Schutz Kritischer Infrastrukturen

Rückenwind durch KRITIS-Dachgesetz?

[16.12.2024] Das KRITIS-Dachgesetz (KRITIS-DachG) stellt neue Anforderungen an den Schutz Kritischer Infrastrukturen. Das Unternehmen EnBW begegnet den Herausforderungen unter anderem durch ein Risikofrüherkennungssystem und die Erstellung von Resilienzplänen.

Seien es der russische Angriffskrieg auf die Ukraine, der Terrorangriff der Hamas auf Israel und die damit entstandene Eskalation der Sicherheitslage im Nahen Osten, der Sabotageakt gegen die Nord-Stream-Pipelines, radikale Klimaaktivisten oder die Cyberattacke auf die Stadtwerke Karlsruhe und auf den für Deutschlands Infrastruktur wichtigen Dienstleister PSI Software: Die hybride Bedrohungslage führt vor Augen, mit welchen Auswirkungen sich insbesondere offene, demokratische Gesellschaften auseinandersetzen müssen.

Um angemessen auf die hybride Bedrohungslage zu reagieren, gab es bereits im Jahr 2008 Bestrebungen seitens der EU-Kommission, entsprechende Rechtsakte zu implementieren. Zu der zweigleisigen Sicherheitsstrategie aus dem Jahr 2020 gehören die CER-Richtlinie (CER-RL) sowie die zweite Richtlinie zur Netz- und Informationssicherheit (NIS2-RL). Die Mitgliedstaaten wären verpflichtet gewesen, die Richtlinien bis zum 17. Oktober 2024 in nationales Recht zu überführen. Das Bundesinnenministerium hat 2022 mit seiner Resilienzstrategie ein Rahmenwerk vorgelegt, um die gesamtgesellschaftliche Widerstandsfähigkeit gegen ein breites Krisenspektrum und die Resilienz gegenüber militärischen und hybriden Bedrohungen zu stärken. Im August 2024 betonte Innenministerin Nancy Faeser im Handelsblatt: „Die Bedrohungen, gegen die wir uns schützen müssen, reichen von Spionage, Sabotage und Cyberattacken bis hin zu Staatsterrorismus.“ Der deutsche Gesetzgeber plant daher nun die Überführung der CER-RL in nationales Recht durch ein Dachgesetz zum Schutz Kritischer Infrastrukturen (KRITIS-DachG). Dieses zielt darauf ab, unklare Zuständigkeiten zu ordnen und die Behördenvielfalt im föderalen System durch sinnvolle enge Vernetzung handhabbar zu gestalten – daher der Begriff Dach.

Risiken frühzeitig erkennen

Regelmäßige Risikoanalysen (Risikoidentifikation und -bewertung) seitens des Staates (nationale Risikoanalyse) und der KRITIS-Betreiber sind eine der Neuerungen, die der Referentenentwurf beinhaltet. Dabei soll die nationale als Grundlage für die betreiberseitige Risikoanalyse dienen, und der Erhebungsradius der Risiken soll einem so genannten All-Gefahren-Ansatz folgen. Der Gesetzgeber verspricht sich hiervon eine umfassende, sektorübergreifende Erhöhung des Schutzniveaus.

Für kapitalmarktorientierte Unternehmen sowie für die allgemeinen gesetzlichen Sorgfaltspflichten eines ordentlichen Geschäftsführers ist ein Risikomanagement verpflichtend durchzuführen. Beim Energieversorger EnBW Energie Baden-Württemberg hat das unternehmensseitig integrierte Risikofrüherkennungssystem – eine erste von vier wesentlichen Komponenten – zum Ziel, bestandsgefährdende Risiken frühzeitig zu erkennen. Neben diesem Baustein gibt die in das Business Continuity Management integrierte Business-Impact-Analyse Aufschluss über besonders schützenswerte, für den Konzern kritische Prozesse – seine so genannten Kronjuwelen.

Synergien sinnvoll nutzen

Im Bereich der Informationssicherheit und IT erfolgt eine Werteinventarisierung mit Blick auf die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Die Konzernsicherheit erhebt Schutzbedarfe hinsichtlich des physischen Schutzes Kritischer Infrastrukturen anhand einer Schutzbedarfsanalyse. All diese verschiedenen Blickwinkel gilt es so zu verknüpfen, dass sie insgesamt der perspektivisch geforderten Risikoanalyse des KRITIS-DachG genügen und Synergien sinnvoll genutzt werden.

Der Referentenentwurf beinhaltet darüber hinaus die Erstellung von Resilienzplänen durch die Betreiber. Zehn Monate nach Registrierung sind Betreiber kritischer Anlagen dazu verpflichtet, verhältnismäßige und geeignete Maßnahmen zur Gewährleistung ihrer Resilienz zu treffen. Auch hier sollen perspektivisch Synergien genutzt und bestehende Maßnahmen aus den zuvor benannten Bereichen, wie beispielsweise der Informationssicherheit, und gegebenenfalls weiteren Fachbereichen, wie der Arbeitssicherheit oder dem Umweltmanagement, in gemeinsamen Resilienzplänen zusammengeführt werden. Maßnahmen etwa aus dem Fachbereich der Konzernsicherheit werden stets sorgfältig in Kooperation mit den Risikoverantwortlichen der Geschäftsbereiche abgewogen. Darüber hinaus wird in Abstimmung mit den zuständigen Behörden über notwendige und verhältnismäßige Maßnahmen beraten. Die Ermittlung neuralgischer Knotenpunkte im Bereich der maritimen Kritischen Infrastruktur ist zum Beispiel Aufgabe der Betreiber. Überwachungsmaßnahmen etwa zum Schutz der maritimen Kritischen Infrastruktur zu ergreifen, ist wiederum Aufgabe der Bundespolizei.

Finale Verabschiedung abwarten

Als Betreiber Kritischer Infrastrukturen bewegt sich die EnBW per se bereits auf einem hohen Resilienz-niveau: Mitarbeitende, Konzepte und Prozesse sind darauf trainiert und ausgelegt, Störungen zu minimieren und diese, sollten sie wider Erwarten auftreten, in ihren Auswirkungen schnell und auf technisch hohem Niveau zu kontrollieren. Dennoch ist die finale Verabschiedung des KRITIS-DachG durch den Gesetzgeber und die damit einhergehende Konkretisierung des aktuellen Referentenentwurfs abzuwarten, damit eine vollumfängliche Prüfung im Hinblick auf das Erreichen der konkreten Anforderungen durch die bereits etablierten Maßnahmen erfolgen kann.

Wichtig ist, die ohnehin großen Herausforderungen der Energiewende vor allem unter dem Aspekt der Versorgungssicherheit immer mitzudenken, um perspektivisch auch eine sektorübergreifende Resilienz zu erreichen.

()

Der Beitrag ist im Schwerpunkt Schutz Kritischer Infrastrukturen der Ausgabe November/Dezember 2024 von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Informationstechnik, EnBW, KRITIS, KRITIS-Dachgesetz (KRITIS-DachG)