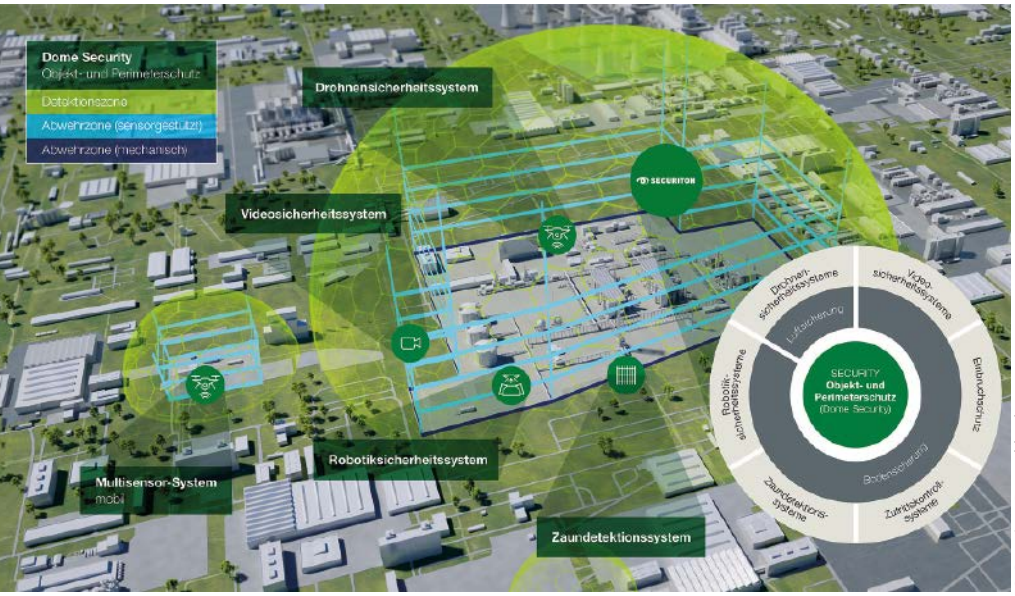
Die Sicherheitsbranche ist gerüstet

KRITIS-Dachgesetz: im Gespräch mit Michael Harter von Securiton

Michael Harter ist Experte für ganzheitlichen Objekt- und Perimeterschutz im strategischen Vertrieb bei Securiton Deutschland. Eines seiner Fachgebiete sind seit mehr als 20 Jahren Sicherheitskonzepte kritischer Infrastrukturen (KRITIS). Aufgrund der aktuellen Entwicklungen haben wir ihn gefragt, welche Konsequenzen und Herausforderungen das KRITIS-Dachgesetz mit sich bringt, das bald in Kraft treten soll.



© Securiton Deutschland

Abb. 1: „Dome Security" ist ein Gesamtkonzept zur Überwachung von Boden und Luftraum über Freiflächen und Gebäude der Lebensmittelproduktion: Kombinierte Sicherheitssysteme spannen sich darüber wie eine schützende Kuppel.

Wie sehen die aktuellen Bedrohungsszenarien für kritische Infrastrukturen aus?

Michael Harter: Wir gehen immer von einem All-Gefahren-Ansatz aus. Kritische Infrastrukturen sind nicht nur von alltäglichen Störungen bedroht, sondern auch von menschlichem und technischem Versagen, extremen Naturereignissen und Sabotageakten. Beim Hochwasser Anfang Juni bspw. musste die Feuerwehr ein Umspannwerk sichern. Erst Anfang Mai brannte es auf einem Gebäudekomplex eines Rüstungskonzerns – eine Spur soll mutmaßlich nach Russland führen. Die deutsche Unterstützung von Sanktionen bei internationalen Konfliktfällen hat die Gefährdungslage noch einmal verschärft.

Der Sektor Lebensmittel ist besonders von Erpressung bedroht. Schon lange, bevor im Ernstfall die Lebensmittelkontrolle vergiftete Waren findet, können vorbeugende Maßnahmen dafür sorgen, dass niemand unbefugt auf ein Gelände kommt und schädigend in Produktionsprozesse einwirken kann.

Welche gesetzlichen Anforderungen kommen auf Betreiber zu?

M. Harter: Es geht nicht mehr nur um IT-Sicherheit. Auch physische Angriffe und Gefahren gilt es abzuwenden. Aktuell haben wir die Situation, dass zwei Verordnungen zeitgleich kommen und daher oft miteinander vermischt werden. Dabei müssen sie getrennt betrachtet werden:

- Die NIS-2-Richtlinie (Network and Information Security Directive) regelt die Cybersicherheit.
- Das KRITIS-Dachgesetz überführt die CER-Richtlinie (EU 2022/2557 beziehungsweise EU RCE Directive) in deutsches Recht. CER steht für Critical Entities Resilience. Die Richtlinie reguliert die Resilienz, also die physische Widerstandskraft, kritischer Infrastrukturen in der Europäischen Union (EU) und fordert vor allem ihre Ausfallsicherheit.

Aber: Jeder Fall ist ein Einzelfall. Nicht jeder Betreiber braucht diese physische Resilienz (CER), allerdings fast jeden betrifft die IT-Sicherheit (NIS-2).

Ist allen Beteiligten bzw. den Verantwortlichen bewusst, was zu tun ist?

M. Harter: Eben nicht durchgängig. Aktuell liegt noch kein Gesetzesentwurf der CER-Richtlinie vor. Das verzögert sich zusehends, unter anderem, weil viele verschiedene Stellen daran mitwirken, die Umsetzbarkeit des vorliegenden Referentenentwurfes zu bewerten, und Vorgaben machen müssen. Für den Sektor Lebensmittel ist unter anderem das Bundesministerium für Ernährung und Landwirtschaft zuständig. Es muss beschreiben, was getan werden soll und welche Schwellenwerte erreicht werden müssen. Dabei drängt die Zeit: Gemäß dem Referentenentwurf müssen sich betroffene Unternehmen noch in 2024 als kritische Infrastruktur registrieren. Zehn Monate später sollen sie bereits die notwendigen Sicherheitsmaßnahmen umgesetzt haben. Das ist sehr wenig Zeit: Sind bauliche Veränderungen erforderlich – etwa, wenn Zäune errichtet werden müssen – vergehen allein dafür schnell bis zu zwölf Monate.

Können Sie sich Ausnahmen zu diesem gedrängten Zeitplan vorstellen?

M. Harter: Die wichtige Frage wird sein: Welcher Erfüllungsgrad wird letztlich verlangt – der Vollschutz, eine fertige Planung oder erst mal „nur" eine abgeschlossene Analyse? Und wie streng wird es gehandhabt werden? Um Ihre Frage zu beantworten: Ich kann mir gut vorstellen, dass für bestimmte Sektoren die Vorgaben etwas kulanter ausfallen könnten.

Gibt es mögliche weitere Unabwägbarkeiten?

M. Harter: Unklar ist etwa auch die Finanzierung der erforderlichen KRITIS-Maßnahmen: Denkbar sind Umlagen für Strom und Gas oder Förderungen. Deswegen richten sich jetzt alle Augen auf den Gesetzgeber. Das nächste Problem ist die Zertifizierung: Für kerntechnische Anlagen haben wir schon seit mehr als 20 Jahren entsprechende Verfahren. Für andere Sektoren gibt es noch keine Grundlagen in dieser Richtung. Die IT ist da schon weiter: Für NIS-2 gibt es unter anderem die ISO 27k (ISO 27000 Normenreihe). Eine weitere große Herausforderung in Zeiten des Fachkräftemangels ist natürlich das Planungs- und Betreuungspersonal – das häufig erst rekrutiert werden muss. Und nicht zuletzt: Wer prüft dann die installierten Anlagen? Das können und sollen weder Betreiber noch Errichter. Auch dieser

Aspekt ist noch ungelöst. Dafür infrage kämen etwa die Behörde unter dem Dach des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) oder ein Zertifizierungsdienstleister. Aktuell ist also noch eine ganze Reihe offener Fragen zu beantworten.

Ganzheitliche Sicherheit ist das Ziel – welche Schritte führen dahin?

M. Harter: Der erste wichtige Schritt ist eine Risikoanalyse für die eigenen Liegenschaften oder Infrastruktureinrichtungen. Der Betreiber muss zunächst die kritischen Bereiche identifizieren. Im nächsten Schritt sollte ein Anbieter gefunden werden, der das Unternehmen bei der Erstellung eines Sicherheitskonzepts im Hinblick auf die jeweiligen Gefahrenpotenziale unterstützt. Jede Liegenschaft muss dabei ganz individuell betrachtet werden. Die Sicherheitsexperten beraten, wie Risiken am besten zu minimieren sind. Dann folgt die betriebswirtschaftliche Berechnung. Was wird tatsächlich geschützt und welche Risiken bleiben bewusst bestehen? Denn das Gesetz lässt da einen gewissen Spielraum – der Aufwand für Maßnahmen muss verhältnismäßig sein.

Müssen sich Betreiber immer für oder gegen eine Maßnahme und das damit verbundene Risiko entscheiden oder gibt es auch Alternativen?

M. Harter: Unter Umständen können organisatorische Maßnahmen technische ersetzen. Lösen umgekehrt technische Maßnahmen organisatorische ab, werden eigentlich immer Risiken weiter minimiert und Personal gespart. Und natürlich fällt Technik bspw. aufgrund von Krankheit auch nicht aus.

Was müssen Sicherheitskonzepte und -systeme für den Objekt- und Perimeterschutz heute können?

© Securiton Deutschland

Abb. 2: Michael Harter, Experte für ganzheitlichen Objekt- und Perimeterschutz im strategischen Vertrieb bei Securiton Deutschland.

M. Harter: Täter und Tatmittel entwickeln sich immer weiter, und mit ihnen die Sicherheitstechnik. Häufig ist Betreibern gar nicht bekannt, welche Möglichkeiten es inzwischen gibt, Fähigkeitslücken in der elektronischen Sicherheit zu schließen. Jeder kennt zum Beispiel Videokameras. Einleuchtend ist, dass im Fall einer manipulierten Charge zur Aufklärung die Videoaufzeichnung der Sicherheitskameras aus ihrem Produktionszeitraum gesichtet werden können. Viele wissen aber nicht, wie intelligent und leistungsfähig Videosicherheit heute darüber hinaus sein kann. Videomanagementsysteme nehmen dem Menschen viele Aufgaben ab – mit dem Vorteil, dass sie nicht ermüden. Noch wichtiger: Eine elektrische Überwachung kann bereits die Tatvorbereitung und das Auskundschaften aufdecken und somit eine Tat verhindern. Das System erkennt mithilfe von intelligenten Videoanalysen definierte Situationen und löst automatisch Alarm aus – etwa, wenn unbefugte Personen versuchen in sensible Bereiche einzudringen. Bausteine eines ganzheitlichen Sicherheitskonzepts sind zusammengefasst: hochfunktionale intelligente Videosicherheitssysteme, Zaundetektion, Einbruchschutz, Zutrittskontrolle oder selbst Drohnendetektion und -abwehr. Keine Frage: All diese Systeme müssen auch selbst IT-sicher sein.

Securiton hat den Begriff „Dome Security" geprägt. Was unterscheidet sie von bisherigen Videosicherheitssystemen?

M. Harter: Dafür arbeiten mehrere oder alle eben genannten Einzelsysteme effizient zusammen. Wir sprechen von „Dome Security", weil sie den Rundumschutz wie eine Kuppel lückenlos über die Liegenschaft spannt. Ein Kernsystem ist dabei auch die Luftsicherheit zum Schutz vor Drohnen, die wir inzwischen als die größte Gefahr aus der vertikalen Dimension verstehen. In der Lebensmittelbranche etwa sind die Gebäude meist klimatisiert und haben Lüftungsschächte – ideale Einfallstore für Drohnen. Dagegen hat Dome Security eine große Wirkung mit kleinen Mitteln. Vor zehn Jahren waren sowohl Drohnen als auch solche ganzheitlichen Abwehrsysteme noch unbezahlbar. Heute ist vieles auch für den zivilen Bereich realisierbar.

Wo bekommen unsere Leserinnen und Leser weitere Informationen?

M. Harter: Wir von Securiton Deutschland haben das Whitepaper „Das KRITIS-Dachgesetz und seine Umsetzung – Höchste Sicherheit für kritische Infrastrukturen" erstellt. Darin sind alle Aspekte herausgearbeitet und erklärt. Wir stellen es kostenfrei zur Verfügung: www.securiton.de/kritis-dachgesetz

Autor: Markus Strübel, Senior Marketingreferent, Securiton Deutschland

Kontakt:
Securiton Deutschland
Hauptsitz Achern
Markus Strübel
Tel.: +49 7841/6223-9739
markus.struebel@securiton.de
www.securiton.de