Das neue KRITIS-Dachgesetz (KRITIS-DachG) ist die nationale Umsetzung Deutschlands der CER-Richtlinie der EU. Mit dieser verpflichtet die EU Anlagenbetreiber im Umfeld kritischer Infrastruktur (siehe Infobox), auf die seit Jahren wachsenden Gefährdungen zu reagieren. Dabei dreht es sich nicht nur um die in den Medien oft genannte Cyberkriminalität, sondern ebenso um den physischen Schutz von Gebäuden.

KRITIS bedeutet auch physischer Schutz von Räumlichkeiten und Gebäuden

Der Fokus liegt hierbei auf dem Schutz dieser kritischen Infrastruktur gegen jegliche Gefährdungen physischer Art – seien es Naturkatastrophen oder von Menschen verursachte Bedrohungen. Denn das deutsche Gesetz geht von einem All-Gefahren-Ansatz aus. Betreiber kritischer Infrastrukturen sollen befähigt sein, gefährdende Vorfälle zu verhindern beziehungsweise diese abzuwehren oder deren Folgen zu begrenzen, um so eine umfassende Resilienz zu erreichen.

Konkret sieht das Gesetz dabei vor, dass die Betreiber geeignete und angemessene technisch sicherheitsbezogene und organisatorische Maßnahmen implementieren müssen, die auf die Technik bezogen „dem Stand der Technik“ entsprechen müssen. Mit anderen Worten: Es wird ein physischer Schutz von Räumlichkeiten gegen Einbruch, Brand und vergleichbare Gefahren sowie die Festlegung von Zugangsrechten gefordert. Detaillierte Vorgaben für die Umsetzung gibt es im Gesetz nicht, dafür aber eine Reihe von Beispielen. Festgelegt ist, dass die Maßnahmen in einem Resilienzplan dokumentiert werden und diese regelmäßig vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) überwacht werden können. Bei Nicht-Einhaltung der Maßnahmen drohen vermutlich Bußgelder in Millionenhöhe.

„Übersetzt man die Anforderungen des KRITIS-DachG in konkrete Komponenten der elektronischen Sicherheitstechnik, so

Jetzt zum KRITIS-Webinar am 22. April 2024 um 08:00 Uhr anmelden!

Unter https://t1p.de/4noxv

Vom KRITIS-DachG betroffene Betriebe

Zu den kritischen Infrastrukturen (KRITIS) zählen Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Darunter fallen Betriebe aus zehn KRITIS-Bereichen: Staat und Verwaltung, Energie, IT und Telekommunikation, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Medien und Kultur, Transport und Verkehr sowie Siedlungsabfall. Somit zählen auch Supermärkte, die im Jahr mehr als 500.000 Personen versorgen (die Schwellengrenze liegt bei 0,869 Tonnen/Jahr Lebensmitteln und 700 l/Jahr nicht alkoholischer Getränke pro Person) zur kritischen Infrastruktur.

müssen Betreiber kritischer Infrastrukturen eine Sicherheitslösung beispielsweise mit Instrumenten und Verfahren zur Überwachung der Umgebung, Detektionsgeräte sowie Zugangskontrollen inklusive Festlegung von Zugangsrechten und Räumlichkeiten und sensiblen Informationen installieren“, sagt Timm Schütz von Telenot.

Die Sicherheitsexperten von Telenot verfügen über jahrelange Erfahrung in der Begleitung von Unternehmen aus dem KRITIS-Bereich. Das Team berät in allen relevanten Fragen rund um den physischen Schutz von Gebäuden und hilft dabei, sich optimal auf die neuen Anforderungen vorzubereiten. Timm Schütz erläutert die Vorgehensweise des Teams von Telenot exemplarisch am Beispiel Einbruchschutz: „Wir klären zunächst mit dem Kunden, ob die Einrichtungen oder Anlagen überhaupt betroffen sind. Um das Objekt dann in einen passenden Grad gemäß DIN VDE 0833-3 beziehungsweise die passende VdS-Klasse einzuordnen, nutzen wir das Betriebsartenverzeichnis VdS 2559. Im Anschluss unterstützen wir den Kunden bei der Erstellung eines Sicherheitskonzepts und

machen eine Musterplanung. Zur Umsetzung des Konzepts gehört für uns auch die Erstellung eines Sicherheitshandbuchs. Dieses dient nicht nur der gesetzlichen Dokumentation, sondern ist ein wichtiges Werkzeug bei der Inbetriebnahme und Instandhaltung durch Fachbetriebe. Außerdem lassen sich die Daten als Grundlage nehmen, falls an einem weiteren Standort eine vergleichbare Sicherheitslösung implementiert werden soll."

Lebensmittelfilialisten, Energieversorger oder auch Rechenzentren ab bestimmten Schwellenwerten gehören laut KRITIS-DachG zur kritischen Infrastruktur. Die Gebäude, in denen sich die Einrichtungen befinden, müssen dann entsprechend gegen unbefugten Zutritt, Einbruch- und Brandgefahren geschützt werden. Oft kommen noch technische Störungen wie Ausfall der Klimatechnik (Erwärmung), Leckagen (Wassereintritt) oder Schmorbrände (Gasentwicklung) zum Tragen, die über eine Gefahrenmeldeanlage detektiert und auch an eine zentrale Meldestelle aufgeschaltet werden können.

Kritische Infrastruktur systematisch schützen

Damit Betreiber von kritischen Infrastrukturen die Resilienz ihrer Anlagen zuverlässig gewährleisten können, wird elektronische Sicherheitstechnik vor einem Einbau auf Herz und Nieren geprüft sowie entsprechend zertifiziert. Telenot hat etwa eine Freigabe für die Verwaltungssoftware compasZ 5500 als Teil des Zutrittskontrollsystems hilock 5000 ZK durch Atruvia, Digitalisierungspartner der Volks- und Raiffeisenbanken erhalten. Auch der Bundesverband der Energie und Wasserwirtschaft (BDEW), gemeinsam mit „Österreichs E-Wirtschaft", hat nach einer Prüfung bestätigt, dass die Einbruchmelde- und Übertragungstechnik von Telenot die strengen Sicherheitsanforderungen des Verbands erfüllt. Erste Energieversorger setzen bereits auf Sicherheitssysteme von Telenot. Ebenso verfügt das Telenot-Brandmeldesystem über alle relevanten Zulassungen, sodass das KRITIS-Thema umfangreich aus einer Hand gelöst werden kann.

Weitere Infos gibt es bei Telenot:

Kontakt Deutschland:
Tel. +49 7361 946-400 · info@telenot.de · telenot.com
Kontakt International:
Tel. +49 7361 946-4990 · info@telenot.com · telenot.com/en
Kontakt Österreich:
Tel. +43 7614 8258-0 · info@telenot.at · telenot.com
Kontakt Schweiz:
Tel. +41 52 544 17 22 · info@telenot.ch · telenot.com
Kontakt Luxemburg:
Tel. +352 44 15 44-1 · telenot@zenner.lu · zenner.lu