wasserwirtschaft wassertechnik

wwt

Praxismagazin für Trink- und Abwassermanagement

10

Oktober 2024

Phosphorrückgewinnung:

Branchendialog will offene Fragen klären und Lösungen erarbeiten

Schutz vor künftigen Epidemien:

Abwassersurvilance soll ab 2025 in Deutschland verstetigt werden

Mit 30 Seiten Special:

Klärschlamm

Im Gespräch mit Michael Harter:

Die Sicherheitsbranche ist gerüstet

Das KRITIS-Dachgesetz soll künftig die physische Sicherheit und Resilienz von kritischen Infrastrukturen (KRITIS) erhöhen. Auf die betreffenden Unternehmen kommen damit neue regulatorische Anforderungen zu, weshalb sie sich jetzt darauf vorbereiten müssen.

In Kürze soll das KRITIS-Dachgesetz in Kraft treten – aber wissen alle KRITIS-Betreiber, was zu tun ist? Michael Harter ist Experte für ganzheitlichen Objekt- und Perimeterschutz. Seit mehr als 20 Jahren entwickelt er Sicherheitskonzepte für kritische Infrastrukturen. wwt hat nachgefragt, welche Konsequenzen und Herausforderungen das KRITIS-Dachgesetz mit sich bringt.

wwt: Herr Harter, wie sehen die aktuellen Bedrohungsszenarien für kritische Infrastrukturen aus?

Harter: Wir gehen immer von einem All-Gefahren-Ansatz aus. Kritische Infrastrukturen sind nicht nur von alltäglichen Störungen, sondern auch von menschlichem und technischem Versagen, extremen Naturereignissen und Sabotageakten bedroht. Beim Hochwasser Anfang Juni beispielsweise 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. Die Infrastruktur und Anlagen zu unserer Versorgung mit dem Lebensmittel Wasser sind wegen ihrer großen gesellschaftlichen Bedeutung besonders gefährdet. Dass gerade sie vor Manipulation und Ausfall geschützt werden müssen, sollte niemand infrage stellen. Schon lange bevor die Qualitätssicherung kontaminiertes Wasser entdeckt, können vorbeugende Maßnahmen dafür sorgen, dass keine unbefugten Personen unentdeckt auf das Gelände bzw. in Anlagen gelangen.

Bild 1 Michael Harter ist für den strategischen Vertrieb bei Securiton Deutschland verantwortlich.

Quelle: Securiton Deutschland

wwt: Welche gesetzlichen Anforderungen kommen auf die Betreiber zu?

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 EU und fordert vor allem ihre Ausfallsicherheit.

Aber: Jeder Fall ist ein Einzelfall. Nicht jeder Betreiber braucht diese physische Resilienz, nicht jeder auch IT-Sicherheit – und umgekehrt.

wwt: Ist allen Beteiligten beziehungsweise den Verantwortlichen bewusst, was zu tun ist?

Harter: Eben nicht durchgängig. Aktuell liegt erst der zweite Referentenentwurf der CER-Richtlinie vor und wir warten auf das finale dritte Papier. Das verzögert sich jedoch zusehends, u. a., weil viele verschiedene Stellen daran mitwirken, die Umsetzbarkeit bewerten und Vorgaben machen müssen. Für den Sektor Lebensmittel ist beispielsweise das Gesundheitsamt 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 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. Einige Liegenschaften der Wasserversorgung sind heute bereits elektronisch gesichert. Es gibt aber auch eine Vielzahl, die bislang nicht geschützt ist. Große Wasserversorger beschäftigen sich intensiv damit, wie die Versorgerinfrastruktur geschützt werden kann. Dabei kann es um einen Schachtdeckel, eine Pumpstation oder ein ganzes Pipelinesystem gehen. Teilweise gibt es unbesetzte Gebäude und Anlagen, bei denen ein Eindringling kaum bemerkt wird.

wwt: Können Sie sich Ausnahmen zu diesem gedrängten Zeitplan vorstellen?

Harter: Die wichtige Frage wird sein: Welcher Erfüllungsgrad wird letztlich verlangt – der Vollschutz, eine fertige Planung oder erst mal „nur“ eine abgeschlossene Analy-

se? Und wie streng wird alles gehandhabt? Ich kann mir gut vorstellen, dass für bestimmte Sektoren die Vorgaben etwas kulanter ausfallen. Die Vereinigung der Fernleitungsnetzbetreiber Gas (FNB Gas) hat in ihrer Stellungnahme zum Referentenentwurf den engen Zeitrahmen kritisiert und die Befürchtung von Engpässen formuliert. BDEW und FNB Gas sind sich einig: Der Staat muss seinen Teil zur Abwehr von terroristischen und militärischen Bedrohungen beitragen.

wwt: Gibt es weitere mögliche Unabwägbarkeiten?

Harter: Unklar ist etwa auch die Finanzierung der erforderlichen KRITIS-Maßnahmen: Denkbar sind Umlagen für Strom, Gas und Wasser oder Förderungen. Deswegen richten sich jetzt alle Augen auf den Gesetzgeber. Das nächste Problem ist die Zertifizierung: Für kerntechnische Anlagen existieren seit mehr als 20 Jahren entsprechende Verfahren. Für andere Sektoren gibt es noch keine Grundlagen. 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 das Planungs- und Betreuungspersonal, das häufig erst rekrutiert werden muss. Und nicht zuletzt: Wer prüft die installierten Anlagen? Das können und sollen weder Betreiber noch Errichter tun. Auch dieser Aspekt ist ungelöst. Dafür infrage käme etwa die Behörde unter dem Dach des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) oder ein Zertifizierungsdienstleister. Aktuell sind also noch einige offene Fragen zu beantworten.

wwt: Ganzheitliche Sicherheit ist das Ziel – welche Schritte führen dahin?

Harter: Der erste wichtige Schritt ist eine Risikoanalyse für die eigenen Liegenschaften oder Infrastruktureinrichtungen. Der Betreiber muss zunächst die kritischen Bereiche identifizieren. Im Folgeschritt sollte ein Anbieter gefunden werden, der das Unternehmen bei der Erstellung eines Sicherheitskonzepts im Hinblick auf die jeweiligen Gefahrenpotenziale unterstützt. Jede Liegenschaft muss dabei 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 einen gewissen Spielraum – der Aufwand für Maßnahmen muss verhältnismäßig sein.

Bild 2 Hochsicherheitsbereiche sind heute nicht nur am Boden Gefahren ausgesetzt. Drohnen werden zunehmend zur Spionage oder Sabotage eingesetzt.
Quelle: Securiton Deutschland

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

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

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

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. Viele wissen aber nicht, wie intelligent und leistungsfähig sie heute sind. Videomanagementsysteme nehmen dem Menschen viele Aufgaben ab – mit dem Vorteil, dass sie nicht ermüden. Noch wichtiger: Eine elektronische 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. All diese Systeme müssen auch selbst IT-sicher sein.

wwt: Vielen Dank für das Gespräch!

Das Gespräch führte Nico Andritschke.

■ ***Securiton Deutschland***
www.securiton.de

Whitepaper

„Das KRITIS-Dachgesetz und seine Umsetzung – höchste Sicherheit für kritische Infrastrukturen"

www.securiton.de/kritis-dachgesetz