



Resiliente Netzbetreiber

Organisationssicherheit garantieren, Risiken minimieren und Krisenfälle sicher beherrschen

von Corinna Semling, Simon Haas, Dr. Sören Patzack und Dr. Olaf Unruh

Organisationssicherheit garantieren, Risiken minimieren und Krisenfälle sicher beherrschen

Netzbetreiber sind gefordert, in ihrer Risikobetrachtung umzudenken und das frühzeitige Erkennen krisenhafter Zustände als Routineaufgaben stärker zu priorisieren. Ob das vorhandene Organisationskonzept dafür geeignet gestaltet ist, lässt sich mit dem vorgestellten Resilienz-Quick-Check überprüfen. Er zielt darauf ab, das Unternehmen bezüglich seines Reifegrads zur Früherkennung, Wiederversorgung und Lernbereitschaft in Krisenfällen zu hinterfragen.

»Blackout nur knapp abgewendet!«¹ So stand es Anfang Juli 2019² in der Presse. Bevor Marc Elsberg seinen Bestseller Blackout im Jahr 2012 veröffentlichte, kamen der breiten Bevölkerung das Szenario eines europaweiten Stromausfalls und die damit einhergehenden Folgen eher abstrakt vor. Doch die direkt erlebbaren Ursachen eines Blackouts, wie die Zunahme extremer Hitzeperioden³ in Mitteleuropa oder die zunehmende Bedrohung durch Cyberangriffe⁴ erwecken den Anschein, dass Ausnahmesituationen mehr und mehr zur Regel werden. Bei kritischen Ereignissen wie Notfällen oder Krisensituationen sollte die Versorgungssicherheit möglichst aufrechterhalten werden. Auch die Resilienz des Netzbetreibers wird immer wichtiger: Bei einem nicht immer vermeidbaren Blackout sollte die Versorgung möglichst schnell wieder hergestellt werden.

Im Folgenden wird ein ganzheitlicher Ansatz zur Bewertung des Organisationskonzepts vorgestellt, um die Resilienz des Netzbetreibers zu bestimmen. Um resilientes Handeln erwarten zu können, sind in der Organisation die

notwendigen Voraussetzungen für präventive Maßnahmen zum Krisenmanagement, zur Krisenbewältigung und zur Nachbereitung zu schaffen. Der vorgestellte Quick-Check schlägt einen ganzheitlichen Ansatz zur Früherkennung von Optimierungsmöglichkeiten in den Handlungsfeldern Mensch, Organisation und Technik als Instrument einer kontinuierlichen Risikobetrachtung vor.

Krisenbewältigung muss Hand in Hand mit Prävention und Nachbereitung gehen

Unter einem Notfall wird ein schwerwiegendes, außergewöhnliches Ereignis und unter einer Krise ein Notfall besonders großen Ausmaßes verstanden⁵. Beide Fälle haben mit einer hohen Wahrscheinlichkeit Personenschäden, erhebliche Sachschäden oder gravierende Beeinträchtigungen der Stromversorgung zur Folge. Maßgeblich für eine sachgerechte Reaktion auf ein Schadensereignis ist die Erkenntnis, wann der Wechsel von einer routinemäßigen Entstörung in der Linienorganisation hin zur Organisation für einen Notfall oder sogar für eine Krisensituation stattfinden muss. Das Hochfahren der Notfall- oder Krisenorganisation liegt in der Verantwortung des Netzbetreibers. Es ist also eine klare Definition notwendig, wann ein Notfall oder eine Krise eintritt. In einer Studie unter Energieversorgern gaben jedoch nur rund 30 % der Unternehmen

an, über keine schriftliche Definition von Notfall zu verfügen⁶.

Im Unterschied zu einer unplanmäßigen Versorgungsunterbrechung als Ereignis, zeichnet sich der Krisenfall in der Regel durch eine unvollständige Informationslage (Wo liegt die Ursache? Welche Anlagen oder Netze sind davon betroffen? Welche Gegenmaßnahmen müssen ergriffen werden?), durch ein hohes Schadensrisiko und durch hohen Zeitdruck aus. Die vorhandenen Empfehlungen für Netzbetreiber im Hinblick auf die Organisation ihres Krisenmanagements sind umfangreich. Von den Hinweisen für das Krisenmanagement des Netzbetreibers, veröffentlicht durch den FNN⁷ bis hin zu Leitfäden von BDEW/VKU/Geode⁸ liegen zahlreiche Empfehlungen vor, nach denen Energieversorger ihre Ablauf- und Aufbauorganisation sowie die Schnittstellen zu weiteren Akteuren ausrichten können. Auf Basis dieser Empfehlungen hat ein Großteil der Netzbetreiber in den vergangenen Jahren ein Krisenmanagement aufgesetzt. Zusätzlich haben Netzbetreiber die Möglichkeit, mit einer TSM-Überprüfung im Rahmen einer freiwilligen Zertifizierung (anknüpfend an die Anwendungsregel VDE-AR-N 4001) ihre Eignung bezüglich Versorgungssicherheit nach außen zu

¹ www.deutschland-kurier.org/stromnetz-drohte-zu-kollabieren-blackout-nur-knapp-abgewendet.

² www.manager-magazin.de/unternehmen/energie/europas-stromnetz-am-rand-von-blackout-a-1248733.html.

³ www.umweltbundesamt.de/themen/die-vergangenen-fuenf-jahre-waren-weltweit-die.

⁴ BSI (2019): Die Lage der IT-Sicherheit in Deutschland. 2018, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6.

⁵ Zum Beispiel VDE (2011): Sicherheit in der Stromversorgung – Hinweise für das Krisenmanagement des Netzbetreibers S 1002. Eine Aktualisierung ist für das Jahr 2020 vorgesehen.

⁶ PWC (2012): Wie gut sind deutsche Energieversorger auf Notfälle vorbereitet. www.pwc.de/de/energiwirtschaft/assets/studie_notfallmanagement_energieversorger.pdf.

⁷ Zum Beispiel VDE (2011): Sicherheit in der Stromversorgung – Hinweise für das Krisenmanagement des Netzbetreibers S 1002. Eine Aktualisierung ist für das Jahr 2020 vorgesehen.

⁸ Zum Beispiel BDEW/VKU/GEODE (2018): Leitfaden: Krisenvorsorge Gas.

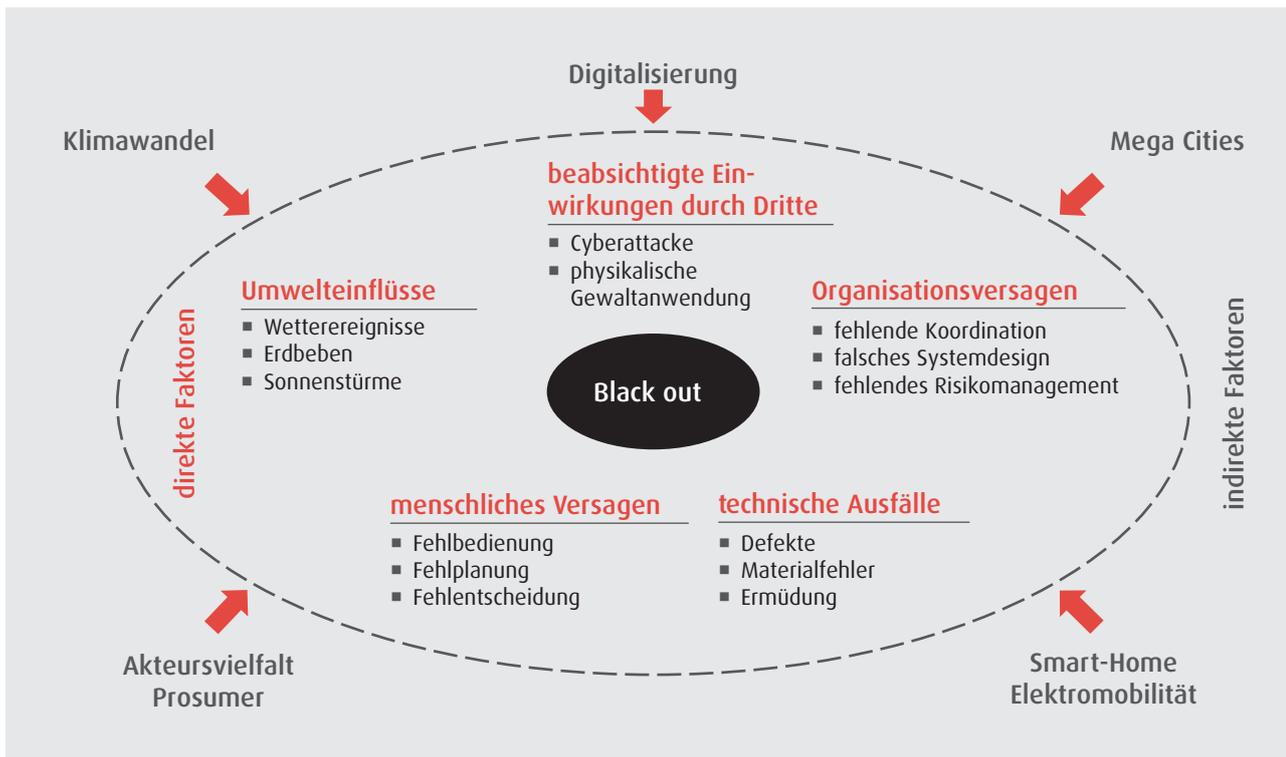


Bild 1. Direkte und indirekte Ursachen für einen Blackout

dokumentieren. Daneben können oder müssen Netzbetreiber außerdem mit Präventionsmaßnahmen im Zuge der Zertifizierung des Informationssicherheits-Managementsystems (ISMS) ausdrücklich ihre Resilienz in Bezug auf Cyber Risiken verstärken, die im Rahmen des Smart-Meter-Rollouts und der Digitalisierung vieler Prozesse auftreten und zu einem Blackout führen können.

Nach dem Gesetz zur Kontrolle und Transparenz von Unternehmensbereichen (KonTraG) sind Unternehmen zur Risikoanalyse im Rahmen eines Risikomanagementprozesses verpflichtet. Dabei wird ein Monitoring und die wirtschaftliche Bewertung von Risiken anhand von Eintrittswahrscheinlichkeiten für Schadensereignisse vorgenommen. Der Schadensfall eines Blackouts stellt ein Einzelereignis mit einer geringen Eintrittswahrscheinlichkeit, aber mit hohem Schadensausmaß dar. In den klassischen Ansätzen des Risikomanagements führen solche Ereignisse zwangsläufig nur zu einem geringen Handlungsdruck für die Organisation. Daher greifen hier die gesetzlichen Regelungen für das Krisenmanagement und verzahnen beide Perspektiven sinnvoll miteinander. Das Risikomanagement erfasst die wirtschaftlichen Folgen des Blackout-Risikos, die prozessualen und technischen Implikationen sind jedoch Teil des Krisenmanagements.

Wie offensiv Energieversorger mit der Verantwortung für ein präventives Krisenmanagement umgehen, kann anhand durchgeführter Übungen ermittelt werden. Eine Befragung ergab, dass im Jahr 2012 rund 22 % der befragten Energieversorger ihre Verfahren und Abläufe einmal im Jahr üben.⁹ Wie sich die Bereitschaft zur präventiven Überprüfung der eigenen Reaktionsfähigkeit im Krisenfall seit dem Jahr 2012 entwickelt hat, ließ sich auch durch ausführliche Recherche nicht ermitteln. Allerdings wurde vom VDE außer den Empfehlungen zur Festlegung der Ablauf- und Aufbauorganisation sowie den damit verbundenen Plänen, Standards, Arbeitshilfen und Handbüchern auch die Durchführung von Krisenübungen aufgelistet. Die konsequente Umsetzung – über die reine Papierlage eines Notfallhandbuchs hinaus – ist jedoch in Zeiten von Effizienzdruck und Optimierungsbemühungen für den Normalbetrieb mitunter anspruchsvoll.

Aktueller Handlungsbedarf für Netzbetreiber

Die Ursachen für einen Blackout können vielfältig sein. Sie können in direkte Fak-

toren, die sich direkt auf die Infrastruktur auswirken, und indirekte Faktoren, mit denen beispielsweise Megatrends beschrieben werden, eingeteilt werden (Bild 1).

Direkte Faktoren sind Umwelteinflüsse, beabsichtigte Einwirkungen durch Dritte, Organisationsversagen sowie menschliches Versagen und technische Ausfälle. Sie können unmittelbar einen Blackout verursachen. Diese Faktoren sind in Bild 1 im inneren Kreis dargestellt und gelten für Netzbetreiber als »beeinflussbar«. Denn Netzbetreiber können in diese Handlungsfelder aktiv eingreifen und durch geeignete Maßnahmen das Risiko eines Blackouts reduzieren. Beispielsweise lassen sich Übungen und Schulungen durchführen, um den inneren Faktor menschlichen Versagens zu entschärfen.

Die indirekten Faktoren Klimawandel, Digitalisierung, Mega Cities, Smart Home und Elektromobilität sowie Akteursvielfalt stehen für sich langsam entwickelnde Trends oder disruptive Veränderungen. Deren Wirkung und vor allem deren Wechselwirkung auf die eigene Organisation lässt sich nur schwer prognostizieren. In Bild 1 sind diese Faktoren außerhalb des gestrichelten Kreises aufgeführt. Für Netzbetreiber sind diese indirekten Faktoren »nicht beeinflussbar«, aber dennoch relevant und sollten berücksichtigt werden.

⁹ PWC (2012): Wie gut sind deutsche Energieversorger auf Notfälle vorbereitet. https://www.pwc.de/de/energiewirtschaft/assets/studie_notfallmanagement_energieversorger.pdf.

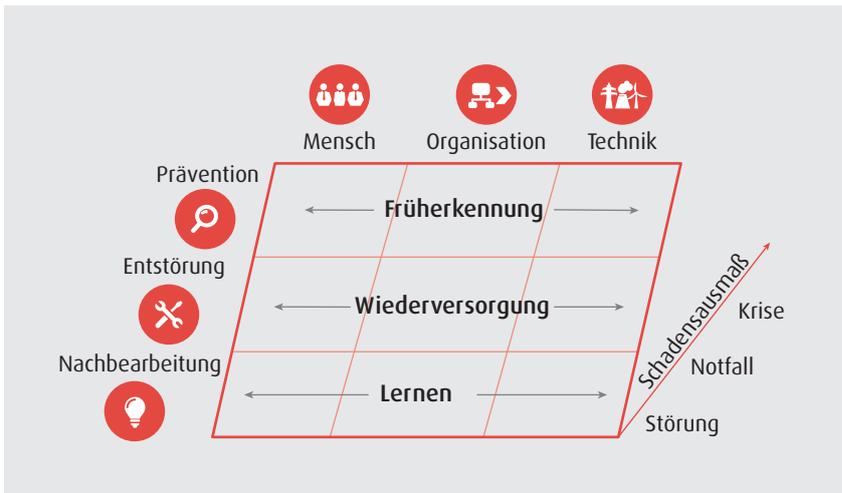


Bild 2. Ganzheitliches Organisationskonzept für resiliente Netzbetreiber

Der Einfluss der indirekten Faktoren auf Netzbetreiber nimmt stetig zu und wird in den kommenden Jahren weiter steigen. Netzbetreiber sehen sich beispielsweise im Zuge der Digitalisierung neuen Herausforderungen und

Risiken gegenüber (zum Beispiel Cyberattacken), die das Risiko eines Blackouts verstärken. Angesichts der durch die Vielfalt an künftigen Akteuren steigenden Dezentralität der Energieversorgung und dem zunehmenden Grad

an Vernetzung werden Blackout-Szenarien in der Energiewirtschaft mittlerweile vielfach diskutiert. Aus diesen Veränderungen ergibt sich ein klarer Handlungsbedarf für Netzbetreiber, mehr zu machen, um sich unter den veränderten Faktoren gegen einen Blackout zu wappnen.

Um finanziellen Schaden und erheblichen Imageschaden zu vermeiden, der mit einem großflächigen Stromausfall einhergeht, ist die Energiewirtschaft gefordert, in ihrer Risikobetrachtung umzudenken und das frühzeitige Erkennen von krisenhaften Zuständen als Routineaufgaben stärker zu priorisieren. Denn außer der gesetzlichen Vorschrift zum Vorhalten einer Krisenmanagementorganisation ist die Risikominimierung im Ereignisfall der Hauptnutzen. Daneben werden vorhandene Mittel auf Basis eines Soll/Ist-Abgleichs in der Prävention zielgerichtet und effizienter eingesetzt und Kosten somit reduziert.

Mensch 	<ul style="list-style-type: none"> Werden in den betrieblichen Qualifizierungen Risikofaktoren für einen Blackout thematisiert? Kann das Personal Störungen hinreichend genau kategorisieren? Werden die Mitarbeiter für Routine und für Störungsfälle im ähnlichen Umfang ausgebildet? Wird das Personal für den Ausfall automatisierter Vorgänge ausreichend geschult? Sind Arten von und Ursachen für menschliche Fehler, die das Risiko von Cyberangriffen erhöhen können, fester Trainingsbestandteil? 								
Organisation 	<ul style="list-style-type: none"> Hat die Organisation oder insbesondere das Management ein Routineverfahren, mit dem die Früherkennung von Blackout-Auslösern thematisiert wird? Existieren dokumentierte und gut erprobte Abläufe für den Störungs- bzw. Notbetrieb? Wie werden Notfall und Krise definiert bzw. unterschieden? Auf welche möglichen Schadensfälle bereiten wir uns vor? 								
Technik 	<table border="1"> <thead> <tr> <th>Phase</th> <th></th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Prävention</td> <td> Netzbetriebsmittel <ul style="list-style-type: none"> Haben wir alle relevanten Informationen zu unseren Netzbetriebsmitteln (z. B. je Betriebsmittelklassen Anzahl, Alter, Typ)? Simulieren wir unsere Netztopographie für mögliche Unterbrechungsfälle? Haben wir genug Messtechnik? Und an den richtigen Stellen? Wie schnell erkennen wir heute Versorgungsunterbrechungen in unseren Ortsnetzen? </td> </tr> <tr> <td style="text-align: center;">Bewältigung</td> <td> Störungsdiagnose <ul style="list-style-type: none"> Ist der Prozess zur Störungsdiagnose im Zusammenspiel aus Leitstelle und Betriebspersonal effizient gestaltet? Funktioniert die Störungsartung reibungslos? Welche Wiederversorgungsstrategie haben wir? Haben wir unsere Wegzeiten für die Entstörungseinsätze optimiert? </td> </tr> <tr> <td style="text-align: center;">Nachbearbeitung</td> <td> Schadensanalyse <ul style="list-style-type: none"> Müssen wir unsere Netzbetriebsmittel stärker diversifizieren? Wird der Netzbetrieb ausreichend durch Digitalisierung unterstützt (IKT, Assistenzsystem, Automatisierung)? Muss unser Netzbetriebskonzept angepasst werden? Werten wir Störungen konsequent aus und berücksichtigen diese in der Planung? </td> </tr> </tbody> </table>	Phase		Prävention	Netzbetriebsmittel <ul style="list-style-type: none"> Haben wir alle relevanten Informationen zu unseren Netzbetriebsmitteln (z. B. je Betriebsmittelklassen Anzahl, Alter, Typ)? Simulieren wir unsere Netztopographie für mögliche Unterbrechungsfälle? Haben wir genug Messtechnik? Und an den richtigen Stellen? Wie schnell erkennen wir heute Versorgungsunterbrechungen in unseren Ortsnetzen? 	Bewältigung	Störungsdiagnose <ul style="list-style-type: none"> Ist der Prozess zur Störungsdiagnose im Zusammenspiel aus Leitstelle und Betriebspersonal effizient gestaltet? Funktioniert die Störungsartung reibungslos? Welche Wiederversorgungsstrategie haben wir? Haben wir unsere Wegzeiten für die Entstörungseinsätze optimiert? 	Nachbearbeitung	Schadensanalyse <ul style="list-style-type: none"> Müssen wir unsere Netzbetriebsmittel stärker diversifizieren? Wird der Netzbetrieb ausreichend durch Digitalisierung unterstützt (IKT, Assistenzsystem, Automatisierung)? Muss unser Netzbetriebskonzept angepasst werden? Werten wir Störungen konsequent aus und berücksichtigen diese in der Planung?
Phase									
Prävention	Netzbetriebsmittel <ul style="list-style-type: none"> Haben wir alle relevanten Informationen zu unseren Netzbetriebsmitteln (z. B. je Betriebsmittelklassen Anzahl, Alter, Typ)? Simulieren wir unsere Netztopographie für mögliche Unterbrechungsfälle? Haben wir genug Messtechnik? Und an den richtigen Stellen? Wie schnell erkennen wir heute Versorgungsunterbrechungen in unseren Ortsnetzen? 								
Bewältigung	Störungsdiagnose <ul style="list-style-type: none"> Ist der Prozess zur Störungsdiagnose im Zusammenspiel aus Leitstelle und Betriebspersonal effizient gestaltet? Funktioniert die Störungsartung reibungslos? Welche Wiederversorgungsstrategie haben wir? Haben wir unsere Wegzeiten für die Entstörungseinsätze optimiert? 								
Nachbearbeitung	Schadensanalyse <ul style="list-style-type: none"> Müssen wir unsere Netzbetriebsmittel stärker diversifizieren? Wird der Netzbetrieb ausreichend durch Digitalisierung unterstützt (IKT, Assistenzsystem, Automatisierung)? Muss unser Netzbetriebskonzept angepasst werden? Werten wir Störungen konsequent aus und berücksichtigen diese in der Planung? 								

detaillierte Ansicht

Bild 3. Beispielhafte Fragen des Quick-Checks »Resilienter Netzbetreiber« (ResiNetzCheck)

Ganzheitliche Organisationsgestaltung als Verzahnung von Risikobetrachtung und Krisenprävention

Diese komplexen und gestiegenen Anforderungen wirken sich auf das Organisationskonzept eines resilienten Netzbetreibers aus. Sie erfordern den Einsatz geeigneter Technik, umfangreiches Wissen und sachgerechte Qualifikationen beim Personal, eingeübte Problemlösungs- und Krisenbewältigungsstrategien, klare Rollen und Verantwortlichkeiten sowie eine gelebte Sicherheitskultur.

Ob das angestrebte ganzheitliche Organisationskonzept geeignet gestaltet ist, kann mit einem Resilienz-Quick-Check geprüft werden. Anhand eines fragen-gestützten Prüfkatalogs wird bewertet, ob ein Netzbetreiber ausreichende organisatorische, technische und personelle Vorbereitung getroffen hat und bezüglich Prävention, Entstörung sowie Nachbereitung von Störungen bis hin zu Blackouts gut aufgestellt ist. So können »Blind Spots« identifiziert werden, in denen Nachholbedarf besteht. Dieser Bewertungsansatz ist in **Bild 2** dargestellt.

Basis des Quick-Checks ist ein umfangreicher Fragenkatalog, der sich in verschiedene Dimensionen aufgliedert. In den Dimensionen Handlungsfelder (Mensch, Organisation, Technik), Handlungszeitraum (Prävention, Bewältigung, Nachbearbeitung) sowie Schadensausmaß (Störung, Notfall, Krise) werden Einschätzungen mit den Mitarbeitern diskutiert. Ergebnis ist eine Bewertung auf einer Skala von »trifft zu« bis »trifft gar nicht zu«. Alle Fragen zielen darauf ab, das Unternehmen bezüglich seines Reifegrads zur Früherkennung von, zur Wiederversorgung bei und zur Lernbereitschaft aus Krisenfällen zu hinterfragen.

In **Bild 3** sind exemplarische Fragen des Quick-Checks in den drei genannten Themenbereichen dargestellt.

Handlungsfeld Mensch

Im Handlungsfeld Mensch stehen personalseitige Faktoren auf individueller Ebene im Fokus – zum Beispiel Situationsbewusstsein oder Ortskenntnis, Qualifikationen, menschliche Fehler oder psychische Beanspruchung. Es werden die betrieblichen Rahmenbedingungen des Wissensaufbaus und der Kompetenzentwicklung der Mitarbeiter für Krisenfälle und Ausnahmesituationen bewertet. Dabei spielen in der Prävention unter anderem die Schnittstellen zu technischen Systemen und deren ergonomische Gestaltung bei der Bedienung eine wichtige Rolle, wie der

Stromausfall in Lübeck im Jahr 2018¹⁰ deutlich demonstrierte.

Weitere Themen sind in der Phase der Krisenbewältigung beispielsweise Verfahren, die den schnellen Aufbau eines Lagebilds unterstützen und in der Phase der Nachbereitung die Einschätzung zum gemeinsamen Verständnis von Fehlerzuständen oder dem Erkennen von Cyberangriffen. Zur Nachbearbeitung wird zudem ermittelt, inwiefern bereits eine nicht-punitiv Fehlerkultur gelebt wird. Das Melden und Analysieren von Fehlern, ohne persönliche Sanktionen fürchten zu müssen, ist in dieser Kultur selbstverständlich, und eigene Fehler werden nicht vertuscht. Ziel der Bewertung im Handlungsfeld Mensch ist es, Lücken und Handlungsbedarf zu erkennen. So kann durch gezielte Maßnahmen beim Personal und bei der Arbeitsgestaltung erreicht werden, dass im Krisenfall – also unter Stress und Zeitdruck – möglichst sicher und fehlerfrei gehandelt wird.

Handlungsfeld Organisation

Das zweite Handlungsfeld thematisiert die organisatorischen Rahmenbedingungen, unter denen Struktur und Prozesse des Krisenmanagements im konkreten Fall aktiviert werden müssen. Diese Sonderorganisation – als eine koordinierende Stabsstelle oder als Team für den Krisenfall – ist hinsichtlich ihrer Handlungs- und Kommunikationsfähigkeit zu überprüfen. Der Quick-Check hinterfragt die vereinbarten Standardprozeduren, die Kommunikationsregeln und die festgelegten Verantwortlichkeiten sowie die Entscheidungsbefugnisse immer mit Blick auf eine hohe Resilienz. Dabei spielen Fragen nach verfügbaren Personalkapazitäten, räumlichen Möglichkeiten oder Einsatzfahrzeugen sowie nach der Verfügbarkeit technischer Mittel eine wichtige Rolle. Vor allem werden das Vorgehen in der Fehlerortung und die häufig komplexen organisationsübergreifenden Abstimmungsprozesse mit anderen Teilen der Krisenorganisation überprüft – zum Beispiel mit der Kommune oder dem übergeordneten Netzbetreiber.

Handlungsfeld Technik

Im dritten Handlungsfeld Technik wird bewertet, ob Netztechnik und eingesetzte Werkzeuge wie Software, Sensorik und Steuerung für einen resilienten Netzbetrieb ausreichen. Dabei können Netzbetriebsmittel selbst Ursache einer Störung sein (zum Beispiel Kabelfehler),

aber auch zur Wiederversorgung herangezogen werden (beispielsweise steuerbare Trennstellen).

Für die Prävention ist es notwendig, relevante Informationen über Netzbetriebsmittel vollständig, in hoher Qualität und transparent aufzubereiten. Die steigende Zahl von Sensoren im Netz hilft, Versorgungsunterbrechungen zu erkennen. So lässt sich durch eine geeignete Anzahl und Platzierung der Sensoren die Effizienz steigern. Darüber hinaus sind geeignete Prozesse zur Störungsdiagnose (Ortung sowie Bewertung) und Wiederversorgung für die Leitstelle und das Betriebspersonal notwendig. Abschließend muss in der Nachbereitung geprüft werden, ob die Störung durch andere Netzbetriebsmittel hätte verhindert werden können (zum Beispiel »Klumpenrisiko«), ob ein gesteigerter Digitalisierungsgrad bei der Bewältigung hilfreich gewesen wäre und welche Auswirkungen die Störung künftig für Planung und Betrieb hat.

Fazit

Der ganzheitliche Organisationsansatz plädiert dafür, den Blackoutfall nicht nur als seltenes Ausnahmeereignis zu denken, das mit der Erfüllung der gesetzlichen Vorgaben kontrolliert werden kann. Resilienz im Netzbetrieb bedeutet vielmehr, proaktiv die komplexer werdenden Anforderungen zu antizipieren und entsprechend gegenüber den eigenen Effizienzüberlegungen zu priorisieren. Der Krisenfall wird damit zu einem eigenen, gleichwertigen Betriebsmodus, der besondere Fähigkeiten von Mensch, Organisation und Technik erfordert. Eine kritische Bestandsaufnahme ist ein erster Schritt zu einer aktiven Auseinandersetzung mit den steigenden Herausforderungen.

>> **Corinna Semling**,
Projekt-Managerin,
BET Büro für Energiewirtschaft und
technische Planung GmbH, Aachen

Simon Haas,
Junior-Berater,
BET Büro für Energiewirtschaft und
technische Planung GmbH, Aachen

Dr. Sören Patzack,
Projekt-Manager,
BET Büro für Energiewirtschaft und
technische Planung GmbH, Aachen

Dr. Olaf Unruh,
Geschäftsführer,
BET Büro für Energiewirtschaft und
technische Planung GmbH, Aachen

>> corinna.sembling@bet-energie.de
>> www.bet-energie.de

¹⁰ www.ln-online.de/Lokales/Luebeck/Stromausfall-Menschliches-Versagen-loeste-Blackout-in-Luebeck-aus.