Kritische Infrastrukturen umfassend schützen

Von Holger Köster

Holger Köster

Geschäftsführer der HERSA-Unternehmensgruppe und Vorsitzender des Fachausschusses Wirtschaftsschutz im BDSW

Manchmal braucht es keine physische Gewalt, um verheerende Schäden anzurichten, mitunter genügt dafür ein Stromausfall. Ein paar Stunden Dunkelheit, und Krankenhäuser geraten in Notbetrieb, Logistikketten brechen zusammen, Wasserwerke stoppen ihre Versorgung: Unsere moderne Gesellschaft ist verletzlicher, als wir glauben möchten.

Kritische Infrastrukturen sind das Rückgrat unseres Landes, zugleich aber auch das bevorzugte Ziel hybrider Angriffe. Umso wichtiger ist es, diese Infrastrukturen nicht nur als technische Systeme zu begreifen. KRITIS sind mehr als Stromnetze, Kläranlagen oder Rechenzentren, sie sind Teil komplexer Versorgungsstrukturen, in denen Prozesse, Menschen und Organisationen ineinandergreifen. Wer sie schützen will, muss deshalb über rein technische Maßnahmen hinausdenken und ganzheitliche, widerstandsfähige Schutzkonzepte entwickeln.

Das geplante KRITIS-Dachgesetz ist ein überfälliger Schritt in diese Richtung. Es soll den Schutz kritischer Einrichtungen auf neue gesetzliche Grundlagen stellen und neben IT- auch physische Sicherheitsmaßnahmen verbindlich einfordern. Der Fachartikel „KRITIS unter Druck: Was das neue Dachgesetz leisten muss“ in dieser Ausgabe zeichnet die Hintergründe und politischen Entwicklungen rund um das Gesetz nach und zeigt auf, was es für Betreiber, Behörden und Sicherheitsdienstleister bedeuten könnte. Dabei wird deutlich: Das Gesetz ist nicht nur ein Regulierungsvorhaben, sondern eine Chance, den Schutz kritischer Infrastrukturen auf eine neue Stufe zu heben, vor allem aber auch eine Chance für Sicherheitsdienstleister, ihre Kompetenzen strategisch einzubringen.

Denn die Sicherheit Kritischer Infrastrukturen lässt sich nicht allein durch Normen oder IT-Schutzmaßnahmen gewährleisten. Sie erfordert ein umfassenderes Verständnis von Verwundbarkeit und Schutz, das auch physische Sicherheitsmaßnahmen, organisatorische Strukturen und klare Zuständigkeiten einbezieht. Zutrittskontrollen, Reaktionspläne, personelle Ressourcen und abgestimmte Prozesse sind ebenso entscheidend wie Firewalls und Verschlüsselung. Der Schutz unserer Infrastruktur ist eine gemeinsame Aufgabe und gelingt nur im Zusammenspiel von Staat und der privaten Sicherheitswirtschaft.

Ihr
Holger Köster

Bild: Nhan Hoang / unsplash.com

KRITIS unter Druck: was das neue Dachgesetz leisten muss

Weichenstellung für mehr Resilienz Kritischer Infrastrukturen

Von Andreas Albrecht

Strom, Wasser, IT, Transport: Kritische Infrastrukturen werden zunehmend zum Ziel hybrider Angriffe. Das geplante KRITIS-Dachgesetz soll für mehr Schutz sorgen. Doch was ist genau geplant? Wer ist betroffen? Und was bedeutet das für die Sicherheitswirtschaft? Ein Überblick.

Andreas Albrecht
Freier Fachredakteur und Journalist

Wenn der Strom ausfällt, ist schnell mehr betroffen als das Licht. Ohne Energie stehen Produktionsanlagen still, Kühlketten sind unterbrochen, Krankenhäuser geraten in Notbetrieb, der Verkehr kollabiert: In Marc Elsbergs Bestseller *„Blackout – Morgen ist es zu spät"* legt ein gezielter Hackerangriff die gesamte europäische Stromversorgung lahm. Die Folgen sind katastrophal: Chaos, Verunsicherung und Kontrollverlust erfassen innerhalb weniger Tage Gesellschaft, Wirtschaft und staatliche Strukturen.

Was im Roman noch Fiktion war, wird heute immer mehr zu einem möglichen realistischen Szenario. Denn die Zahl gezielter Angriffe auf Kritische Infrastrukturen (KRITIS) nimmt stetig zu, und diese verlaufen selten eindimensional. Sabotage trifft auf Cyberattacke, Erpressung auf menschliches Versagen, digitale Schwachstellen auf physische Lücken: Immer häufiger sind es hybride Bedrohungen, die Sicherheitsverantwortliche vor immer größere Herausforderungen stellen, im Energiesektor ebenso wie in der Gesundheitsversorgung, bei Wasserwerken, im Transport oder in der Logistik.

Das KRITIS-Dachgesetz kommt – aber wann?

Der politische Wille, Kritische Infrastrukturen besser zu schützen, ist deutlich erkennbar, wie unter anderem die intensiven Bemühungen um das KRITIS-Dachgesetz zeigen, das auf einer klaren europäischen Vorgabe basiert. Konkret geht es um die Umsetzung der EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie), die im Januar 2023 in Kraft getreten ist. Sie verpflichtet die Mitgliedstaaten, verbindliche nationale Regelungen zu schaffen, die den Schutz Kritischer Infrastrukturen sektorenübergreifend verbessern, im digitalen, aber vor allem auch im physischen Bereich.

Die neue Bundesregierung hat diesen Anspruch bereits Ende Februar 2025 im Koalitionsvertrag verankert, wenn auch äußerst lakonisch. Mit einem einzigen Satz wird hier ein KRITIS-Dachgesetz angekündigt (Zeile 2698), erklärt wird nichts.

Auch ein endgültiger Gesetzestext lässt weiter auf sich warten. Nach der Verschiebung des ursprünglich für Oktober 2024 vorgesehenen Gesetzes gilt unter Branchenexperten aktuell eine Verabschiedung Ende 2025 bis Anfang 2026 als realistischer Zeitrahmen. Klar ist aber bereits jetzt: Im Zentrum des KRITIS-Dachgeset-

Bild: Dmytro Vynohradov / unsplash.com

zes wird ein ganzheitlicher Ansatz stehen, der nicht nur digitale Risiken abdecken soll, sondern auch physische Gefahren berücksichtigt. Damit wird erstmals gesetzlich verankert, dass Betreiber von KRITIS-Einrichtungen nicht nur Firewalls und Verschlüsselung brauchen, sondern auch physische Sicherheitsmaßnahmen wie Zäune, Zutrittskontrolle, Videoüberwachung oder Objektschutz.

Ein Perspektivwechsel, der tief greift. Denn von dem neuen Gesetz werden nicht nur Großkonzerne mit eigener Sicherheitsabteilung, sondern auch kleinere Betreiber betroffen sein, etwa kommunale Wasserwerke, regionale Gesundheitsdienstleister oder mittelständische Logistikunternehmen. Viele von ihnen werden dann zum ersten Mal mit sicherheitsrechtlichen Pflichten konfrontiert und wissen dies möglicherweise heute noch nicht einmal.

Herausforderung und Chance zugleich für Sicherheitsdienstleister

Für die private Sicherheitswirtschaft zeichnen sich dabei neben neuen Herausforderungen auch neue Chancen ab. Denn mit der Einführung des KRITIS-Dachgesetzes steigt nicht nur der Druck auf die Betreiber, auch Dienstleister werden verstärkt in die Verantwortung kommen. Viele kleinere Unternehmen, insbesondere im kommunalen oder mittelständischen Bereich, dürften noch nicht über das notwendige Know-how verfügen, um komplexe Risikoanalysen, Sicherheitskonzepte oder Interventionspläne eigenständig zu entwickeln und umzusetzen. Die Folge: Der Bedarf an spezialisierter externer Unterstützung dürfte deutlich steigen, sowohl technologisch als auch personell. Für Anbieter aus der Sicherheitswirtschaft könnte sich damit ein dynamisch wachsender Markt eröffnen, der nicht nur kurzfristige Schutzmaßnahmen, sondern langfristige Sicherheitsarchitekturen verlangt.

Diese Entwicklung unterstreicht auch ein gemeinsames Grundsatzpapier des Bundesverbandes Sicherheitstechnik (BHE) und des Verbands für Sicherheitstechnik (VfS), in dem von einem grundlegenden „Paradigmenwechsel in der Sicherheitsarchitektur Deutschlands“ die Rede ist und ein sektorenübergreifender technologieoffener Ansatz gefordert wird. Zugleich mahnen die Verbände an, dass Zuständigkeiten klar definiert und gesetzliche Vorgaben realistisch umsetzbar sein müssten. Andernfalls drohten Überforderung und Ineffizienz, insbesondere bei kleineren KRITIS-Betreibern.

BBK: Kontrolle mit Fragezeichen

Eine zentrale Rolle bei der Umsetzung des KRITIS-Dachgesetzes soll das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) übernehmen. Als koordinierende Stelle ist es künftig dafür verantwortlich, KRITIS-Akteure zu identifizieren, Mindestanforderungen zu definieren und die Einhaltung zu überwachen. Damit wird das BBK zur Schnittstelle zwischen staatlicher Aufsicht, Betreiberverantwortung und Fachwissen aus Wirtschaft und Verbänden.

Doch dieser koordinierende Anspruch ist ambitioniert – und nicht frei von Kritik. Die zivilgesellschaftliche Initiative Open KRITIS etwa warnt vor einem zu weit gefassten oder unklar abgegrenzten Geltungsbereich. Sie fordert transpa-

rente Kriterien für die KRITIS-Zugehörigkeit, realistische Umsetzungsfristen und eine bessere Berücksichtigung bestehender Sicherheitsstrukturen. Ziel müsse es sein, Mehrarbeit zu vermeiden und stattdessen Synergien zu nutzen.

Mehr als IT: physische Sicherheit wird zur Pflicht

Ein wesentlicher Fortschritt des geplanten Gesetzes ist die Abkehr von der bisherigen Fokussierung auf IT-Sicherheit. Künftig sollen auch physische Risiken systematisch erfasst und entsprechende Sicherheitsmaßnahmen vorgeschrieben werden – von der Zutrittskontrolle über Videoüberwachung in einzelnen Betrieben bis hin zum Perimeterschutz ganzer Liegenschaften.

Für Sicherheitsdienstleister bedeutet das: Gefragt sind keine isolierten Produkte, sondern ganzheitliche Konzepte. Wer sich als Partner der Betreiber positionieren will, muss die betrieblichen Abläufe verstehen, branchenspezifische Risiken einordnen und praxistaugliche Lösungen entwickeln.

Investitionen mit Hebelwirkung

Allerdings stellt sich angesichts des zu erwartenden Aufwands eine entscheidende Frage: Wer soll das alles bezahlen? Der Verband für Sicherheitstechnik (VfS) plädiert hier für staatliche Investitionsimpulse. Konkret fordert er ein jährliches Budget von 20 Milliarden Euro zur Unterstützung von Mittelstand und KRITIS-Betreibern.

Ob diese Mittel in dieser Größenordnung fließen werden, bleibt abzuwarten. Klar ist jedoch: Ohne zusätzliche finanzielle Mittel, wie Förderprogramme oder steuerliche Anreize, könnten viele Unternehmen bei der Umsetzung der KRITIS-Anforderungen schnell an ihre Grenzen stoßen.

Es bleibt also für alle Beteiligten in Bezug auf das kommende KRITIS-Dachgesetz noch einiges zu tun. Für Betreiber bedeutet das: Sie müssen in Schutzmaßnahmen investieren, Risiken analysieren und Betriebsabläufe strukturieren. Für Sicherheitsdienstleister gilt es, kompetent zu beraten und tragfähige Lösungen zu liefern. Und für die Politik? Sie muss aus der Ankündigung endlich eine Verbindlichkeit machen. Sonst bleibt das „Dach" weiter im Rohbau stecken.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

BKA – Bundeslagebild Wirtschaftskriminalität 2024

Die polizeilich registrierten Wirtschaftsdelikte im Jahr 2024 stiegen gegenüber dem Vorjahr um 57,6 Prozent auf insgesamt 61.358 Fälle an. Hauptgrund hierfür ist eine Zunahme von 847,6 Prozent bei Fällen von Betrug und Abrechnungsbetrug im Gesundheitswesen. Zudem gewinnt das Tatmittel Internet mehr an Relevanz. Die Gesamtschadenssumme wird auf 2,76 Milliarden Euro beziffert.
www.bka.de

FitNIS2-Navigator bietet Hilfe bei NIS2-Umsetzung

Deutschland sicher im Netz e. V. (DsiN) mit der Universität Paderborn stellt ein kostenfreies Online-Tool zur Verfügung, das KMU-Unternehmen bei der Umsetzung der EU-Richtlinie NIS2 unterstützt. Das auch vom BMWE geförderte Projekt hilft mittels eines Navigators dabei, den individuellen Handlungsbedarf zu erkennen und konkrete Maßnahmen zur IT-Sicherheit zu entwickeln.
www.fitnis2.de

EHI-Studie: Inventurdifferenzen 2025

Die Studie ermittelt für das Jahr 2024 durchschnittliche Inventurdifferenzen in Höhe von 0,64 Prozent, bewertet zu Einkaufspreisen in Relation zum Nettoumsatz. Im gesamten stationären deutschen Einzelhandel summieren sich die Inventurdifferenzen auf 4,95 Milliarden Euro. Damit sind die Inventurdifferenzen im Vergleich zum Vorjahr um rund drei Prozent gestiegen.
www.ehi.org

CyMon 2025: Befragung zur Cybersicherheit

Der Kurzbericht zu den Umfrageergebnissen der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamts für Sicherheit in der Informationstechnik (BSI). Sieben Prozent der befragten Bürger waren allein in den vergangenen zwölf Monaten von Cyberkriminalität betroffen. Am wichtigsten sind für Informationssuchende Handlungsempfehlungen für den Ernstfall.
www.bsi.bund.de

RA Dr. Berthold Stoppelkamp
zuständiges Geschäftsführungsmitglied für den Fachausschuss Wirtschaftsschutz im BDSW