KRITIS-Schutz

Resilienz ist Pflicht

[18.08.2026] Mit dem KRITIS-Dachgesetz sind Städte und Gemeinden unter Zugzwang: Bis Mai 2027 müssen Schutzkonzepte stehen. Doch zwischen gesetzlicher Pflicht und gelebter Resilienz klafft häufig noch eine gefährliche Lücke.

Wenn heute das Thema Sicherheit aufkommt, richtet sich der Blick fast reflexhaft auf militärische Fähigkeiten, Rüstungsausgaben, NATO-Verpflichtungen und die zahlreichen geopolitischen Konflikte. Dabei hängt die Resilienz moderner Gesellschaften auch maßgeblich vom zivilen Alltag ab, beispielsweise von der Funktionsfähigkeit zentraler Versorgungs- und Steuerungssysteme.

Kritische Infrastrukturen bilden das Rückgrat wirtschaftlicher und gesellschaftlicher Prozesse. Sie sind das stille Versprechen des modernen Staates an seine Bürger: Wir kümmern uns darum, dass alles Nötige funktioniert. Angesichts gezielter Sabotageakte, Cyber-Angriffen, terroristischer Gefahren und extremer Wetterereignisse steht dieses Versprechen unter Druck. Denn fällt eine kritische Schaltstelle in der Energieversorgung, in Pumpstationen, Leitwarten oder Rechenzentren aus, können Versorgungsengpässe, wirtschaftliche Schäden und erhebliche Störungen der öffentlichen Sicherheit entstehen.

Neuer All-Gefahren-Ansatz

Mit dem KRITIS-Dachgesetz entsteht erstmals ein einheitlicher, sektorübergreifender Rechtsrahmen, der bis zum 17. Mai 2027 die Umsetzung konkreter Schutzmaßnahmen verlangt. Jede Führungskraft in der kommunalen Versorgungswirtschaft sollte sich mit den praktischen Auswirkungen, den größten Verwundbarkeiten und den Anforderungen an eine belastbare Risikoanalyse vertraut machen.

Mit dem KRITIS-Dachgesetz (KRITISDachG) wird die EU-CER-Richtlinie in deutsches Recht umgesetzt. Damit wird ein fundamentaler Paradigmenwechsel in Sicherheitsfragen eingeleitet. Im Gegensatz zu bisherigen Regelungen verfolgt das neue Regelwerk einen All-Gefahren-Ansatz. Dieser berücksichtigt und behandelt Naturkatastrophen, physische Sabotageakte, Terroranschläge und Cyber-Angriffe gleichrangig.

Für Betreiber Kritischer Infrastrukturen in Sektoren wie Energie, Wasser, Gesundheit, Transport und Telekommunikation ergeben sich daraus verbindliche Pflichten: Sie müssen Risiken strukturiert erfassen und analysieren, umfassende Schutzkonzepte erarbeiten, ein Meldesystem für Störungen etablieren, regelmäßige Audits durchführen und nachweisen, dass ihre getroffenen Resilienzmaßnahmen wirksam sind.

Bestandsaufnahme als Anfang

Betreiber Kritischer Infrastrukturen müssen die Sicherheit ihrer Anlagen und Prozesse systematisch überprüfen und stärken. In der Praxis beginnt dies stets mit einer Bestandsaufnahme: Welche kritischen Schutzgüter besitzt das Unternehmen? Welche Anlagen, Systeme und Prozesse sind für die Erbringung der Versorgungsleistung unverzichtbar? Dabei müssen physische Anlagen ebenso berücksichtigt werden wie IT-Systeme oder Betriebsmittel, deren Ausfall die Erbringung der kritischen Dienstleistung unmittelbar

gefährden würde.

In der Energieversorgung zählen dazu beispielsweise Schalt- und Messanlagen, Speicher oder zentrale Netzknoten. Auch dezentral gelegene, unbesetzte Trafostationen und Netzübergabepunkte gelten als kritisch. Darüber hinaus sollten IT- und OT-Systeme, wie beispielsweise Netzleittechnik oder SCADA-Systeme, sowie personelle Schlüsselressourcen in Leitstellen und Bereitschaftsdiensten auf den Prüfstand gestellt werden. Gleiches gilt für externe Abhängigkeiten, etwa von der Telekommunikation, der Notstromversorgung, Treibstoffen oder spezialisierten Dienstleistern.

Risiken bewerten

Auf die erste Bestandsaufnahme folgt eine strukturierte Risikobeurteilung, beispielsweise nach ISO 31000. Dabei werden mögliche Bedrohungen systematisch identifiziert, analysiert und bewertet. Ferner müssen künftig sämtliche Risiken erfasst werden, die den Betrieb kritischer Anlagen beeinträchtigen können. Dazu zählen zum Beispiel Sabotage und Vandalismus an Umspannwerken, Trafostationen oder Netzverteilstationen ebenso wie der Diebstahl von Kupfer oder Metallteilen, die Manipulation von Anlagen oder unbefugter Zutritt zum Betriebsgelände. Zudem gewinnen Cyber-Angriffe auf Netzleitstellen, SCADA-Systeme oder Fernwirktechnik, über die Strom- und Wärmenetze gesteuert werden, zunehmend an Relevanz.

Nur so ergibt sich ein realistisches Lagebild, das im nächsten Schritt die Prognose von Eintrittswahrscheinlichkeiten für jedes identifizierte und analysierte Risiko sowie die Bewertung des potenziellen Schadensausmaßes ermöglicht. Dabei darf nicht allein die Klassifizierung der Gefahren im Vordergrund stehen, sondern es muss vielmehr eine Priorisierung für die Handlungsstrategie erfolgen. Von entscheidender Bedeutung ist die Frage, welche Störungen zu Versorgungsunterbrechungen oder großflächigen Ausfällen führen.

Ein besonderer Fokus sollte auf die sogenannten Kaskadeneffekte zwischen den verschiedenen Infrastrukturen gelegt werden. Ein Beispiel: Wenn ein Umspannwerk oder eine Netzleitstelle manipuliert wird und ausfällt, kann dies nicht nur große Teile der lokalen und regionalen Stromversorgung betreffen. Nach dem Domino-Prinzip können auch weitere abhängige Systeme in Mitleidenschaft gezogen werden, was eine Kette von Folgestörungen auslöst. So kann in einem Wasserwerk wegen eines Stromausfalls die Pumpentechnik stillstehen, was die Trinkwasserversorgung und den Druck im Netz beeinträchtigt.

Maßnahmen festlegen

Nachdem die Risikobeurteilung abgeschlossen ist, müssen geeignete und verhältnismäßige Schutzmaßnahmen definiert werden. Dabei ist das Zusammenspiel aus baulichen, technischen, organisatorischen und personellen Schritten entscheidend. Konkrete Maßnahmen können beispielsweise Zutrittskontrollen für Umspannwerke und Netzleitstellen sein. Im IT-Bereich sind die Segmentierung von IT- und OT-Systemen, sichere Fernzugänge sowie regelmäßige Sicherheitsupdates für Leittechnik und SCADA-Systeme empfehlenswert.

Auf organisatorischer Ebene sind belastbare Krisen- und Notfallpläne mit klaren Entscheidungs- und Eskalationswegen sowie personelle Maßnahmen, allen voran Sensibilisierungstrainings für die Mitarbeitenden, von Bedeutung. Es empfiehlt sich darüber hinaus, in wiederkehrenden Abständen Tests von Notfall- und Krisenplänen sowie Übungen für Beschäftigte in Leitstellen oder Netzbetriebszentralen durchzuführen.

()

• www.seccon-group.de
• Dieser Beitrag ist im Schwerpunkt KRITIS-Schutz der Ausgabe Juli/August 2026 von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Informationstechnik, KRITIS-Dachgesetz (KRITIS-DachG), Kritische Infrastrukturen (KRITIS), Resilienz, SecCon Group