Orth Kluth Newsletter Öffentliches Wirtschaftsrecht / IP / IT / Datenrecht

KRITIS-Dachgesetz

- Stärkung der Resilienz und umfassender Schutz kritischer Infrastrukturen -

Von der Stromversorgung über die Lebensmittelproduktion und die Gesundheitsversorgung bis zur Telekommunikation – Kritische Infrastrukturen (KRITIS) sind Grundvoraussetzung für jegliche staatliche, wirtschaftliche und gesellschaftliche Tätigkeit. Funktionsstörungen oder Ausfälle von KRITIS können zu nachhaltig wirkenden Versorgungsengpässen und erheblichen Störungen der öffentlichen Sicherheit und Ordnung führen.

Vor diesem Hintergrund überrascht es, dass KRITIS bisher nur im Teilbereich Cybersicherheit durch das sog. „Bundessicherheits-Gesetz“ (BSI-Gesetz) und das sog. „IT-Sicherheitsgesetz 2.0“ rechtlich reguliert ist. Noch in diesem Jahr soll zudem das NIS-2-Umsetzungsgesetz in Kraft treten, das zu einer erheblichen Erweiterung der verpflichteten Unternehmen führt (siehe unser Newsletter vom 28. Mai 2024 zum Thema „Neue Pflichten für Unternehmen im Bereich der IT-Sicherheit“). Die federführende Zuständigkeit für das Thema IT-Sicherheit liegt beim Bundesamt für Sicherheit in der Informationstechnik (BSI).

Mögliche Gefahren betreffen jedoch nicht nur die digitale, sondern ebenso die analoge Welt: Naturkatastrophen, Pandemien, Terroranschläge, Kriege, Sabotage, menschliches Versagen und vieles mehr.

Der Europäische Gesetzgeber hat dies erkannt und bereits Mitte Dezember 2022 die sog. **CER-Richtlinie** über die Resilienz kritischer Einrichtungen (RL (EU) 2022/2557) erlassen, die nunmehr in das nationales Recht der EU-Mitgliedstaaten umgesetzt werden muss. Der deutsche Gesetzgeber plant hierfür die Verabschiedung eines sog. **KRITIS-Dachgesetzes** im Oktober 2024, welches bereits als 2. Referentenentwurf vorliegt (nachfolgend: **KRITIS-DG-E**). Der mit diesem Gesetz bezweckte sektorübergreifende physische Schutz im Sinne einer Stärkung der Resilienz von Betreibern kritischer Anlagen nach dem "All-Gefahrenansatz" soll neben die bereits existierenden Regelungen zur Cybersicherheit treten, gleichzeitig aber eine größtmögliche Kohärenz vorsehen.

Der KRITIS-DG-E trifft keine sektoren- oder branchenspezifischen Regelungen, sondern gibt vielmehr "abstrakt" vor, dass in allen KRITIS-Sektoren geeignete oder branchenspezifische Maßnahmen zum physischen Schutz von Betreibern kritischer Anlagen zu treffen sind. Zugleich soll ein Prozess aufgesetzt werden, der eine Entwicklung von Schutzstandards durch die Verbände, Risikobewertungen durch die Betreiber, eine Erstellung von Resilienz-Plänen sowie auch die Durchführung von Überprüfungen durch die zuständigen Behörden umfasst. Eine zentrale Rolle wird hier eine Behörde spielen, von deren Existenz vor der Pandemie vermutlich nur wenige wussten: Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).

Was sind die Ziele des KRITIS-DG-E?

Der KRITIS-DG-E zielt darauf ab:

- Einheitliche, bundesweite und sektorübergreifende **Mindeststandards und Maßnahmen** für die physische Resilienz kritischer Anlagen festzulegen.
- Betreibern kritischer Anlagen Klarheit über ihre wirtschaftliche und gesellschaftliche Bedeutung sowie die daraus folgenden Pflichten zu geben.
- Die Aufrechterhaltung des Geschäftsbetriebs zu jeder Zeit und die schnelle Wiederherstellung bei Störungen oder Ausfällen zu gewährleisten.
- Ein Verfahren für **Risikobewertungen und** ein **Störungsmonitoring** für alle relevanten Sektoren zu implementieren, um kontinuierlich Risiken und signifikante Störungen überwachen zu können.

Wer ist betroffen?

Adressaten des KRITIS-DG-E werden voraussichtlich Unternehmen sein, die

1. Anlagen aus einem der nachfolgenden Sektoren:
   - Energie
   - Wasser
   - Ernährung
   - Gesundheit
   - Informationstechnik und Telekommunikation
   - Transport und Verkehr
   - Finanz- und Versicherungswesen
   - Abfälle
   - Weltraum und
   - Öffentliche Verwaltung
2. Essenziell für die Grundversorgung Deutschlands und
3. Versorgen mehr als 500.000 Personen

Der Gesetzgeber soll dazu befugt sein, mittels Verordnung **zusätzliche Betreiber** kritischer Einrichtungen zu bestimmen. Diese Auswahl basiert auf nationalen Risikoanalysen und -bewertungen. Entscheidende Faktoren sind unter anderem die Bedeutung der Dienstleistung für andere Sektoren und die Anzahl der Nutzer, die auf diese angewiesen sind.

Mit dem neuen Rahmenwerk wird die Zahl der als KRITIS klassifizierten Unternehmen und Institutionen **signifikant steigen**, wobei Schätzungen von bis zu 22.000 zusätzlichen Betreibern ausgehen.

Was ist zu tun?

1. **Registrierungspflicht**

Innerhalb von drei Monaten nach Einstufung als Betreiber kritischer Anlagen müssen sich diese beim BKK registrieren.

2. **Risikoanalysen und –bewertungen**
   - Diese sind mindestens alle vier Jahre durchzuführen.
   - Dabei sollen nationale Risikoanalysen berücksichtigt werden sowie auch andere vertrauenswürdige Quellen.
   - Spezifische Risiken, die die Handlungsfähigkeit der Wirtschaft beeinträchtigen können, sollen einbezogen werden.
3. **Resilienz-Maßnahmen und Resilienz-Plan**

   Geeignete und verhältnismäßige Maßnahmen zur Gewährleistung der Resilienz sind innerhalb von 10 Monaten nach Registrierung umzusetzen.

   - Maßnahmen sollen Vorfälle verhindern, Schutz bieten, auf Vorfälle reagieren, Wiederherstellung sichern und Sicherheitsmanagement gewährleisten.
   - Maßnahmen basieren auf nationalen Risikoanalysen und eigener Risikobewertung.
   - Resilienzplan, der die Maßnahmen und zugrunde liegenden Erwägungen dokumentiert, muss erstellt und angewendet werden.
4. **Meldepflicht für Vorfälle**
   - Vorfälle, die kritische Dienstleistungen erheblich stören, sind unverzüglich zu melden.
   - Erste Meldung innerhalb von 24 Stunden, ausführlicher Bericht innerhalb eines Monats nach Kenntnis des Vorfalls.
   - Meldungen müssen bestimmte Informationen enthalten, um Art, Ursache und Auswirkungen des Vorfalls zu ermitteln.

Wie ist der Zeitplan?

1. **Umsetzungsfrist der CER-Richtlinie**

   Alle EU-Mitgliedstaaten müssen bis zum 17. Oktober 2024 die europäische Cybersicherheitsrichtlinie (CER-Richtlinie) in nationales Recht umwandeln.

2. **Deutscher Gesetzentwurf**

   Der im Dezember 2023 vorgestellte Referentenentwurf soll in diesem Jahr das parlamentarische Verfahren durchlaufen und tritt am Tag nach der Verkündung in Kraft (voraussichtlich im Oktober 2024).

3. **Inkrafttreten der Verpflichtungen**

   - **Pflichten der Anlagenbetreiber:**

     Beginnen ab dem 1. Januar 2026 schrittweise zu gelten.

   - **Bußgeldvorschriften:**

     Treten ab dem 1. Januar 2027 in Kraft und werden ebenfalls schrittweise eingeführt.

4. **Registrierung und Kontaktstelle**

   - Betreiber müssen nach Inkrafttreten der für ihren Sektor relevanten Rechtsverordnung ihre Anlage innerhalb von drei Monaten registrieren.
   - Eine Kontaktstelle oder Kontaktperson beim BKK ist zu benennen.

5. **Risikoanalyse und -bewertung**

   - Erste Durchführung neun Monate (durch zuständiges Ministerium) bzw. zehn Monate (durch Betreiber) nach der Registrierung.
   - Wiederholung alle vier Jahre.

6. **Resilienzplan**

   - Erstellung eines Plans mit Maßnahmen zur Widerstandsfähigkeit der Anlage binnen zehn Monaten nach Registrierung.
   - Erster Nachweis des Resilienzplans zu einem vom BKK mitgeteilten Termin.
   - Aktualisierung des Resilienzplans alle zwei Jahre.

Was können wir für Sie tun?

Wir werden das Gesetzgebungsverfahren zum KRITIS-DG weiterhin genau beobachten und Sie proaktiv über relevante Neuigkeiten und Entwicklungen informieren.

Bitte beachten Sie, dass die Umsetzung der neuen Anforderungen eine sorgfältige Planung und Anpassung Ihrer internen Prozesse erfordern wird. Wir stehen bereit, Sie bei der Bewertung der Auswirkungen dieser Gesetzgebung auf Ihr Unternehmen zu unterstützen und gemeinsam mit Ihnen Strategien für eine erfolgreiche Implementierung der geforderten Maßnahmen zu entwickeln.

Ihre Ansprechpartner

Marieke Schwarz
Rechtsanwältin, Fachanwältin für Verwaltungsrecht, Salary Partnerin

T +49 211 60035-422
marieke.schwarz@orthkluth.com

Dr. David Brosende
Rechtsanwalt, Salary Partner

T +49 30 509320-131
david.brosende@orthkluth.com

Felix Meurer
Rechtsanwalt, Senior Associate

T +49 30 50 9320-117
felix.meurer@orthkluth.com

One Team.
One Goal.