Interview

Schocks absorbieren

[10.08.2026] Die Energiebranche fordert klare Regeln für den Schutz Kritischer Infrastrukturen. stadt+werk sprach mit Kerstin Andreae, BDEW, und Ingbert Liebing, VKU, über die Bedrohungslage und mögliche Wege zu höherer Sicherheit.

Frau Andreae, wie bewerten Sie aktuell die Verwundbarkeit des deutschen Energiesystems angesichts der gestiegenen sicherheitspolitischen Risiken?

Andreae: Das deutsche Energiesystem ist leistungsfähig und robust, aber die Verwundbarkeit ist angesichts der sicherheitspolitischen Lage real. Energie-Infrastrukturen sind heute mögliche Ziele von Sabotage, Cyber-Angriffen, Ausspähung und hybriden Bedrohungen. Ein weit verzweigtes Netz lässt sich nie an jedem Punkt vollständig schützen. Deshalb müssen wir Resilienz breit denken — also nicht nur Angriffe verhindern, sondern auch Schäden begrenzen und Versorgung schnell wiederherstellen. Hinzu kommt: Die hybride Lage ist auch rechtlich eine Herausforderung. Wir bewegen uns in einem Graubereich, das heißt, wir haben weder eine klassische Friedenslage noch einen Verteidigungsfall. Für diese Situation sind viele Zuständigkeiten, Befugnisse und Haftungsregeln bislang nicht ausreichend ausgelegt, etwa beim Informationsaustausch, bei der Drohnenabwehr oder dem Einsatz von Sicherheitsbehörden. Dafür braucht die Branche jetzt klare Regeln, eine wirksame Detektion und Abwehr von Drohnen, einen gesicherten Informationsaustausch mit den Sicherheitsbehörden und eine verlässliche Finanzierung zusätzlicher Schutzmaßnahmen.

Herr Liebing, teilen Sie diese Einschätzung – und wo sehen Sie aus kommunaler Perspektive die größten Risiken?

Liebing: Ja, grundsätzlich teile ich die Einschätzung. 100-prozentige Sicherheit gibt es nicht, gab es nie und wird es nie geben. Aber die Bedrohungslage hat sich deutlich verschärft. Es geht vor allem darum, sich bestmöglich auf die Szenarien vorzubereiten. Risiken bestehen vor allem bei der physischen Sicherung kritischer Punkte, bei Cyber-Angriffen auf operative Systeme sowie bei Engpässen bei Personal und Material im Störfall. Hinzu kommen Abhängigkeiten von externen Dienstleistern und Lieferketten. Die Abwehr von Terrorangriffen und Anschlägen auf unsere Infrastruktur ist Aufgabe von Bund und Ländern, die das Gewaltmonopol innehaben. Stadtwerke sind weder die Polizei noch die Bundeswehr.

Sie betonen, dass ein vollständiger Schutz nicht möglich ist. Wie definieren Sie ein realistisches Zielniveau für Resilienz im Energiesystem?

Andreae: Resilienz im Energiesektor muss generell systemisch gedacht werden. Nur wenn alle einzelnen Bereiche ein hohes Maß an Resilienz erfüllen und wir auch die Wechselwirkungen zwischen Teilsystemen beachten, erreichen wir eine hohe Resilienz im Gesamtsystem. Wir brauchen daher einen Dreiklang aus Vorsorge, Vorbereitung auf effektive Krisenbewältigung sowie kontinuierlicher Analyse und Monitoring. Das sogenannte Business Continuity Management umfasst neben der Wiederherstellungsstrategie unter anderem eine vorausschauende Risikoanalyse und regelmäßige Übungen. Ziel muss ein Energiesystem sein, das Schocks absorbiert, sich schnell erholt und lernend anpasst, ohne Wettbewerbsfähigkeit und Klimaziele aus dem Blick zu verlieren. Resilienz ist die zentrale Voraussetzung für Versorgungssicherheit

und Souveränität.

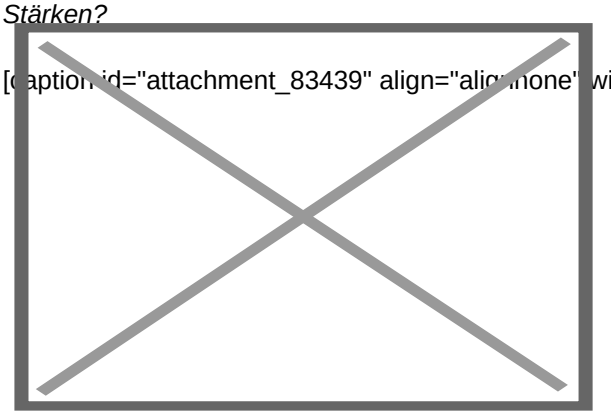
„100-prozentige Sicherheit gibt es nicht, gab es nie und wird es nie geben.“

Was muss getan werden, um den Schutz Kritischer Infrastrukturen zu verbessern?

Andreae: Um den KRITIS-Schutz zukunftssicher aufzustellen, sind klare Zuständigkeiten, vereinfachte Nachweise und Bürokratieabbau ebenso notwendig wie eine praxistaugliche Umsetzung der NIS2- und CER-Richtlinien. EU-Standards für die IT-Sicherheit digitaler Komponenten sind essenziell und sollten handelspolitisch flankiert werden. IT-Prozesse müssen mit betrieblichen Abläufen ganzheitlich gedacht werden.

Was bedeutet dieses Ziel konkret für kommunale Versorger – wo liegen deren Grenzen, aber auch ihre Stärken?

[caption id="attachment_83439" align="alignnone" width="300"]



Ingbert Liebing (Bildquelle: VKU / Felix Krumbholz Photography)[/caption]

Liebing: Resilienz braucht meiner Meinung nach Dezentralisierung. Die dezentrale Organisation der Verteilnetzbetreiber stärkt beispielsweise die Resilienz des Stromsystems. Bildlich gesprochen: In den Verteilnetzen steuert nicht nur ein Server das System, sondern viele. Ein erfolgreicher Angriff auf einen Server, über den zentral die gesamte Stromversorgung gesteuert würde, würde immer mehr Schaden anrichten als ein gelungener Angriff auf einen Server, der nur eines von vielen hundert Netzen steuert. Deshalb baut die Ukraine gerade ihr bisher sehr zentralistisches Energiesystem hin zur Dezentralität um.

Wo sehen Sie Stärken und Schwächen der Stadtwerke beim Thema Schutz Kritischer Infrastrukturen?

Liebing: Eine Stärke der Stadtwerke und Verteilnetzbetreiber ist die Nähe zu den kommunalen Entscheidern und ihre regionale Vernetzung. Kommunale Versorger können im Ernstfall schnell reagieren und kennen ihre Infrastruktur genau. Grenzen liegen bei Ressourcen, steigender Komplexität und teils widersprüchlichen Vorgaben. Resilienz gelingt daher vor allem im Zusammenspiel: mit Kooperationen, klaren Regeln und praktikablen Standards.

„Resilienz im Energiesektor muss systemisch gedacht werden.“

Welche Lehren zieht die Energiebranche aus dem Stromausfall Anfang des Jahres in Berlin, insbesondere für Prävention und schnelle Wiederherstellung?

Andreae: Die zentrale Lehre lautet: Die Umsetzung konkreter Resilienzmaßnahmen muss noch stärker priorisiert werden. Dazu gehören Schwachstellenanalysen, klar definierte Krisenprozesse, regional abgestimmte Unterstützungsstrukturen, ausreichende Reservematerialien, eine funktionierende Notfallkommunikation sowie rechtssichere Finanzierungswege. Denn am Ende zählt nicht nur der Grad unserer Vorbereitung, sondern vor allem, wie schnell wir nach einem Angriff die Versorgung wiederherstellen können.

Wie gut sind kommunale Unternehmen derzeit darauf vorbereitet, vergleichbare Krisen innerhalb kurzer Zeit zu bewältigen?

Liebing: Die Vorbereitung hat sich verbessert: Notfallpläne, Übungen und Krisenstrukturen sind vielerorts etabliert. Dennoch bleiben Herausforderungen: bei parallelen Störungen, bei Materialverfügbarkeit und durchaus auch bei eigentlich abgestimmten Abläufen mit externen Stellen. Wir sind gut unterwegs, aber es ginge noch besser. Wir haben dazu Vorschläge gemacht: Mobile Netzersatzanlagen, Blockheizkraftwerke und Gasturbinen im Umfang von mehreren einhundert Megawatt Leistung müssen über Deutschland verteilt in regionalen Versorgungssicherheitshubs vorgehalten werden. Ziel sollte sein, dass der Strom nach 24 Stunden zumindest provisorisch wieder fließt.

Der BDEW fordert eine Überprüfung der Transparenzpflichten. Wo sehen Sie aktuell sicherheitskritische Risiken durch zu weitgehende Offenlegung?

Andreae: Vorab möchte ich unterstreichen: Transparenz in einer Demokratie ist zu Recht ein sehr hohes Gut. Zugleich muss uns bewusst sein, dass öffentlich zugängliche Infrastrukturinformationen gezielt für Angriffe missbraucht werden können. Neue technologische Entwicklungen, zum Beispiel digitale Kartendienste und Anwendungen Künstlicher Intelligenz, machen zudem die systematische Auswertung solcher Daten immer einfacher. Wir sehen daher dringenden Handlungsbedarf, Transparenzanforderungen und Sicherheitsinteressen neu zu justieren. Dabei geht es nicht um generelle Abschaffung, sondern um eine Überprüfung und Abwägung.

Wie erleben kommunale Unternehmen diese Anforderungen im Alltag – und wo besteht aus Ihrer Sicht konkreter Anpassungsbedarf?

Liebing: Viele Unternehmen erleben einen Spagat zwischen Transparenz und Sicherheit. Teilweise werden sensible Informationen öffentlich, weil sie öffentlich bekannt gemacht werden müssen. Das erhöht das Risiko. Hier braucht es klarere und einheitliche Abwägungen: notwendige Transparenz ja, aber nur ohne zusätzliche Angriffsflächen.

Wie gut funktioniert aktuell die Zusammenarbeit zwischen Energieunternehmen, Staat und Sicherheitsbehörden?

Andreae: Die Zusammenarbeit zwischen Energieunternehmen, Staat und Sicherheitsbehörden ist in den vergangenen Jahren deutlich enger geworden und funktioniert bereits gut. Gerade etablierte Strukturen wie UP KRITIS zeigen, wie wertvoll ein vertrauensvoller, strukturierter Austausch zwischen Betreibern, Behörden und Staat sein kann. Solche Formate schaffen gemeinsame Lagebilder, stärken persönliche Netzwerke und helfen, Anforderungen aus der Praxis frühzeitig in staatliche Planungen einzubringen. Gleichzeitig hat der Anschlag auf das Berliner Stromnetz gezeigt, dass wir diese Zusammenarbeit weiterentwickeln müssen. Physische Angriffe, Drohnenüberflüge, Sabotage, Cyber-Angriffe und Desinformation lassen sich nicht mehr sauber voneinander trennen. Deshalb reicht es nicht, wenn Zusammenarbeit nur anlassbezogen oder in einzelnen Fachkreisen gut funktioniert. Wir brauchen

belastbare Schnittstellen, klare Zuständigkeiten und eingeübte Verfahren für den Ernstfall.

Was muss also getan werden?

Andreae: Aus Sicht der Energiebranche ist besonders wichtig, dass Informationen schneller, zielgerichteter und rechtssicherer fließen. Unternehmen brauchen frühzeitige, verwertbare Lage-Informationen von Sicherheitsbehörden. Umgekehrt müssen Betreiber Hinweise, Beobachtungen und Bedarfe einbringen können, ohne dass unklare Zuständigkeiten, Haftungsfragen oder Geheimschutzanforderungen den Austausch erschweren. Gerade beim Schutz sensibler Infrastrukturdaten, bei Drohnenvorfällen, bei Sicherheitsüberprüfungen und bei Krisenlagen unterhalb des Verteidigungsfalls besteht noch Anpassungsbedarf. Resilienz ist eine gemeinsame Aufgabe.

Herr Liebing, Sie sprechen von einer gesamtstaatlichen Aufgabe: Wo hakt es konkret in der Abstimmung zwischen Bund, Ländern und Kommunen?

Liebing: Herausfordernd sind vor allem unklare Zuständigkeiten und wenig eingeübte Abläufe in sehr komplexen Lagen. Für die Praxis ist entscheidend, schnell zu wissen, wer führt und wer unterstützt. Hier braucht es noch klarere Strukturen, noch verbindlichere Prozesse und Übung, Übung, Übung.

Welche regulatorischen Anpassungen sind notwendig, damit Unternehmen schneller in Resilienzmaßnahmen investieren können?

Andreae: Unternehmen können nur dann schneller in Resilienz investieren, wenn der regulatorische Rahmen klare Anforderungen definiert, eine rechtssichere Umsetzung ermöglicht und die Refinanzierung sicherstellt. Das KRITIS-Dachgesetz ist ein wichtiger Schritt, muss aber zügig, praxistauglich und eng verzahnt mit bestehenden Regelwerken unterlegt werden.

Was schlagen Sie vor, wie sollte das KRITIS-Dachgesetz von der Politik ergänzt werden?

Andreae: Erstens braucht es verlässliche und branchenspezifische Anforderungen gemäß KRITIS-Dachgesetz. Resilienz sollte risikobasiert statt über starre Maßnahmenlisten definiert werden: Unternehmen müssen je nach Anlage, Netzfunktion und Bedrohungslage geeignete Maßnahmen wie Redundanz, Lagerhaltung, Business Continuity Management, Notfallkommunikation oder Wiederanlaufplanung wählen können. Zweitens müssen Kosten regulatorisch anerkannt und refinanzierbar sein. Schutz- und Resilienzmaßnahmen dienen der Versorgungssicherheit und der staatlichen Sicherheitsvorsorge. Dafür braucht es klare Kosten- und Entgeltanerkennung sowie ergänzende Finanzierungswege wie Mittel aus dem Verteidigungshaushalt und einen Resilienz-Fonds.

Wie sollte die Finanzierung solcher Maßnahmen langfristig abgesichert werden?

Liebing: Resilienz ist Teil der öffentlichen Daseinsvorsorge. Die Umsetzung dieser Maßnahmen erfordert erhebliche Investitionen. Deshalb braucht es neben regulatorischer Anerkennung zusätzliche staatliche Instrumente. Wir fordern, dass die Finanzierung über die nach Artikel 109 Grundgesetz geschaffene Ausnahme von der Schuldenbremse für Landesverteidigung und Bevölkerungsschutz sowie aus dem Sondervermögen Infrastruktur und Klimaneutralität (SVIK) sichergestellt wird. Entscheidend ist Planungssicherheit, damit Investitionen verlässlich getätigt werden können.

„Notfallpläne, Übungen und Krisenstrukturen sind vielerorts etabliert.“

Welche drei Maßnahmen sollten kurzfristig priorisiert werden, um die Resilienz des Energiesystems spürbar zu erhöhen?

Andreae: Ich würde kurzfristig folgende drei Maßnahmen in den Vordergrund stellen. Die erste ist der Schutz sensibler Informationen. Wir müssen genauer hinschauen, welche Daten wirklich öffentlich verfügbar sein müssen — und welche Details im Zweifel eher helfen, Kritische Infrastrukturen auszuspähen. Transparenz bleibt wichtig, aber bei Netztopologien, Standorten, Kapazitäten oder Schutzbereichen brauchen wir mehr Augenmaß. Der zweite Hebel ist die Fähigkeit, nach einem Vorfall schnell wieder handlungsfähig zu sein. Dafür müssen Unternehmen noch besser wissen, wo die besonders kritischen Punkte liegen, welches Material verfügbar ist und welche Provisorien kurzfristig eingesetzt werden können. Entscheidend ist nicht nur der Schutz vor einem Angriff, sondern auch die Geschwindigkeit der Wiederherstellung. Und drittens müssen wir die Zusammenarbeit mit Staat und Sicherheitsbehörden verbindlicher organisieren. In der Praxis braucht es feste Ansprechpartner, gemeinsame Übungen, regionale Netzwerke und klare Regeln für den Informationsaustausch. Gerade bei Drohnenvorfällen oder in hybriden Lagen darf nicht erst im Ernstfall geklärt werden, wer zuständig ist und was rechtlich möglich ist.

Und welche politische Entscheidung ist aus Ihrer Sicht jetzt ausschlaggebend, damit diese Maßnahmen auch umgesetzt werden?

Liebing: Entscheidend ist ein klarer politischer Rahmen mit gesicherter Finanzierung. Ohne verlässliche Refinanzierung und praktikable Vorgaben werden Investitionen zu langsam erfolgen. Jetzt braucht es Tempo und dafür mehr Investitionssicherheit und weniger Komplexität.

()

• www.bdew.de
• www.vku.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: Politik, BDEW, Kritische Infrastrukturen (KRITIS), Verband kommunaler Unternehmen (VKU)