

Resilienz als Führungsaufgabe: Wie Stadtwerke ihre Handlungsfähigkeit in der Dauerkrise sichern

Lucien Lenssen

Gezielte Angriffe und sicherheitsrelevante Störungen sind für Stadtwerke und Netzbetreiber keine Ausnahme mehr, sondern Teil der aktuellen Risikolage im Energiesystem. Unternehmen, die jetzt nur auf IT-Sicherheit und Checklisten setzen bzw. Resilienz an Krisenstäbe und in einzelne Projekte delegieren, setzen zu kurz an. Gefragt sind Geschäftsführungen, die Resilienz als strategische Querschnittsaufgabe verstehen und ihre Organisation so aufstellen, dass sie auch unter Dauerstress steuer- und lernfähig bleibt.

Warum Resilienz neu gedacht werden muss

Die Rahmenbedingungen der Energiewirtschaft haben sich in den letzten Jahren grundlegend verändert: Digitalisierung, Dezentralisierung, extreme Wetterereignisse, Cyberangriffe, Sabotageakte sowie geopolitische Spannungen überlagern sich zu einer multidimensionalen Krisenlage. Parallel steigt der regulatorische Druck durch Vorgaben wie NIS2 und das KRITIS-Dachgesetz, die Resilienz erstmals in einen verbindlichen gesetzlichen Rahmen stellen.

Lange Zeit dominierte bei vielen Energieversorgern eine reine Präventionslogik: Es galt die Annahme, dass sich die meisten Ereignisse verhindern lassen, sofern Risiken nur ausreichend identifiziert und kontrolliert werden. Diese Strategie greift heute zu kurz. Die Bandbreite potenzieller Störungen ist zu groß, um jedes Szenario vollständig abdecken zu können. Entscheidend wird vielmehr die organisationale Reaktionsfähigkeit: Wie schnell kann ein Unternehmen auf eine Störung reagieren, wirksame Maßnahmen zur Eindämmung umsetzen und – was am wichtigsten ist – aus diesen Ereignissen lernen, um sich kontinuierlich an neue Gefahrenlagen anzupassen?

Resilienz beschreibt in der Energiewirtschaft daher mehr als technische Robustheit. Sie umfasst die Fähigkeit, Belastungen zu absorbieren, Funktionsfähigkeit wiederherzustellen und aus Störungen systematisch zu lernen. Für Stadtwerke und Netzbetreiber bedeutet das konkret: Sie müssen ihre Versorgungsaufgaben auch unter außergewöhnlichen Bedingungen aufrechterhalten, Wiederanläufe sicherstellen und die Organisation kontinuierlich weiterentwickeln.



Geschäftsführungen sind gefordert, Resilienz als strategische Aufgabe zu begreifen und entsprechende Organisationsmaßnahmen konsequent zu entwickeln

Bild: Adobe Stock

Ein Blick in die Ukraine zeigt, was das im Extremfall bedeutet. Trotz massiver Raketen- und Drohnenangriffe auf Umspannwerke, Kraftwerke und Leitungen ist die Stromversorgung nicht vollständig zusammengebrochen. Netzbetreiber halten das System durch schnelle Reparaturen, flexible Netzführung und Kooperation mit europäischen Übertragungsnetzbetreibern stabil genug, um großflächige Blackouts zu vermeiden. Resilienz ersetzt keine Gewaltfreiheit. Sie entscheidet aber darüber, ob ein Energiesystem funktionsfähig bleibt, wenn der Ernstfall eintritt.

KRITIS-Dachgesetz: von der Compliance zur Steuerungsaufgabe

Mit dem KRITIS-Dachgesetz (KRITIS-DachG) setzt der Gesetzgeber die europäische Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen (sog. CER-Richtlinie) um und verschärft die Anforderungen an Betreiber kritischer Anlagen deutlich. Neben erweiterten

Pflichten zur physischen Absicherung, zu Risikoanalysen, Resilienzplänen und Meldeprozessen wurden Meldepflichten konkretisiert und Bußgelder angehoben. Sicherheitsrelevante Vorfälle sind unverzüglich, in der Regel innerhalb von 24 Stunden, zu melden.

Resilienz lässt sich damit nicht mehr auf IT-Sicherheit reduzieren. Betroffen sind wesentliche Teile der Wertschöpfungskette, wie der Einkauf sicherheitsrelevanter IT- und OT-Komponenten, der Netzbetrieb, Lieferketten und Schlüsselpositionen. Die Einstufung als kritische Anlage erfolgt dabei in der Regel ab einem Versorgungsumfang von 500.000 Einwohnern. Dieser Schwellenwert ist weiterhin umstritten, weil so kleinere, regional bedeutende Infrastrukturen aus dem unmittelbaren Anwendungsbereich des Gesetzes herausfallen. Zusätzlich können die Länder per Verordnung weitere Anlagen als kritisch definieren, was die Bewertung der eigenen Betroffenheit für viele Versorger weiter erschwert.

Damit verschiebt sich der Fokus von der Einhaltung punktueller Compliance-Vorgaben hin zu einer ganzheitlichen Steuerungsaufgabe. Es reicht nicht, einzelne Meldekettens und Resilienzpläne zu etablieren. Gefordert ist eine integrierte Sicht, die gesetzliche Risikoanalysen, internes Risikomanagement, Governance-Strukturen und operative Maßnahmen zusammenführt. Dies ist eine Führungsaufgabe.

Ein verbreitetes Gegenargument lautet: „Wir erfüllen die regulatorischen Mindestanforderungen, mehr können wir uns nicht leisten.“ Diese Sicht verkennt zweierlei. Erstens schützen Mindestanforderungen vor Bußgeldern, nicht vor langanhaltenden Versorgungskrisen. Zweitens steigen die Erwartungen von Politik und Öffentlichkeit: Im Krisenfall wird nicht gefragt, ob ein Stadtwerk compliant war, sondern ob es seinen Versorgungsauftrag erfüllt hat.

Entscheidungsfragen der Geschäftsführung

Auf Geschäftsführungsebene liegen einige Kernentscheidungen, die quer zu allen Fachfragen stehen und nicht delegiert werden können. Am Anfang steht meist eine scheinbar einfache, tatsächlich aber komplexe Leitfrage: Wo setzen wir an? Sie klärt zum einen die Betroffenheit – also die Frage, ob und in welchem Umfang das KRITIS-Dachgesetz greift – und zum anderen die Priorisierung von Handlungsfeldern.

Daraus ergeben sich fünf typische Entscheidungsfelder (siehe Abb. 1):

1. Systemkritische Prozesse: Welche Geschäftsprozesse müssen unter allen Umständen funktionieren, um den Versorgungsauftrag zu erfüllen?
2. Akzeptables Restrisiko: Welches Restrisiko ist tragbar? Wo beginnt die rote Linie für Investitionen?
3. Verantwortung und Governance: Wer trägt die Gesamtverantwortung für Resilienz und entscheidet im Ernstfall?
4. Finanzielle Prioritäten: Wie viel Budget fließt jährlich in Resilienz gegenüber anderen strategischen Vorhaben?
5. Integration von Regulierung und Strategie: Wie werden gesetzliche Risikoanalysen in bestehende Strategie, Risikosteuerung und Investitionsplanung integriert?

In der Praxis werden diese Fragen häufig fragmentiert beantwortet. IT, Technik, Krisenstab, Risikomanagement und HR entwickeln jeweils eigene Perspektiven ohne übergeordnete Priorisierung und Orchestrierung. Das führt zu Doppelarbeit, Lücken, widersprüchlichen Risikobildern und im Ernstfall zu unklaren Entscheidungswegen.

In Gesprächen hören wir häufig: „Das Thema ist wichtig, aber aktuell haben wir dafür keine Kapazitäten.“ Das ist menschlich verständlich, strategisch jedoch riskant. Denn Resilienz-Entscheidungen sind nicht optional, sondern werden im Ernstfall rückwirkend bewertet – von Aufsichts-räten, der Kommunalpolitik, den Medien und der Öffentlichkeit. Dabei gilt: Auch Nicht-Handeln ist eine Entscheidung, allerdings ohne bewusste Priorisierung. Es ist die Kernaufgabe der Führung, diese Komplexität zu bändigen und klare Leitplanken für das Handeln zu setzen.

Realität in Stadtwerken

Die Lage in Stadtwerken und Netzbetreibern ist ambivalent. Einerseits ist das Problembewusstsein bei vielen Informationssicherheitsbeauftragten, Krisenmanagern und Fachverantwortlichen hoch. Die IT-Sicherheit ist, nicht zuletzt durch frühere Regulierung, solide aufgestellt. Strukturen eines Informationssicherheits-Managementsystems (ISMS) existieren und werden formal bedient.

Andererseits bleibt Resilienz oft auf Teilbereiche beschränkt. IT-Sicherheit wird mit Gesamtschutz gleichgesetzt, während phy-

sische Infrastruktur, OT-Systeme, Lieferketten, Personalrisiken und Wissensabgänge nur punktuell betrachtet werden. Die Stromausfälle in Berlin im Januar zeigten: Kritische Hardware und physische Redundanzen fehlen häufig in Risikobetrachtungen.

Klare Unterschiede zeigen sich zwischen kleineren und größeren Netzbetreibern. Kleinere Häuser haben oft erste Leitfäden erstellt und einzelne Themen aufgearbeitet, stehen beim Aufbau eines belastbaren Krisen- und Resilienzmanagements jedoch noch am Anfang – insbesondere bei Cybersicherheit und regelmäßigen Übungen. Größere Netzbetreiber zeigen dagegen ein deutlich strukturierteres Bild. Ihre Prozesse und Verantwortlichkeiten sind klarer geregelt und mögliche Krisenszenarien werden häufiger und systematischer durchgespielt.

Gerade kleine und mittlere Versorger stehen vor einem Dilemma: Sie erkennen die Risiken, sehen sich jedoch durch begrenzte Budgets und personelle Engpässe überfordert. Tausende Kilometer an Mittel- und Niederspannungsleitungen, weitverzweigte Wasserversorgungsnetze sowie unzählige Transformatorenstationen mit öffentlich zugänglichen Knotenpunkten werfen die drängende Frage auf, was zuerst angegangen werden soll. Diese Überlastung führt dazu, dass bekannte Schwachstellen zwar registriert, aber mangels systematischer Priorisierung nicht konsequent behoben werden.

Reifegradmodelle (siehe Abb. 2) liefern Orientierung, suggerieren aber manchmal mehr Sicherheit, als tatsächlich vorliegt. Sie bewerten Dokumentation häufig hö-



Abb. 1 Entscheidungsrad für Geschäftsführungen: nicht delegierbare Entscheidungen zur Resilienzsteuerung
Quelle: eigene Darstellung



her als tatsächliche Funktionalität unter Stress. Ein ausgefeilter Plan ohne Übung bleibt im Ernstfall wirkungslos. Der wahre Reifegrad zeigt sich erst, wenn Prozesse unter Belastung getestet wurden.

Papierlage und Praxis klaffen auseinander. Krisenhandbücher, Notfallpläne und Leitfäden existieren in vielen Versorgungsunternehmen, werden aber selten unter realistischen Bedingungen eingeübt. Zwar finden punktuell Übungen statt, diese beziehen jedoch nicht alle relevanten Akteure ein. Statt gezielt Schwachstellen aufzudecken, bestätigen sie eher bestehende Strukturen. Damit bleibt Resilienz eine formale Anforderung. Sie wird nicht zum praktischen Bestandteil der Organisationskultur.

Governance als zentraler Hebel

In vielen Häusern zeigt sich ein klares Muster: Resilienz scheitert selten am fehlenden Fachwissen, sondern an Steuerung und Zuständigkeiten. Rollen bleiben unklar, Mandate unscharf und die Schnittstellen zwischen IT, Technik, Krisenstab, Compliance und Geschäftsführung sind nicht eindeutig geregelt. Im Ereignisfall drohen Verzögerungen, Doppelzuständigkeiten und Unsicherheit darüber, wer tatsächlich entscheidet.

Ein psychologischer Effekt verschärft dies. Die Wahrscheinlichkeit, selbst Opfer eines Angriffs auf IT-Systeme oder physische Infrastruktur zu werden, wird von vielen unterschätzt. Die verbreitete Haltung „Uns wird schon nichts passieren“ passt nicht zur Bedrohungslage. Aus Beratungserfahrung ergibt sich ein anderes Mindset: Wir müssen davon ausgehen, dass es uns trifft. Offen bleibt, wann und mit welchen Auswirkungen.

Das KRITIS-Dachgesetz erhöht den Druck zusätzlich. Es bringt neue Pflichten, Akteure und Zuständigkeiten ins Spiel. Länder können weitere kritische Anlagen definieren, während die Meldewege über mehrere Behördenebenen verlaufen und unterschiedliche Regelwerke ineinandergreifen. Ohne klare interne Zuständigkeiten entstehen Spannungen zwischen gesetzlichen Anforderungen und Unternehmensabläufen. Eine belastbare Governance ist deshalb kein „Nice-to-have“, sondern Voraussetzung dafür, regulatorische Vorgaben überhaupt wirksam umsetzen zu können.

Reifere Organisationen zeichnen sich durch einige gemeinsame Merkmale aus:

- eine eindeutig verankerte Gesamtverantwortung für Resilienz, häufig in Form einer zentralen Stelle oder eines „Resilience Officer“;
- klare Eskalations- und Entscheidungswege für den Krisenfall, einschließlich Vertretungsregelungen und Budgetkompetenzen;
- eine feste Verankerung von Resilienzthemen in Geschäftsführungssitzungen und – wo relevant – in Aufsichtsratsgremien;
- ein systematisches Prozessmanagement als Basis für Risikoanalysen, Notfallpläne und Übungen.

Solche Steuerungsmodelle schaffen Transparenz und entlasten die operativen Bereiche. Resilienz wird von einem „IT-Thema“ oder einer Spezialaufgabe einzelner Stäbe zu einer geführten Querschnittsaufgabe, bei der Geschäftsführung, Fachbereiche und externe Partner in einem gemeinsamen Orchestringsmodell zusammenarbeiten.

Finanzierung: Kapitalallokation statt Technikfrage

Resilienz kostet Geld. Sie erfordert nicht nur Aufmerksamkeit, sondern auch finanzielle Mittel. Während IT-Sicherheitsbudgets vielerorts bereits existieren, beginnen die Herausforderungen bei der physischen Infrastruktur, Redundanzen und den baulich-technischen Schutzmaßnahmen.

Geplante Förderpakete auf europäischer Ebene mit einem dreistelligen Millionenbetrag für Deutschland sind angesichts des Investitionsbedarfs eher ein symbolischer Beitrag. Ergänzend plant die Bundesregierung einen Resilienzfonds zum Schutz kritischer Infrastruktur mit bis zu 500 Mio. € jährlich und insgesamt rund 2 Mrd. €. Auch dieses Volumen liegt deutlich unter dem kumulierten Bedarf. Zwar lassen sich bestimmte Investitionen in die Netzinfrastuktur über Netzentgelte refinanzieren, etwa wenn sie unmittelbar der Versorgungssicherheit dienen und regulatorisch anerkannt werden. Viele Maßnahmen zur Resilienzsteigerung – etwa zusätzliche Redundanzen, bauliche Schutzmaßnahmen oder organisatorische Vorkehrungen wie Krisenübungen – sind jedoch nur eingeschränkt oder gar nicht umlagefähig und belasten damit direkt das Ergebnis. Hinzu kommt: Kommunale Anteilseigner stehen selbst unter Ertragsdruck und schränken die Investitionsspielräume der Stadtwerke zusätzlich ein.

Damit wird Resilienz auch zur Frage der Kapitalallokation. Geschäftsführungen müssen abwägen: Wie gewichten wir Maßnahmen zur Absicherung kritischer Infrastruktur im Verhältnis zu Netzausbau, Dekarbonisierung und Digitalisierung? In vielen Häusern tauchen KRITIS-Themen bislang jedoch nicht systematisch in Mehrjahresplanungen, Investitionsprogrammen oder Kreditgesprächen auf.

Ein häufiger Einwand lautet: „Wir können nicht für jedes hypothetische Szenario Rücklagen bilden.“ Das ist korrekt. Resilienz bedeutet jedoch nicht, jede denkbare Eventualität finanziell abzusichern, sondern bewusste Schwerpunkte zu setzen. Wer allerdings die Vorsorge vernachlässigt, riskiert, dass ein einziges Schadensereignis die finanziellen Spielräume über Jahre hinweg bindet und damit genau

jene Investitionen blockiert, die das Unternehmen zukunftsfähig machen will.

Wer nicht aktiv wird, nimmt ein doppeltes Risiko in Kauf: explodierende Schadenskosten im Krisenfall sowie wachsende Haftungs- und Sanktionsgefahren durch verschärfte regulatorische Vorgaben. Neben den unmittelbaren wirtschaftlichen Folgen rückt damit auch die persönliche Verantwortung der Geschäftsführung stärker in den Fokus, denn erweiterte Transparenz- und Meldepflichten gehen mit deutlich erhöhten Bußgeldern und einer engeren Erwartungshaltung von Aufsichtsrat, Eigentümern und Aufsichtsbehörden einher. Wird im Nachhinein sichtbar, dass bekannte Risiken über längere Zeit ignoriert oder gesetzliche Anforderungen nur formal erfüllt wurden, kann dies schnell zur Frage der eigenen Organhaftung und Glaubwürdigkeit werden.

Resilienzinvestitionen dürfen daher kein isoliertes Fachthema bleiben. Sie müssen strategisch in die Finanzplanung, die Berichterstattung an den Aufsichtsrat und den Bankendialog eingebettet werden, bevor der erste Ernstfall zur unfreiwilligen Argumentationshilfe wird.

Resilienz im Verbund

In der Praxis entsteht echte Resilienz häufig dort, wo Stadtwerke und Netzbetreiber über die eigene Organisationsgrenze hinausdenken. Wer Betriebsmittel, Spezialwissen und Krisenerfahrung mit anderen teilt, erweitert seinen Handlungsspielraum deutlich.

Beispiele zeigen dies konkret (siehe Abb. 3). So gibt es etwa Stadtwerke, die gemeinsam ein Notfalllager für Betriebsmittel

finanzieren, um im Ereignisfall schneller reagieren zu können, ohne dass jedes Unternehmen sämtliche Redundanzen allein vorhalten muss. Andere teilen sich selten benötigte Spezialkompetenzen, etwa im Bereich Cybersicherheit, statt punktuelle Vollzeitstellen aufzubauen. Solche Kooperationsmodelle senken Kosten, erhöhen die Varianz verfügbarer Ressourcen und steigern damit die Resilienz des Gesamtsystems.

Auch im Krisenmanagement zeigt sich: Übungen mit Katastrophenschutzbehörden, Landkreisen und anderen KRITIS-Betreibern schaffen ein gemeinsames Lageverständnis und eine gemeinsame Sprache. Die Beteiligten berichten, dass der gruppenpsychologische Lerneffekt solcher Übungen teilweise wichtiger ist als die Detailausgestaltung einzelner Szenarien. Dazu gehören das Kennenlernen der handelnden Personen, das Erleben von Entscheidungsdynamiken und das Verständnis typischer Kommunikationsmuster.

Für kleinere Stadtwerke ist zudem der Austausch mit größeren Netzbetreibern und Kooperationsnetzwerken essenziell. Resilienz-Checks, Reifegradmodelle und Best Practices helfen, die eigene Situation zu verorten, Prioritäten zu setzen und Fehler zu vermeiden.

Vom Papier zur Praxis

Resilienz entsteht im Alltag, nicht in Gesetzestexten und Präsentationen. Entscheidend ist, ob Prozesse, Pläne und Strukturen unter Stress funktionieren. Dazu braucht es regelmäßige Übungen, Tests und Simulationen, die bewusst Schwachstellen aufdecken. Praxisnahe

Ansätze setzen auf einfache, aber wirksame Tests: Was passiert beispielsweise, wenn eine Schlüsselperson plötzlich ausfällt? Wie reagiert die Organisation bei einem gezielten EDV-Blackout? Wer entscheidet, wenn die Geschäftsführung nicht erreichbar ist? Solche Simulationen machen Abhängigkeiten, Lücken und implizite Annahmen sichtbar.

Für den Einstieg bedarf es keines Großprojekts. Sechs pragmatische Schritte machen Resilienz sofort greifbar:

1. Zentrale Notfallkontakte bündeln: Eine konsolidierte Liste interner und externer Schlüsselkontakte erstellen – von IT- und Netzspezialisten über Dienstleister bis hin zu den zuständigen Behörden.
2. Kritische Systeme priorisieren: Die zehn wichtigsten IT- und OT-Systeme identifizieren und eine verbindliche Wiederanlaufreihenfolge festlegen.
3. Entscheidungsbefugnisse klären: Kompetenzen für den Ernstfall dokumentieren. Wer darf Ad-hoc-Maßnahmen wie Umschaltungen, Abschaltungen oder die externe Krisenkommunikation freigeben?
4. Notfallpläne vereinfachen: Bestehende Pläne und komplexe Handbücher auf zwei bis drei Seiten verdichten, idealerweise in Form von handlungsorientierten Checklisten statt Textdokumenten.
5. Mini-Krisenübung durchführen: Eine 60-minütige „Table-Top-Übung“ (Tischübung) mit der Führungsebene und Schlüsselrollen auf Basis eines realistischen Szenarios durchführen.
6. Lerngewinne festhalten: Nach jeder Störung eine 30-minütige Rückschau durchführen, um drei konkrete Optimierungsmaßnahmen für die Praxis abzuleiten.

Resilienzdimension	ohne Kooperation	mit Kooperation
physische Sicherheit	eigene Lager, begrenzte Redundanz, hohe Kosten	gemeinsame Ressourcenpools, höhere Verfügbarkeit, geteilte Kosten
Cyber- & IT-Sicherheit	Einzelbesetzung, punktuelle Expertise	geteilte Spezialisten, kontinuierliche Kompetenz
Organisation & Governance	Interne Silos, fehlender Rundumblick	Austausch-Formate, Peer-Learning, Best-Practices
Personal & Kultur	Einzeltrainings, Lernen aus eigenen Fehlern	gemeinsame Krisenübungen und Schulungsplattformen, Fehler anderer vermeiden
externe Vernetzung & Kommunikation	ad-hoc-Abstimmung, häufig formelle Kontakte, mangelndes Verständnis	regelmäßige Behörden- und Netzwerkübungen, informelle Kontakte, gemeinsames Verständnis
wirtschaftliche Stabilität	Abhängigkeit von Kerngeschäft, fehlende Flexibilität und Geschwindigkeit	diversifizierte Geschäfts- und Kooperationsmodelle, Flexibilität und Geschwindigkeit als Wettbewerbsvorteil

Abb. 3 Kooperation als Resilienzhebel: Kooperation wirkt entlang zentraler Dimensionen des resilienten Stadtwerks
Quelle: eigene Darstellung

Entscheidend für den Erfolg sind dabei weniger theoretisch perfekte Szenarien als vielmehr eine konsequente Nachbereitung mit klarem Fokus auf den strategischen Lerngewinn, die Bereitschaft, Schwachstellen offen zu benennen und systematisch zu bearbeiten, sowie die systematische Einbindung aller relevanten Akteure – von der Führungsebene über die Fachbereiche bis hin zu externen Partnern. In diesem Prozess nimmt die Führung eine wichtige Doppelrolle ein. Sie muss nicht nur die notwendigen Ressourcen

cen und Rahmenbedingungen für die Krisenvorsorge bereitstellen, sondern auch maßgeblich die Lernkultur im Unternehmen prägen. Das Vorbild der Führung entscheidet darüber, ob Resilienz als lästige Pflicht wahrgenommen wird oder als strategische Chance, die eigene Handlungsfähigkeit dauerhaft zu sichern.

Fazit: Führung macht Resilienz gestaltbar

Resilienz ist eine dauerhafte Organisationsaufgabe, kein Projekt mit einem definierten Endpunkt. Die Bedrohungslage wird sich weiter verändern, regulatorische

Vorgaben werden nachgeschärft und technologische und personelle Rahmenbedingungen bleiben dynamisch.

Gerade deshalb muss Resilienz auf Führungsebene verankert werden. Geschäftsführungen und Führungsteams in der Energiewirtschaft entscheiden darüber, wie bewusst sie Risiken adressieren, wie sie Governance und Finanzierung ausgestalten und wie konsequent sie als Unternehmen aus Ereignissen lernen. Sie setzen die Klammer über technische, organisatorische und kulturelle Maßnahmen und machen Resilienz damit gestaltbar statt zufällig.

Frühzeitiges Handeln schafft Wettbewerbsvorteile. Stadtwerke und Netzbetreiber sollten daher jetzt damit beginnen, systemkritische Prozesse zu identifizieren, Restrisiken zu definieren, die Governance zu klären, finanzielle Prioritäten zu setzen und eine lernorientierte Übungskultur zu etablieren. Dabei geht es nicht um maximale Absicherung, sondern um gesicherte Handlungsfähigkeit auch im Unvorhersehbaren.

*L. Lenssen, Bereichsleiter Beratung, Die Netzwerkpartner e. V., Essen
lucien.lenssen@dienetzerpartner.com*

Neue Gaskraftwerke: Studie kritisiert „Südbonus“

Bis 2030 plant die Bundesregierung den Bau von 20-GW-Gaskraftwerken, die zur Netzsicherheit und -stabilität beitragen sollen. Der entsprechende Gesetzgebungsvorschlag steht noch aus – vorgesehen ist jedoch, zwei Drittel der insgesamt ausgeschriebenen Kraftwerkskapazitäten im „netztechnischen Süden“ zu errichten, um Netzengpässe und den damit verbundenen Redispatch-Bedarf zu reduzieren. Der netztechnische Süden, für den der „Südbonus“ gelten soll, umfasst eine Zone, die aus Baden-Württemberg, Bayern, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz und dem Saarland besteht.

Mit dem Südbonus soll eine regionale Steuerungskomponente in den Ausschreibungsprozess der neuen Kraftwerkskapazitäten eingebracht werden, dessen Konsequenzen das Fraunhofer IEG zusammen mit der Consentec GmbH in einer Studie für die LEAG Clean Power GmbH untersucht hat. Vorgesehen ist, den Südbonus als fixen Reduktionswert auszugestalten, der sich mindernd auf die Zuschlagskennziffer auswirkt, die für die Gebotsreihung ausschlaggebend ist. Die Höhe des Reduktionswerts soll sich an den systemischen Kosteneinsparungen orientieren, die sich aus einer regionalen Steuerung ergeben. Angedacht ist eine Größenordnung von 200–300 €/kW installierter Leistung.

Südbonus und Redispatch-Vergütung

Dem Südbonus stellen Fraunhofer IEG und Consentec die Redispatch-Vergütung als Maßnahme gegenüber, die die Wirtschaftlichkeit eines Kraftwerks abhängig vom Standort beeinflussen kann. Die Redispatch-Vergütung sieht neben der Vergütung der operativen Kosten als jährliche Fixkostenerstattung auch eine Kompensation des anteiligen Werteverbrauchs vor. Aktuell kommt dies vor allem Kraftwerksstandorten im netztechnischen Süden zugute, da sie einen aktuell positiven Redispatch-Saldo aufweisen. Die Analyse zielt somit darauf, die potenziell kumulative Wirkung von Südbonus und Redispatch-Vergütung insbesondere hinsichtlich des anteiligen Werteverbrauchs und mögliche Folgen für Förderkosten und Kapazitätsallokation in den Blick zu nehmen.

In der näheren Betrachtung bezweifeln Fraunhofer IEG und Consentec, dass die Einführung eines Südbonus zusätzlich zur bereits bestehenden Redispatch-Vergütung wirtschaftlich sinnvoll ist. Kurzfristig betrachtet wird der Redispatch-Bedarf weiterhin hoch bleiben. Rückläufig wird er erst langfristig mit einem systemdienlichen Kapazitätszubau sowie einem stringenten Netzausbau. Die Redispatch-Vergütung sieht eine anteilige Fixkostenerstattung für Kraftwerke vor, die zur Erhöhung der Einspeiseleistung im Redispatch in Anspruch genommen werden. Da Redispatch-Maßnahmen aktuell im netztechnischen Süden greifen, ergebe sich daraus eine mögliche wirtschaftliche Bevorteilung für diese Standorte.

Zweifel am volkswirtschaftlichen Nutzen

Die negative Bewertung der volkswirtschaftlichen Kosten-Nutzen-Analyse begründen Fraunhofer IEG und Consentec mit den Unsicherheiten der tatsächlich eintretenden Vergütung. Sind die Erlöse groß genug, um die etwaigen Kostennachteile von Süd-Kraftwerken auszugleichen bzw. sie überzukompensieren, hätte dies Auswirkungen auf das letzte Drittel der auszuschreibenden Kapazitäten, die nicht dem Südbonus unterfallen. Diese Nordstandorte würden bei der Gebotslegung übermäßig benachteiligt, d. h., der „Südbonus“ würde zu einer ineffizient hohen Beanreicherung der Südstandorte führen.

Die Vergütung des anteiligen Werteverbrauchs im Redispatch über die Lebensdauer einer Anlage im Süden könne eine Größenordnung erreichen, die mit dem Südbonus vergleichbar sei, so Fraunhofer IEG und Consentec. Um negative Konsequenzen zu vermeiden, wird daher der Ausschluss neu ausgeschriebener Anlagen von der anteiligen Werteverbrauchsvergütung vorgeschlagen. Alternativ sei auch die Rückzahlung erhaltener anteiliger Werteverbrauchsvergütungen im Rahmen des beihilferechtlich vorgegebenen Clawback-Mechanismus möglich.

Die Studie „Analyse der langfristigen Maßnahmenwirkung der anteiligen Werteverbrauchskompensation vor dem Hintergrund eines „Südbonus für Kraftwerke“ ist abrufbar unter: https://www.ieg.fraunhofer.de/content/dam/ieg/deutsch/dokumente/pressemitteilungen/Kurzstudie_AnteiligerWerteverbrauch_final.pdf