Das neue KRITIS-Dachgesetz – Überblick und Lösungsansätze für Netzbetreiber

Von Markus Heinrich und Cosmo Grühn

In den vergangenen Jahren häuften sich physische Angriffe auf kritische Infrastrukturen in Deutschland. Erst am 03.01.2026 hatte ein Brandanschlag auf das Berliner Stromnetz schlimme Folgen – ein großflächiger Stromausfall betraf 45.000 Haushalte. Der Anschlag reiht sich in eine Vielzahl von Ereignissen ein, die gezeigt haben, wie verletzlich Deutschlands und Europas Versorgungsinfrastruktur sein kann. Dieser wachsenden Bedrohung für die inländische Infrastruktur will die Bundesregierung mit dem KRITIS-Dachgesetz (KRITIS-DachG) begegnen und so einen übergreifenden Rahmen zur Erhöhung der Resilienz kritischer Anlagen schaffen. Dieser Artikel soll den Gesetzgebungsprozess sowie die entscheidenden rechtlichen Grundlagen des KRITIS-DachG mit Fokus auf Netzbetreiber beleuchten. Außerdem werden die verschiedenen Zuständigkeiten und Entscheidungsspielräume staatlicher Stellen mit denen der Betreiber gespiegelt und Möglichkeiten der Zusammenarbeit dargelegt, um aufzuzeigen, was die Betreiber kritischer Infrastruktur mit Inkrafttreten des Gesetzes erwartet.

Überblick über die rechtlichen Grundlagen des KRITIS-DachG

Der Gesetzgeber setzt mit dem KRITIS-DachG die „CER-Richtlinie“ der EU in nationales Recht um, welche die Mitgliedstaaten dazu verpflichtet, kritische Einrichtungen zu identifizieren und die physische Widerstandsfähigkeit gegenüber Bedrohungen wie Naturgefahren, Terroranschlägen, versehentlichen oder absichtlichen Beschädigungen/Angriffen zu stärken. Diese Gesetzgebung stellt damit erstmals eine einheitliche, bundesgesetzliche, sektorenübergreifende Maßnahme zur Stärkung der Resilienz von kritischer Infrastruktur dar. Unter Resilienz versteht das KRITIS-DachG dabei die Fähigkeit des Betreibers einer kritischen Anlage, einen Vorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, ihn abzuwehren und die Folgen eines solchen Vorfalls zu begrenzen.

Der Gesetzgebungsprozess, der sich seit dem ersten Referentenentwurf vom 25. Juli 2023 erheblich in die Länge gezogen hatte, ist nun beinahe abgeschlossen. Das KRITIS-DachG wurde im September 2025 vom Bundeskabinett beschlossen und am 29. Januar 2026 nach weiteren Änderungen durch den Innenausschuss im Bundestag angenommen. Für ein Inkrafttreten bedarf es somit nur noch der Zustimmung des Bundesrates und mit der Verkündung ist somit jederzeit zu rechen.

Neben die Schutzrichtung des KRITIS-DachG tritt zudem das bereits im Dezember 2025 in Kraft getretene NIS2-Umsetzungsgesetz (NIS2-UmsG). Wäh-

rend das KRITIS-DachG ausschließlich auf den physischen Schutz kritischer Anlagen abzielt, bezweckt das NIS2-UmsG die Erhöhung der Cybersicherheit kritischer Anlagen, indem es die Netzwerk- und Informationssicherheit adressiert.

Betroffene Sektoren

Die erste Weichenstellung für Netzbetreiber betrifft die Frage, ob man überhaupt vom Anwendungsbereich des KRITIS-DachG erfasst ist. Durch die Regelung werden – anders als im NIS2-UmsG – ausschließlich Kritische Infrastrukturen sowie Kritische Anlagen in die Pflicht genommen. Kritisch ist eine Anlage insbesondere dann, wenn sie der Versorgung der Allgemeinheit in den Sektoren Energie, Wasser und Telekommunikation dient und deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde. Der Schwellenwert, ab dem eine Anlage grundsätzlich als kritisch einzuordnen ist, beträgt laut § 5 Abs. 2 S. 2 KRITIS-DachG 500.000 von der Anlage versorgte Einwohner. Ob von dieser Einwohnerzahl auszugehen ist, wird durch eine separate, noch zu erlassende Rechtsverordnung bestimmt. Derzeit können die Werte der einschlägigen, erst im Dezember neu aufgelegten Verordnung für das NIS2-UmsG als Richtschnur dienen. Gemäß dieser sog. BSI-KritisVO gelten z. B. Gasverteilernetze ab 5.190 GWh/Jahr und Wassernetze ab einer verteilten Wassermenge von 22 Mio. m^3/Jahr als 500.000 Einwohner versorgend und damit als KRITIS.

Verpflichtungen für Betreiber kritischer Anlagen

Bezüglich des Pflichtenkanons sieht das KRITIS-DachG verschiedene, einander ergänzende Regelungen vor. Im Mittelpunkt für Netzbetreiber steht dabei die Frage, wie der physische KRITIS-Schutz insbesondere bei schwer zu überwachenden Großinfrastrukturen wie Stromtrassen, Wasserversorgungsnetzen oder Pipelines in der Praxis erreicht werden kann.
Die Betreiber treffen insbesondere folgende Pflichten:

a. Registrierungspflicht

Unternehmen müssen sich zunächst selbstständig als Betreiber kritischer Anlagen identifizieren und innerhalb von drei Monaten, nachdem eine Anlage als KRITIS gilt, beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das die national zuständige Behörde für die Resilienz Kritischer Anlagen wird, registrieren. Darüber hinaus muss eine Kontaktstelle zum BBK eingerichtet werden. Außerdem müssen Änderungen der registrierungspflichtigen Angaben an der Anlage innerhalb von zwei Wochen beim BBK gemeldet werden. Geänderte Werte des Versorgungsgrads sind wiederum einmal jährlich zu übermitteln.

b. Risikoanalyse

Betreiber müssen mindestens alle vier Jahre ab der Registrierung eine Risikoanalyse durchführen. Diese muss naturbedingte, klimatische und vom Menschen verursachte Risiken, die die Handlungsfähigkeit der Wirtschaft bedrohen – darunter vor allem gesundheitliche und alle wesentlichen Risiken für den Binnenmarkt und die Bevölkerung – berücksichtigen. Weiterhin werden Risiken der Verfügbarkeit der kritischen Dienstleistung durch Abhängigkeit von anderen Betreibern und anderen Sektoren in die Analyse mit aufgenommen.
Das BBK wird hierzu auf seiner Webseite Muster und weitere Hilfestellungen bereithalten.

c. Resilienzmaßnahmen

Kern der Pflichten, die das KRITIS-DachG für Betreiber vorsieht, umfasst die Regelung bezüglich der von Betreibern zu ergreifenden Resilienzmaßnahmen. Betreiber kritischer Anlagen sind verpflichtet, Maßnahmen zur Gewährleistung ihrer Resilienz zu treffen, um

- 1. das Auftreten von Vorfällen zu verhindern,
- 2. einen angemessenen physischen Schutz von Liegenschaften und kritischen Anlagen zu gewährleisten,
- 3. auf Vorfälle zu reagieren, sie abzuwehren und die negativen Auswirkungen solcher Vorfälle zu begrenzen und
- 4. nach Vorfällen die zügige Wiederherstellung der kritischen Dienstleistung zu gewährleisten.

Resilienzmaßnahmen umfassen damit also neben der Prävention auch die tatsächlichen Möglichkeiten der Abwehr eines physischen Angriffes sowie die Fähigkeit, die Folgen erfolgreicher Angriffe zu beseitigen.
Zur Umsetzung dieser Pflichten sieht das KRITIS-DachG keine sektoralen oder branchenspezifischen Regelungen, sondern lediglich abstrakte Vorgaben für geeignete und verhältnismäßige Maßnahmen zum physischen Infrastrukturschutz von den Betreibern kritischer Anlagen vor. Danach sind die Betreiber Kritischer Anlagen verpflichtet, geeignete und verhältnismäßige technische und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu treffen. Solche Maßnahmen sind verhältnismäßig, wenn der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls oder einer Beeinträchtigung der Kritischen Dienstleistung zu den Folgen ihres Ausfalls oder ihrer Beeinträchtigung angemessen erscheint. Um dieses Ziel zu erreichen, sind zusammenwirkende Maßnahmen erforderlich.
Das KRITIS-DachG enthält ein allgemeines, beispielhaftes Repertoire an solchen Maßnahmen, das aufgrund der Vielgestaltigkeit der Sachverhalte abstrakt gehalten ist. Enthalten sind z. B. Vorgaben zum Objektschutz,

Zugangskontrollen, sicheren Lieferketten, Zugangsberechtigungen und Übungen. Festzuhalten ist dabei, dass es Betreibern ermöglicht wird, auf branchenspezifische Resilienzstandards zurückzugreifen. Diese Branchenstandards müssen zwar eine BBK-Eignungsfeststellung bestehen und im Einvernehmen mit dem BSI durchgeführt werden, liefern Betreibern aber die Möglichkeit, sich an bestehenden anerkannten Resilienzstandards (z. B. DIN EN 17483 zum Schutz der KRITIS durch private Sicherheitsdienstleister) zu orientieren. Es ist zu erwarten, dass die einschlägigen Branchenverbände (z. B. DVGW, VDE) hier entsprechende Werke veröffentlichen.

Zur Einrichtung der gesetzlichen Resilienzmaßnahmen helfen den Betreibern darüber hinaus die Ergebnisse der oben unter Punkt b beschriebenen Risikoanalyse.

Letztlich unterliegt eine ausgewählte Resilienzmaßnahme stets der Abwägung zwischen Wirtschaftlichkeit, Eintrittswahrscheinlichkeit und Schadensausmaß, sodass regelmäßig die Gebotenheit einer Resilienzmaßnahme vom Einzelfall abhängen wird. Wichtig ist aus Betreibersicht, die getroffene Abwägung für den Schadensfall möglichst genau zu dokumentieren.

Dass die mit Blick auf die aktuelle Bedrohungslage sinnvollen Schutzmaßnahmen darüber hinaus auch rechtlichen Restriktionen unterliegen, zeigt ein Blick auf die aktuelle Handhabung des Drohnenschutzes. Kaum ein sicherheitspolitisches Thema hat eine ähnliche Brisanz entwickelt und zugleich die strukturelle Verwundbarkeit zentraler Infrastruktur so deutlich offengelegt. Die Abwehr von unerlaubten und gefährdenden Drohnen ist dabei weiterhin eine polizeiliche Aufgabe und die normierte Befugnis zum eigenständigen Schutz vor unbemannten Luftfahrzeugen wurde nicht an private Betreiber abgegeben. Vielmehr bleibt es bei der dargestellten, abstrakt gehaltenen Pflicht zur Durchführung von Resilienzmaßnahmen. Es ist Netzbetreibern somit weiterhin unmöglich, sich Spionagedrohnen eigenständig zu entledigen. Dennoch ist eine Mitwirkung der Netzbetreiber bei der Drohnenabwehr nicht ausgeschlossen. Insbesondere trifft die Betreiber bei Spionagemaßnahmen eine Meldepflicht (siehe dazu unten unter Punkt e).

d. Resilienzplan

Außerdem sind die Resilienzmaßnahmen in einem Resilienzplan zu dokumentieren. Hierdurch sollen die den Maßnahmen zugrunde liegenden Erwägungen dargelegt und ein Bezug zur Risikoanalyse und Bewertung genommen werden. Dies dient insbesondere der erforderlichen Darstellung der vorgesehen Maßnahmen durch die Betreiber gegenüber dem BBK.

e. Meldepflicht

Abschließend sind Betreiber kritischer Anlagen verpflichtet, Vorfälle, die die Erbringung kritischer Dienstleistungen erheblich stören oder erheblich stören könnten, unverzüglich an eine von BBK und BSI gemeinsam eingerichtete Meldestelle zu melden; Einzelheiten zum Meldeverfahren werden auf der BBK-Webseite veröffentlicht. Der Inhalt der Meldung umfasst dabei die Anzahl und Anteil der von der Störung Betroffenen, die bisherige und voraussichtliche Dauer der Störung sowie das voraussichtlich betroffene geografische Gebiet der Störung.

Für den Erfolg von Abwehrmaßnahmen ist dabei der Faktor Zeit entscheidend. Deshalb muss bereits innerhalb der ersten 24 Stunden nach Kenntnisnahme des Vorfalls eine erste Meldung abgegeben werden. Spätestens einen Monat danach wird ein ausführlicher Bericht fällig.

Zuständigkeiten und Zusammenarbeit von Netzbetreibern und Behörden

Die zentrale Anlaufstelle für die ordnungsgemäße Anwendung und erforderlichenfalls die Durchsetzung des KRITIS-DachG ist das BBK. Neben dem BBK sind überdies in verschiedenen Sektoren ausgewählte Behörden für die Umsetzung des KRITIS-DachG verantwortlich. So trifft diese Kompetenz im Sektor Gas- und Stromversorgung beispielsweise die Bundesnetzagentur. Welche Zuständigkeiten sich in einem Katastrophenfall zwischen Betreibern und anderen Behörden des Katastrophenschutzes ergeben, ist durch das KRITIS-DachG jedoch nicht abschließend geregelt. Sicher ist nur, dass in Katastrophenfällen Abläufe schnell, effizient und unkompliziert umgesetzt werden müssen. Wie sich bereits in der Handhabung des Drohnenschutzes gezeigt hat, hat es der Gesetzgeber jedoch vermieden, durch das KRITIS-DachG konkrete Verpflichtungen und Befugnisse zwischen Betreibern und staatlichen Behörden aufzuteilen.

Dies demonstriert die inhaltliche Spannung, die dem Gesetz zu Grunde liegt: Auf der einen Seite steht der Staat, dem es grundsätzlich obliegt, wichtige gesellschaftliche Funktionen aufrechtzuerhalten, der gleichzeitig aber weder über die Ressourcen noch die Expertise verfügt, um die Resilienz der kritischen Einrichtungen zu gewährleisten. Auf der anderen Seite stehen die Betreiber, die über Resilienzmaßnahmen oft im Rahmen einer Kosten-Nutzen-Abwägung entscheiden und so ggf. hinter vom Gesetzgeber gewünschten Sicherheitsniveaus zurückbleiben.

Das gilt insbesondere auch in Bezug auf den Schutz vor terroristischen oder militärischen Angriffen durch Drittstaaten. Ausreichende Resilienzmaßnahmen sind für viele Betreiber hier nur unter unverhältnismäßig hohem Aufwand zu erreichen.

Dies macht deutlich, dass die Aufgaben der verschiedenen zivilen und staatlichen Akteure im Bereich der Gefahrenabwehr und des Bevölkerungsschutzes in Bezug auf den Schutz kritischer Einrichtungen im KRITIS-DachG klarer definiert werden sollten. Modelle, die diese Rollenverteilung im Wege der Öffentlich-Privaten Partnerschaften oder Ansätzen der Selbstregulierung im Sinne einer corporate social responsibility, in der die Resilienz kritischer Einrichtungen als öffentliches Gut verstanden wird, zu lösen versuchen, wurden dabei bislang nicht in das Gesetz aufgenommen – eine Ausnahme bilden die kommenden, bereits angesprochenen technischen Regelwerke der einschlägigen Fachverbände, die voraussichtlich an der ein- oder anderen Stelle für Klarheit sorgen können; zumindest für Gas- und Stromleitungen haben diese über § 49 Abs. 2 EnWG fast Gesetzesrang.

Fazit und Handlungsempfehlungen

Es ist damit zu rechnen, dass Angriffe auf Europas kritische Infrastrukturen weiter zunehmen werden. Insbesondere, weil die konkrete Rollenverteilung in Katastrophenfällen durch das KRITIS-DachG nicht eindeutig zugewiesen ist, ist für Netzbetreiber eine proaktive Zusammenarbeit mit staatlichen Behörden ratsam. Überdies ist bei der Umsetzung von Resilienzmaßnahmen sowie in tatsächlichen Katastrophenfällen die Information und Zusammenarbeit mit lokalen und nationalen Polizeibehörden aufgrund der diesen zustehenden, weitreichenden Befugnisse zweckmäßig. Außerdem gilt es derzeit, diejenigen Risiken auszuschließen, die sich aus Netzbetreibersicht bereits abstellen oder wenigstens verringern lassen.

Wie oben angesprochen, gibt es bereits technisches Regelwerk, das (auch) auf den physischen Schutz von Anlagen abzielt und in dessen Umsetzung spätestens jetzt eingetreten werden sollte. Es ist davon auszugehen, dass vorerst bereits praxiserprobte und belastbare Vorgehensweisen als Orientierungshilfe für Resilienzmaßnahmen der Betreiber im Vordergrund stehen werden. Als präventive Maßnahmen stehen daher die Überprüfung der physischen Sicherheitsvorkehrungen und Videoüberwachung der Zaunsysteme zumindest an „überschaubaren“ Stellen im Netz wie z. B. Gas-Druckregelstationen oder Umspannwerken im Mittelpunkt. Insbesondere sollten dabei nach Möglichkeit auch manuell bedienbare Elemente wie beispielsweise Handräder ersetzt werden. Auch sind Netzbetreiber zu einer engen Zusammenarbeit mit der Bundespolizei und lokalen Polizeibehörden angehalten. Denn diese verfügen nicht nur über die Expertise in der Handhabung der Überprüfung verschiedener Sicherheitssysteme. Durch die Zusammenarbeit werden die Polizeibehörden auch auf die Relevanz der Anlagen aufmerksam gemacht und sind so in der Lage, in Ernstfällen ihre gesetzgeberisch übertragenen Kompetenzen auszuüben, um tatsächlichen Gefahren zu begegnen.

Darüber hinaus lassen sich Risiken im Rahmen einer Gefahrenabwehr insbesondere gegen fahrlässiges Handeln Dritter bereits jetzt durch verschiedene Maßnahmen effektiv verringern. Hierzu zählt z. B. eine sichere Beauskunftung unterirdischer Infrastruktur im Zuge von Baumaßnahmen über einen allgemein bekannten Eingang wie das Auskunftsportal der Netzbetreibergenossenschaft BIL eG, der zugleich eine restriktive/kleinflächige Beantwortung durch den Betreiber selbst nach dessen eigenen Sicherheitsstandards ermöglicht. Eine Mitwirkung hier schützt darüber hinaus vor induktiven Beeinflussungen der eigenen Infrastruktur durch Hoch- und Höchstspannungsleitungen in der Nähe, da ein großer Teil der Hoch- und Höchstspannungsnetzbetreiber bereits jetzt die gemeinsam mit der BIL eG entwickelte Funktion der „Spannfeldanalyse“ zur Auffindung potenziell beeinflusster Rohrleitungen nutzt. Hinzu tritt der Zugriff auf netzgebietsspezifische Katastrophenwarnungen in Kooperation mit KATWARN/NINA sowie eine Koordinierung von Leitungsbaumaßnahmen in Zusammenarbeit mit dem Infrastrukturatlas der Bundesnetzagentur.

SCHLAGWÖRTER: KRITIS-Dachgesetz, Schutz kritischer Infrastrukturen, Resilienz kritischer Anlagen, Risikoanalysen und Meldepflichten

AUTOREN

RA **Markus Heinrich**
Wolter Hoppenberg, Köln, und Vorstand der BIL eG, Bonn
Tel. +49 221 272686-475
heinrich@wolter-hoppenberg.de

Cosmo Grühn
Wolter Hoppenberg Rechtsanwälte Partnerschaft mbB, Hamm