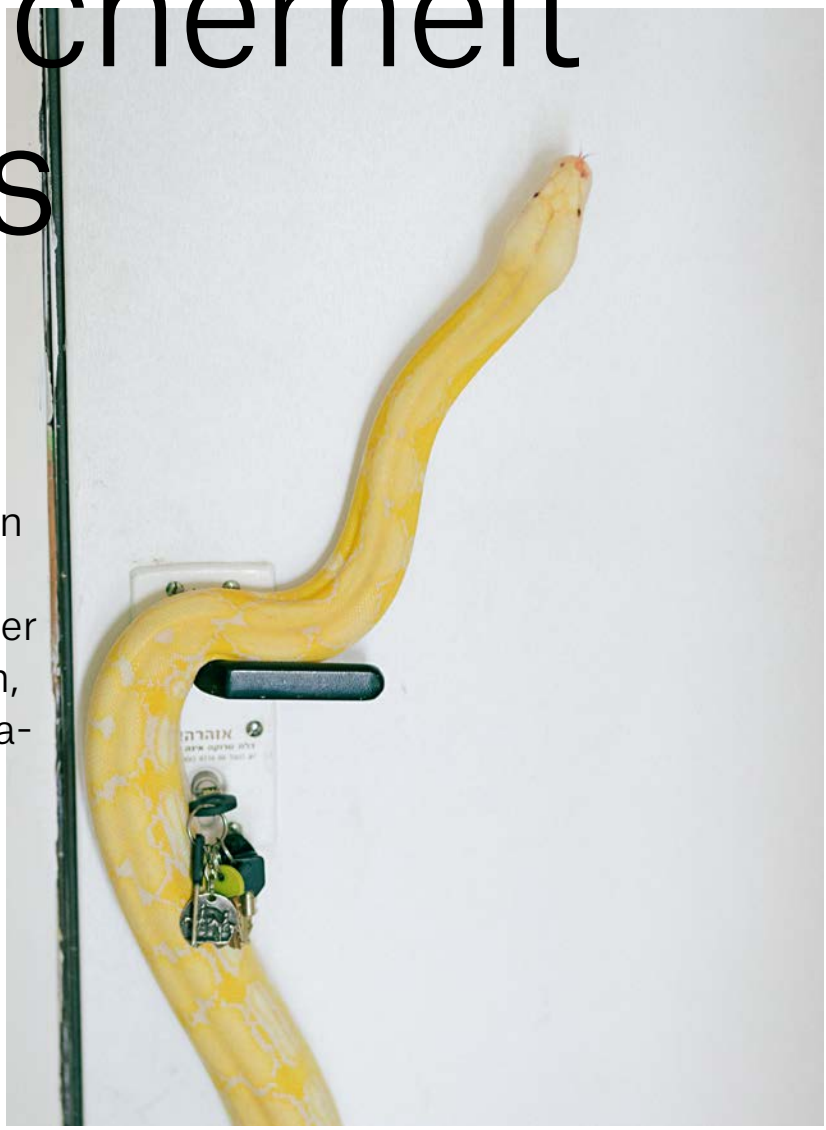
Mehr Sicherheit für Kritis



Das Kritis-Dachgesetz verpflichtet Betreiber kritischer Infrastrukturen zu verstärkten Schutzmaßnahmen. Davon sind nicht nur Energieversorger betroffen, sondern alle Firmen, die als Teil der kritischen Infrastruktur eingestuft werden. Das können bis zu 30.000 Organisationen sein.

Von Daniela Furkel

● Im November 2024 hat das Bundeskabinett seinen Entwurf für das Kritis-Dachgesetz beschlossen. Nach dem Inkrafttreten werden diejenigen Organisationen, die als kritische Infrastrukturen (kurz: Kritis) gelten, dazu verpflichtet, bis 2026 umfassende Maßnahmen zu ihrem physikalischen und digitalen Schutz zu ergreifen. „Dies sind Organisationen oder 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“, zitiert Mate Ursic, Business Development bei Dormakaba, die offizielle Definition. „Wie viele Unternehmen betroffen sind, ist keinesfalls selbsterklärend“, fährt er fort und sagt, dass Schätzungen zufolge bis zu 30.000 Betreiber und deren kritische Anlagen unter das neue Gesetz fallen können. Zu den Sektoren zählen unter anderem Energie, Transport und Verkehr, Gesundheit, Wasser und Ernährung, IT und Telekommunikation, Kommunen und öffentliche Einrichtungen sowie Finanzwesen und Versicherung.

„Nicht nur große Unternehmen sind betroffen, sondern auch viele Mittelständler“, ergänzt Rainer K. Füess, Vice President Marketing und Partner bei Atoria. Wie er in der Nachfrage der Unternehmen nach Informationen in Webinaren oder Whitepapern festgestellt hat, ist das offenbar noch nicht bei allen Betrieben angekommen. „Das mag daran liegen, dass noch nicht klar ist, wann das Kritis-Dachgesetz in Kraft tritt. Trotzdem sollten sich die Unternehmen schon jetzt damit beschäftigen.

Folgen für die Zutrittskontrolle

Was bedeutet das für die Zutrittskontrolle bei den Kritis-Unternehmen? „Sie sollten ihre bestehenden Zutrittskontrollsysteme überprüfen und an die neuen Sicherheitsanforderungen anpassen. Zutrittskontrolle muss sicherstellen, dass nur berechtigte Personen Zutritt erhalten und dies nachvollziehbar, revisionssicher und digital dokumentiert wird“, erklärt Samuel Wyss, Teamlead Product Management Access Control bei Interflex

Foto: Rona Bar & Ofek Avshalom / Connected Archives

Datensysteme. Die Unternehmen müssen sich im Klaren darüber sein, welche Gefahren bestehen, wer potenzielle Angreifer sein könnten und welche Bereiche physisch geschützt werden müssen. Er rät dazu, die bestehenden Systeme zu analysieren, um sicherzustellen, dass diese dem Stand der Technik entsprechen. Seiner Empfehlung nach sollten Unternehmen ein Zutrittskontrollsystem implementieren, das folgende Aspekte abdeckt:

- Vergabe von Zutrittsberechtigungen: Es sollte klar geregelt sein, wer zu welchem Zeitpunkt und aus welchem Grund Zutritt erhält.
- Compliance: Es muss nachvollziehbar sein, wer wann wem Zutrittsberechtigungen erteilt hat.
- Protokollierung der Zutrittsbewegungen: Es muss dokumentiert werden, wer wann und wo Zutritt hatte.

„Zusätzlich sollten Unternehmen eine dynamische Rechtevergabe nutzen, die sich aus der Organisation oder den Aufgaben ableitet“, sagt er. Hierbei können Mitarbeitende zeitlich begrenzte Zutrittsrechte für bestimmte Bereiche beantragen, die über einen mehrstufigen Freigabe-Workflow geprüft werden. Die Anfragen und Entscheidungen werden dokumentiert, damit gesetzliche und interne Richtlinien eingehalten werden. Sein Fazit: „Unternehmen, die bisher auf traditionelle Schließsysteme gesetzt haben, sollten auf moderne Zutrittskontrollsysteme umstellen, da diese die notwendige Protokollierung bieten und die erforderlichen Sicherheitskonzepte unterstützen, um aus unserer Sicht den gesetzlichen Anforderungen gerecht zu werden und Sicherheitslücken zu schließen.“

Diese Technik gilt als unsicher

Das sagt ganz ähnlich auch Rainer Füess: „Wer vor zwei Jahren eine Zutrittskontrolle eines namhaften Anbieters eingeführt hat, kann davon ausgehen, dass diese State of the Art ist. Aber wenn das System 15 Jahre alt ist, muss man genauer hinschauen.“ Denn meist ist es einfacher zu sagen, was unsicher ist – von Ausweismedien bis zu Schließanlagen – als in einem Satz die Technologien aufzuzählen, die die Kritis-Kriterien erfüllen. Als unsicher gelten zum Beispiel überholte Anlagen, die keine zentrale Protokollierung der Zutrittsbewegungen bieten. „Das erschwert Nachweise, ermöglicht den Verlust von Bewegungsdaten und verlangsamt die Reaktion auf sicherheitskritische Vorfälle“, so Samuel Wyss.

Rainer Füess ergänzt: „Nicht alle RFID-Systeme oder Ausweisverfahren bieten die benötigte Sicherheit.“ Als Beispiele nennt er die Ausweisverfahren Legic Prime und Mifare Classic.

„Diese wurden bereits vor 15 Jahren gehackt, sind aber immer noch in vielen Anwendungen wie Zutrittskontrolle und Zeiterfassung im Einsatz“, sagt Mate Ursic und fährt fort: „Mit einem vergleichsweise einfachen Gerät, einem RFID-Reader aus dem Internet für rund 200 Euro, kann man zuerst eine Zutrittskarte auslesen und das Gerät dann so umschalten, dass es die Karte elektronisch nachbildet. Am Ende lassen sich mit dem RFID-Reader all jene Türen öffnen oder Anwendungen nutzen, zu denen auch die Originalkarte Zutritt gewährt hätte.“ Laut den Anbietern gibt es modernere Verfahren, die nach dem heutigen Stand als sicher gelten, zum Beispiel Legic Advant oder Mifare Desfire.

Auch den traditionellen Schlüssel sollen Kritis-Unternehmen hinterfragen. Das Patent des Schlüssels sei nur zeitlich begrenzt gültig und nach zehn oder 20 Jahren ausgelaufen, so Mate Ursic: „Nach Ablauf des Patents könnte jeder den Schlüssel kopieren. Ähnlich verhält es sich, wenn Schlüssel verloren gingen, verlegt wurden oder man den Überblick verloren hat, wer wo mit welchen Berechtigungen Zutritt hat. All dies bedeutet, dass die Lebensdauer eines Schlosses ausgelaufen ist“, sagt er.

Kritis-Unternehmen müssen sich im Klaren darüber sein, welche Gefahren bestehen, wer potenzielle Angreifer sein könnten und welche Bereiche physisch geschützt werden müssen.

Die eigene Resilienz stärken

Das Kritis-Dachgesetz bringt noch viel mehr mit sich als die beschriebenen Folgen für die Zutrittskontrolle. Den Betreibern kritischer Anlagen werden Maßnahmen auferlegt, die ihre Resilienz stärken können. Dazu gehört die Erarbeitung und Umsetzung von Resilienzplänen, in denen auf der Basis von Risikoanalysen dargestellt wird, welche technischen, sicherheitsbezogenen und organisatorischen Maßnahmen zur Stärkung der Resilienz getroffen werden. Es gilt, unbefugten Zutritt zu verhindern und die physische Infrastruktur, das Personal sowie andere Vermögenswerte vor Risiken und Bedrohung zu schützen.

Zum aktuellen Stand ist jedoch noch vieles unklar. „Es herrscht eine allgemeine Verunsicherung gegenüber den aktuellen und künftigen rechtlichen Vorgaben. Es fehlen klare Regelungen. Wir hoffen, dass der Gesetzgeber diesbezüglich entweder nachschärft und Handlungsanweisungen gibt oder Spielräume lässt, solange die eingesetzten Sicherheitsmaßnahmen dem vielzitierten ‚Stand der Technik‘ entsprechen“, sagt Samuel Wyss. Trotz fehlender Klarheit rät Rainer Füess, sich schon jetzt mit dem Thema zu beschäftigen und die bislang eingesetzte Hard- und Software unter die Lupe zu nehmen: „Denn das Kritis-Dachgesetz kommt in jedem Fall auf die Unternehmen zu.“