Ä8 Schutz und Resilienz der kritischen Energieinfrastruktur in Leipzig

Antragsteller*in: Marco Tiedtke (KV Leipzig)

Änderungsantrag zu A3

Nach Zeile 46 einfügen:

1. Technische Resilienz

Stromversorgung als Voraussetzung für weitere kritische Infrastrukturen ist die technische Resilienz maßgeblich.

Für Stromversorgung:

- Konsequente Umsetzung des n-1-Prinzips (eine Anbindung mehr als notwendig, in räumlicher Trennungvoneinander) auf allen Netzebenen (Höchstspannung, Mittelspannung, Niederspannung): Bei Ausfall einer beliebigen Komponente (Leitung, Transformator, Knotenpunkt) muss die Versorgung über alternative Pfade aufrechterhalten bleiben.
- Umbau von Stern- und Stichstrukturen zu Ringnetzen, um redundante Versorgungswege zu schaffen.
- Schnelle Ersatzversorgungsmechanismen und automatische Lastumschaltung bei Störungen.
- (Vertiefung der) Zusammenarbeit mit den Leipziger Stadtwerken zur systematischen Identifikation und Beseitigung von Single Points of Failure im Leipziger Stromnetz.

Für Mobilfunkinfrastruktur:

- Redundante Anbindung von Mobilfunkmasten an verschiedene Stromversorgungswege.
- Regelmäßige Prüfung ob die Stadt Leipzig und zugehörige Unternehmungen nach KritisV oder NIS-2 planen oder handeln müssen
- Notstromversorgung von relevanten Mobilfunkstandorten für mindestens 72 Stunden.
- Prüfung und Förderung alternativer Backhaul-Verbindungen (Glasfaser, Richtfunk) zur Vermeidung von Single Points of Failure in der Datenanbindung.
- Förderung des Ausbaus des 5G-Netzes mit Fokus auf Versorgungssicherheit kritischer Einrichtungen.

2. Dezentrale Energieversorgung und Inselfähigkeit

- (Massiver) Ausbau von Photovoltaik-Anlagen mit Batteriespeichern auf kommunalen Gebäuden, insbesondere an Schulen, Krankenhäusern, Feuerwachen, Kita- und Pflegeeinrichtungen, Verwaltungsgebäuden und Notunterkünften.
- Inselbetriebsfähigkeit für kritische städtische Liegenschaften, damit diese bei großflächigem Stromausfall weiterhin autonom versorgt werden können.
- Förderung von Quartierspeichern und Energiegemeinschaften, um dezentrale Versorgungsinseln zu schaffen.
- Netzintegration dezentraler Erzeugung zur Erhöhung der Versorgungssicherheit.

3. Offener Zugang zu KRITIS-Daten für Sicherheit

Anstelle von Geheimhaltung, die das Risiko von Baggerbissen erhöht und Einsatzkräfte bei Großschadenslagen gefährdet:

- Beibehaltung und Verbesserung öffentlich zugänglicher Leitungspläne für Tiefbauunternehmen zur Vermeidung versehentlicher Beschädigungen (die Hauptursache für Störungen).
- Bereitstellung präziser Infrastrukturdaten für Feuerwehr, THW und Rettungsdienste zur schnellen und sicheren Bewältigung von Großschadenslagen.
- Verzicht auf „Security through Obscurity": Die physische Erkennbarkeit von Infrastruktur (Masten, Umspannwerke, Trassen) macht Geheimhaltung praktisch wirkungslos.

4. Investition statt Überwachung

Verzicht auf ineffektive symbolische Sicherheitsmaßnahmen:

- Keine Ausweitung der Videoüberwachung im öffentlichen Raum zum KRITIS-Schutz, da Kameras Sabotagen nicht verhindern, sondern allenfalls Ermittlungsansätze nach erfolgter Tat liefern.
- Umleitung dieser Ressourcen in technische Resilienzmaßnahmen, die tatsächlich Versorgungsausfälle verhindern.

Stattdessen
Investition in Substanz:

- Die für Überwachungsinfrastruktur vorgesehenen Mittel sind in Netzredundanz, dezentrale Energieerzeugung und Speicherlösungen zu investieren.

5. Krisen- und Notfallmanagement

- Aktualisierung kommunaler Notfall- und Krisenpläne für großflächige Stromausfälle unter Berücksichtigung von Mobilfunkausfällen.
- Regelmäßige realistische Übungen mit Feuerwehr, Rettungsdiensten, Polizei, Energieversorgern und Mobilfunkbetreibern, die gleichzeitige Ausfälle von Strom und Mobilfunk simulieren.
- Sicherstellung der Notstromversorgung für kritische kommunale Einrichtungen und Mobilfunkstandorte in deren Nähe.
- Etablierung alternativer Kommunikationswege (BOS-Funk, Satellitentelefonie) für Einsatzkräfte.

6. Kooperation und Infrastruktur-Monitoring

- Etablierung eines regelmäßigen Austauschs zwischen Stadtverwaltung, Leipziger Stadtwerken, Mobilfunkbetreibern, Polizei, Feuerwehr und Katastrophenschutz.
    - Transparente Dokumentation der Netzresilienz:
      Wo existieren Single Points of Failure? Welche Stadtteile sind bei Ausfall bestimmter Komponenten in welchem Umfang betroffen?
- Jährlicher (öffentlicher) Resilienzbericht über den Zustand der kritischen Infrastruktur in Leipzig.

7. Information und Empowerment der Bevölkerung

- Entwicklung einer städtischen Informationskampagne zur persönlichen Vorsorge bei längerem Strom- und Mobilfunkausfall.
- Bereitstellung praktischer Handreichungen: Notvorräte, batteriebetriebene Radios, Powerbanks, Treffpunkte bei Kommunikationsausfall.
- Förderung von Nachbarschaftsnetzwerken zur gegenseitigen Unterstützung in Krisenlagen.

8. Zivilmilitärische Zusammenarbeit (ZMZ)

- Sicherstellung klar geregelter Kommunikationswege zur Bundeswehr im Rahmen des Katastrophenschutzes für unterstützende Hilfeleistungen bei großflächigen Ausfällen.

9. Förderung und Finanzierung

- Aktive Akquise von Bundes- und Landesmitteln aus Förderprogrammen für Klimaschutz, Digitalisierung und Katastrophenschutz.
- Priorisierung von Resilienzinvestitionen bei der Haushaltsplanung.
- Einbindung der Leipziger Stadtwerke als strategischer Partner mit entsprechenden Investitionsverpflichtungen.
- Erforderliche zusätzliche Mittel sind dem Stadtrat mit konkreten Kostenkalkulationen und Wirkungsabschätzungen vorzulegen.

10. Berichtswesen und Evaluation

- Erster ausführlicher Bericht nach 12 Monaten über:
  - Identifizierte Single Points of Failure
  - Begonnene Resilienzmaßnahmen
  - Investitionsstand bei PV-Anlagen und Speichern
  - Stand der Mobilfunk-Notstromversorgung
- Jährlicher Fortschrittsbericht danach mit messbaren Resilienzindikatoren.

Begründung

Der Berliner Stromausfall vom Januar 2026 hat gezeigt: Symbolische Sicherheitsmaßnahmen wie Videoüberwachung und Geheimhaltung von Infrastrukturdaten bieten keine echte Resilienz. Sie scheitern an grundlegenden technischen Realitäten:

1. Kameras verhindern keine Störungen – weder durch Sabotage noch durch Naturereignisse oder Bauunfälle. Sie liefern allenfalls nachträgliche Ermittlungsansätze.
2. Geheimhaltung erhöht das Risiko – Leitungen bleiben physisch sichtbar, während Tiefbauunternehmen und Einsatzkräfte behindert werden.
3. Nur technische Redundanz schützt – Das n-1-Prinzip gewährleistet, dass ein einzelner Schaden nicht zum Versorgungsausfall führt, unabhängig vom Auslöser.

4. Mobilfunk ist kritische Infrastruktur – In Krisenlagen sind Smartphone-Alarme, Notrufe und Kommunikation zwischen Einsatzkräften unverzichtbar. Mobilfunk muss in die Resilienzstrategie integriert werden.

Die AG KRITIS formuliert es treffend: „Wer ernsthaft Infrastruktursicherheit betreiben will, muss bereit sein, in technische Substanz zu investieren statt in symbolische Sicherheitsmaßnahmen."

Leipzig muss den Mut haben, echte Prävention durch strukturelle Resilienz umzusetzen statt auf reflexartige, aber wirkungslose Überwachungsmaßnahmen zu setzen.

Quellen:

- AG KRITIS: N-1 oder Stromausfall – Berlins Infrastrukturproblem hat eine technische Lösung
- Bundesnetzagentur: Definition n-1-Kriterium