, siehe den Gesetzentwurf der Bundesregierung, BT-Drs. 21/1501, 9, 30. Die Beschlussempfehlung hat diese Beschränkung gestrichen, um sicherzustellen, dass auch die Kunden kleinerer Telekommunikationsanbieter geschützt werden können, siehe den Bericht des Innenausschusses, BT-Drs. 21/2782, 18, 21.

74 Die Vorschrift führt § 7c BSIG 2021 fort, siehe die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 142. § 16 Abs. 2 BSIG sieht zukünftig auch eine Selbstvornahme durch das BSI vor, vgl. den Bericht des Innenausschusses, BT-Drs. 21/2782, 21.

75 Die Vorschrift führt § 7d BSIG 2021 fort, siehe die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510, 32, 143.

76 Nach Ziff. 3 der Allgemeinverfügung Nr. 63/2021, ABl. BNetzA 2021, 905, werden als Betreiber mit erhöhtem Gefährdungspotential die „Betreiber öffentlicher Telekommunikationsnetze des Mobilfunks der 5. Generation mit Frequenzzuteilungen" festgelegt.

77 Die Informationsseite der Bundesnetzagentur über die „Konsultation zur Überarbeitung des Kataloges von Sicherheitsanforderungen" ist abrufbar unter https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/Konsultation/start.html (zuletzt abgerufen am 7.1.2026).

78 Bundesnetzagentur, Katalog von Sicherheitsanforderungen (Entwurfsfassung), 10/2025, abrufbar unter https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/Konsultation/EntwurfKatalog.pdf?__blob=publicationFilev=4 (zuletzt abgerufen am 7.1.2026).

79 Bundesnetzagentur (Fn. 78), Ziff. 4.4.4 lit. a tir. 3.

80 Bundesnetzagentur (Fn. 78), Ziff. 4.4.4 lit. b tir. 2.

81 Bundesnetzagentur (Fn. 78), Ziff. 4.4.4 lit. c tir. 3.

6. Sonderregelungen für den Energiesektor

a) Netz- und Informationssicherheit

Die Regelungstechnik für den Energiesektor entspricht im Anwendungsbereich der NIS-2-Richtlinie (EU) 2022/2555 der im Telekommunikationssektor: Die Betreiber von (wichtigen und besonders wichtigen) Energieversorgungsnetzen, Energieanlagen oder digitalen Energiediensten werden zunächst vom BSIG erfasst (§ 28 Abs. 1 und 2 BSIG). Dann wird die Geltung des Gesetzes in weiten Teilen wieder zurückgenommen.[82] Schließlich werden die Regeln des BSIG im EnWG nachgebildet.[83] Die Regelungstechnik gleicht mitunter einem Verweisungsparcours: So erfassen § 28 Abs. 1 und 2 BSIG zunächst Energieversorgungsnetze, § 28 Abs. 5 BSIG nimmt dann die Unternehmen von der Geltung (u. a.) der §§ 32 und 36 BSIG aus. § 5d Abs. 3 EnWG bildet schließlich § 32 Abs. 1 BSIG nahezu wörtlich nach und erklärt im Übrigen § 32 Abs. 2 bis 5 und § 36 BSIG für entsprechend anwendbar. Hier wäre eine einfachere Regelungstechnik möglich gewesen.

Eine Besonderheit des Energiesektors – den dieser allerdings mit dem Telekommunikationssektor teilt – ist ein verbindlicher IT-Sicherheitskatalog (§ 5c Abs. 2 EnWG).[84] Anders als im Telekommunikationssektor macht das Gesetz für dessen Inhalt sehr konkrete Vorgaben (§ 5c Abs. 3 EnWG).[85] Bislang hat das EnWG hinsichtlich der IT-Sicherheitskataloge zwischen Betreibern, die der kritischen Infrastruktur zugeordnet werden, und sonstigen Betreibern differenziert (§ 11 Abs. 1a und 1b EnWG). Diese Differenzierung wird aufgegeben.[86] Der IT-Sicherheitskatalog muss alle zwei Jahre überprüft und bei Bedarf aktualisiert werden (§ 5c Abs. 2 S. 6 EnWG). Bedenkt man, dass der „aktuelle" Sicherheitskatalog Ende 2025 auf dem Stand von August 2015 war, erscheint das eine naheliegende Anforderung für die Zukunft.

Die Bundesnetzagentur hat im Mai 2025 Eckpunkte für zwei neue IT-Sicherheitskataloge nach dem alten § 11 Abs. 1a und 1b EnWG zur Konsultation gestellt.[87] Diese Eckpunkte haben sich mit der Umsetzung der NIS-2-Richtlinie (EU) 2022/2555 überschnitten und berücksichtigen dementsprechend auch nicht die Vorgaben des § 5c Abs. 3 EnWG. Die Eckpunkte verdeutlichen allerdings, dass sich die Bundesnetzagentur auch zukünftig an Normen der Internationalen Organisation für Normung (International Organization for Standardization, ISO) und der Internationalen Elektrotechnischen Kommission (International Electrotechnical Commission, IEC) – und zwar „in ihrer aktuellen englischsprachigen Fassung"[88] – orientieren will.[89] Basis soll dabei (weiterhin) die ISO/IEC 27001 sein. Auch bislang wird auf diese Norm – ebenfalls „in der jeweils geltenden Fassung" – verwiesen.[90] Diese Regelungstechnik ist nicht unproblematisch: Es werden nämlich dynamisch – noch dazu fremdsprachige – (technische) Normen von Gesetzes wegen zur verbindlichen Pflichtenkonkretisierung herangezogen, auf deren Entstehung der deutsche Gesetzgeber – noch dazu vermittelt durch die Ermächtigung einer Bundesoberbehörde – allenfalls einen höchst mittelbaren Einfluss hat.[91]

Schließlich bestehen – auch bislang schon – zusätzliche Meldepflichten bei Versorgungsstörungen. Betreiber von Energieversorgungsnetzen müssen die Bundesnetzagentur bei Störungen für lebenswichtige Bedarfe unverzüglich unterrichten (§ 13 Abs. 8 und § 52 S. 6 EnWG).[92]

b) Resilienz kritischer Anlagen

Während der Telekommunikationssektor weitgehend aus der Umsetzung im KRITISDachG-RegE ausgenommen wird,[93] werden die Vorschriften des KRITISDachG-RegE durch weitere Vorgaben im EnWG für den Energiesektor ergänzt.[94]

Eine wesentliche Besonderheit ist dabei, dass die Bundesnetzagentur – neben dem BBK – auch für die Überwachung der Resilienzmaßnahmen zuständig ist (§ 5f Abs. 1 EnWG-RegE). Außerdem kann die Bundesnetzagentur einen „Sicherheitskatalog für die physische Resilienz" erlassen (§ 5f Abs. 2 EnWG-RegE).

IV. Aufsicht und Bußgelder

Zuständige Behörde für die Aufsicht ist im Bereich des BSIG (§ 3 BSIG) grundsätzlich das BSI. Der KRITISDachG-RegE verteilt die Zuständigkeiten auf verschiedene Behörden – u. a. die Bundesnetzagentur, das BSI sowie das Eisenbahn-Bundesamt (§ 3 Abs. 1 KRITISDachG-RegE). Weitere Zuständigkeiten können durch Rechtsverordnung geregelt werden (§ 3 Abs. 3 KRITISDachG-RegE). Für die Durchführung des Gesetzes ist zudem in zahlreichen Vorschriften das BBK verantwortlich.[95]

Verstöße gegen das BSIG sowie das künftige KRITISDachG sind bußgeldbewehrt (bzw. werden es sein). Das BSIG sieht hierbei – in Umsetzung von Art. 34 der NIS-2-Richtlinie (EU) 2022/2555 – Bußgelder bis zu zehn Millionen Euro oder 2 % des weltweiten Jahresgesamtumsatzes vor (§ 65 BSIG). Betrachtet man die Auswirkungen, die Verstöße gegen Sicherungspflichten für das Gemeinwohl haben können, so ist dieser Betrag – insbesondere zu den 4 % des Jahresumsatzes, welche die DSGVO vorsieht (Art. 83 Abs. 5 und 6 DSGVO) – kaum zu hoch gegriffen. Erstaunlich ist demgegenüber der Bußgeldrahmen des KRITISDachG-RegE, welcher bis maximal 500.000 Euro reicht (§ 24 KRITISDachG-RegE). Diese Differenz ist im Vergleich zum BSIG allenfalls dadurch erklärbar, dass die NIS-2-Richtlinie (EU) 2022/2555 Vorgaben zur Höhe

82 In § 28 Abs. 5 Nr. 2 BSIG hinsichtlich der §§ 30, 31, 32, 35, 36, 38, 39, 61 und 62 BSIG.

83 § 5d Abs. 3 EnWG entspricht etwa § 32 Abs. 1 BSIG und § 5e EnWG entspricht § 38 BSIG. Siehe zum Entwurf des § 5c EnWG *Appelt/Enzmann/Selzer*, DuD 2025, 379.

84 Das Gesetz sieht den Erlass eines IT-Sicherheitskatalogs vor, die Bundesnetzagentur kann aber auch gesonderte IT-Sicherheitskataloge erlassen (§ 5c Abs. 2 S. 2 EnWG).

85 Die Vorgaben entsprechen § 30 Abs. 2 BSIG. Vgl. insoweit auch die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/1501, 95, 181. Während in den übrigen Sektoren (mit einer gewissen Ausnahme für Telekommunikation) die konkrete Umsetzung den Unternehmen überlassen wird, können im Energiesektor verbindliche Vorgaben hierfür gemacht werden.

86 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 21/1501, 95, 181. Der Anwendungsbereich des „allgemeinen" IT-Sicherheitskatalogs wird damit erweitert. Dem soll durch Übergangsfristen Rechnung getragen werden.

87 Bundesnetzagentur, Festlegungsverfahren „Erstellung eines IT-Sicherheitskatalogs nach § 11 Abs. 1a und 1b EnWG" – Az. 4.12.10.01.

88 Siehe etwa Bundesnetzagentur, Eckpunkte zur Festlegung zum Az. 4.12.10.01, Zeile 229.

89 In den Vorbemerkungen des Konsultationsdokuments heißt es bereits: „Ziel ist es, die Kataloge einander anzunähern und die Kataloge noch enger an den prozessorientierten Managementsystemansatz der ISO/IEC 27001 anzulehnen".

90 Etwa Bundesnetzagentur, IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, 8/2015, E. I. (S. 8): „Dementsprechend haben Netzbetreiber ein ISMS zu implementieren, das den Anforderungen der DIN ISO/IEC 27001 in der jeweils geltenden Fassung genügt".

91 Aus gutem Grund verweist etwa § 5 Abs. 1 BEMFV auf eine konkrete Fassung – nämlich „Ausgabe August 2009" – einer bestimmten Norm des Deutschen Instituts für Normung (DIN). Grundsätzlich sind dynamische Verweisungen auf Normen nach der Rechtsprechung des BVerwG – etwa BVerwG, Urt. v. 27.6.2013 – Az. 3 C 21.12, Rn. 41 – verfassungsrechtlich zulässig. Allerdings „darf das nicht in einer Weise geschehen, dass der Bürger schrankenlos einer Normsetzungsgewalt ausgeliefert ist, die ihm gegenüber weder staatlich noch mitgliedschaftlich legitimiert ist" (Rn. 42). Es kommt insoweit „wesentlich auf den Umfang der Verweisung an" (Rn. 43).

92 Siehe auch *Hardt/Stummer*, DuD 2025, 720, 724.

93 Siehe oben, unter 4. b) aa) und 5. a).

94 Art. 2 des Gesetzentwurfs der Bundesregierung, BT-Drs. 21/2510, 9, 28 ff.

95 Dieses ist nach § 3 Abs. 1 KRITISDachG-RegE zudem zentrale Anlaufstelle i. S. d. CER-Richtlinie (EU) 2022/2557.

der Bußgelder enthält, während die CER-Richtlinie (EU) 2022/2557 es bei der Standardfloskel belässt, wonach Mitgliedstaaten „wirksam[e], verhältnismäßig[e] und abschreckend[e]" Sanktionen vorsehen müssen (Art. 22 der CER-Richtlinie [EU] 2022/2557).

V. Fazit

Der Schutz kritischer Infrastrukturen sowie die Netz- und Informationssicherheit in wichtigen und besonders wichtigen Einrichtungen sind gesamtgesellschaftlich und unionsweit zu bewältigende Aufgaben. Die Umsetzung der NIS-2-Richtlinie (EU) 2022/2555 sowie der CER-Richtlinie (EU) 2022/2557 leistet hierzu einen entscheidenden Beitrag. Die Regelungstechnik ist – teilweise historisch bedingt – höchst komplex. Der Gesetzgeber wechselt dabei zwischen sektorübergreifenden Regelungen im BSIG und dem KRITISDachG-RegE sowie sektorspezifischen Regelungen – vor allem für die Netzwirtschaften Telekommunikation und Energie – im TKG sowie im EnWG. Das führt mitunter zu einem Verweisungsparcours durch die Gesetze, die Unternehmen erst erfassen, dann wieder ausschließen, um aus einem anderen Gesetz dann auf das ursprüngliche Gesetz zurückzuverweisen.[96] Nicht leichter wird der Zugang zum Recht durch zahlreiche Verordnungsermächtigungen – im Falle des KRITISDachG-RegE noch dazu einer Vielzahl von Ministerien – zur Regelung weiterer Fragen. Hinzu kommen verschiedene Sicherheitskataloge – insbesondere der Bundesnetzagentur. Schließlich verfügt die Kommission über zahlreiche Ermächtigungen zum Erlass von Durchführungsrechtsakten, die ggf. das nationale Recht überlagern. Ob diese Vielzahl von Regelungsakten – vom Gesetz bis hinunter zu Sicherheitskatalogen und Meldevorgaben von Behörden – dem Anliegen dient, die digitale Resilienz der EU zu stärken, wird die Zukunft erst zeigen müssen.

96 Dabei bedient sich der Gesetzgeber zudem unterschiedlicher Regelungstechniken. So werden die Begriffe „erheblicher Sicherheitsvorfall" und „Sicherheitsvorfall" im BSIG – erwartbar – bei den „Begriffsbestimmungen" in § 2 Nr. 11 und Nr. 40 legaldefiniert. Im TKG hingegen wird zwar der „Sicherheitsvorfall" schon bei den „Begriffsbestimmungen" in § 3 Nr. 53 legaldefiniert, der „erhebliche Sicherheitsvorfall" allerdings erst in § 168 Abs. 3. Deutlich schwerer wiegen Unterschiede bei den Bußgeldern für unterlassene Meldungen nach § 32 BSIG bzw. § 168 TKG. Das BSIG sieht hierfür – über § 65 Abs. 2 Nr. 4 i. V. m. Abs. 5 Nr. 1 lit. a – Bußgelder bis 10 Millionen Euro oder – über Abs. 6 – bis 2 % des Gesamtumsatzes vor; das TKG begnügt sich für den gleichen Verstoß – über § 228 Abs. 2 Nr. 39 i. V. m. Abs. 7 Nr. 6 – mit lediglich 10.000 Euro. Das ist umso unverständlicher, als im Gesetzgebungsverfahren § 228 Abs. 2 Nr. 39 TKG gesehen und redaktionell angepasst wurde, vgl. den Gesetzentwurf der Bundesregierung, BT-Drs. 21/1501, 9, 91.

Christopher Meissner

Das neue KRITIS-Schutzregime im Energiesektor

NIS-2, CER und nationales Umsetzungsrecht

Der Beitrag untersucht das neue Schutzregime für kritische Infrastrukturen im Energiesektor unter besonderer Berücksichtigung der Verzahnung von Netz-und-Informations-Sicherheits-Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), Richtlinie (EU) 2022/2557 über die Resilienz kritischer Infrastrukturen („Critical Entities Resilience"- bzw. CER-Richtlinie) und nationalem Umsetzungsrecht. Angesichts aktueller Bedrohungen beleuchtet er die rechtlichen Herausforderungen und praktischen Implikationen für Betreiber kritischer Infrastrukturen der Energieversorgung.

I. Einleitung

Der Schutz kritischer Infrastrukturen stellt im Kontext der Energiewirtschaft eine zentrale Herausforderung dar, die durch geopolitische Unsicherheiten, eskalierende Cyberbedrohungen sowie physische Vulnerabilitäten wie Sabotageakte oder klimabedingte Extremwetterereignisse verschärft wird. Die Energieversorgung als systemrelevanter Sektor unterliegt hierbei einer dualen Bedrohungsdimension: digitalen Angriffen auf Informations- und Kommunikationssysteme einerseits und physischen Beeinträchtigungen von Anlagen andererseits. Auf unionsrechtlicher Ebene hat der EU-Gesetzgeber mit der NIS-2-Richtlinie (EU) 2022/2555 und der CER-Richtlinie (EU) 2022/2557 ein kohärentes Regelwerk geschaffen, das eine harmonisierte Steigerung der Resilienz anstrebt.

In der Bundesrepublik Deutschland wurde die NIS-2-Richtlinie (EU) 2022/2555 durch das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" (im Folgenden: „NIS-2-Umsetzungsgesetz")[1] umgesetzt, welches am 6. Dezember 2025 in Kraft getreten ist und die Richtlinienvorgaben vor allem in einer Neufassung des BSIG implementiert hat. Die CER-Richtlinie (EU) 2022/2557 soll ihre nationale Umsetzung im „Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITISDachG)" finden. Das Bundeskabinett hat den Regierungsentwurf am 10. September 2025 beschlossen.[2] Der Bundestag hat den Entwurf in erster Lesung am 6. November 2025 beraten und an den federführenden Innenausschuss überwiesen.[3] Eine Sachverständigenanhörung fand am 1. Dezember 2025 statt. Das Gesetzgebungsverfahren befindet sich Mitte Januar 2026 noch in der Ausschussberatung; eine Verabschiedung durch Bundestag und Bundesrat sowie eine Verkündung im Bundesgesetzblatt stehen noch aus. Ein Inkrafttreten wird im Laufe des Jahres 2026 – voraussichtlich nicht vor Sommer 2026 – erwartet.

Das EnWG in seiner aktuellen Fassung fungiert als sektorale Schnittstelle, die eine kohärente Integration gewährleistet, insbesondere durch Änderungen in §§ 5c bis 5e EnWG zur Stärkung der informationstechnologischen (IT-) Sicherheit und Resilienz.[4] Es integriert auf diese Weise sektorale Spezifika und vermeidet Mehrfachregulierungen. Der vorliegende Beitrag unternimmt eine systematische Analyse der

1 BGBl. 2025 I, 301. Im Referentenentwurf des Bundesministeriums des Inneren war das Gesetz noch als „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)" bezeichnet worden.
2 Gesetzentwurf der Bundesregierung, BT-Drs. 21/2510.
3 BT-Plenarprotokoll 21/37, 4063 (D).
4 *Teichmann*, EnWZ 2025, 400, 406.