Qualität und Vertrauen als Basis für Resilienz

Von Holger Köster

Holger Köster

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

Der Schutz Kritischer Infrastrukturen befindet sich in einer entscheidenden Phase. Neue Bedrohungslagen, technologische Entwicklungen und die fortschreitende europäische Regulierung stellen etablierte Strukturen auf den Prüfstand. Der politische Wille, Sicherheit stärker zu vereinheitlichen und Resilienz verbindlich zu verankern, spiegelt sich unter anderem in Richtlinien wie NIS2, der CER-Richtlinie und im geplanten KRITIS-Dachgesetz wider.

Diese Vorgaben schaffen nicht nur neue Pflichten, sondern auch Orientierung. Sie helfen, entlang der gesamten Sicherheitskette ein gemeinsames Verständnis von Qualität und Verantwortlichkeit zu etablieren. Für die private Sicherheitswirtschaft bedeutet das, sich weiterzuentwickeln: vom operativen Dienstleister hin zu einem Partner, der regulatorische, technische und organisatorische Anforderungen zusammenführt.

Ein wichtiger Schritt auf diesem Weg ist unter anderem die Etablierung der europäischen Normenreihe DIN EN 17483 „Private Sicherheitsdienstleistungen – Schutz Kritischer Infrastrukturen“. Sie schafft erstmals einen einheitlichen Rahmen für die qualitätsgesicherte Planung, Ausschreibung und Umsetzung von Sicherheitsdienstleistungen in besonders sensiblen Bereichen, von der Energieversorgung über das Gesundheitswesen bis hin zu Transport und Logistik. Die Normenreihe wird in den kommenden Jahren weitere Sektoren abdecken und damit zu einem zentralen Referenzpunkt für den KRITIS-Schutz in Europa werden.

Sicherheit ist heute also weit mehr als die Summe technischer und personeller Maßnahmen. Sie entsteht dort, wo Fachwissen, Erfahrung und Vertrauen zwischen Betreibern, Behörden, Planern und Dienstleistern zusammenkommen. Eine resiliente Sicherheitslandschaft braucht gemeinsame Standards, offene Kommunikation und die Bereitschaft, voneinander zu lernen.

Wenn es gelingt, diese Haltung fest in der Branche zu verankern, werden die neuen Regulierungen auch nicht als Bürde empfunden, sondern vielmehr als Chance, die Qualität der Sicherheitsbranche langfristig auf ein neues Niveau zu heben. Das ist der Weg, den wir im Interesse unserer Kunden, unserer Beschäftigten und der Stabilität unseres Landes gemeinsam gehen sollten.

Ihr
Holger Köster

Bild: # 1781271560 / istockphoto.com

Neue Verantwortung im KRITIS-Schutz

Wie Sicherheitsdienstleister zu strategischen Partnern werden

Von Andreas Albrecht

Zwischen Zeitenwende, Gesetzesnovellen und wachsender Bedrohungslage verändern sich die Anforderungen an den Schutz Kritischer Infrastrukturen grundlegend. Sicherheitsdienstleister können in diesem Wandel mehr sein als reine Ausführende, wenn sie ihre Rolle als gestaltende Partner annehmen.

Andreas Albrecht
Freier Fachredakteur
und Journalist

Kritische Infrastrukturen sind das funktionale Rückgrat unseres Gemeinwesens, vom Energiesektor über die Gesundheitsversorgung bis hin zur Wasserwirtschaft, Logistik und Telekommunikation. Ihre Bedeutung ist unstrittig, ebenso aber auch ihre zunehmende Gefährdung. Cyberangriffe, hybride Bedrohungen, Sabotageakte, geopolitische Risiken und Naturkatastrophen treffen auf Strukturen, die vielerorts historisch gewachsen, aber nicht krisenfest sind.

Politik und Verwaltung haben darauf mit neuen gesetzlichen Vorgaben, erweiterten Berichtspflichten und verbindlichen Anforderungen an Betreiber reagiert. Gleichzeitig eröffnen sich dadurch neue Handlungsspielräume für die Sicherheitswirtschaft, insbesondere für Dienstleister, die bereit sind, sich strategisch aufzustellen und ihre Kompetenzen über die operative Ebene hinaus beratend, koordinierend und integrativ einzubringen.

Neue Spielregeln für den KRITIS-Schutz

Mit dem vor kurzem verabschiedeten NIS-2-Gesetz, dem geplanten KRITIS-Dachgesetz und Normen wie der EN 17483 werden die Rahmenbedingungen für den Schutz Kritischer Infrastrukturen derzeit grundlegend neu definiert. Ziel ist es, im digitalen wie im physischen Bereich einheitliche Standards zu schaffen, Sicherheitslücken zu schließen und die Resilienz systemrelevanter Einrichtungen zu erhöhen.

Betreiber müssen künftig umfassende Risikoanalysen und Schutzkonzepte vorlegen, Mindestanforderungen an Sicherheitsmaßnahmen erfüllen und deren Wirksamkeit regelmäßig dokumentieren. Hinzu kommen neue Vorgaben zur sektorübergreifenden Zusammenarbeit und eine engere Verzahnung von IT- und physischer Sicherheit.

Besonders die geplante EN 17483, die ein europaweites Rahmenwerk für die strukturierte Sicherheitsplanung und -umsetzung vorsieht, erhöht den Druck auf Betreiber, ihr Sicherheitsniveau systematisch zu überprüfen und gegebenenfalls anzupassen. Hier eröffnet sich ein neues Aufgabenfeld für Sicherheitsdienstleister, die ihr Know-how gezielt einbringen können.

Vom Dienstleister zum Partner

In der Vergangenheit wurden Sicherheitsdienstleister oft vor allem als ausführende Akteure betrachtet, die Bewachung, Kontrollgänge oder Videoaufschaltungen übernehmen. Doch dieses Verständnis verändert sich zunehmend. Immer mehr Betreiber erkennen, dass Sicherheit nicht allein delegierbar ist, sondern abgestimmt und gesteuert werden muss. Daraus ergibt sich ein wachsender Beratungsbedarf, insbesondere bei der Umsetzung neuer gesetzlicher Anforderungen und beim Aufbau strukturierter Sicherheitsmanagementsysteme.

Dienstleister, die regulatorische Vorgaben kennen, Schwachstellenanalysen mitentwickeln, Schnittstellen zu Behörden professionell bedienen und technische wie organisatorische Aspekte miteinander verknüpfen, werden zu unverzichtbaren Partnern. Diese Entwicklung verläuft schrittweise, ist jedoch deutlich spürbar. Gefragt sind Akteure, die Sicherheit als vernetztes System begreifen und sie im Spannungsfeld zwischen Betriebsrealität, Normen, IT-Anforderungen und Budgetvorgaben vermitteln können.

Ganzheitliche Sicherheitsplanung als Zukunftsmodell

Zunehmend setzt sich die Erkenntnis durch, dass Sicherheit kein isoliertes Produkt ist, das einfach eingekauft werden kann. Vielmehr ist Sicherheit das Ergebnis abgestimmter Prozesse und Verantwortlichkeiten. Unter dem Begriff einer

„ganzheitlichen Sicherheitsplanung“ lässt sich dieser Ansatz prägnant beschreiben. Gemeint ist das Zusammenspiel verschiedener Maßnahmen, Zuständigkeiten und Technologien, das sich an einer gemeinsamen Risiko- und Resilienzstrategie orientiert.

Für Sicherheitsdienstleister bedeutet das, auf Augenhöhe mit Behörden, Planungsbüros und IT-Experten zu agieren und Technik nicht nur zu installieren und zu bedienen, sondern zu planen und in übergreifende Sicherheitskonzepte einzubetten. Ebenso gehört es dazu, den physischen und digitalen Sicherheitsbedarf mit dem Kunden individuell zu analysieren und gesetzliche Vorgaben wie NIS2 oder das KRITIS-Dachgesetz aktiv in die Beratung einzubeziehen.

Dazu gehört auch der kommende Cyber Resilience Act (CRA). Ab Dezember 2027 dürfen in der Europäischen Union Produkte, die den gesetzlichen Bestimmungen des CRA nicht entsprechen, weder neu in die EU eingeführt noch – was noch entscheidender ist – weiterverwendet werden. Auch wenn der CRA in erster Linie Hersteller digitaler Produkte betrifft, hat er indirekte Auswirkungen auf Betreiber, etwa bei der Produktauswahl oder beim Nachweis sicherer Betriebsumgebungen. Dienstleister, die hier Orientierung geben können, zeigen technisches Verständnis, Marktkenntnis und Weitblick.

Normen als Leitplanken für Qualität

Eine der zentralen Herausforderungen auf dem Weg zu mehr Resilienz ist der kompetente Umgang mit neuen Normen und Vorschriften. Viele Betreiber sehen sich mit einer Vielzahl von Regelwerken konfrontiert und fragen sich, welche Anforderungen verbindlich sind und wie sich Compliance nachweisen lässt, ohne den laufenden Betrieb zu beeinträchtigen.

Sicherheitsdienstleister können hier wertvolle Unterstützung leisten, wenn sie die relevanten Normen und Gesetze kennen und in kundenorientierte Prozesse übersetzen. Wichtig ist dabei unter anderem die europäische Normenreihe DIN EN 17483 „Private Sicherheitsdienstleistungen – Schutz Kritischer Infrastrukturen“, die als strategisches Fundament für qualitätsgesicherte Sicherheitsdienstleistungen in sensiblen Bereichen gilt. Sie besteht derzeit aus drei veröffentlichten Teilen: Teil 1 definiert allgemeine Anforderungen an Sicherheitsdienstleistungen, Teil 2 legt spezifische Anforderungen für Flughafen- und Luftsicherheitsdienstleistungen fest, während Teil 3 den Bereich der maritimen Sicherheit und der Seehäfen abdeckt. Weitere sektorspezifische Normenteile, etwa für Energie, Gesundheit oder Transport, werden in den kommenden Jahren folgen.


Bild: # 1529581768 / istockphoto.com

Die Normenreihe trägt entscheidend dazu bei, Qualitätsstandards europaweit zu harmonisieren und Sicherheit als Bestandteil der europäischen Resilienzstrategie zu verankern. Sie bildet zudem eine einheitliche Grundlage für die qualitätsorientierte Ausschreibung und Gestaltung von Sicherheitsdienstleistungen im Rahmen der europäischen CER-Richtlinie, deren Umsetzung in Deutschland über das KRITIS-Dachgesetz erfolgt.

Von der Dienstleistung zur Sicherheitskultur

Zukunftsfähige Sicherheit bemisst sich nicht allein an Technik und Personalstärke, sondern an der Resilienz des Gesamtsystems. Dienstleister, die dieses Verständnis teilen, bieten ihren Kunden mehr als operative Unterstützung: Sie begleiten den Wandel, helfen bei der Bewertung neuer Gefährdungslagen, integrieren technische und organisatorische Maßnahmen und schaffen durch kontinuierliche Kommunikation die Grundlage für eine gelebte Sicherheitskultur.

Industrie 4.0, Lieferkettenstörungen, geopolitische Spannungen und Fachkräftemangel machen deutlich, dass es nicht mehr ausreicht, nur auf einzelne Gefahren zu reagieren. Gefragt sind Partner, die Sicherheit ganzheitlich denken, systemisch planen und nachhaltig verankern.

Verantwortung übernehmen, Chancen nutzen

Der Wandel im KRITIS-Schutz ist in vollem Gange – regulatorisch, technisch und organisatorisch. Betreiber werden in den kommenden Jahren verstärkt in Technik, Prozesse, Know-how und Beratung investieren müssen. Sicherheitsdienstleister, die über den reinen Auftrag hinausdenken, neue Qualifikationen aufbauen und regulatorisches Wissen vermitteln, können einen entscheidenden Beitrag zur Zukunftssicherheit Kritischer Infrastrukturen leisten. Wer diese Verantwortung annimmt, wird nicht nur gebraucht, sondern vor allem auch geschätzt.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

Bitkom Wirtschaftsschutz-Studie 2025

Um 22,6 Milliarden Euro stieg der finanzielle Schaden von 2024 auf 2025, der der deutschen Wirtschaft im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden ist. Damit liegt die Summe bei 289,2 Milliarden Euro. Rund 70 Prozent davon sind auf Cyberangriffe zurückzuführen. Hierzu wurden 1.002 Unternehmen aller Branchen repräsentativ befragt.
www.bitkom.org

BBK-Ratgeber: Vorsorgen für Krisen und im Katastrophenfall

Der neue Ratgeber fasst Vorbereitungs- und Handlungsempfehlungen für verschiedene Notsituationen zusammen. Extreme Wetterereignisse nehmen zu. Selbst ein Krieg scheint nicht mehr ausgeschlossen zu sein. Der Ratgeber unterstützt leicht erklärt, wie man Extremsituationen möglichst sicher meistern kann.
www.bbk.bund.de

Die BfV-Reihe CYBER INSIGHT „Im Schatten des Cyberspace“

Fast täglich gibt es Nachrichten über Datenlecks, Hackerangriffe oder staatlich unterstützte Cyberoperationen. Wie muss man solche Angriffe einordnen? Wer sind die Akteure und welche konkreten Ziele verfolgen Angreifer? Welche Methoden nutzen unterschiedliche Akteure für ihre Attacken? Die Reihe CYBER INSIGHT ist ein Informationsangebot für alle, die mehr wissen wollen.
www.verfassungsschutz.de

Cyber risk trends 2025

Versicherte Großunternehmen entwickeln eine zunehmende Widerstandsfähigkeit gegen Cyberattacken. Wie eine aktuelle Analyse von Allianz Commercial zeigt, ist die Schwere der Cyberschäden in der ersten Jahreshälfte 2025 um mehr als 50 Prozent zurückgegangen. Gleichzeitig sank die Häufigkeit von Großschäden über einer Million Euro um rund 30 Prozent.
www.commercial.allianz.com

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

Bild: # 1196878716 / istockphoto.com