

KRITIS

Von der Risikoanalyse zur Resilienz

[29.10.2026] Cyber-Angriffe, Naturgefahren und technische Ausfälle erhöhen die Risiken für Energieversorger. Ein ganzheitlicher Ansatz hilft, Risiken finanziell zu bewerten, Maßnahmen zu priorisieren und die Versorgung schneller wiederherzustellen.

Ransomware in der Leitwarte, ein sabotiertes Umspannwerk oder ein IT-Systemausfall beim vorgelagerten Dienstleister: Für Betreiber Kritischer Energie-Infrastrukturen ist die Frage längst nicht mehr, ob ein solches Ereignis eintritt, sondern wie schnell die Versorgung danach wieder stabil läuft. Strom- und Gasnetze, Wärmeversorgung und Lade-Infrastruktur sind hochgradig vernetzt und digital gesteuert und damit anfällig für Cyber-Angriffe, technisches Versagen und Wetterextreme. Geopolitische Spannungen, KI-gestützte Angriffe und die zunehmende Verschmelzung von IT- und OT-Systemen verschärfen die Lage zusätzlich. Ein einzelner Vorfall kann heute ganze Prozessketten lahmlegen und binnen Stunden zu einem regionalen Versorgungsausfall führen.

Mit dem KRITIS-Dachgesetz und der NIS2-Richtlinie wächst der regulatorische Druck auf Energieversorger. Während die NIS2-Richtlinie vor allem auf Cyber-Sicherheit abzielt, verlangt das KRITIS-Dachgesetz einen All-Hazards-Ansatz. Daher dürfen Risiken nicht mehr isoliert nach Zuständigkeit oder Fachbereich betrachtet werden, sondern müssen ganzheitlich und nachvollziehbar bewertet werden. Viele Unternehmen reagieren darauf zunächst mit dem Aufbau eines Informationssicherheits-Managementsystems (ISMS) oder dem Ausbau ihres Business Continuity Managements (BCM). Beides sind wichtige Bausteine, reichen jedoch allein nicht aus. Ein ISMS schützt vor allem die IT- und OT-Systeme, ein BCM sichert den Wiederanlauf, doch beide betrachten Risiken meist isoliert und zeigen nicht, wie sich Cyber-, Sach- und Lieferkettenrisiken gegenseitig verstärken. Wer KRITIS nur als Pflichtübung versteht, verpasst die eigentliche Chance: Resilienz, die über die Mindestanforderungen hinausgeht, schützt nicht nur vor Bußgeldern, sondern auch vor echten wirtschaftlichen Schäden, Reputationsverlust und Versorgungsausfällen.

Risiken vergleichen

Ein bewährter Ansatz zur Risikobetrachtung berücksichtigt vier Elemente: Exposures, also Menschen, Vermögenswerte, Daten, Prozesse und Infrastrukturen, deren finanzieller Wert nur so belastbar ist wie die zugrunde liegende Wertermittlung, gerade bei Umspannwerken, Trafostationen und Sondermaschinen mit sich stetig ändernden Wiederbeschaffungswerten; Hazards als natürliche, technische oder menschengemachte Gefahren; Controls als bestehende Schutzmaßnahmen; sowie das Event selbst, also die konkrete Betriebsstörung. Erst das Zusammenspiel dieser vier Faktoren veranschaulicht, wie kritisch ein Risiko ist. Für Energieversorger bedeutet das, Umspannwerke, Leitsysteme und Fernwirktechnik ebenso einzubeziehen wie Lieferketten, IT-Dienstleister und Mitarbeitende. Beyond Compliance bedeutet, Risiken so zu quantifizieren und zu steuern, dass Investitionsentscheidungen auf einer belastbaren Grundlage getroffen werden und nicht auf einer Checkliste beruhen.

Budgets gezielt lenken

Datenbasierte, quantitative Verfahren lösen zunehmend klassische qualitative Bewertungsraster ab. In Kombination mit bedrohungsspezifischen Datenquellen wie Cyber-Threat-Intelligence-Feeds und Schadendaten aus der Versicherungswirtschaft lässt sich der finanzielle Einfluss eines Cyber-Angriffs auf die Energieversorgung heute finanziell abschätzen. Das liefert Energieversorgern eine ökonomische Entscheidungsgrundlage, um Budgets für Resilienzmaßnahmen gezielt dorthin zu lenken, wo sie den größten Effekt erzielen, und macht Cyber-Sicherheit im Vorstand und in der Investitionsplanung verhandelbar.

Ein belastbares Sicherheitskonzept setzt genau an dieser Schnittstelle an. Der Erfahrung nach braucht es im Kern eine ehrliche Bestandsaufnahme der eigenen Cyber-Reife, von Governance- und Compliance-Bewertungen über Penetrationstests bis hin zu Phishing-Simulationen, Awareness-Schulungen und Krisenmanagementübungen für den Ernstfall. Ebenso entscheidend ist der Blick auf die physische Seite. Standorte müssen nach einheitlichen Kriterien auf Naturgefahren und bauliche Schwachstellen bewertet werden, um daraus konkrete Verbesserungsmaßnahmen abzuleiten. Wer zusätzlich die physischen Klimarisiken über das gesamte Portfolio hinweg aufzeigt, kann Anpassungsmaßnahmen dort priorisieren, wo sie den größten Effekt haben. Digitale Tools helfen schließlich dabei, dieses Bild nicht nur einmalig zu erstellen, sondern eigenständig und dauerhaft aktuell zu halten.

Vorgehen in vier Schritten

Ein belastbares Vorgehen folgt dabei typischerweise vier Schritten. Zunächst werden Gefahren, Risiken und bestehende Kontrollmaßnahmen an den relevanten Standorten identifiziert. Anschließend erfolgt die Risikoeinschätzung nach einheitlichen Kriterien wie Bauweise, Nutzung, Schutzmaßnahmen und externen Gefahren, ergänzt um eine Analyse möglicher Betriebsunterbrechungen. Darauf aufbauend werden die finanziellen Auswirkungen konkreter Verlustszenarien quantifiziert. Im letzten Schritt begleiten Risikoingenieure die Umsetzung priorisierter Verbesserungsmaßnahmen. Dieser Kreislauf aus Identifikation, Einschätzung, Quantifizierung und Verbesserung macht Resilienz zu einem kontinuierlichen Managementthema und nicht zu einer einmaligen Prüfung vor dem nächsten Audit.

Wiederbeschaffungswerte von Umspannwerken, Trafostationen, Leitsystemen und Sondermaschinen verändern sich kontinuierlich, etwa durch steigende Bau-, Material- und Montagekosten sowie laufende Investitionen. Wer seine Versicherungssummen nicht regelmäßig aktualisiert, riskiert im Schadenfall eine Unterversicherung oder zahlt unnötig hohe Prämien aufgrund von Überversicherung. Aus Sicht des Unternehmens Zurich Resilience Solutions braucht es dafür präzise Wertermittlungen für Gebäude, Maschinen und technische Einrichtungen, die je nach Bedarf auf Basis verfügbarer Objekt- und Marktdaten oder durch anerkannte Gutachter vor Ort erfolgen und sich an international anerkannten Standards orientieren. Wer seine Werte auf einer so belastbaren Grundlage ermittelt, kann im Schadenfall auf verlässliche Zahlen zurückgreifen. Physische und digitale Resilienz sind damit zwei Seiten derselben Medaille.

Energieversorger, die KRITIS-Anforderungen und NIS2 als Ausgangspunkt statt als Endpunkt begreifen, verschaffen sich einen echten Vorsprung. Wer Risiken ganzheitlich identifiziert, finanziell quantifiziert und auf Basis verlässlicher Vermögenswerte bewertet, trifft fundiertere Entscheidungen und ist im Ernstfall schneller wieder handlungsfähig. Beyond Compliance heißt am Ende, Sicherheit nicht als Kostenstelle, sondern als Wettbewerbsvorteil zu verstehen.

- Hier finden Sie weitere Informationen zu Zurich Resilience Solutions.

Dieser Beitrag ist im Schwerpunkt Cyber-Sicherheit der Ausgabe September/Oktober 2026 von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Informationstechnik, Cyber-Sicherheit, Kritische Infrastrukturen (KRITIS), Zurich Resilience Solutions Deutschland