KRITIS-Betreiber

Schutz kritischer Infrastrukturen: Technik kann Täter stellen

Nach Anschlägen und Drohnenüberflügen rückt der physische Schutz von Energieanlagen in den Fokus. Die Technik ist da, sagt Sicherheitsexperte Thomas Hermes – doch viele Betreiber zögern noch, wirklich anzufangen.

Artikel von Stephanie Gust
veröffentlicht am 23.01.2026, 16:07 Uhr

Die Energiebranche braucht auch im Schwarzfall ein sicheres Kommunikationsnetz für Sprache und Daten. Bild: © IgorZh/AdobeStock

Der Brandanschlag auf eine Berliner Stromtrasse zu Jahresbeginn war kein Einzelfall. Mehrere ähnliche Vorfälle und wiederkehrende Drohnenüberflüge über sensible Anlagen haben gezeigt, wie verwundbar zentrale Infrastrukturen sind. Die Debatte über den Schutz kritischer Energieanlagen hat seitdem deutlich an Schärfe gewonnen.

Für Sicherheitsexperten ist die Lage allerdings nicht neu. Die technischen Lösungen für einen besseren Objekt- und Sabotageschutz existieren längst. Das Problem liegt weniger in der Technik als in der Umsetzung.

"Viele wissen, was zu tun ist, aber sie fangen nicht an"

"Viele wissen, was zu tun ist, aber sie fangen nicht an", sagt Thomas Hermes, Leiter des Geschäftsfelds Energie bei Securiton Deutschland und Vorsitzender eines Fachausschusses im BHE Bundesverband Sicherheitstechnik. Seit Jahren berät er Energieversorger und Netzbetreiber zu Perimeter- und Objektschutz. Seine Beobachtung ist ernüchternd. In zahlreichen Unternehmen werde noch immer abgewartet, statt konkrete Maßnahmen zu ergreifen.

> »
> Physische Sicherheit ist ohne IT-Sicherheit nicht zu haben – und umgekehrt.«

Was das KRITIS-Dachgesetz verlangt – und offenlässt

Der regulatorische Rahmen soll mit dem geplanten KRITIS-Dachgesetz klarer werden. Das Gesetz setzt auf einen All-Risk-Ansatz und verpflichtet Betreiber kritischer Anlagen zu Risikoanalysen und Resilienzplänen. Konkrete technische Vorgaben enthält der Entwurf bislang nicht. Die Details sollen über nachgelagerte Rechtsverordnungen des Bundesinnenministeriums geregelt werden. Für Hermes ist das nachvollziehbar, aber unzureichend. Er erwartet, dass die Verordnungen stärker präzisieren, welche Mindeststandards gelten sollen. Schon heute sei absehbar, dass einige Schwellenwerte zu hoch angesetzt seien.

Analysepflicht trifft auf Personalmangel

Zentral bleibt die Frage, wie Betreiber ihre Verwundbarkeit systematisch bewerten. Derzeit muss jedes Stadtwerk, jeder Netzbetreiber und jeder Versorger diese All-Risk-Analyse weitgehend eigenständig erstellen. Hermes sieht darin ein strukturelles Problem. Es gebe schlicht zu wenige Planer und Experten, die solche Analysen durchführen könnten. Eine fundierte Bewertung könne mehrere Monate dauern. Für Tausende potenziell betroffene Unternehmen sei das kaum leistbar.

Branche braucht Blaupausen statt Einzelkämpfertum

Sinnvoll wären aus Hermes' Sicht branchenweite Blaupausen oder Mindeststandards, erarbeitet über Fachverbände in Abstimmung mit Behörden wie BBK und BSI. Kooperationen zwischen Stadtwerken hält er ebenfalls für sinnvoll, da Netzbetreiber in diesem Punkt nicht im Wettbewerb stünden. Gleichzeitig beobachtet er Zurückhaltung in den Verbänden. Viele wollten ihren Mitgliedern keine hohen Kosten zumuten, solange der Gesetzgeber nicht klarer werde.

Perimeter, Videoanalyse und "Dome Security"

Technisch sind die Möglichkeiten bereits weit entwickelt. Moderne Perimetersysteme kombinieren mechanische Barrieren wie Zäune mit intelligenter Detektion. Hochauflösende Videoanalyse kann Eindringversuche frühzeitig erkennen und Fehlalarme reduzieren. Ergänzend kommen Drohnendetektions- und Abwehrsysteme zum Einsatz.

Hermes spricht von "Dome Security", einer Art Schutzkuppel über dem Gelände, die Boden- und Luftraumrisiken gemeinsam adressiert. Drohnen ließen sich heute erkennen, verfolgen und in definierte Bereiche umlenken oder kontrolliert landen. Militärische Drohnen wären dagegen Aufgabe von Bundeswehr oder Bundespolizei.

Millionenkosten – aber nicht für jede Anlage

Solche Systeme können allerdings teuer sein. Eine leistungsfähige Drohnenabwehr liege schnell im hohen sechs- bis siebenstelligen Bereich. Für besonders systemrelevante Anlagen könne das sinnvoll sein, sagt Hermes. Für jedes Umspannwerk sei es dagegen weder realistisch noch verhältnismäßig.

Praxis zeigt: Technik kann Täter stellen

Dass physische Sicherheit wirkt, zeigen Praxisbeispiele. Einige Übertragungsnetzbetreiber haben bereits früh eigene Sicherheitsstellen unterhalb der Vorstandsebene geschaffen und dutzende Anlagen nachgerüstet. In mehreren Fällen wurden Täter erfasst und der Polizei übergeben.

Zuletzt sei 2025 in einem 110-kV-Umspannwerk ein Eindringling nachts mit Hilfe lückenloser Perimeterdetektionssysteme gegen 23.40 Uhr entdeckt und festgenommen worden. Details zu Standorten oder Technik nennt Hermes aus Sicherheitsgründen nicht. Für ihn belegt der Fall jedoch, dass gut konzipierte Systeme zuverlässig funktionieren.

NIS 2 ist nicht das Dachgesetz – beides gehört zusammen

Auch die Abgrenzung zu NIS 2 ist wichtig. Während NIS 2 vor allem Cybersicherheit und IT-Prozesse regelt, zielt das KRITIS-Dachgesetz auf physische Resilienz. Beide Ebenen gehören zusammen. Wie in der IT brauche es auch im Objektschutz klare Prozesse, Verantwortlichkeiten und kontinuierliche Verbesserung.

Was Vorstände jetzt tun sollten

Für Geschäftsführungen und Vorstände bedeutet das, Sabotageschutz fest im Business Continuity Management zu verankern. Es brauche eigene Stellen, realistische Budgetabschätzungen und den Mut, mit Pilotprojekten zu starten. Viele Fragen ergäben sich erst in der Praxis, sagt Hermes. Wer nur plane und zögere, verliere Zeit.

Ausblick und Appell

Entscheidend wird sein, wie das Bundesinnenministerium die angekündigten Rechtsverordnungen ausformt. Sie müssen Orientierung geben, ohne sensible Details preiszugeben. Gleichzeitig braucht es politischen Willen, den physischen Schutz kritischer Energieinfrastrukturen verbindlicher zu machen.
Am Ende bleibt ein einfacher, aber zentraler Appell. Klein anfangen ist kein Problem – nicht anfangen ist es. Technik und Know-how sind vorhanden. "Betreiber kritischer Infrastrukturen müssen jetzt loslegen", so Hermes

NIS 2 und KRITIS-Dachgesetz

Worin liegt der Unterschied?

Zielrichtung

• **NIS 2** fokussiert auf Cybersicherheit.
Unternehmen müssen ein strukturiertes Informationssicherheits-Managementsystem aufbauen, Risiken bewerten, Vorfälle melden und ihre IT-Sicherheit regelmäßig nachweisen, häufig orientiert an ISO 27001.
• **KRITIS-Dachgesetz** zielt auf die physische Resilienz kritischer Anlagen.
Gefordert sind Risikoanalysen, Resilienzpläne sowie Maßnahmen zu Objekt- und Perimeterschutz, Zutrittskontrolle und Notfallreaktion.

Gemeinsame Logik

Beide Regelwerke folgen demselben Prinzip:
Risiken erkennen, Maßnahmen festlegen, regelmäßig überprüfen und kontinuierlich verbessern. In beiden Fällen stehen Prozesse und Verantwortlichkeiten im Mittelpunkt.

Wesentliche Unterschiede

• **Detailgrad**: NIS 2 ist bereits konkreter ausgestaltet und mit klareren Prüfmechanismen hinterlegt.
Das KRITIS-Dachgesetz bleibt bislang auf einer übergeordneten Ebene und verweist auf künftige Rechtsverordnungen des Bundesinnenministeriums.
• **Schutzobjekt**: NIS 2 schützt vor allem digitale Systeme und Netze.
Das Dachgesetz schützt Gebäude, Anlagen und physische Prozesse.

Warum beides zusammen nötig ist

Moderne Perimeter- und Videosysteme sind selbst IT-basiert und damit cyberangreifbar. Umgekehrt hilft die beste IT-Sicherheit wenig, wenn physische Zugänge unzureichend geschützt sind. Erst das Zusammenspiel von NIS 2 und KRITIS-Dachgesetz schafft echte Resilienz.

Haben Sie Fehler entdeckt? Wollen Sie uns Ihre Meinung mitteilen? Dann kontaktieren Sie unsere Redaktion gerne unter redaktion@zfk.de.