Kapellmann
Rechtsanwälte

CER-Richtlinie und KRITIS-Dachgesetz: Neue Pflichten für Betreiber kritischer Infrastrukturen

Physische Resilienz wird Pflicht – Was Unternehmen jetzt wissen müssen

Spätestens seit dem Stromausfall in Berlin ist die CER-Richtlinie in aller Munde. Das hierzu korrespondierende Umsetzungsgesetz wurde am 29.01.2026 vom Deutschen Bundestag beschlossen.

Doch was bedeutet diese neue EU-Regulierung konkret für Ihr Unternehmen? Dieser Blogbeitrag soll Ihnen einen ersten Überblick über die wichtigsten Anforderungen geben und aufzeigen, welche Branchen betroffen sind.

1. CER UND NIS 2 – ZWEI SEITEN DERSELBEN MEDAILLE

Ziel der CER-Richtlinie (Critical Entities Resilience Directive EU 2022/2557) ist es, dass Betreiber kritischer Infrastrukturen ihre physische Widerstandsfähigkeit gegen Bedrohungen stärken. Anders als die NIS 2-Richtlinie, die Cybersicherheit regelt, fokussiert sich CER auf physische Risiken wie Naturkatastrophen, Terroranschläge oder Sabotage.

Beide Regelwerke greifen jedoch an entscheidenden Stellen ineinander – mit erheblichen Konsequenzen für Unternehmen, die kritische Infrastrukturen planen, errichten oder betreiben.

Aktueller Stand der Umsetzung:

Am 29.01.2026 hat der Deutsche Bundestag den Gesetzesentwurf der Bundesregierung „zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen" (KRITIS-Dachgesetz/KRITISDachG) (BT-Drucksache 21/2510 vom 03.11.2025) in der vom Innenausschuss geänderten Fassung (BT-Drucksache 21/3906 vom 28.01.2026) beschlossen.

Das KRITISDachG tritt neben die bestehenden IT-Sicherheitsregelungen (BSI-Gesetz = NIS 2-Umsetzung, DORA) und adressiert ausdrücklich den physischen Schutz und die physische Resilienz nach dem All-Gefahren-Ansatz, wobei größtmögliche Kohärenz zu den Cybersicherheitsvorgaben angestrebt wird.

2. WARUM DIE CER-RICHTLINIE JETZT RELEVANT WIRD

Im Kern geht es darum, dass Einrichtungen, deren Ausfall erhebliche Auswirkungen auf Gesellschaft, Wirtschaft oder öffentliche Sicherheit hätte, systematisch gegen physische Bedrohungen geschützt werden müssen.

Die wichtigsten Bedrohungsszenarien:

- Naturkatastrophen wie Hochwasser, Stürme, Erdbeben oder extreme Wetterereignisse;
- Terroranschläge und Sabotage (wie der Anschlag auf die Strominfrastruktur in Berlin im Januar 2026);
- Unfälle und Pandemien;
- Gesundheitsgefahren und sicherheitsrelevante Vorfälle.

Die zunehmenden Extremwetterereignisse durch den Klimawandel und die gestiegene Bedrohungslage haben die EU veranlasst, die bisherigen Regelungen deutlich zu verschärfen. Der jüngste Anschlag auf die Berliner Strominfrastruktur unterstreicht die Dringlichkeit dieser Maßnahmen.

3. WELCHE SEKTOREN UND BETREIBER SIND BETROFFEN?

3.1 Sektoren

Die CER-Richtlinie erfasst Betreiber in folgenden Sektoren:

1. **Energie** – Stromerzeugung, Stromnetze, Erdgas, Öl, Wasserstoff, Fernwärme;
2. **Transport Verkehr** – Luftfahrt, Schienenverkehr, Schifffahrt, Straßenverkehr, öffentlicher Personennahverkehr;
3. **Finanzwesen;**
4. **Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende;**
5. **Gesundheitswesen** – Krankenhäuser, Pharmazeutische Industrie, Labore;
6. **Wasser;**
7. **Ernährung;**
8. **Informationstechnik und Telekommunikation**– Rechenzentren, Cloud-Computing-Dienste, Telekommunikation;

9. **Weltraum;**
10. **Siedlungsabfallentsorgung.**

3.2 Identifizierungskriterien – Bin ich betroffen?

Für die Frage der Betroffenheit sind (zusammengefasst) zwei zentrale Kriterien entscheidend:

Erstens – Bedeutung der Tätigkeit:

- Wie viele Menschen sind auf die Dienstleistung angewiesen?
- Wie abhängig sind andere Sektoren davon?
- Welchen Marktanteil hat der Betreiber?

Zweitens – Schwere einer möglichen Störung:

- Wie gravierend wären die Auswirkungen bei Ausfall?
- Wie lange würde eine Störung andauern?
- Wie groß wäre die geografische Reichweite?

Faustformel: Große Betreiber mit erheblicher volkswirtschaftlicher oder gesellschaftlicher Bedeutung sind in der Regel betroffen. Kleine, rein lokale Anbieter meist nicht – es sei denn, sie haben eine besondere Bedeutung (etwa als einziges Krankenhaus in einer Region).

Die Schwellenwerte sind in Abhängigkeit der jeweiligen Anwendungsbereiche (Sektoren) ausgestaltet (bspw. Menge des zur Verfügung gestellten Stroms). Insoweit gilt die (weitere) Faustformel: Einrichtungen, die mehr als 500.000 Einwohner versorgen oder bei denen eine Störung erhebliche wirtschaftliche oder gesellschaftliche Auswirkungen hätte, werden vom Anwendungsbereich erfasst sein.

Eine Einzelfallprüfung ist allerdings unerlässlich, da die Faustformel nur einen groben Richtwert für die Schwellenwerte darstellt.

Besonders kritisch: Einrichtungen von europäischer Bedeutung, deren Ausfall Auswirkungen auf mindestens sechs EU-Mitgliedstaaten hätte. Für diese gelten verschärfte Anforderungen.

Besonderheit: Landesidentifizierung auch unterhalb der Schwellenwerte

Die Bundesländer erhalten eigene Identifizierungsbefugnisse. Die Länder können kritische Anlagen für kritische Dienstleistungen, die alleine in ihrer Zuständigkeit liegen, auch dann als kritisch identifizieren, wenn diese die Schwellenwerte der Bundesverordnung nicht erfüllen.

Das bedeutet: Auch kleinere, regional bedeutsame Einrichtungen können unter das KRITISDachG fallen, wenn das jeweilige Bundesland sie als kritisch einstuft – etwa ein regional wichtiges Krankenhaus, ein bedeutender regionaler Verkehrsknotenpunkt oder eine lokal unverzichtbare Wasserversorgung.

Typischerweise betroffene Einrichtungen:

- Energieversorger, Kraftwerke, Windparks, Netzbetreiber, Stadtwerke;
- Verkehrsknotenpunkte wie Flughäfen, Bahnhöfe, Häfen;
- Krankenhäuser, Pharmaunternehmen, medizinische Labore;

- Wasserversorger, Kläranlagen;
- Rechenzentren, Telekommunikationsanbieter;
- Große Lebensmittelproduzenten, -händler und -logistiker;
- Banken und Finanzdienstleister mit systemischer Bedeutung.

4. WELCHE PFLICHTEN ENTSTEHEN FÜR BETROFFENE BETREIBER?

Für versorgungsrelevante IT sind über das allgemeine Schutzniveau hinausgehende Maßnahmen angemessen; der verpflichtende Einsatz von Systemen zur Angriffserkennung ist normiert. Solche Systeme analysieren fortlaufend Parameter, erkennen Bedrohungen frühzeitig und triggern Gegenmaßnahmen (typisch: SIEM, IDS/IPS, SOC).

4.1 Registrierungspflichten

Betroffene Betreiber müssen sich bei den zuständigen Behörden registrieren lassen. Die Registrierung umfasst:

- Grundlegende Informationen über die kritische Anlage und ihre Bedeutung, wie (nicht abschließend) Name des Betreibers, Kontaktdaten, den einschlägigen Sektor und die Branche, Kategorie und Versorgungsgrad;
- Meldung der bei ihnen zum Einsatz kommenden Typen von kritischen Komponenten gemäß § 2 Nummer 23 des BSI-Gesetzes (IT-Hardware und -Software).

Diese Informationen über kritische Komponenten sind ausschließlich an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu übermitteln.

Das bedeutet: Betreiber müssen nicht nur ihre Infrastruktur melden, sondern auch transparent machen, welche kritischen IT-Komponenten sie einsetzen – ein wichtiger Schritt zur Vernetzung von physischer und Cyber-Resilienz.

4.2 Risikobewertung – Die Grundlage allen Handelns

Betreiber kritischer Einrichtungen müssen mindestens alle vier Jahre (im Bedarfsfall öfter) systematisch analysieren, welchen Bedrohungen ihre Einrichtung ausgesetzt ist, wie verwundbar sie gegenüber diesen Bedrohungen ist und welche Auswirkungen ein Ausfall hätte.

Beispielhaft bedeutet das:

Bedrohungen identifizieren:

- Naturkatastrophen am Standort (Hochwasser, Sturm, Hitze, Erdbeben);
- Terroristische Bedrohungslagen und Sabotage;
- Unfallszenarien;
- Gesundheitsgefahren (Pandemien);
- Sabotagerisiken.

Verwundbarkeiten bewerten:

- Schwachstellen in der baulichen Infrastruktur;
- Abhängigkeiten von externen Versorgern (Strom, Treibstoff, Telekommunikation);

- Anfälligkeit der IT-Systeme für physische Beeinträchtigungen;
- Personalabhängigkeiten;
- Sicherheitslücken im Perimeter.

Auswirkungen analysieren:

- Anzahl betroffener Menschen;
- Wirtschaftliche Schäden durch Betriebsunterbrechung;
- Auswirkungen auf Lieferketten und abhängige Wirtschaftssektoren;
- Dauer der Wiederherstellung;
- Reputationsschäden.

Praxisbeispiele zur Veranschaulichung:

- **Energieversorger:** Analyse von Hochwasserrisiken für Umspannwerke, Sturmschäden an Freileitungen, Sabotagerisiken für Netzinfrastruktur;
- **Krankenhäuser:** Bewertung von Evakuierungsszenarien bei Brand, Pandemievorsorge, Ausfall der Stromversorgung für lebenserhaltende Systeme;
- **Wasserversorger:** Gefährdung von Brunnen durch Hochwasser, Sabotage von Aufbereitungsanlagen, Lieferkettenabhängigkeiten bei Chemikalien;
- **Verkehrsinfrastruktur (z.B. Flughäfen, Bahnhöfe):** Extremwetterauswirkungen auf Betriebsflächen, Terrorrisiken, Ausfall kritischer Versorgung (Strom, Treibstoff);
- **Rechenzentren:** Überschwemmungsrisiken, Kühlungsausfall bei Hitze, physische Angriffe auf die Gebäudeinfrastruktur.

4.3 Resilienzmaßnahmen – Vom Konzept zur Umsetzung

Betreiber müssen verhältnismäßige Maßnahmen zur Gewährleistung der Resilienz kritischer Anlagen treffen. Die zu ergreifenden Maßnahmen sollen auf Grundlage der nationalen Risikoanalysen und Risikobewertungen sowie der Risikoanalyse und Risikobewertung des Betreibers beruhen.

Ziele der Resilienzmaßnahmen (§ 13 Abs. 1 KRITISDachG):

Die zu ergreifenden Maßnahmen sollen dazu dienen:

1. Vorfälle zu verhindern;
2. Den physischen Schutz kritischer Anlagen zu gewährleisten;
3. Angemessen zu reagieren und abzuwehren;
4. Negative Auswirkungen zu begrenzen;
5. Eine zügige Wiederherstellung der kritischen Dienstleistung sicherzustellen.

Verhältnismäßigkeit – Zweck-Mittel-Abwägung:

Die Maßnahmen müssen insgesamt verhältnismäßig sein. Der **Stand der Technik** soll eingehalten werden. Für die Bewertung der Verhältnismäßigkeit ist eine Zweck-Mittel-Relation vorzunehmen, bei der insbesondere der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls gegen das Risiko eines Vorfalls abzuwägen ist. Wirtschaftliche Aspekte, darunter die Leistungsfähigkeit des Betreibers, zu berücksichtigen sind.

Wichtig: Es besteht keine strikte Verpflichtung zur Einhaltung des Stands der Technik. Soweit die Abwägung allerdings zu dem Ergebnis kommt, dass der Stand der Technik notwendig ist, dies wirtschaftlich leistbar ist und ansonsten ein nicht hinnehmbares Risiko besteht, ist der Stand der Technik einzuhalten.

Gesetzlich genannte beispielhafte Maßnahmen (§ 13 Abs. 2 KRITISDachG):

Als zu ergreifende Maßnahmen, um die notwendige Resilienz zu schaffen, nennt das Gesetz folgende (nicht abschließende) Beispiele:

- Notfallvorsorge;
- Objektschutz (baulich, technisch und organisatorisch);
- Überwachung, Detektion und Zugangskontrollen;
- Risiko- und Krisenmanagement sowie Alarmabläufe;
- Notstromversorgung und alternative Lieferketten;
- Sicherheitsmanagement für Mitarbeitende (einschließlich externer Dienstleister);
- Schulungen und Übungen.

Mögliche praktische Ausgestaltung (beispielhafte Veranschaulichung):

Im Rahmen der Ausgestaltung kommen folgende beispielhafte Umsetzungsmöglichkeiten in Betracht. Ob und welche Maßnahmen ergriffen werden sollten, ist dabei stets einzelfallbezogen zu prüfen und zu bewerten.

Objektschutz: Hochwasserschutz, Perimeterschutzsysteme, Videoüberwachung kritischer Bereiche, Zutrittskontrollsysteme, Besucherregelungen.

Notstromversorgung und alternative Lieferketten: Notstromaggregate für kritische Systeme, redundante Energieversorgung, Verträge mit mehreren Lieferanten, Lagervorräte für kritische Verbrauchsmaterialien.

Risiko- und Krisenmanagement: Notfallpläne für verschiedene Szenarien, Krisenstabsstrukturen, Kommunikationspläne, Evakuierungspläne.

Schulungen und Übungen: Regelmäßige Sicherheitsunterweisungen, Spezialschulungen für Krisenteams, realistische Übungen verschiedener Notfallszenarien.

Branchenspezifische Beispiele: Energiesektor (Hochwasserschutz für Umspannwerke, Ersatzteillager), Gesundheitswesen (Notstrom für OP-Säle, Medikamentenvorräte), Wasserversorgung (alternative Wasserquellen, Notstrom für Pumpwerke), Verkehr (Hochwasserschutz für Betriebsflächen, redundante Kommunikation).

Hinweis: Diese Beispiele dienen ausschließlich der Veranschaulichung. Die konkreten Anforderungen ergeben sich aus der individuellen Risikoanalyse sowie den noch zu erlassenden Rechtsverordnungen und Leitlinien des BBK.

Konkretisierung durch Standards:

Das BMI kann sektorenübergreifende Mindestanforderungen per Rechtsverordnung festlegen. Betreiber und Branchenverbände können branchenspezifische Resilienzstandards vorschlagen, deren Geeignetheit das BBK feststellen kann.

Die Sektorspezifische Verordnungsermächtigungen für Bundesressorts und Länder treten dabei erst am 01.01.2030 in Kraft.

4.4 Resilienzplan – Dokumentation ist Pflicht

Alle Ergebnisse und Maßnahmen müssen in einem schriftlichen Resilienzplan dokumentiert werden. Dieser Plan ist das zentrale Dokument, mit dem der Betreiber gegenüber den Behörden nachweist, dass er seinen Pflichten nachkommt.

Der Resilienzplan muss enthalten:

- Die vollständige Risikobewertung für alle relevanten Infrastrukturbereiche;
- Den Katalog aller implementierten technischen Schutzmaßnahmen;
- Die Beschreibung der organisatorischen Vorkehrungen;
- Klare Verantwortlichkeiten und Zuständigkeiten (auch auf Geschäftsführungsebene);
- Zeitpläne für Umsetzung und regelmäßige Überprüfung;
- Detaillierte Notfall- und Wiederherstellungspläne;
- Kommunikationsstrategien für verschiedene Krisenszenarien;
- Dokumentation der Koordination mit Dienstleistern und Behörden;
- Nachweis regelmäßiger Übungen und deren Auswertung.

Der Resilienzplan muss mindestens nach Durchführung der Risikoanalyse und Risikobewertung (d.h. mindestens alle vier Jahre, im Bedarfsfalle früher) aktualisiert werden und ist bei wesentlichen Änderungen anzupassen.

4.5 Meldepflichten – Schnelle Reaktion im Krisenfall

Wenn es trotz aller Vorkehrungen zu einem erheblichen Vorfall kommt – etwa einem Ausfall einer wichtigen Anlage, einem Sabotageakt, einem schweren Unfall oder einer Naturkatastrophe, die die Einrichtung beschädigt – greifen strenge Meldepflichten.

Konkret bedeutet dies:

- **Erstmeldung:** Meldung unverzüglich, spätestens innerhalb von 24 Stunden an die zentrale Meldestelle beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK);
- **Eingangsbestätigung:** Das BBK sendet unverzüglich eine Eingangsbestätigung der Vorfallsmeldung;
- **Unterstützung:** Das BBK gibt dem Betreiber unverzüglich Rückmeldung mit Informationen und Leitlinien, die bei der Reaktion auf den Vorfall unterstützen;
- **Zwischenstandsbericht/Abschlussbericht:** Innerhalbeines Monats ist ein ausführlicher Zwischenstandsbericht oder Abschlussbericht zu erstellen und zu melden;
- **Gemeinsame Plattform:** Die Meldungen erfolgen über eine gemeinsame Plattform mit dem BSI, um Doppelmeldungen zu vermeiden.

Regelmäßige Lagebilder:

Das BBK erstellt regelmäßige und anlassbezogene Lagebilder zur Situation kritischer Anlagen und stellt diese den

zuständigen Behörden, Landesbehörden und den Betreibern selbst zur Verfügung. Betreiber erhalten damit wichtige Informationen über aktuelle Bedrohungslagen und können ihre Schutzmaßnahmen entsprechend anpassen.

4.6 Behördenkooperation und Sanktionen

Betreiber müssen mit den zuständigen Behörden kooperieren, Inspektionen zulassen, Dokumente vorlegen und Anordnungen befolgen.

Bei Verstößen drohen erhebliche Konsequenzen:

Während der ursprüngliche Entwurf Bußgelder bis zu 500.000 Euro vorsah, wurde die Sanktionsregelung im parlamentarischen Verfahren deutlich verschärft. Die aktuelle Fassung sieht nun eine gestaffelte Bußgeldstruktur vor:

- **In schwerwiegenden Fällen:** Geldbußen bis zu **einer Million Euro;**
- **In anderen Fällen:** Geldbußen bis zu 500.000 Euro, 200.000 Euro oder 100.000 Euro, je nach Art und Schwere des Verstoßes.

Besonders schwerwiegend werden bewertet:

- Unterlassung oder unzureichende Durchführung von Risikobewertungen;
- Fehlende oder unzureichende Resilienzmaßnahmen;
- Verletzung von Meldepflichten;
- Verweigerung der Behördenkooperation.

Darüber hinaus können Betriebseinschränkungen oder -Untersagungen angeordnet werden, wenn erhebliche Sicherheitsmängel festgestellt werden.

5. PRAXISHINWEIS: BESONDERE HERAUSFORDERUNG BEI DER UMSETZUNG BEI HOCHVERNETZTEN INFRASTRUKTUREN

Besondere Komplexität bei hochvernetzten Infrastrukturen

In der Praxis dürfte die Umsetzung der Resilienzpflichten insbesondere für komplexe, hochvernetzte Infrastrukturen herausfordernd sein. Beispielhaft, ohne dass es hierzu konkrete Regelungen im Gesetzesentwurf gibt, seien erwähnt:

Flughäfen vereinen zahlreiche kritische Funktionen unter einem Dach: Flugsicherung, Passagierterminals, Gepäcklogistik, Betankungssysteme, Energieversorgung, IT-Infrastruktur und Ver- und Entsorgungssysteme. Eine Risikoanalyse muss hier die Wechselwirkungen zwischen diesen Systemen erfassen – etwa wenn ein Stromausfall gleichzeitig die Gepäckförderung, die Terminalbeleuchtung und die Flugsicherungssysteme betrifft.

Krankenhäuser stehen vor ähnlichen Herausforderungen: Medizinische Geräte, Notstromversorgung, Klimatisierung, Wasserversorgung, Aufzüge für Bettentransporte, IT-Systeme für Patientendaten und Medikamentenlager müssen in einer integrierten Risikobetrachtung erfasst werden.

Energieerzeugungsanlagen vereinen zahlreiche interdependente Systeme: Prozessleittechnik, Netzleittechnik, Einspeisemanagement, Mess- und Regelsysteme sowie Notabschaltsysteme. Ein Vorfall in einem Teilbereich kann kaskadierende Auswirkungen auf die gesamte Stromversorgung haben. Die Risikoanalyse muss die Wechselwirkungen zwischen diesen Systemen erfassen – etwa wenn ein Ausfall der Leittechnik gleichzeitig die Stromerzeugung und die Netzstabilität beeinträchtigt.

Wasserversorgungsanlagen stehen vor ähnlichen Herausforderungen: Brunnen- und Pumpsteuerungen, Aufbereitungsanlagen, Mess- und Überwachungssysteme, SCADA-Systeme und Leitnetzverwaltung müssen in einer integrierten Risikobetrachtung erfasst werden. Die Trinkwasserversorgung muss jederzeit gewährleistet sein, was besondere Anforderungen an Redundanzen und Notfallpläne stellt.

Multi-Stakeholder-Umgebungen

Eine weitere praktische Herausforderung ergibt sich dort, wo Betreiber kritischer Anlagen auf Dienstleistungen Dritter angewiesen sind oder selbst Dienstleister einsetzen:

- **Flughafenbetreiber** müssen mit Airlines, Bodendiensten, Flugsicherung, Bundespolizei, Zoll und externen Dienstleistern (Catering, Reinigung, Sicherheitsdienste) koordinieren.
- **Rechenzentren** sind auf Telekommunikationsanbieter, Stromversorger und Kühlsystemwartung angewiesen.
- **Hafenbetreiber** interagieren mit Reedereien, Spediteuren, Zoll und verschiedenen Logistikdienstleistern.

Die Resilienzmaßnahmen müssen diese Abhängigkeiten berücksichtigen, auch wenn die jeweiligen Betreiber nur begrenzten Einfluss auf externe Dienstleister haben.

Integration in bestehende Sicherheitskonzepte

Viele Betreiber kritischer Anlagen unterliegen bereits heute verschiedenen Sicherheits- und Compliance-Anforderungen:

- IT-Sicherheit nach BSI-Gesetz;
- Arbeitsschutz und Betriebssicherheit;
- Umweltschutzauflagen;
- Datenschutz (DSGVO);
- Branchenspezifische Regelwerke (z.B. luftverkehrsrechtliche Sicherheitsvorschriften, kerntechnische Sicherheit, Lebensmittelsicherheit).

Die neuen Resilienzpflichten sollten sinnvollerweise in diese bestehenden Managementsysteme integriert werden, um Doppelstrukturen zu vermeiden. Synergien zwischen IT-Sicherheit (Cyber-Resilienz) und physischer Resilienz sollten genutzt werden.

Empfehlung: Eine frühzeitige Bestandsaufnahme vorhandener Sicherheitskonzepte und deren Abgleich mit den neuen Anforderungen kann helfen, Effizienzgewinne zu realisieren und den Umsetzungsaufwand zu optimieren.

6. EVALUIERUNG UND MÖGLICHE AUSWEITUNG

Das Bundesministerium des Innern wird das Gesetz regelmäßig evaluieren. Die Evaluierung erfolgt alle fünf Jahre, erstmalig jedoch bereits zwei Jahre nach Inkrafttreten.

Gegenstand der ersten Evaluierung werden insbesondere sein:

- Die Identifizierung der Betreiber kritischer Anlagen (sind die richtigen Betreiber erfasst?);
- Die Ausgestaltung des Regelschwellenwertes (sind 500.000 Einwohner der richtige Schwellenwert?);
- Die Höhe der Bußgelder (sind die Sanktionen wirksam und angemessen?);

- Die Frage der Notwendigkeit eines Zertifizierungssystems.

Was bedeutet das für Unternehmen?

Es ist wahrscheinlich, dass der Anwendungsbereich in den kommenden Jahren ausgeweitet wird:

- Absenkung der Schwellenwerte könnte mehr Betreiber erfassen;
- Zusätzliche Sektoren könnten hinzukommen;
- Verschärfung der Anforderungen ist möglich;
- Einführung von Zertifizierungspflichten denkbar.

Empfehlung: Auch wenn Ihr Unternehmen derzeit knapp unterhalb der Schwellenwerte liegt, sollten Sie sich mit den CER-/KRITISDachG-Anforderungen vertraut machen und ggf. bereits präventiv Maßnahmen ergreifen. Eine spätere Anpassung wird dann deutlich einfacher.

7. WAS SOLLEN UNTERNEHMEN JETZT TUN?

7.1 Sofortmaßnahmen:

- Betroffenheitsprüfung
- Überblick verschaffen (Abhängigkeiten/Stakeholdereinbeziehung)
- Starten der Risikobewertung
- Prüfung bestehender Maßnahmen
- Koordinierung mit NIS 2/BISG

7.2. Mittelfristige Schritte

- Entwicklung eines umfassenden Resilienzplans
- Implementierung aller erforderlichen technischen und organisatorischen Maßnahmen
- Etablierung von Governance-Strukturen
- Mitarbeiterschulungen und Übungen
- Vorbereitung von Behördenkooperation

7.3. Langfristige strategische Ausrichtung

- Integration von Resilienz in Unternehmensstrategie
- Nutzung der Resilienz als Wettbewerbsvorteil
- Vorbereitung auf anstehende Evaluierungen

8. FAZIT: HERAUSFORDERUNG UND CHANCE ZUGLEICH

Die CER-Richtlinie und das KRITISDachG stellen einen Paradigmenwechsel in der Regulierung kritischer Infrastrukturen

dar. Betreiber kritischer Einrichtungen müssen künftig systematisch ihre physische Resilienz gegen eine Vielzahl von Bedrohungen stärken.

Die jüngsten Entwicklungen – insbesondere der Anschlag auf die Berliner Strominfrastruktur und die daraus resultierenden Verschärfungen sowie die nunmehr sehr zeitnahe Beschluss des Deutschen Bundestages – zeigen: Das Thema hat höchste politische Priorität. Die Anforderungen werden ernst genommen und konsequent durchgesetzt.

Wer frühzeitig handelt, profitiert mehrfach:

- **Compliance-Sicherheit:** Vermeidung von Bußgeldern bis zu einer Million Euro und Reputationsschäden;
- **Tatsächliche Sicherheit:** Schutz vor realen Bedrohungen und Minimierung von Ausfallrisiken;
- **Wettbewerbsvorteile:** Positionierung als zuverlässiger, sicherer Partner;
- **Kosteneffizienz:** Frühe Integration in Investitionsplanung ist günstiger als nachträgliche Anpassungen;
- **ESG-Performance:** Resilienz und Klimaanpassung sind zentrale ESG-Kriterien;
- **Vorbereitung auf Ausweitung:** Bei der Evaluierung nach zwei Jahren gut aufgestellt sein.

Die Anforderungen sind komplex, aber mit strukturiertem Vorgehen, klaren Verantwortlichkeiten und fachkundiger Beratung umsetzbar.

9. WIE WIR SIE UNTERSTÜTZEN KÖNNEN

Als spezialisierte Kanzlei mit umfassender Expertise im IT-, Infrastruktur-, Bau- und Regulierungsrecht sowie den vorhandenen Schnittmengenkenntnissen begleiten wir Sie umfassend bei allen Fragen rund um die CER-Richtlinie und das KRITIS-Dachgesetz.

Kontaktieren Sie › **Dr. Sven Marco Hartwig** jederzeit – er berät Sie gerne.

› **zurück**