Das Szenario eines Blackouts ist real

Bei der Cybersicherheit herrscht grosser Fachkräftemangel, auch darum bleibt ein schwerer Angriff auf das Schweizer Stromnetz wahrscheinlich - Gérald Kurth

Trotz Massnahmen des Bundes bleiben Hackerangriffe eine Bedrohung für die Stromversorgung. Imago

Der elektrische Weltuntergang findet in Österreich statt. Oder besser: Hätte stattfinden sollen. 2019 warnte einer seiner Propheten, der Blackout- und Krisenvorsorgeexperte Herbert Saurugg, vor einem europäischen Stromausfall «in den nächsten fünf Jahren». Schon 2012 standen in Marc Elsbergs Technik-Thriller «Blackout» manipulierte, sogenannte intelligente Stromzähler am Anfang des Stromkollapses. Diese Smart Meters sind mittlerweile fast in jedem neueren Sicherungskasten verbaut.

Dass Stromzähler gehackt werden, ist nach wie vor ein Risiko. Das Blackout- Szenario ist also weder überbordende literarische Phantasie noch kommerziell getriebene Panikmache. Ohne Elektrizität geht nichts. Bei einem Stromausfall bricht die öffentliche Ordnung zusammen, der Verkehr steht still, die Versorgung mit lebenswichtigen Gütern bricht ab. Panik breitet sich aus, es kommt zu Plünderungen und sozialen Unruhen.

Der drohende Stromkollaps macht regelmässig Schlagzeilen: In Deutschland war die sogenannte Dunkelflaute im Dezember wochenlang Thema. Gerade eben stand Grossbritannien kurz vor einem landesweiten Stromausfall beziehungsweise vor Flächenabschaltungen. In beiden Fällen führte der Rückgang der Windenergie in Kombination mit erhöhter Stromnachfrage zu grosser Unsicherheit. Dänemark lieferte in letzter Sekunde über die neue Seekabelverbindung Viking Link Strom, kurz bevor in Britannien die Lichter wohl ausgegangen wären.

Die Schweiz als Stromdrehscheibe Europas mit 41 grenzüberschreitenden Leitungen ist immer mitbetroffen, wenn in einem Nachbarland eine – letztlich politisch bedingte – Dunkelflaute (AKW-Abschaltungen, Verzicht auf fossile Energien) eintritt.

Gravierender als die Mangellage

Das passiert laut Noël Graber, Mediensprecher beim nationalen Netzbetreiber Swissgrid, tendenziell häufiger. Swissgrid könne damit aber umgehen: «Internationale Redispatch-Massnahmen, also Eingriffe zur Anpassung der Leistungseinspeisung von Kraftwerken, gehören zur Routine des Netzbetriebes und kommen regelmässig vor.» Einer der wichtigen Vorteile des europäischen Verbundnetzes sei es, dass sich die Länder gegenseitig aushälfen, wenn sich Engpässe im Netz abzeichneten. Graber betont, dass die Schweiz auch deswegen «bisher nie» vor einem Blackout gestanden habe, seit Swissgrid für das Übertragungsnetz verantwortlich sei. Dank zahlreichen Speicherseen hat die Schweiz zudem bedeutende, kurzfristig abrufbare Stromreserven.

Das ist beruhigend, aber kein Grund zur Entwarnung. Viel gravierender als eine absehbare Mangellage wären für die Schweiz ohnehin die Auswirkungen von Cybersabotage. Kritische

Infrastrukturen, staatliche Institutionen, Unternehmen: Sie alle müssen damit rechnen, Opfer eines Cyberangriffs zu werden. Die Grenzen zwischen Nation-State-Akteuren, Erpressern oder Terrorgruppen verfliessen dabei zunehmend. Globalisierung bedeutet auch, dass ein digitaler Angriff auf die kritische Infrastruktur eines Landes Auswirkungen am anderen Ende der Welt haben kann. Kritische Infrastrukturen werden angegriffen, mit dem Ziel, Geld zu erpressen. Vor dem Hintergrund zunehmender geopolitischer Verwerfungen, aber auch, um einem anderen Staat Schaden zuzufügen.

Das wohl illustrativste Beispiel dafür, lange vor der russischen Invasion in der Ukraine 2022: Beim verheerenden Angriff von Sandworm, der Cybereinheit des russischen Militärnachrichtendienstes (GRU), frass sich 2015 Schadsoftware in kurzer Zeit durch die westukrainische Netzinfrastruktur. Von einem Angriff zwei Jahre später war nicht nur das weltgrösste Logistikunternehmen Maersk – wegen eines infizierten Computers – betroffen, sondern auch der staatliche russische Ölkonzern Rosneft. Russische Stellen schickten also eine Cyberwaffe los, deren Zerstörungspotenzial sie selber nicht präzise hatten einschätzen können.

Schwächen sind erkannt
2020 wurde zwar der Verband der europäischen Stromnetzbetreiber angegriffen, die Swissgrid-Systeme waren aber nicht kompromittiert. 2021 liess sich Swissgrid bewusst von ethischen Hackern angreifen, um Schwachstellen in der Netzarchitektur aufzuspüren. «Cybersicherheit ist für uns als Betreiberin der wichtigsten kritischen Infrastruktur der Schweiz zentral. Entsprechend haben wir uns in den letzten Jahren in diesem Bereich verstärkt», unterstreicht Graber.

Ist das Vorgehen von Swissgrid repräsentativ für den Rest der Branche? Sehr lange setzte die Schweiz auf freiwillige Massnahmen der Unternehmen. Mindestens im Strombereich führte dies aber nicht zu überzeugenden Ergebnissen. «Sensibilisierung und Aufklärung allein reichen nicht aus», betont Matthias Galus. Er ist beim Bundesamt für Energie Leiter der Sektion Geoinformation & Digital Innovation und war 2021 verantwortlicher Projektleiter einer umfangreichen Analyse.

Die Ergebnisse der damaligen Bestandesaufnahme zur «Cyber-Sicherheit und -Resilienz für die Schweizer Stromwirtschaft» stufte er als «bedenklich» ein. Das bedeutet auch: Komplexe, vernetzte Systeme sind so sicher wie ihr schwächstes Glied. Überspitzt ausgedrückt: Swissgrid mag zwar eine gehärtete Festung sein. Wenn jedoch ein Angreifer beim lokalen Stromproduzenten wegen veralteter Software mühelos eindringt, können in einer vernetzten Infrastruktur auch die professionellsten Schutzmassnahmen unterlaufen werden.

Die Stromunternehmen waren 2021 mehrheitlich ungenügend bis schlecht geschützt. Besonders schwach aufgestellt waren die Firmen beim Erkennen von Angriffen beziehungsweise bei der Rückkehr zum Normalbetrieb. Nach der ernüchternden Analyse vor vier Jahren hat sich, wie Galus unterstreicht, auf politischer und regulatorischer Ebene jedoch einiges getan.

Seit dem 1. Juli 2024 sind die Unternehmen der Stromwirtschaft per Stromversorgungsverordnung verpflichtet, einen Cybersecurity-Standard einzuhalten. Die Einhaltung der Vorgaben bei den Unternehmen wird von der Eidgenössischen Elektrizitätskommission geprüft. Im September 2023 beschloss das Parlament mit dem

veränderten Informationssicherheitsgesetz eine Meldepflicht für Betreiber kritischer Infrastrukturen. Im Juni 2024 war die Schweiz Mitorganisatorin der Übung «Cyber Europe». Über dreissig Betriebe nahmen an der Simulierung eines Cyberangriffs auf den Schweizer Energiesektor teil.

Zu Beginn dieses Jahres ist zudem die erweiterte Cybersicherheitsverordnung in Kraft getreten. Sie konkretisiert die Meldepflicht und legt Ausnahmen fest. Nun verfügt das Bundesamt für Kommunikation im Rahmen der nationalen Cyberstrategie über zwei spezialisierte Einheiten: Die Sektionen Marktzugang und Cybersicherheit sowie Sicherheit Netze und Dienste prüfen Netzsicherheit und -verfügbarkeit sowie Funkanlagen auf Einhaltung von Datenschutz und Privatsphäre.

Systeme nicht resilienter
Das Problembewusstsein in den Institutionen ist gewachsen. Noch aber sind die Systeme bei den Unternehmen nicht messbar resilienter geworden. Die Stromversorgungsverordnung definiert erst seit Mitte 2024 verpflichtende Mindestanforderungen auf Basis internationaler Normen für kritische Infrastrukturen. Das Anforderungsniveau richtet sich nach der Bedeutung des Unternehmens für die Schweizer Stromversorgung. Wo die Unternehmen bei der Umsetzung der entsprechenden Massnahmen jeweils stehen, ist nicht bekannt. «Wirksame Audits könnten einen Weg darstellen», sagt Matthias Galus vom Bundesamt für Energie.

Solche Überprüfungen der Sicherheitsstandards müssen von den besten Cybersecurity-Experten vorgenommen werden. Bloss: Qualifizierte Fachleute für Informationssicherheit und Sicherheitsarchitektur sind weltweit Mangelware, auch in der Schweiz. Mit Blick auf die sich verschärfende Bedrohungslage besteht deshalb dringender politischer Handlungsbedarf. Ein strategisches Bekenntnis zu einer grossen Ausbildungsinitiative ist das Gebot der Stunde. Die Eidgenossenschaft braucht schnell viele Cyber-Cracks auf der Seite des Gesetzes. Es wird länger als eine Legislaturperiode dauern und viel Geld kosten, bis diese Leute fit für den Markt oder die entsprechenden Bundesstellen sind. Die Schweiz wird aber kaum darum herumkommen, wenn sie ihre Stromversorgung – das Nervenzentrum aller kritischen Infrastrukturen – wirksam gegen Cyberangriffe schützen will.