

Foto: Ingo Bartussek - stock.adobe.com

Es gibt eine Reihe von möglichen Auslöseereignissen, die zu einem Versorgungsausfall führen können. Zum Schutz sollte man auf Resilienz und Perimetersicherheit setzen.

Resilienz & Perimeterschutz

Um Versorgungsausfälle zu verhindern oder abzuschwächen, ist Perimeterschutz essenziell. Er muss aber ins Gesamtkonzept eingebunden sein.

THOMAS FRIEDLMEIER

Das europäische Energie-Versorgungssystem zählt zu den verlässlichsten der Welt. Gleichzeitig nehmen – von der öffentlichen Wahrnehmung weitgehend unbeachtet – die Instabilitäten im europäischen Versorgungssystem stark zu. Wir verlassen uns auf die stabilen Zeiten der Vergangenheit mit sehr hoher Versorgungssicherheit und übersehen dabei die sich immer rascher ändernden Rahmenbedingungen (Rückspiegeleffekt). Je sicherer ein System scheint, desto anfälliger wird es gegenüber großen Störungen und desto weniger sind die Menschen auf einen solchen Fall vorbereitet (Sicherheits- beziehungsweise Verletzlichkeitsparadoxon).

Bisherige Ereignisse haben gezeigt, dass in der Regel eine Verkettung von an und für sich beherrschbaren Störungen einen Dominoeffekt bewirkt, der heute innerhalb weniger Sekunden zum Ausfall der Infrastruktur in weiten Teilen Europas führen kann. Viele Insider sind sich jedoch einig, dass es nicht mehr eine Frage des ob, sondern nur mehr des wann ist, bis es in Europa zu einem europaweiten Strom-, Infrastruktur- und/oder Versorgungsausfall kommt!

„Perimeterschutz dient als eine konkrete Maßnahme zur Verhinderung eines Versorgungsfalles."

Thomas Friedlmeier, Technischer Leiter der Lokavis Sicherheitstechnik GmbH.

Gründe und Auslöseereignisse für Krisen

Es gibt eine Reihe von möglichen Auslöseereignissen, die zu einem Versorgungsausfall führen können: technische Störungen und Fehler, menschliches Versagen, Naturereignisse, Sonnenstürme, Cyber-Angriffe, Terroranschläge et cetera. Es ist auch bekannt, dass der Umbau der Energieversorgung hin zu mehr erneuerbaren Energien zu größerer Instabilität der Netze führt. Parallel zum Ausbau der schwankungsintensiveren Solar- und Windkapazitäten werden konventionelle (und verlässlichere) Energieträger abgeschaltet. Massive Speicher- und Notfallkapazitäten müssen erst geschaffen werden. Der geplante Wegfall konventioneller, versorgungssicherer Kapazitäten trifft auf die politisch forcierte Elektrifizierung der Mobilität.

Das Bewusstsein um diese Verwundbarkeit ist zwar in der Zwischenzeit gestiegen, jedoch ist der Vorbereitungsgrad nach wie vor keinesfalls ausreichend. Immer wieder spielen dabei auch betriebswirtschaftliche Überlegungen, die sich vorwiegend an der Wachstum- oder Gewinnsteigerung orientieren, eine wichtige Rolle. Redundanzen und Reserven stellen in diesem Kontext totes Kapital dar, auf das man gerne verzichten möchte. Damit sind zukünftig weitreichende negative Folgen zu erwarten (aging infrastructures) und die dadurch verursachten Folgekosten und -schäden werden um ein Vielfaches höher sein.

Häufig wird angenommen, dass ein europaweiter Versorgungsausfall nur ein etwas größerer Stromausfall ist und dass die dafür vorhandenen Notfallpläne ausreichen würden. Aber dies kann ein folgenschwerer Trugschluss sein: ein Blackout führt zeitnah zum Ausfall weitgehend aller wichtigen stromabhängigen Infrastrukturen. Zeitnah mit dem Strom fällt so gut wie die gesamte Telekommunikation aus. Damit stehen die beiden wichtigsten Kritischen Infrastrukturen, ohne die so gut wie gar nichts funktioniert, nicht mehr zur Verfügung. Corona hat wiederum gezeigt, dass in westlichen Gesellschaften vielfach Systeme geschaffen wurden, die nur unter optimalen Bedingungen funktionieren. Sie sind fragil und nicht dafür geschaffen, mit größeren erwartbaren Störungen fertig zu werden. Just-in Time Mentalität, Kostensenkungswahn, Abhängigkeiten von Lieferketten und chinesischen Produktionsmonopolen – sogar bei kritischer Infrastruktur – zeugen von eklatanten Mängeln in Risikoverständnis, Risikobewusstsein, Risikovorsorge und Risikomanagement. Erfolgreiches Risikomanagement erfordert prospektive Risiken durchdacht zu haben.

Resilienz und Robustheit sind Grundvoraussetzung

Mit Resilienz wird die Fähigkeit verstanden, Störungen nicht nur zu verhindern, sondern mit diesen auch erfolgreich umzugehen. Etwa, um wieder möglichst rasch den Ausgangszustand zu erreichen oder noch besser, um auf zukünftige Störungen noch besser vorbereitet zu sein. Es geht daher primär nicht um die Verhinderung, sondern um die Vorwegnahme („Antizipation“) beziehungsweise aktive Bewältigung von möglichen beziehungsweise bereits eingetretenen Störungen. Der Begriff der „Resilienz“ scheint nicht wirklich zu technischen Problemen zu passen, auch wenn er dafür gerne verwendet wird. Für technische Systeme oder Infrastrukturen wird daher auch der Begriff der Robustheit verwendet.

Versorgungssicherheit bei den Kritischen Infrastrukturen ist für die Gesellschaft überlebenswichtig! Die Existenz unserer Gesellschaft ist abhängig von der Sicherstellung ihrer Versorgung mit verschiedensten Produkten, Funktionen und Dienstleistungen. Organisationen und Einrichtungen aus den Sektoren Energie, Transport und Verkehr, Wasser, Finanz- und Versicherungswesen, Ernährung, Medien und Kultur, Staat und Verwaltung, Gesundheit sowie Informationstechnik und Telekommunikation zählen zu den Kritischen Infrastrukturen. Sie haben eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen – eine Störung oder Zerstörung kann schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche oder soziale Wohl der Bevölkerung oder die effektive Funktionsweise von Regierungen haben. Für Betreiber kritischer Infrastrukturen ist es wichtig, sich der bestehenden Gefahren bewusst zu machen und sich darauf einzustellen. Das bedeutet, Risiken im Vorfeld von Ereignissen so weit wie möglich zu erfassen, zu mindern und sich auf unvermeidbare Krisenfälle bestmöglich vorzubereiten.

Vorbeugen ist besser als Heilen – diese universelle Wahrheit hat ihre Gültigkeit in nahezu allen Lebensbereichen. Die Kosten eines eingetretenen Schadenfalls übersteigen fast immer die Kosten der Prävention. Generell ist es entschuldbar, ein Risikoereignis nicht korrekt vorherzusagen, nicht aber, Systeme zu konstruieren, die gegenüber dem Eintreten des Ereignisses fragil sind. Viel wirkungsvoller wäre es indes, vorbereitet zu sein. Mit entsprechender Prävention tritt Resilienz an die Stelle von Fragilität

Eine große Hürde stellt unser bisher erfolgreiches Wirtschafts- und Wachstumsdenken dar, das einen resilienten Systemwandel nur in sehr engen Bahnen zulässt. Jeder langfristig erfolgreiche Systemumbau erfordert kurzfristig einen höheren Ressourcenaufwand. Unser derzeitig gelebtes Effizienzstreben steht dabei im Widerspruch zu Reserven und Redundanzen, welche jedoch für ein robustes Systemdesign unerlässlich sind. Damit ist die Frage mehr nach der Effektivität, also dem Erreichen der richtigen Ziele zu stellen.

Schutz der Außengrenzen als essenzielle Maßnahme

Perimeterschutz dient als eine konkrete Maßnahme zur Verhinderung eines Versorgungsfalles. Die Sicherheitstechnik darf dabei keine Kompromisse eingehen. Die Anlagen sind 24 Stunden an 365 Tagen im Jahr im Einsatz und müssen jederzeit zuverlässig und störungsfrei arbeiten, um im entscheidenden Moment das Alarmsignal abzugeben, das Leben und Sachwerte rettet.

Höchste Ansprüche erfüllen hochwertige Perimetersysteme, die Kritische Infrastrukturen an der ersten Verteidigungslinie gegen Attacken, Sabotage, Diebstahl oder Personenschaden absichern. Der entscheidende Vorteil dieser Perimetersysteme liegt darin, dass durch eine sehr frühzeitige Detektion im Außenbereich wertvolle Reaktionszeit für Interventionsmaßnahmen gewonnen wird. Um ein Objekt wirkungsvoll zu schützen, sollte die Widerstandszeit gleich oder größer der Zeit sein, die das Sicherheitspersonal vom Zeitpunkt der Meldung bis zum Eintreffen am Meldeort benötigt.

Eine Strategie zur Etablierung eines effektiven Perimeterschutzes besteht aus Maßnahmen unterschiedlicher Bereiche. Dazu gehören mechanisch-bauliche, organisatorisch-personelle und elektronische Detektionsmaßnahmen. Entscheidend ist, dass die gewählten Einzelmaßnahmen untereinander abgestimmt sind und sich in ihrem Zusammenwirken additiv auf die Gesamtzielsetzung auswirken. Detektion kann am Perimeter (zum Beispiel über das Sensorkabel am Zaun), im Boden (etwa über das Sensorkabel im Boden) oder über dem Boden (beispielsweise Infrarot-Lichtschranke) ausgelöst werden.

Planung, Einbau und Instandhaltung einer Perimeter-Sicherungs-Anlage sollten durch spezielle Fachfirmen erfolgen. Denn am Anfang einer Perimetersicherung steht eine projektspezifische Sicherheitsanalyse sowie ein daraus abgeleitetes Sicherheitskonzept. Dieses ist von Fachfirmen (Planer und Errichter) in enger Zusammenarbeit mit dem Betreiber zu erstellen und wird für jedes Objekt individuell erarbeitet. ■

lokavis sicherheitstechnik GmbH:
www.lokavis-sicherheit.de