Downloaded from Blogs on 24.10.2026 20:42

Öffentlicher Sektor - Zukunft gestalten Blog
By PwC Deutschland | 21 October 2026

Neue Resilienzpflichten für die öffentliche Hand

Das KRITIS-Dachgesetz schafft neue Pflichten für Betreiber kritischer Infrastrukturen, lässt aber auch wichtige Fragen offen

Downloaded from Blogs on 24.10.2026 20:42

Anfang Januar 2026 fiel in Teilen Berlins der Strom aus. Mitten im Winter! Tagelang waren rund 45.000 Haushalte und etwa 2.200 Unternehmen im Südwesten der Hauptstadt ohne Strom und Heizung. Ursache war ein Brandanschlag auf eine Kabelbrücke im Stadtteil Lichterfelde, der mehrere Hochspannungskabel schwer beschädigte. Das war der längste Blackout in Berlin seit Gründung der Bundesrepublik. Vor solchen und ähnlichen Angriffen auf kritische Infrastrukturen soll das KRITIS-Dachgesetz (KRITIS-DachG) schützen. Es ist im März 2026 in Kraft getreten. Mit dem Gesetz setzt Deutschland die europäische Critical-Entities-Resilience(CER)-Richtlinie (EU) 2022/2557 in nationales Recht um und ergänzt das geltende Network-Information-Security (NIS)-2-Umsetzungsgesetz.

Physische Resilienz kritischer Infrastruktur sicherstellen

Dem KRITIS-Dachgesetz zufolge müssen Betreiber kritischer Infrastrukturen neben der digitalen nun auch die physische Resilienz ihrer Anlagen sicherstellen. Die Anlagen mussten sie bis zum 17. Juli 2026 beim zuständigen Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) registrieren. Bundesweit betrifft das KRITIS-DachG rund 2.000 Betreiber. Weil die öffentliche Hand oft selbst kritische Anlagen betreibt, bringt das neue Gesetz auch für sie relevante Änderungen.

Für viele der vom KRITIS-Dachgesetz betroffenen Bereiche sind die Kommunen verantwortlich. In Deutschland sind es meist die Stadtwerke, die die Energie-, Wasser- und Abwassernetze betreiben. So vertritt der Verband kommunaler Unternehmen (VKU) mehr als 1.600 kommunale Unternehmen. Die VKU-Mitglieder halten beim Trinkwasser einen Marktanteil von rund 88 Prozent. Bei Wärme sind es 72 Prozent, bei Strom 66 Prozent. Die öffentliche Hand ist damit nicht nur Aufsicht, sondern selbst Verpflichtete.

Geschäftsleitungen haften bei Versäumnissen persönlich

Das Gesetz definiert zehn Sektoren – die öffentliche Verwaltung gehört nicht dazu (§ 4 Abs. 1). Erstmals erfasst es aber eng definierte Einrichtungen der Bundesverwaltung über einen Sonderweg (§ 7). Dazu zählen nur das Bundeskanzleramt, die Bundesministerien und die oder der Beauftragte der Bundesregierung für Kultur und Medien. Grundsätzlich müssen Geschäftsleitungen die Resilienzmaßnahmen beschließen und deren Umsetzung sicherstellen. Bei Versäumnissen haften sie persönlich nach § 43 GmbHG bzw. § 93 AktG. Behördenleitungen gelten jedoch nicht als Geschäftsleitung – sie trifft diese Haftung also nicht (§ 2 Nr. 11).

Selbst die Bundesverwaltung erfasst das Gesetz nicht vollständig: Das Auswärtige Amt und das Verteidigungsministerium sind weitgehend ausgenommen (§ 7 Abs. 1). Länder und Kommunen hat der Gesetzgeber überhaupt nicht ausdrücklich adressiert. Vor genau dieser Lücke hatten Sachverständige in der Anhörung zum Gesetz gewarnt. Sie kritisierten, dass für die Daseinsvorsorge und den Verwaltungsvollzug keine verbindlichen Vorgaben gelten.

Länderöffnungsklausel erlaubt regionales Nachschärfen

Vom KRITIS-Dachgesetz betroffen sind grundsätzlich Betreiber kritischer Infrastrukturen, die typischerweise mindestens 500.000 Menschen versorgen. Der Deutsche Landkreistag beispielsweise hält diese Grenze für

Downloaded from Blogs on 24.10.2026 20:42

zu hoch angesetzt. Denn gerade in ländlichen Regionen lägen viele Versorger unterhalb dieser Schwelle. Ihre Anlagen seien dennoch kritisch für die Versorgung. So würde das Gesetz relevante Strukturen zunächst nicht erfassen. Die Länder haben allerdings Gestaltungsspielraum: Sie dürfen kritische Anlagen, die allein in ihrer Zuständigkeit liegen, selbst identifizieren. Rechtsgrundlage ist die Länderöffnungsklausel in § 5 Abs. 7 des KRITIS-Dachgesetzes. So lässt sich der Schutz regional nachschärfen.

Für die Praxis außerdem relevant: Aufwendige Schutzmaßnahmen umzusetzen, erfordert erhebliche Investitionen. Vor allem kleinere kommunale Unternehmen stoßen dabei an organisatorische und finanzielle Grenzen. Deshalb fordert der VKU praxistaugliche Fristen, klare Zuständigkeiten und eine gesicherte Refinanzierung. Die kommunalen Spitzenverbände halten höhere Sicherheitsstandards für dringend erforderlich, sehen deren Umsetzung jedoch nur bei verlässlicher Finanzierung als realistisch an. Dies verlangt auch der Landkreistag.
Betreiber kritischer Infrastrukturen müssen sicherheitsrelevante Vorfälle künftig an das BBK melden. Für sie werden dadurch klare Meldeketten und eine saubere, nachvollziehbare Dokumentation wichtiger. Sachverständige fordern zudem gemeinsame Lagebilder und abgestimmte Standards auf allen Verwaltungsebenen.

Erste Risikoanalyse bis spätestens Mitte April 2027

Nach der Registrierung folgt ein enger Fahrplan: Die erste Risikoanalyse müssen Betreiber kritischer Infrastrukturen spätestens neun Monate nach der Registrierung vorlegen, also spätestens Mitte April 2027. Die Resilienzmaßnahmen, der Resilienzplan und das Meldewesen greifen zehn Monate nach der Registrierung, also spätestens Mitte Mai 2027. Danach müssen Betreiber kritischer Infrastrukturen die Risikoanalyse alle vier Jahre wiederholen. Die Aufsicht und die Sanktionen werden allerdings erst ab dem Jahr 2027 vollumfänglich wirksam. Wichtig ist außerdem: Für viele KRITIS-Betreiber gilt automatisch auch die NIS-2-Richtlinie, die die Cyber- und Informationssicherheit regelt. Das erhöht die Komplexität – und die Dringlichkeit, beide Regularien integriert zu betrachten. (Kommunale) Betreiber sollten daher die für sie geltenden NIS-2- und KRITIS-Pflichten früh harmonisieren, um Doppelstrukturen zu vermeiden.

Ansprechpartner:
Dr. Nicolas Sonder

Zu weiteren PwC Blogs

Keywords

Digitalisierung, Netzbetreiber, Stromnetz

Downloaded from Blogs on 24.10.2026 20:42

Contact

Prof. Dr. Rainer Bernnat

Frankfurt am Main

rainer.bernnat@pwc.com