KÖTTER SICHERHEITSBRIEF

Exklusive Informationen für Entscheider

Ausgabe 01 | 2023

Dem Worst Case vorbeugen: Kritische Infrastruktur umfassend schützen

Energie, Nahrungsmittelversorgung, Gesundheits- und Verkehrswesen, IT und Telekommunikation: Kritische Infrastrukturen (KRITIS) wie u. a. diese stellen das Funktionieren des Gemeinwesens sicher. Entsprechend groß ist die Gefährdung z. B. durch Sabotage, Spionage und Cybercrime. Auch hier hat der Krieg gegen die Ukraine für eine Zeitenwende gesorgt. Machten Attacken auf KRITIS zuvor noch 20 % aller von Staaten verübten Cyberangriffe aus, legte der Anteil nach Microsoft-Analyse infolge der russischen Invasion auf 40 % zu. Der KRITIS-Schutz erfordert nicht alleine deshalb einen engen Schulterschluss von Staat, Unternehmen und Sicherheitswirtschaft.

OP-Verschiebungen nach Cyberangriffen, Lösegeld-Erpressung durch Datendiebstahl, physische Angriffe auf die Verkehrsinfrastruktur – Beispiele für die massiven Risiken, denen KRITIS-Einrichtungen jeglicher Größe und Couleur ausgesetzt sind.

„Dabei sind die digitalen, technischen oder physischen Attacken deshalb so erfolgreich, weil das Schutzlevel vieler staatlicher Institutionen, aber auch das zahlreicher KRITIS-Unternehmen nicht Schritt hält mit dem Angriffspotenzial der kriminellen Akteure“, verdeutlicht Dirk H. Bürhaus, Geschäftsführer der zur KÖTTER Unternehmensgruppe gehörenden German Business Protection (GBP), im Interview. Erforderlich sei daher ein integratives und individuelles Risiko- und Sicherheitsmanagement, das auf einem funktionierenden Frühwarnsystem basiert und u. a. die Vorgaben der neuen EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience/CER-Richtlinie) berücksichtigt.

Um den Worst Case eines Blackout z. B. im Stromnetz zu vermeiden, der Kaskadeneffekte wie Ausfälle in Produktionsbereichen nach sich ziehen würde, sollen mit einem neuen, auf der CER-Richtlinie beruhenden KRITIS-Dachgesetz auch die Vorgaben für Betreiber in Deutschland verschärft werden. Mit Blick auf die Gesetzgebung kritisiert KÖTTER Sicherheitsbeirats-Mitglied Dr. Harald Olschok die nicht ausreichende Berücksichtigung der Sicherheitswirtschaft im Eckpunktepapier.

„Viele KRITIS-Betreiber wiegen sich in falscher Sicherheit und müssen umdenken“

Herr Dr. Olschok, selten standen die Kritischen Infrastrukturen, KRITIS, so stark im Fokus des öffentlichen Interesses wie aktuell. Wie groß sind die Gefahren?
Dr. Harald Olschok: Die Gefährdungslage für die Wirtschaft und KRITIS ist hoch. Das verdeutlichen z. B. Zahlen der BITKOM-Studie zum Wirtschaftsschutz: demnach wurde praktisch jedes Unternehmen in Deutschland im vergangenen Jahr durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage geschädigt. Die Anfälligkeit von KRITIS wiederum haben die Sabotageakte gegen die Verkehrsinfrastruktur und die Gaspipelines Nord Stream klar gezeigt.

Was sind die Ursachen?
Olschok: Dazu nochmal die Studie: Sie ergab, dass die Zahl der Cyberattacken auf KRITIS-Unternehmen in den letzten zwölf Monaten bei der Hälfte der Befragten stark zugenommen hat. Für die kommenden zwölf Monate rechnen 51% mit noch heftigeren Attacken. Sprunghaft angestiegen sind zuletzt die Angriffe aus Russland und China. Sehr bedenklich stimmt die Einschätzung, dass die Abgrenzung zwischen kriminellen Banden und staatlich gesteuerten Gruppen zunehmend schwerfällt.

Wie ist Deutschland bei der Gefahrenabwehr aufgestellt, Herr Bürhaus?
Dirk H. Bürhaus: Die Struktur staatlicher und privater Gefahrenabwehr im Bereich KRITIS ist klar geregelt. Grundsätzlich sind die Betreiber für die Sicherheit verantwortlich – Ausnahmen bilden hoheitliche Bereiche wie z. B. Verkehrsflughäfen. Bei der Umsetzung kooperieren Betreiber und öffentliche Hand zumeist mit Sicherheitsdienstleistern. Hier besteht auf der örtlichen und fachlichen Ebene eine gute Zusammenarbeit. Knackpunkt sind die übergeordneten Prozesse: Speziell aufgrund der Vielzahl an Auflagen, die sich häufig überlappen und strikte Richtwerte haben, gerät die ganzheitliche Betrachtung von Sicherheit oft zu stark in den Hintergrund.

In welchen Sektoren läuft die Risikoprävention gut und wo besteht Nachholbedarf?
Bürhaus: Sehr gut sind wir in den national wie international reglementierten Bereichen – z. B. Flug- und Seehäfen oder auch der kerntechnischen Industrie – unterwegs. Dabei greifen internationale Standards und klare gesetzliche Vorgaben, die Betreibern helfen, konkrete Maßnahmen zu strukturieren und umzusetzen. Das ist in vielen anderen, vor allem auch produktionsrelevanten Bereichen wie etwa der Chemie- und Metall-Branche leider nicht so stark ausgeprägt. Dort werden die Sicherheitsstandards erheblich vom „Risikoappetit“ der Betreiber geprägt – also ihrer individuell bestehenden Bereitschaft, Risiken einzugehen.

Was ist also erforderlich: Größere Investitionsbereitschaft der jeweiligen Player oder doch eher mehr gesetzliche Vorgaben?
Bürhaus: Zu wenige gesetzliche Vorgaben sind bestimmt kein Thema. Ihre Masse und die Vielzahl behördlicher Ansprechpartner machen es schon heute Unternehmen fast unmöglich, einen Überblick über die Regelungen zu behalten und darauf basierend klare Sicherheitsstrukturen zu schaffen. Aber auch viele Betreiber müssen umdenken: Wegen der in Deutschland stark ausgeprägten „Versicherungsmentalität“

> **„Die Sicherheitswirtschaft muss explizit in die KRITIS-Gesetzgebung aufgenommen werden.“**
> Dr. Harald Olschok

kommen saubere Risikoanalysen und Präventionskonzepte häufig zu kurz. Heißt: Zahlreiche Unternehmen wiegen sich in falscher Sicherheit und riskieren im Worst Case ihre Existenz, weil etwa nach einem Großbrand die Produktion nicht schnell genug ans Laufen kommt und Versicherungsschutz dann wenig hilft.

Um u. a. solchen Szenarien vorzubeugen, hat das Bundesinnenministerium Ende 2022 ein Eckpunktepapier zum KRITIS-Schutz vorgelegt. Ihre Bewertung?
Olschok: Mit dem KRITIS-Dachgesetz werden die Schnittstellen zwischen dem Cyberschutz und erstmals auch dem physischen Schutz von KRITIS berücksichtigt. Das ist aus Sicht der Sicherheitswirtschaft absolut zu begrüßen. Zentrales Ziel muss es dabei sein, eine Sicherheitspartnerschaft zwischen Staat und Wirtschaft auf Augenhöhe zu entwickeln, wie es die Allianz für Sicherheit in der Wirtschaft Norddeutschland zutreffend formuliert hat.

Dr. Harald Olschok

Dr. Harald Olschok (Foto) ist Mitglied des KÖTTER Sicherheitsbeirates. Bis zum Frühjahr 2022 prägte er als Hauptgeschäftsführer des Bundesverbandes der Sicherheitswirtschaft (BDSW) und der Bundesvereinigung Deutscher Geld- und Wertdienste (BDGW) maßgeblich die Entwicklung der Branche. Seit April 2018 war er zudem geschäftsführendes Präsidiumsmitglied des BDSW. Als Fachbeirat fungierte er darüber hinaus viele Jahre im Masterstudiengang Sicherheits-Management an der Hochschule für Wirtschaft und Recht in Berlin, an der er im jetzt gestarteten Sommersemester zum Honorarprofessor bestellt worden ist.

Aufgrund der von Deutschland bis Herbst 2024 umzusetzenden EU-Richtlinie müssen sich somit auch hiesige Unternehmen auf schärfere Sicherheitsvorgaben einstellen?
Bürhaus: Es ist höchste Zeit – und die EU-Richtlinie macht in jedem Fall klare Vorgaben. Zentral sind zwei Aspekte. Erstens: eindeutige, nicht wegdelegierbare Verantwortung von Vorstand bzw. Geschäftsführung – also gemäß dem Credo: Sicherheit ist Chefsache. Zweitens: Diese Verantwortung der Leitungsebene muss verbunden werden mit eindeutigen, durch die Behörden vor Ort zu kontrollierenden Anforderungen an die Unternehmen. Im Fokus stehen hier eine

saubere Business-Impact-Analyse und ein darauf aufbauendes Business Continuity Management, kurz BCM.

Was folgt hieraus konkret – und welche Rolle spielt dabei z. B. die EN 17483?
Bürhaus: Der Reihe nach, also zunächst zu den Vorteilen der o. a. Strategie. Sie zeigt zum einen auch Folgen solcher Schadensereignisse auf, die landläufig oft als unwahrscheinlich gelten. Denn: Der Angriff auf die Ukraine und die Corona-Pandemie sollten vor Augen geführt haben, dass nichts mehr unmöglich ist. Zum anderen denken die meisten Unternehmen zu szenariobasiert in den Kategorien von Epidemien, Hochwassern, Blackouts etc. BCM hingegen ist ressourcenorientiert – zielt also darauf ab, welche konkreten Folgen das Fehlen bestimmter Ressourcen für die jeweiligen Geschäftsprozesse hat. Die Industrie sollte daher verstärkt Beratungs- und Unterstützungsangebote spezialisierter Consultants – z. B. der zu unserer Gruppe gehörenden German Business Protection, GBP – in Anspruch nehmen.

… und das Stichwort EN 17483?
Bürhaus: Der Rückgriff auf vorhandene BCM-Best-Practices in Verbindung mit der zwingend erforderlichen Zertifizierung privater Sicherheitsdienstleister gemäß EN 17483 wird den KRITIS-Schutz deutlich nach vorne bringen. Denn die europäische Normenreihe macht konkrete und messbare Vorgaben für die Dienstleisterauswahl, wodurch ein einheitlich hohes Niveau bei der Sicherheit umgesetzt werden kann.

… und das immer einhergehend mit der Vergabe nach dem Bestbieter-Prinzip …
Bürhaus: Eine solche generelle gesetzliche Vorgabe für den KRITIS-Sektor ist absolut wünschenswert und sollte von der Politik dringend umgesetzt werden. Aber dies entbindet Unternehmen und öffentliche Institutionen nicht von ihrer eigenen Verantwortung. Heißt: Sie sollten von sich aus die Vorzüge einer rechtssicheren Vergabe unter Anwendung des Bestbieter-Prinzips erkennen. Hier hält das Bestbieter-Handbuch des europäischen Dachverbandes des Sicherheitsgewerbes CoESS Kriterien für qualitätszentrierte Ausschreibungen bereit.

Herr Dr. Olschok, Sie kritisieren zudem die fehlende Berücksichtigung der Sicherheitswirtschaft im BMI-Papier. Warum?
Olschok: Der Schutz von Einrichtungen und Anlagen im Bereich KRITIS erfolgt seit Jahrzehnten fast ausschließlich durch private Sicherheitsdienste. Dafür gibt es teilweise spezialgesetzliche Vorgaben an die Qualifizierung und Zuverlässigkeitsüberprüfung der Sicherheitskräfte. Die Bundesregierung will nun angesichts dieser uneinheitlichen Regelungen für den physischen Schutz von KRITIS sowie der angeführten neuen EU-Vorgaben ein gesetzliches Gesamtsystem entwickeln. Das geht nicht ohne die Sicherheitswirtschaft. Sie muss explizit in die KRITIS-Gesetzgebung aufgenommen werden mit konkreten Anforderungen an die Leistungsfähigkeit der Sicherheitsunternehmen. Vorbildcharakter hat der KRITIS-Bereich „Finanz- und Versicherungswesen“. Dort werden die Bargeldversorgung und -logistik als kritische Dienstleistungen aufgeführt. Eine Aufgabe, die die Deutsche Bundesbank gemeinsam mit den Wertdienstleistungsunternehmen wahrnimmt.

Im Gegensatz zur CER-Richtlinie sind das BMI-Papier und die öffentliche Debatte also zu stark auf staatliche Behörden und KRITIS-Anbieter verengt?
Bürhaus: Eindeutig. Während in der CER-Richtlinie die Sicherheitsdienstleister benannt sind, gehen die Überlegungen in Deutschland bisher weitgehend an ihnen vorbei. Und das, obwohl unsere Branche seit Langem ein zentraler Faktor beim KRITIS-Schutz ist. Der einzig logische und zielführende Schritt muss daher die Integration unserer Leistungsangebote in eine gesamtheitliche Betrachtung sein. Dazu bietet es sich geradezu an, dies entsprechend im KRITIS-Dachgesetz zu konkretisieren.

„Unternehmen und öffentliche Institutionen sollten die Vorzüge einer rechtssicheren Vergabe unter Anwendung des Bestbieter-Prinzips erkennen.“
Dirk H. Bürhaus

Herr Dr. Olschok, Sie plädieren gleichzeitig für die Sicherheitswirtschaft als Kritische Infrastruktur. Worin liegt die Bedeutung?
Olschok: Hier geht der Blick zurück zur Corona-Zeit mit u. a. Schul- und Kindergartenschließungen sowie lokalen Ausgangssperren. Ausnahmen galten nur für systemrelevante Berufe: Deren Beschäftigte konnten etwa ihre Kinder in Notbetreuungen unterbringen. Das galt für private Sicherheitskräfte trotz ihrer wichtigen Funktion u. a. für die öffentliche Sicherheit und den Wirtschaftsschutz nur in wenigen Bundesländern, zudem wurden sie von der EU-Kommission bei Grenzgängern als systemrelevant eingestuft. Dieser Flickenteppich muss beseitigt werden. In das KRITIS-Dachgesetz müssen Sicherheitskräfte bundesweit als systemrelevant aufgenommen werden.

Und welche Rolle spielt die zugesagte eigene Gesetzgebung für die Branche?
Olschok: Das BMI hat eine einmalige Chance: Mit der Verabschiedung eines eigenen Gesetzes für das Sicherheitsgewerbe und für KRITIS kann Deutschland noch sicherer sowie die Rolle der Sicherheitswirtschaft für die Gefahrenabwehr gestärkt werden. Konkrete Vorschläge für ein Sicherheitsgewerbegesetz liegen vom Verband und aus dem Hause KÖTTER vor. Sie sehen höhere Anforderungen an die Leistungsfähigkeit des Unternehmens und an die Qualifizierung der Beschäftigten vor. Wir sind gespannt auf die beiden Gesetzentwürfe.

Das Interview führte Carsten Gronwald, Pressesprecher der KÖTTER GmbH & Co. KG Verwaltungsdienstleistungen.

Dirk H. Bürhaus
Dirk H. Bürhaus (Foto) ist Geschäftsführender Direktor in der KÖTTER Unternehmensgruppe. Zudem ist er u. a. im Vorstand des Bundesverbandes der Sicherheitswirtschaft engagiert, ist langjähriges Mitglied der ASIS International (der weltweit größten Organisation für Fragen der Sicherheit in der privaten Wirtschaft) und wirkt in verschiedenen Arbeitskreisen im europäischen Dachverband des Bewachungsgewerbes CoESS mit. Darüber hinaus leitet der 55-Jährige mehrere Arbeitsgruppen im DIN und CEN und ist zuständig für die Arbeitsgruppe, welche die Normenreihe EN 17483 entworfen hat.

Zahlen und Fakten zu den Kritischen Infrastrukturen in Deutschland

Die KRITIS-Sektoren in der Übersicht

- 2011 haben sich Bund und Länder auf eine einheitliche Einteilung der Kritischen Infrastrukturen (KRITIS) in neun Sektoren verständigt.
- Dazu zählen: Energie, Ernährung, Finanz- und Versicherungswesen, Gesundheit, Informationstechnik und Telekommunikation, Medien und Kultur, Staat und Verwaltung, Transport und Verkehr sowie Wasser. 2021 kam mit der „Siedlungsabfallentsorgung“ ein zusätzlicher Sektor hinzu.
- Die Sicherheitswirtschaft übernimmt u. a. mit Risiko- und Business Continuity Management (BCM) und der darauf basierenden Umsetzung spezifischer Sicherheitskonzepte mit personeller und technischer Sicherheit eine zentrale Rolle beim KRITIS-Schutz.

Die Gesetzeslage auf einen Blick

- Aktuell gibt es in Deutschland noch kein ebenen-, sektor- und gefahrenübergreifendes Gesetz zum KRITIS-Schutz.
- Das wird sich ändern: Die Bundesregierung bereitet eine Rahmengesetzgebung (KRITIS-Dachgesetz) vor, die auf Basis der EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience/CER-Richtlinie) bis spätestens zum Herbst 2024 in Kraft treten muss.
  (Quelle: www.bbk.bund.de, eigene Recherche)

KÖTTER Services

Security
Cleaning
Personal Service
Facility Services

IMPRESSUM

© KÖTTER Sicherheitsbrief wird herausgegeben von der Presse- und Öffentlichkeitsarbeit der KÖTTER GmbH & Co. KG Verwaltungsdienstleistungen, Essen.
Redaktion: Carsten Gronwald, Tel.: +49 201 2788-126, E-Mail: presse@koetter.de.

Fotos: S. 1, Titelmotiv: © studio v-zwoelf – stock.adobe.com; S. 2, Herr Dr. Olschok: © KÖTTER Services; S. 2, Herr Bürhaus: © KÖTTER Services; S. 4, Sicherheitstechniker: © KÖTTER Services

Adressänderung: Möchten Sie uns eine Adressänderung mitteilen oder haben Sie sonstige Hinweise zum Versand? Schicken Sie uns eine E-Mail an redaktion@koetter.de

KÖTTER Services im Social Web:

Sie lesen lieber digital? Nutzen Sie unser E-Paper

koetter.de/sicherheitsbrief

Ihr Kontakt zur KÖTTER Unternehmensgruppe:

Wilhelm-Beckmann-Straße 7
45307 Essen

Hotline: +49 201 2788-388
Telefax: +49 201 2788-488

E-Mail: info@koetter.de
Internet: koetter.de