

der gemeinderat

Das unabhängige Magazin für die kommunale Praxis

www.treffpunkt-kommune.de

Kosten unter Kontrolle

GEBÜHREN FÜR DEN FRIEDHOF
RECHTSSICHER KALKULIEREN



EXTRA: DIE BESTEN

*Stromnetze*

Den Blackout im Blick

Wie soll es sein: Sollten Stadtwerke und kommunale Unternehmen stärker in den Schutz ihrer Anlagen investieren oder in den Aufbau redundanter Systeme – oder beides?

DER AUTOR

Jan Syré ist Mitglied des Vorstands und Politischer Sprecher im VST – Verband Sichere Transport- und Verteilnetze/ KRITIS e.V.

Der Strom fließt wieder in Berlin nach dem Brandanschlag auf die Infrastruktur, die Frage aber bleibt: Wie lässt sich die Sicherheit der kommunalen Stromnetze gewährleisten? Der Appell vom Verbandsexperten Jan Syré: Sabotageschutz und Redundanz gleichzeitig denken – und realisieren, um wie viel es dabei geht.

Die Sicherheit der Stromnetze stellt eine der größten Herausforderungen für Kommunen und Stadtwerke dar. Der Brandanschlag auf eine relevante Berliner Stromkabelbrücke im Januar 2026 hat die Verwundbarkeit kritischer Infrastrukturen durch gezielte Angriffe spektakulär ins öffentliche Bewusstsein gerückt. Von großflächigen Stromausfällen bis zu erheblichen Einschränkungen der Daseinsvorsorge reichten die Auswirkungen des Vorfalls. Infolgedessen ist eine umfassende Analyse der aktuellen Schutzmechanismen und der Resilienz kommunaler Stromnetze unerlässlich, um die Versorgungssicherheit nachhaltig zu gewährleisten.

Sabotageakte, hybride Bedrohungen und gezielte Störungen rücken näher an den Alltag heran, während die Bevölkerung eine Versorgung erwartet, die selbst im Krisenfall stabil bleibt. Für Stadtwerke und kommunale Unternehmen stellt sich damit eine zentrale Frage: Sollten sie stärker in den Schutz ihrer Anlagen investieren – oder in den Aufbau redundanter Systeme, die einen schnellen Wiederanlauf ermöglichen? Die Antwort fällt zunehmend eindeutig aus: Es geht nicht um ein Entweder-oder, sondern um ein intelligentes Zusammenspiel beider Sicherheitsphilosophien.

Der Schutz vor Sabotage bleibt ein unverzichtbarer Bestandteil der Daseinsvor-



Foto: Adobe Stock/luchschentF

sorge. Zugangskontrollen, Überwachungssysteme, bauliche Maßnahmen und geschultes Personal können die Wahrscheinlichkeit eines erfolgreichen Angriffs deutlich reduzieren. Doch selbst die beste Prävention stößt an Grenzen. Kritische Infrastrukturen sind weit verzweigt, oft über große Flächen verteilt und nicht vollständig abschottbar.

HUNDERTPROZENTIGER SCHUTZ IST NICHT REALISIERBAR

Grundsätzlich ist es so gut wie unmöglich, die Versorgungsinfrastrukturen zu 100 Prozent gegen Angriffe zu schützen. Weder in der Stadt noch auf dem Land. Es gibt allein rund 500.000 Strommasten in Deutschland in der Fläche – diese eine Zahl mag verdeutlichen, welchen Herausforderungen man sich stellen muss.

Die jetzt im Januar 2026 oder auch beim ersten Anschlag im Sommer letzten Jahres in Berlin zerstörten Komponenten liegen leider nicht auf Lager, sondern müssen teilweise erst hergestellt und vor Ort schrittweise wieder aufgebaut werden – unter widrigen Wetterbedingungen Anfang Januar, die erhebliche physische Herausforderungen an die Fachleute wie an das Material stellten. →



Foto: Adobe Stock/Fotolyse

Der Bundestag hat Ende Januar das neue Gesetz zum Schutz kritischer Infrastruktur beschlossen. Eine der Herausforderungen bleibt die Umsetzung – nicht jeder Strommast lässt sich sichern.

Wer darum allein auf Abwehr setzt, riskiert im Ernstfall lange Ausfallzeiten – und damit genau das, was verhindert werden soll: eine Versorgungslücke, die das Vertrauen der Bevölkerung erschüttert.

WAS REDUNDANZ BRINGEN KANN

Deshalb gewinnt die zweite Sicherheitslinie an Bedeutung: Redundanz. Sie akzeptiert, dass Störungen nie vollständig auszuschließen sind, und sorgt dafür, dass ein Ausfall nicht zur Krise wird. Alternative Einspeisepunkte, mobile Notstrom- oder Wasseraufbereitungseinheiten, redundante Leitstellen oder die Fähigkeit zum Inselbetrieb im Stromnetz sind Beispiele dafür, wie kommunale Unternehmen ihre Resilienz erhöhen können. Redundanz ist kein Zeichen von Schwäche, sondern Ausdruck einer modernen Sicherheitskultur, die auf Robustheit statt auf Unverwundbarkeit setzt.

Gerade das Zusammenspiel beider Ansätze macht Systeme widerstandsfähig.

Schutzmaßnahmen gewinnen an Wirksamkeit, wenn Angreifer wissen, dass ein Ausfall kaum Wirkung zeigt. Gleichzeitig ermöglicht Redundanz, Anlagen zeitweise vom Netz zu nehmen, um sie zu modernisieren oder zu härten – ohne die Versorgung zu gefährden.

TRAINING IN NEUER KOMPLEXITÄT

Für die Praxis bedeutet das: Übungen und Sicherheitstests müssen sich weiterentwickeln. Künftig sollten Szenarien nicht mehr isoliert betrachtet werden. Stattdessen gilt es, kombinierte Lagen zu trainieren – etwa einen Einbruch in eine Netzstation, gefolgt von der Umschaltung auf Ersatzpfade; oder einen Cyberangriff auf die Leitstelle, der den Übergang in den manuellen Betrieb erfordert.

Ebenso wichtig ist die Verzahnung technischer, organisatorischer und kommunikativer Elemente. Eine Störung betrifft nicht nur den Netzbetrieb, sondern auch die Krisenkommunikation, die Zusammenarbeit mit Feuerwehr, Polizei

und THW sowie die Entscheidungswege in Verwaltung und Politik.

„Das voraussichtlich im ersten Quartal 2026 in Kraft tretende KRITIS-Dachgesetz und das Ende 2025 in Kraft getretene NIS2-Umsetzungsgesetz werden zusammen zu einem deutlich höheren und ganzheitlicheren Sicherheitsniveau von Versorgungsnetzen führen“, sagt Markus Heinrich, Justiziar des VST-Kritis. „Cyber, physische und organisatorische Resilienzplichten werden erstmals systematisch verzahnt. Für Betreiber von Energie, Wasser und sonstigen Versorgungsnetzen bedeutet das mehr Pflichten, aber auch mehr Verlässlichkeit und Standardisierung in Planung, Betrieb und Krisenbewältigung.“

DASEINSVORSORGE ALS ZENTRALES GUT

Stresstests sollten regelmäßig stattfinden und nicht als einmalige Pflichtübung verstanden werden. Wiederanlaufzeiten müssen gemessen, Redundanzpfade unter realistischen Bedingungen geprüft und Schwachstellen systematisch ausgewertet werden. Die gewonnenen Erkenntnisse sollten direkt in Investitionsentscheidungen einfließen – denn Resilienz ist kein Zustand, sondern ein fortlaufender Prozess.

Am Ende geht es um mehr als technische Sicherheit. Kommunale Unternehmen tragen Verantwortung für das Vertrauen der Bevölkerung in die Daseinsvorsorge. Dieses Vertrauen entsteht, wenn klar wird, dass sowohl der Schutz der Netze als auch der schnelle Wiederanlauf im Ernstfall gewährleistet sind. Wer beides zusammendenkt, schafft nicht nur Sicherheit, sondern Stabilität – und damit die Grundlage für eine verlässliche Versorgung in einer zunehmend unsicheren Welt.

In Berlin waren viele daran beteiligt: Polizei, THW, Rettungsdienste, Feuerwehr, Bundeswehr und Netzbetreiber aus dem gesamten Bundesgebiet sowie viele ehrenamtliche Helfer vor Ort. Mit großem Einsatz, mit Personal und Material wurde solidarisch geholfen – in der Nachbarschaft und über Grenzen hinweg, Hand in Hand. Dieses Engagement zeigt, was es bedeutet, füreinander da zu sein, wenn es darauf ankommt – im Dunkeln, in Eiseskälte, im Stress, im Ernstfall.

Jan Syrë