GRM® Global Regulation

# CER – Die Mauer muss weg

## Getrennt was zusammengehört

Paul Friedrich
Dr. Waldemar Grudzien

Mai 2026
Synopse

## Anmerkung der Autoren

- Die horizontale Aufspaltung der Resilienz in Cybersicherheit (NIS2) und physische Sicherheit (CER) in zwei Gesetze wird in der vertikalen Regulierung widerlegt
- Die CER-Richtlinie selbst hebt durch Erwägungsgründe 20 und 21 diese Trennung auf
- Inhalte aus der CER-Richtlinie können ohne großen Aufwand in die NIS2-Richtlinie überführt werden, analog das nationale Vorgehen der Überführung von Inhalten des KRITIS-Dachgesetzes in das BSI-Gesetz
- Unterschiedliche Klassifikatoren der Betroffenheit aus beiden Gesetzen stellen Wirtschaft vor unnötig hohe Komplexität
- Das KRITISDachG ist erst mit der Veröffentlichung der bis zu neun Rechtsverordnungen legal definiert, erwartet für Sommer 2026
- Resilienzpflichten aus KRITISDachG lassen sich am besten im Rahmen des anerkannten BSI 200-4 Standards umsetzen
- CER auf europäischer Ebene sowie KRITISDachG national sollten in NIS2 resp. BSIG überführt und zurückgezogen werden – das spart Ressourcen bei den Betroffenen und erhöht ihre Gesamtsicherheit

## Einführung

Das deutsche Regulationstableau der technisch-organisatorischen Resilienz von kritischen Anlagen / Dienstleistungen / Infrastrukturen ist mit dem Inkrafttreten des KRITISDachG am 17. März 2026 vollendet. Es ergänzt die Regelungen zur Cybersicherheit in Form des BSI-Gesetzes um den Bereich der physischen Sicherheit. Zum Tableau gehören horizontal auf europäischer Ebene die NIS2- sowie die CER-Richtlinie und auf deutscher Seite BSIG, KRITIS-V und KRITISDachG, je nach Sektor gesellen sich noch Spezialgesetze hinzu – siehe Abbildung 1.

**Regulierung von Cybersicherheit und physische Sicherheit in kritischen Sektoren in Europa und Deutschland**

✗ Nicht präsent ✓ Präsent

**Wirkungsrichtung der Gesetze** — *Horizontal*

*Vertikal*

| Sektoren | Cybersicherheit | NIS2 BSIG | CER KRITISDachG | Physische Sicherheit |
|---|---|---|---|---|
| Energie | NCCS (VO 2024/1336 für Strom) | ✓ | ✓ | - |
| | - | ✓ | ✓ | EnWG, AtG |
| Transport & Verkehr | EASA (Teil IS für Luftfahrt), Durchführungsrechtsakte für Schiene/See | ✓ | ✓ | - |
| | - | ✓ | ✓ | AEG, LuftSiG, StVG / FStrG |
| Finanzen | DORA | ✗ | ✗ | - |
| | - | ✓ | ✓ | KWG, VAG |
| Leistungen für Arbeitssuchende | eIDAS 2.0 | ✓ | ✗ | - |
| | - | ✓ | ✓ | - |
| Gesundheit | MDR (VO 2017/745), IVDR (VO 2017/746), EHDS (VO 2025/327) | ✓ | ✗ | - |
| | - | ✓ | ✓ | SGB V, KHZG, MPDG, AMG |
| Wasser | Trinkwasser (RL 2020/2184) | ✓ | ✓ | - |
| | - | ✓ | ✓ | WHG, TrinkwV |
| Ernährung | - | ✓ | ✓ | - |
| | - | ✓ | ✓ | LFGB, ESVG |
| IT & Telekommunikation | CRA (VO 2024/2847) | ✓ | ✗ | - |
| | - | ✓ | ✓ | TKG |
| Weltraum | EU-Weltraumstrategie (2023), EU Space Act (Entwurf 2025) | ✓ | ✗ | - |
| | - | ✓ | ✓ | SatDSiG / SatDSiV, RAGG, TKG |
| Abfallentsorgung | - | ✓ | ✓ | - |
| | - | ✓ | ✓ | KrWG |

*Abbildung 1: Cyber- und physische Sicherheit werden in EU und Deutschland zumeist zusammen behandelt*

Es muss die Frage gestellt werden, warum horizontal europäisch wie national die Resilienz in Cybersicherheit und physische Sicherheit untergliedert wird, zumal sie in der vertikalen Spezialgesetzgebung jäh und folgerichtig gemeinsam betrachtet wird, wie Abbildung 1 eindrucksvoll belegt. Wahrscheinlich muss die Allzweckausrede „historische Entwicklung“ herhalten, nichtsdestotrotz hatten sowohl der europäische als auch der deutsche Gesetzgeber die Chance Resilienz gesamthaft mit allen Facetten in einem Gesetzeswerk zu behandeln. Es verbleibt die Hoffnung auf Vereinigung beider Facetten in der nächsten Revision. Bis dahin lohnt das Studium der vorliegenden Synopse und die gewonnene Erkenntnis, dass zusammen gehört was derzeit getrennt behandelt wird.

In unserer Synopse „NIS2 – Und täglich grüßt das Murmeltier“ haben wir uns bereits mit der NIS2-Richtlinie und ihrer deutschen Umsetzung durch BSIG und KRITIS-V befasst, d.h. mit der Cybersicherheit. Hier folgt nun mit der physischen Sicherheit nach CER-Richtlinie und KRITISDachG der zweite Teil.

## Struktur der CER-Richtlinie

In Abbildung 2 ist die CER-Richtlinie mit ihren 29 Artikeln dargestellt. Die darauffolgende Abbildung stellt das KRITISDachG dar. Für die Anwendbarkeit von Cybersicherheit und physischer Sicherheit wird das Ausschlussprinzip verwendet, gilt doch gemäß Artikel 1 (2) CER die „CER-Richtlinie nicht für Angelegenheiten, die unter die NIS2-Richtlinie fallen“.

Und weiter: „Angesichts der Beziehung zwischen physischer Sicherheit und Cybersicherheit kritischer Einrichtungen gewährleisten die Mitgliedstaaten eine koordinierte Umsetzung der vorliegenden Richtlinie und der Richtlinie (EU) 2022/2555.“ Das ist die vertane Chance des deutschen Gesetzgebers aus zwei – BSIG und KRITISDachG – eins zu machen.

**Überblick CER-Richtlinie**

| Kapitel | Artikelgruppe | Artikel | Titel |
|---|---|---|---|
| 1 Allgemeine Bestimmungen | 1 - 3 | 1 | Gegenstand und Anwendungsbereich |
| | | 2 | Begriffsbestimmungen |
| | | 3 | Mindestharmonisierung |
| 2 Nationale Rahmen für die Resilienz kritischer Einrichtungen | 4 - 11 | 4 | Strategien für die Resilienz kritischer Einrichtungen |
| | | 5 | Risikobewertung durch die Mitgliedsstaaten |
| | | 6 | Ermittlung kritischer Einrichtungen |
| | | 7 | Erhebliche Störung |
| | | 8 | Kritische Einrichtungen in den Sektoren Banken, Finanzmarktinfrastruktur und digitale Infrastruktur |
| | | 9 | Zuständige Behörden und zentrale Anlaufstelle |
| | | 10 | Unterstützung kritischer Einrichtungen durch die Mitgliedstaaten |
| | | 11 | Zusammenarbeit zwischen Mitgliedstaaten |
| 3 Resilienz kritischer Einrichtungen | 12 - 16 | 12 | Risikobewertungen durch kritische Einrichtungen |
| | | 13 | Resilienzmaßnahmen kritischer Einrichtungen |
| | | 14 | Zuverlässigkeitsüberprüfungen |
| | | 15 | Meldung von Sicherheitsvorfällen |
| | | 16 | Normen |
| 4 Krit. Einrichtun-gen mit bes. Bedeutung für Europa | 17 - 18 | 17 | Ermittlung kritischer Einrichtungen, die von besonderer Bedeutung für Europa sind |
| | | 18 | Beratungsmissionen |
| 5 Zusammenarbeit und Berichterstattung | 19 - 20 | 19 | Gruppe für die Resilienz kritischer Einrichtungen |
| | | 20 | Unterstützung der zuständigen Behörden und kritischen Einrichtungen durch die Kommission |
| 6 Aufsicht und Durchsetzung | 21 - 22 | 21 | Aufsicht und Durchsetzung |
| | | 22 | Sanktionen |
| 7 Delegierte Rechtsakte und Durchführungs-rechtsakte | 23 - 24 | 23 | Ausübung der Befugnisübertragung |
| | | 24 | Ausschussverfahren |
| 8 Schluss-bestimmungen | 25 - 29 | 25 | Berichterstattung und Überprüfung |
| | | 26 | Umsetzung |
| | | 27 | Aufhebung der Richtlinie 2008/114/EG |
| | | 28 | Inkrafttreten |
| | | 29 | Adressaten |

1: Vorschlag des Europäischen Parlaments f ür eine Richtlinie zur Änderung der NIS2-Richtlinie (EU) hinsichtlich Vereinfachungsmaßnahmen und der Angleichung an den Vorschla g für das Gesetz zur Cybersicherheit | 2: vom 20.01.2026

*Abbildung 2: Überblick CER-Richtlinie*

Artikel 8 CER schließt die Anwendung der Richtlinie für kritische Einrichtungen in den Sektoren Banken, Finanzmarktinfrastruktur und digitale Infrastruktur genauso aus wie die Erwägungsgründe (ERW) 20 und 21. Allerdings fungieren beide Erwägungsgründe als „Türöffner“ für nationale Regelungen, welche eine höhere Resilienz vorschreiben: ERW 20 schließt bei Anwendbarkeit der NIS2-Richtlinie für Einrichtungen im Bereich digitale Infrastruktursektor, ERW 21 bei Anwendbarkeit der DORA-Verordnung für Finanzunternehmen die in Artikel 11 und in Kapitel III, IV und VI der CER-Richtlinie festgelegten Verpflichtungen aus, „damit Doppelarbeit und unnötiger Verwaltungsaufwand vermieden werden“. Jedoch schreiben beide Erwägungsgründe die Ermittlung der Einrichtungen im Bereich digitale Infrastruktur resp. im Finanzsektor als kritische Einrichtungen auf der Grundlage der in der CER-Richtlinie vorgesehenen Kriterien und Verfahren vor.

## Struktur KRITIS Dachgesetz

Das KRITIS Dachgesetz (KRITISDachG) besteht aus 26 Paragrafen (Abbildung 3). Neun Paragrafen sind ganz (§§ 9, 10, 12 bis 16, 18, 20) oder teilweise (§§ 3 (8), 19 (2), 21 (6)) nicht anwendbar auf den Finanzsektor, nur bei elf Paragrafen sind Betreiber kritischer Einrichtungen der Adressat, davon neun unmittelbar (§§4, 8, 12, 13, 14, 18, 20, 24, 26) und zwei mittelbar (§§5, 9). Es folgt eine kurze Würdigung der Paragrafen in Form einer Tour de Force:

- Paragraf 1 strotzt der Bundesregierung eine Strategie zur Verbesserung der Resilienz kritischer Infrastrukturen ab. Das kann nur begrüßt werden.

- Aus Paragraf 3 muss abgespeichert werden, dass das BBK die sog. Zentrale Anlaufstelle für alle Betroffenen ist und die zuständige Behörde je nach Sektor variiert.
- Paragraf 4 bestimmt den Geltungsbereich auf 10 Sektoren (siehe Abbildung 4) und schränkt diesen gleichzeitig für bestimmte Sektoren ein. Zusätzlich wird eine Rechtsverordnung (siehe Abbildung 5) zur Bestimmung der kritischen Dienstleistungen in den Sektoren eingeführt. Aus berufener Quelle ist zu vernehmen, dass die Entwürfe zur Benennung der kritischen Dienstleistungen sehr weit fortgeschritten und für den Sommer 2026 zu erwarten sind.
- Paragraf 5 führt den Technicus Terminus „Erheblichkeit einer Anlage“ ein. Demnach qualifiziert die Erheblichkeit eine „kritische Anlage“ als eine Anlage, die für die Erbringung einer kritischen Dienstleistung erheblich ist. Zur Identifizierung der Erheblichkeit dienen die Klassifikatoren Kategorie der Anlage, Schwellwert für den Regelwert von 500.000 zu versorgende Einwohner und Stichtag. Erst eine „kritische Anlage“ muss die Anforderungen aus weiteren Paragrafen erfüllen.
- Paragraf 8 regelt die Registrierung kritischer Anlagen beim BBK. Da §8 mit §33 BSIG korrespondiert, müssen sich die Unternehmen, welche sich bis zum 6. März 2026 beim BSI aus dem BSIG heraus zu registrieren hatten, nun kein zweites Mal beim BBK registrieren. Alle anderen betroffenen Unternehmen müssen diese Registrierung vornehmen.
- Die nächsten zwei Paragrafen 9 und 10 adressieren kritische Einrichtungen mit besonderer Bedeutung für Europa und sollten diese nicht weiter belasten, denn diese sind nur besonders bedeutend, wenn sie über eine entsprechende Größe und Marktmacht verfügen und somit bereits seit längerem bestens reguliert sind.
- Der nächste Duopol der Paragrafen 11 und 12 befasst sich mit Risikoanalysen und Risikobewertungen. Paragraf 11 regelt deren Erstellung durch staatliche zuständige Behörden, Paragraf 12 durch Betreiber kritischer Anlagen. Die Betreiber haben dabei die nationalen Risikoanalysen und Risikobewertungen aus Paragraf 11 zu berücksichtigen. Dazu zwei Anmerkungen:
    - Aus dem CIAA-Kanon der Schutzziele wird einzig die Verfügbarkeit als Risikoeinfluss genannt. Das ist insofern bemerkenswert, als dass der Bruch der physischen Sicherheit auch Folgen für die anderen drei Schutzziele haben kann.
    - Beide Ersteller müssen die Risikobetrachtungen „im Bedarfsfall, mindestens jedoch alle vier Jahre“ durchführen. Das ist im Lichte der sonstigen Regulierungen und ihren zumeist einjährigen Zyklen als großzügig anzusehen.
- In Paragraf 13 spielt mit den Resilienzpflichten die Musik in diesem Gesetz. Es geht um Maßnahmen im Lebenszyklus von Vorfällen und zum physischen Schutz von Liegenschaften und kritischen Anlagen. Betreiber müssen die Maßnahmen in einem Resilienzplan „darstellen und diese anwenden“. Für Details siehe Abbildung 6.
- Paragraf 14 führt sektorenübergreifende und sektorspezifische Mindest-anforderungen sowie branchenspezifische Resilienzstandards ein. Mit dem ersten Ansatz kann das BMI zur Konkretisierung der Verpflichtungen nach § 13 Absatz 1 sektorübergreifende Mindestanforderungen bestimmen. Mit dem zweiten Ansatz wird eine Brücke zu den „branchenspezifischen

Sicherheitsstandards“ (B3S) der NIS1/IT-SiGv1.0-Ära geschlagen. Während somit der zweite Ansatz bekannt und bewährt ist, kann die Community mit Spannung die entsprechende Rechtsverordnung erwarten.

**Überblick KRITIS-Dachgesetz (KRITISDachG)** — Adressat ist Betreiber | Nicht anwendbar auf Finanzsektor[1]

| Paragraf | Titel |
|---|---|
| 1 | Nationale KRITIS-Resilienzstrategie |
| 2 | Begriffsbestimmungen |
| 3 | Zentrale Anlaufstelle; zuständige Behörde; behördliche Zusammenarbeit; Verordnungsermächtigung [2] |
| 4 | Geltungsbereich; Sektoren; Verordnungsermächtigung |
| 5 | Erheblichkeit einer Anlage für die Erbringung kritischer Dienstleistungen; Feststellungsbefugnis; Verordnungsermächtigungen |
| 6 | Sonstige Resilienzregelungen und Resilienzmaßnahmen |
| 7 | Einrichtungen der Bundesverwaltung; Geltung der Vorschriften für Betreiber kritischer Anlagen und allgemeine Feststellungen |
| 8 | Registrierung kritischer Anlagen; Geltungszeitpunkt |
| 9 | Kritische Einrichtungen von besonderer Bedeutung für Europa |
| 10 | Beratungsmission bei Einrichtungen von besonderer Bedeutung für Europa |
| 11 | Nationale Risikoanalysen und Risikobewertungen; Verordnungsermächtigung |
| 12 | Risikoanalyse und Risikobewertung des Betreibers kritischer Anlagen; Verordnungsermächtigung |
| 13 | Resilienzpflichten der Betreiber kritischer Anlagen; Resilienzplan |
| 14 | Sektorenübergreifende und sektorspezifische Mindestanforderungen; branchenspezifische Resilienzstandards; Verordnungsermächtigungen |
| 15 | Vorrang von Durchführungsrechtsakten der Europäischen Kommission zu Resilienzpflichten |
| 16 | Nachweise und behördliche Anordnungen zu Resilienzpflichten |
| 17 | Gleichwertigkeit von Nachweisen und sonstigen öffentlich-rechtlichen Verpflichtungen; Verordnungsermächtigung |
| 18 | Meldewesen für Vorfälle; Verordnungsermächtigung |
| 19 | Unterstützung der Betreiber kritischer Anlagen; freiwillige Beratungsmission [3] |
| 20 | Umsetzungs- und Überwachungspflicht für Geschäftsleitungen |
| 21 | Berichtspflichten[4] |
| 22 | Ausnahmebescheid |
| 23 | Verarbeitung personenbezogener Daten |
| 24 | Bußgeldvorschriften |
| 25 | Evaluierung |
| 26 | Anwendungsbestimmung und Übergangsregelung |

1: gilt nach §4 (2) KRITISDachG für weitere Betreiber kritischer Anlagen nicht | 2: Nur Absatz 8 gilt nicht für Finanzsektor | 3: Nur Absatz 2 gilt nicht für Finanzsektor | 4: Nur Absatz 6 gilt nicht für Finanzsektor

*Abbildung 3: Überblick KRITIS Dachgesetz*

- Die zwei Paragrafen 16 und 17 nennen die Evidenzartefakte der Resilienzpflichten: Nachweise aus § 39 BSIG (Nachweispflichten für Betreiber kritischer Anlagen), Auditberichte, Prüfungen durch die zuständige Behörde oder Zertifizierungen. Zusätzlich kann die zuständige Behörde bei Mängeln einen Mängelbeseitigungsplan inklusive Nachweise der Beseitigung verlangen.
- Paragraf 18 regelt das Meldewesen. Es gibt die Pflicht zu einem Erstbericht 24 Stunden nach Kenntnis des Vorfalls und zu einem „ausführlichen“ Bericht nach einem Monat. Zwischenberichte werden nur indirekt durch die Pflicht der Aktualisierung der Erstmeldung bei einem „andauernden Vorfall“ gefordert.
- Paragraf 19 regelt die Unterstützungsleistungen der Betreiber kritischer Anlagen durch das BBK (Vorlagen, Muster, Leitlinien, Beratungen, Schulungen, Übungen) sowie das BMI (Beratungsmission). Eine Beratungsmission soll klären, ob der Betreiber die Verpflichtungen der §§12, 13 und 18 erfüllt hat. In Paragraf 19 sollte klargestellt werden, dass es bei Beratungsmissionen ausschließlich um „kritische Einrichtungen von besonderer Bedeutung für Europa“ (wie Artikel 18 CER einschränkt) und keinesfalls um jede kritische Anlage geht.
- Paragraf 20 betont die Umsetzungs- und Überwachungspflicht für Geschäftsleitungen. Damit setzt auch das KRITISDachG die Tradition fort, Dinge die klar sind – die Geschäftsleitung ist generell für den Erfolg und Misserfolg einer Unternehmung verantwortlich – nochmals zu unterstreichen. Die Verantwortung wird hier auf die Resilienzmaßnahmen (§ 13) ausgedehnt.
- Von den restlichen Paragrafen ist für Betreiber nur noch Paragraf 24 interessant, womit wir bei den Bußgeldern wären, die gestaffelt nach Zuwiderhandlung in die vier Klassen 100k, 200k, 500k und 1 Mio. Euro sind.

## Betroffene Sektoren

In Abbildung 4 sind alle betroffenen Sektoren nach KRITIS-V, BSIG und KRITISDachG zusammengestellt. Kritische Anlagen nach KRITIS-V sind automatisch besonders wichtige Anlagen nach BSIG. Die KRITIS-V wird für das BSIG mitgeführt, um eine Verbindung zu den „kritischen Infrastrukturen“ aus der NIS1/IT-SiGv1.0-Ära herzustellen und diese Infrastrukturen in die Nomenklatur und Klassifikation nach NIS2 / BSIG zu überführen. Das KRITIS Dachgesetz vereint die kritischen Anlagen aus der KRITIS-Verordnung mit den besonders wichtigen Einrichtungen aus dem BSI-Gesetz.

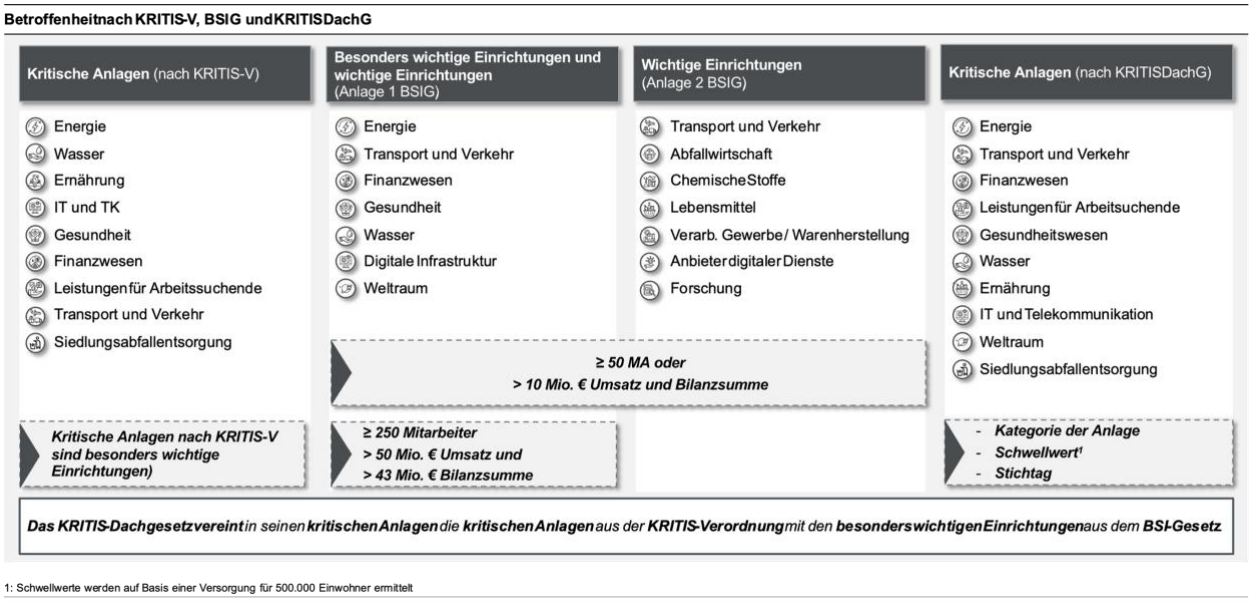


*Abbildung 4: Betroffene Sektoren und kritische Anlagen nach BSIG resp. KRITIS-V*

Damit werden die Sektoren der Cyberwelt der NIS2-Richtlinie mit den Sektoren der physischen Welt der CER-Richtlinie sprachlich vereinheitlicht. Diese Zusammenführung ist überaus wichtig für die Akzeptanz und Praktikabilität beider Gesetzespakete. Der Ausdruck Gesetzespaket ist zutreffend, denn das KRITISDachG begründet neun weitere Rechtsverordnungen wie in Abbildung 5 dargestellt.

Was bedeutet das Ganze für ein Unternehmen, dass sowohl das BSIG als auch das KRITISDachG erfüllen muss, für das somit keine Ausnahmeregelung gilt wie zum Beispiel für DORA-regulierte Finanzunternehmen? Dieses Unternehmen muss zuerst die Betroffenheiten aus beiden Gesetzen bestimmen, d.h. Schwellwerte für Mitarbeiter, Umsatz und Bilanz nach dem BSIG sowie nach KRITISDachG für Erheblichkeit, die Regelversorgung von 500.000 Einwohnern und Kategorien von Anlagen. Es folgen die Beachtung der Anforderungen aus beiden Gesetzen und die Ableitung von Maßnahmen für diese zweifach vorliegenden Anforderungen. Dieses Setting muss dann noch in den vorhandenen Risikomanagement-Rahmen eingebunden werden.

## Rechtsverordnungen aus KRITISDachG

Von den neun Verordnungen zum KRITISDachG sind aus Sicht der Wirtschaft besonders wichtig die Rechtsverordnung nach §4 (3) KRITISDachG (Nr. 2 in Abbildung 5) zur Bestimmung der kritischen Dienstleistungen in den zehn kritischen Sektoren sowie die

Rechtsverordnung nach §5 (1) KRITISDachG (Nr. 3 in Abbildung 5) zur Bestimmung der Kategorien von Anlagen, Schwellwerten und Stichtagen. Mit diesen drei Klassifikatoren wird die Erheblichkeit einer Anlage und in Folge diese Anlage als kritisch bestimmt.

Weitere interessante Rechtsverordnungen betreffen die methodischen und inhaltlichen Vorgaben für Risikoanalysen und Risikobewertungen für zuständige Stellen nach §11 (8) resp. für Betreiber kritischer Anlagen nach §12 (3). Herausragende Bedeutung erhält auch die Rechtsverordnung nach §14 (1) KRITISDachG (Nr. 7 in Abbildung 5) zur Konkretisierung von Verpflichtungen aus §13 (1) zu sektorübergreifenden Mindestanforderungen. Es bleibt abzuwarten welche Rechtsverordnungen das BBK tatsächlich erlässt und wann diese veröffentlicht werden.

**Rechtsverordnungen im KRITISDachG**

| | KRITISDachG | Inhalt der Rechtsverordnung |
|---|---|---|
| 1 | §3 (3) | **Das BMI kann für weitere kritische Dienstleistungen**, die in der Rechtsverordnung nach § 4 Absatz 3 festgelegt werden, **zuständige Bundesbehörden festlegen**. Für die kritische Dienstleistung des Betriebs von Bodeninfrastrukturen für die Erbringung weltraumgestützter Dienste im Sektor Weltraum kann das Bundesministerium für Forschung, Technologie und Raumfahrt eine oder mehrere zuständige Bundesbehörden festlegen. |
| 2 | §4 (3) | **Das BMI bestimmt die kritischen Dienstleistungen**, die jeweils zu den Sektoren nach Absatz 1 gehören. |
| 3 | §5 (1) | Das BMI bestimmt 1. **Kategorien von Anlagen**, 2. allgemeine […] **Schwellenwerte zum Versorgungsgrad**, bei deren Erreichen eine Anlage einer bestimmten Kategorie nach Nummer 1 nach einem bestimmten Stichtag als erheblich für die Erbringung einer kritischen Dienstleistung gilt und bei deren Unterschreiten eine Anlage nach einem bestimmten Stichtag nicht mehr als solches gilt, 3. **Stichtage** nach Nummer 2 sowie 4. Kategorien von Anlagen, die unabhängig von Nummer 2 als erheblich für die Erbringung einer kritischen Dienstleistung gelten. |
| 4 | §5 (7) | Das BMI kann Kriterien und Verfahren festlegen, mit denen die Länder feststellen können, ob eine Anlage für die Erbringung einer kritischen Dienstleistung erheblich ist, ohne die Voraussetzungen der Rechtsverordnung des Absatzes 1 Satz 1 zu erfüllen. Die Länder können dies für Anlagen feststellen, bei denen für die betroffene Dienstleistung eine Landesbehörde die zuständige Behörde ist. Bei der Festlegung der Kriterien werden die Kriterien nach Absatz 2 berücksichtigt. |
| 5 | §11 (8) | Das **BMI kann methodische und inhaltliche Vorgaben für die Risikoanalysen und Risikobewertungen** der nach Absatz 1 Satz 1 und 2 **zuständigen Stellen** bestimmen. |
| 6 | §12 (3) | Das **BMI kann inhaltliche und methodische Vorgaben einschließlich Vorlagen und Muster für die Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen bestimmen**. Das BMI kann die Ermächtigung nach Satz 1 durch Rechtsverordnung auf das BBK übertragen. |
| 7 | §14 (1) | Das **BMI kann zur Konkretisierung der Verpflichtungen nach § 13 Absatz 1 sektorenübergreifende Mindestanforderungen bestimmen**. Das BMI kann die Ermächtigung nach Satz 1 durch Rechtsverordnung auf das BBK übertragen. |
| 8 | §17 (3) | Das BMI kann feststellen, dass bestimmte **Verpflichtungen** auf Grund sonstiger öffentlich-rechtlicher Vorschriften, die auch für Betreiber kritischer Anlagen gelten, **gleichwertig** mit bestimmten Verpflichtungen sind, die für Betreiber kritischer Anlagen nach diesem Gesetz gelten. (4) Die Verpflichtungen nach diesem Gesetz gelten als eingehalten, soweit die in der Rechtsverordnung nach Absatz 3 Satz 1 als diesen gleichwertig festgestellten sonstigen Verpflichtungen eingehalten werden. Feststellungen anderer Behörden zur Einhaltung der sonstigen Verpflichtungen sind bindend. |
| 9 | §18 (7) | Das **BBK übermittelt den zuständigen Behörden**, den nach § 3 (5) benannten Landesbehörden sowie den nach § 11 (1) zuständigen Stellen **Auswertungen zu Vorfallsmeldungen** vorab zw. BBK und den Empfängern abgestimmter Prozesse zur Weitergabe und Wahrung der Vertraulichkeit. Das BMI kann die Prozesse zur Weitergabe der Meldungen an die Länder regeln. Die Rechtsverordnung beschreibt die Rahmenbedingungen, insb. die technischen und personellen Voraussetzungen, Kriterien für eine Weiterleitung von Meldungen und die Prozessbeschreibung für den Informationsaustausch. |

*Abbildung 5: Rechtsverordnungen im KRITISDachG*

Abbildung 6 fasst die Resilienzpflichten der Betreiber kritischer Anlagen nach §13 zusammen und gibt einen Ausblick auf eine stringentere Lösung. Die Anforderung des Paragrafen formuliert Absatz 1 mit vier Kernaufgaben. Diese werden durch Maßnahmen gemäß der Absätze 2 und 3 konkretisiert. Bei der Auswahl der Maßnahmen müssen die nationalen und Betreiber-eigenen Risikoanalysen und Risikobewertungen berücksichtigt werden. Zu guter Letzt stellt das BBK gemäß Absatz 4 Vorlagen für den Resilienzplan zur Verfügung.

Eine Anmerkung zur Maßnahme „Zugangskontrollen“: Es ist davon auszugehen, dass der Gesetzgeber „Zutrittskontrollen“, anstatt Zugangskontrollen adressieren wollte. Das KRITISDachG formuliert Anforderungen an den physischen Schutz, somit an den Zutritt. Zugang adressiert den Zugang zu Systemen, Anwendungen und Infrastrukturen im Sinne der logischen Ermächtigung, wohingegen der Zutritt die physische Ermächtigung zu Gebäuden und Räumen beschreibt.

Auf der rechten Seite von Abbildung 6 ist Artikel 13 übersetzt in die Nomenklatur des BSI-Standards 200-4 „Business Continuity Management“. Der deutsche Gesetzgeber hätte anstatt Artikel 13 diesen BSI-Standard referenzieren und mit diesem Wink den Unternehmen eine ihnen bereits bekannte Herangehensweise an die Hand geben können.

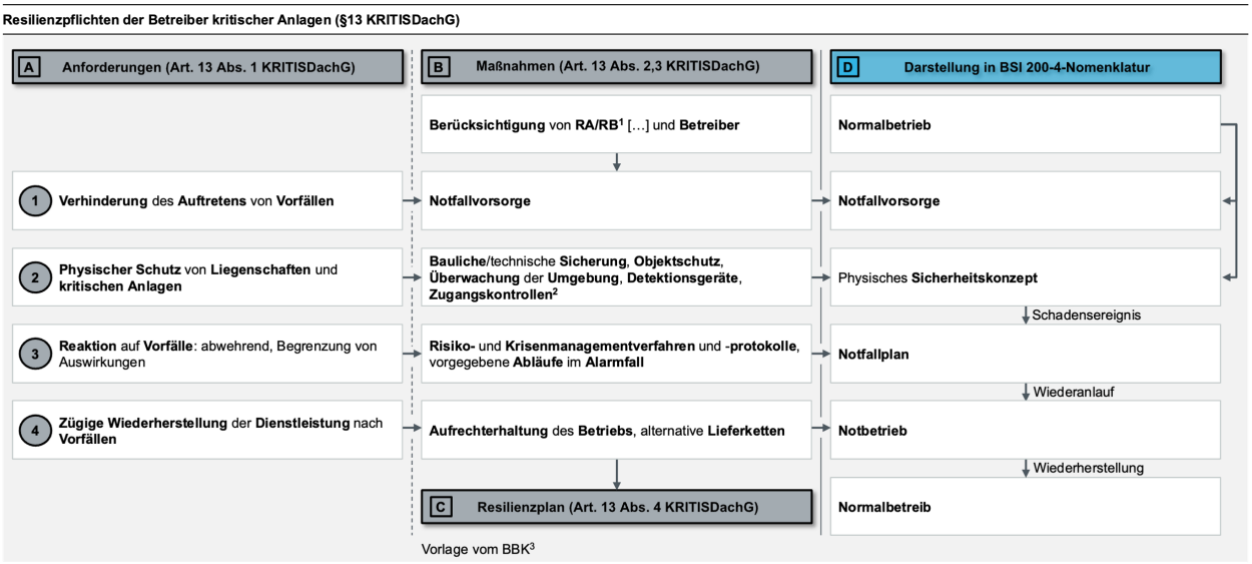


*Abbildung 6: Resilienzpflichten der Betreiber kritischer Anlagen (§13 KRITISDachG), Notation nach BSI 200-4*

## Lösungsvorschlag

Wie einleitend angemerkt, halten die Autoren die Unterteilung der Resilienz in Cybersicherheit und physische Sicherheit und ihre getrennte Behandlung durch die EU in den zwei Richtlinien NIS2 und CER für die zweitbeste Lösung. Besser ist die gemeinsame Betrachtung beider Themen in einem Gesetzeswerk. Hierfür sprechen gewichtige Gründe:

- In anerkannten Standards wie ISO/IEC 27001 für Informationssicherheit oder wichtigen Regulierungen wie DORA wird physische Sicherheit selbstverständlich als ein inhärenter Bestandteil der Gesamtsicherheit behandelt.
- Es macht sachlogisch keinen Sinn einen, wenn auch wichtigen Bereich, aus dem Anforderungskanon eines Sicherheitskatalogs herauszulösen und isoliert zu betrachten. Bedingt durch die Trennung werden Interdependenzen zwischen den einzelnen Sicherheitsdomänen nicht oder nur unklar gesehen und behandelt.
- Zwei Regelwerke bedürfen zwei Managementsysteme, die doppelte Strukturen in Personal, Technik und Organisation und letztendlich Zeit und Geld erfordern.
- Soll diese Trennung aufrechterhalten werden, so sollte die physische Sicherheit aus der NIS2-Richtlinie komplett herausgelöst werden, da sonst die Doppel-regulierung verstärkt wird.
- Zu guter Letzt eine Argumentation gegen diese Trennung durch das Gesetz selbst: Im ERW 20 CER wird argumentiert, dass für Einrichtungen im digitalen Infrastruktursektor die Anforderungen aus der NIS2-Richtlinie den aus der CER-Richtlinie „zumindest gleichwertig“ sind und aus diesem Grund sollten die in Artikel 11 und in Kapitel III, IV und VI der CER-Richtlinie festgelegten Verpflichtungen für diese Einrichtungen nicht gelten, „damit Doppelarbeit und unnötiger Verwaltungsaufwand vermieden werden“. D.h., der Ausschluss der

Gültigkeit der CER-Richtlinie für Einrichtungen im Bereich digitaler Infrastruktursektor wird damit begründet, dass die NIS2-Richtlinie auch die physische Sicherheit hinreichend regelt. Für andere Sektoren aber nicht. Dieser logische Widerspruch – der Ausschluss gilt nur für einen Sektor – und dieser Zirkelschluss – ein Gesetz (NIS2) regelt etwas (physische Sicherheit) für einen Sektor, was es nicht regelt – sind durch nichts zu rechtfertigen.

In der Summe erhöht diese Doppelregulierung aus NIS2 und CER resp. die deutsche Umsetzung aus BSIG / KRITIS-V und KRITISDachG nicht die Resilienz der Betreiber kritischer Anlagen, sondern schwächt diese aufgrund der doppelten Aufwände. Die Vereinigung beider Sicherheitssphären zu einem Regelwerk sollte Ziel der nächsten Revision sein, sowohl auf EU-Ebene als auch national. Dabei sollte die CER-Richtlinie in die NIS-Richtlinie integriert werden resp. das KRITISDachG in das BSIG.

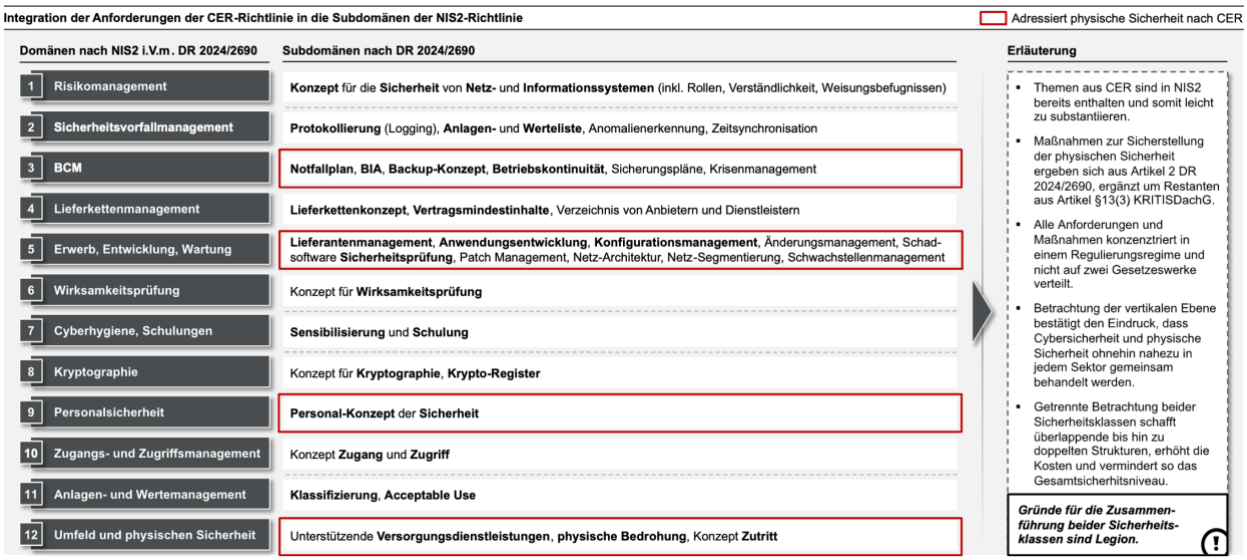


*Abbildung 7: Einbettung der physischen Sicherheit nach CER in den NIS2-Domänenzuschnitt*

Mit anderen Worten: Die NIS2-Richtlinie wird, wie in unserer Synopse „NIS2 – Und täglich grüßt das Murmeltier“ beschrieben mit Maßnahmen nach DR 2024/2690 zu insgesamt 12 Sicherheitsdomänen erfüllt. Dabei werden die Ziele der physischen Sicherheit aus CER in die passenden Domänen von NIS2 integriert (Abbildung 7). Im Gegenzug werden CER auf EU-Ebene und KRITISDachG auf deutscher Ebene zurückgezogen. Das vereint was zusammengehört, vermeidet Doppelregulierung, senkt die Compliance-Aufwände und erhöht so die Resilienz der kritischen Anlagen.

## Quellen

1. Richtlinie (EU) 2022/2557, vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen (CER)

2. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz - BSIG), Ausfertigungsdatum: 02.12.2025

3. Verordnung zur Bestimmung kritischer Anlagen nach dem BSIGesetz (BSI-Kritisverordnung - BSI-KritisV), Ausfertigungsdatum: 22.04.2016

4. Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz - KRITISDachG), 11.03.2026

## Autoren

**Paul Friedrich**
Managing Director

Paul bringt als forensischer Ermittlungsspezialist eine besondere Perspektive auf Risikomanagement mit. Als verlässlicher Ansprechpartner in vertraulichen Angelegenheiten hat er namhafte Fälle in unterschiedlichen Finanzplätzen betreut. Mit seiner Expertise im Risiko- und Finanzmanagement sorgt er dafür, dass auch komplexe Projektumgebungen im Tagesgeschäft reibungslos funktionieren.

**Mail:** pfr@globalregulation.com

**Dr. Waldemar Grudzien**
Managing Director

Waldemar ist Experte für finanzaufsichtliche Prüfungen, Informationssicherheit und Datenschutz. Er unterstützt Kunden in allen Phasen aufsichtsrechtlicher Prüfungen sowie bei der Einhaltung von Informationssicherheits- und Datenschutzanforderungen. Ein besonderer Schwerpunkt seiner Arbeit liegt auf der Bewertung und Steuerung von Compliance-Risiken im regulatorischen Umfeld.

**Mail:** wgr@globalregulation.com

## Über Global Regulation Management

GRM hebelt Regulierung. Unsere Mission ist der Aufbau regelkonformer Unternehmensstrukturen für global agierende Organisationen. Dabei setzen wir auf ein tiefes Verständnis von Geschäftsprozessen, den rechtlichen Anforderungen in Zielmärkten sowie den gezielten Einsatz moderner Softwarelösungen. Die enge Verzahnung von Geschäftsentwicklung, Risikomanagement und regulatorischen Vorgaben in einer globalisierten Wirtschaftswelt stehen im Mittelpunkt. Das Ergebnis unserer Arbeit sind sichere, rechtskonforme und international operierende Unternehmensstrukturen.

## Copyright-Anspruch

## Kontakt

Global Regulation Management AG
Baarerstrasse 52
6300 Zug
Schweiz

info@globalregulation.com
**globalregulation.com**